Tivoli System Automation for Multiplatforms 4.1.0.7

Guia de Instalação e Configuração



Nota!

Antes de utilizar estas informações e o produto suportado por elas, consulte as informações no "Avisos" na página 133.

Esta edição do *Guia de instalação e configuração do System Automation for Multiplatforms* se aplica à Versão 4, Liberação 1, Modificação 0 do IBM Tivoli System Automation for Multiplatforms, número do programa 5724-M00, e a todas as liberações e modificações subsequentes deste produto, até que seja indicado de outra forma em novas edições.

Esta edição substitui a S517-1566-01.

A IBM[®] agradece seus comentários. Um formulário para comentários dos leitores pode estar incluído no verso desta publicação. Outra alternativa é enviar seus comentário para o seguinte endereço:

IBM Brasil - Centro de Traduções Rodovia Francisco Aguirra Proença (SP 101) Km 09, Chácaras Assay CEP 13185-900 Hortolândia, SP

FAX (Germany): 07031 16-3456 FAX (Outros países): 49 7031 16-3456

E-mail na Internet: eservdoc@de.ibm.com

Se desejar uma resposta, certifique-se de incluir seu nome, endereço, número de telefone ou número de FAX.

Certifique-se de incluir o seguinte em seu comentário ou nota:

Título e número do pedido deste manual

Número da página ou tópico relacionado ao comentário

Ao enviar informações para a IBM, o Cliente concede à IBM um direito não exclusivo para usar ou distribuir as informações da forma que julgar apropriada sem incorrer em qualquer obrigação para com o Cliente.

© Copyright International Business Machines Corporation 2006, 2021.

Índice

Figuras	vii
Tabelas	ix
Sobre este guia	xi
Nuem deve usar este guia	vi
Onde Encontrar Informações Adicionais	xi xi
Convenções	xi
ISO 9000	xii
Informações relacionadas ao RSCT	xii
Como Obter Publicações	xii
Como Entrar em Contato por E-mail	xii
O Que Há de Novo Nesta Liberação	xiii
Capítulo 1. Planejamento	1
Planejamento da Instalação	1
Empacotando	1
Pré-requisitos	2
Preparando a Instalação	9
Planejando o novo suporte de plataforma	
Planejamento para uma Infraestrutura de Rede Altamente Disponível	10
Planejamento para Dispositivos de Armazenamento	11
Usando Dispositivos de Armazenamento de Caminho Único	11
Usando Dispositivos de Armazenamento com Caminhos Múltiplos	12
Usando Interfaces de Rede	14
Duas Redes Separadas Fisicamente, ServiceIP Movido entre os Nós	14
Três redes lógicas em uma rede física, mover ServiceIP entre as interfaces de rede	15
Duas Redes Separadas Fisicamente, Roteamento Dinâmico e VIPA	17
Ligação de Interface	18
Usando uma Interface Ethernet	19
Capítulo 2. Instalando	23
Fazendo Upgrade	23
Fazendo Upgrade de uma Versão Try & Buy para uma Versão Completa do Produto	23
Fazendo Upgrade de uma Versão Anterior à Versão 4.1	23
Instalando o System Automation for Multiplatforms	24
Executando a instalação	24
Migrando o Domínio de Automação do Sistema	27
Pós-instalação	34
Tornando Grupos de Volumes Compartilhados com Capacidade de Concorrência Aprimorada no AIX	ء 34
Procedimento de Retrocesso	
Desinstalando	
Instalando em novos sistemas operacionais	
Migração do SLES 12 para o SLES 15 ou do RHEL 6 para o RHEL 7/8	38
Instalando fix packs de serviço	
Obtendo Fix Packs	
Convenções de Nomenclatura do Archive	39

Instruções de uso para archives específicos da plataforma	39
Instalando serviço para o System Automation for Multiplatforms	40
Desinstalando o Serviço	41
Instalando o recurso extended disaster recovery (xDR)	41
Pacote xDR	41
Pré-requisitos de xDR	42
Instalando a licença do recurso XDR	42
Fazendo Upgrade do Recurso xDR de uma Versão Inferior a 4.1	
Desinstalando o recurso XDR	
Instalando a política de alta disponibilidade do SAP	43
Construte 2. Configurando	45
	45
Configurando o comportamento de automação do sistema	
Automation	45
Automation	/ 4
	/ 44 مرار
Evemples	47
Configurando o desempatador	40 // 8
Desempatador de disco compartilhado	50 50
Desempatador de rede	50
desempatador de NES	01 63
Cloud Tie Breaker	69
Substituindo o Ouorum Operacional	72
Configurando o Adantador de Automação de Ponta a Ponta	
Iniciando o diálogo de configuração do adaptador de automação de ponta a ponta	
Definindo as Configurações do Adaptador de Automação	
Replicando os Arguivos de Configuração do adaptador de automação de ponta a ponta	81
Tornando o Adaptador de Automação de Ponta a Ponta Altamente Disponível	81
Configurando no Modo Silencioso	82
Detectando Falhas da Interface de Rede	85
Usando Ethernet on Power Systems virtualizado	85
Executando no Linux on System z sob z/VM	86
Ativando a Pulsação de Disco	86
Protegendo Recursos Críticos (Comutador de Segurança)	88
Ativando o Suporte IPv6	89
Configurando o adaptador de automação com uma conta de usuário não raiz	90
Configurando a segurança para sistemas operacionais específicos	90
Executando o script de configuração do adaptador do usuário não raiz	92
Serviço e Manutenção	96
Alterando o ID do usuário do adaptador não raiz	96
Removendo a configuração do adaptador não raiz	
Limitações	97
Canitula A. Tuta duanda	~~~
	99
Consoles de Eventos	99
Tivoli Netcool/UMN1Dus	100
Ativanda a garação do evento	108
Ativando a geração de evento	108
Auvalido o Publicador Osarido a Internace da Linna de Comandos	109 109
Tivoli Business Service Manader (TRSM)	109 110
Integrando o System Automation for Multiplatforms	111
Pré-requisitos	110 110
Configurando o TBSM	110
Integrando recursos do System Automation e TBSM	
Customizando Visualizações do TBSM para Incluir Informações do System Automation	116
s i	-

Capítulo 5. Protegendo	121
Gerenciando Autorização para Usuários que Acessam o Cluster	
Configurando IDs do Usuário não Root para a Interface da Linha de Comandos	121
Autorização Padrão Modificada para Usuários não Root que Usam o RSCT Nível 2.5.4.0 ou	Superior124
Limitações da Configuração de Segurança de não Root	124
Protegendo a Conexão com o Adaptador de Automação de Ponta a Ponta Usando SSL	126
Gerar Keystore e Truststore com Chaves SSL Públicas e Privadas	126
Ativar a Segurança SSL em Configurações do Adaptador de Automação	
Usando o IBM Support Assistant	131
Instalando o IBM Support Assistant e o Plug-in do Tivoli System Automation for Multiplatfo	orms 131
Avisos	133
Marcas comerciais	134
Índice Remissivo	135

Figuras

1. Símbolos Utilizados neste Guiaxii
2. Problemas ao planejar uma rede de alta disponibilidade11
3. Dois Nós, Duas Interfaces, Duas Redes Separadas Fisicamente15
4. Dois Nós, Duas Interfaces, Uma Rede Física16
5. Duas Redes Separadas Fisicamente, Roteamento Dinâmico e VIPA
6. Interfaces de Rede Ligadas a um Dispositivo de Rede Lógica18
7. Dois Nós, Uma Interface
8. Dois Nós, Uma Interface – Falha na Interface
9. Verificando os números das versões ativa e instalada 29
10. Ambiente do adaptador de automação de ponta a ponta em clusters do UNIX e Linux antes da versão 4.1
11. Ambiente do adaptador de automação de ponta a ponta disponível com versão 4.1
12. Logs do sistema de cluster de dois nós63
13. Visão geral do ambiente do adaptador de automação de ponta a ponta em um cluster do System Automation for Multiplatforms
14. Janela principal do diálogo de configuração do adaptador de automação de ponta a ponta74
15. Falha de rede em um cenário de dois nós com um disco compartilhado
16. Falha do nó em um cenário de dois nós com um disco compartilhado87
17. Arquitetura Básica para TBSM111
18. Editor de modelo de árvore
19. Editor de Modelo de Árvore do TBSM119
20. Geração de Keystore e Truststore usando SSL127

Tabelas

1. Convenções de destaque usadas neste manualxi
2. Versões do DVD do produto1
3. Archive para plataformas Linux
4. Archive para plataformas AIX
5. Plataformas UNIX e Linux suportadas do System Automation for Multiplatforms
6. Configuração de rede para um cluster de dois nós com interfaces de rede14
7. Vantagens e desvantagens de uma configuração de dois nós com interfaces de rede15
8. Configuração de rede para três redes lógicas em uma rede física16
9. Vantagens e desvantagens de uma configuração de rede para três redes lógicas em uma rede física16
10. Configuração de rede de duas redes fisicamente separadas17
11. Vantagens e desvantagens para uma configuração de rede de duas redes fisicamente separadas 18
12. Configuração de rede para interfaces de rede física ligadas18
13. Vantagens e desvantagens de uma configuração de rede para interfaces de rede física ligadas19
14. Configuração de rede de um cluster de dois nós com interfaces Ethernet19
15. Vantagens e desvantagens de um cluster de dois nós com interfaces Ethernet20
16. Idiomas e códigos de idiomas suportados pelo System Automation for Multiplatforms em sistemas Linux
17. Idiomas e códigos de idioma suportados pelo Tivoli System Automation em sistemas AIX26
18. Archive para sistemas operacionais Linux
19. Archive para sistemas operacionais Linux de 64 bits
20. Archive para sistemas operacionais AIX
21. Comparação dos Desempatadores com Base na Rede e com Base no Disco
22. Nome de arquivos em um cluster de dois nós70

23. Arquivos de propriedades de entrada gerados
24. Métodos de proteção de quorum operacional
25. Tipos de classes de eventos do System Automation Application Manager
26. Atributos de status do System Automation for Multiplatforms usados em eventos de mudança de status de recurso (alerts.status)101
27. Identificação do recurso, do domínio, do evento (alerts.status)101
28. Outros atributos usados em eventos de mudança de status do recurso (alerts.status)102
29. Eventos de mudança de status do domínio (alerts.status)103
30. Campos existentes do arquivo de regras para eventos do System Automation103
31. Estado composto para mapeamento de gravidade do OMNIbus 104
32. Mapeamento de Gravidade EIF para OMNIbus105
33. Mapeamento de Eventos de Mudança de Estado de Recurso do System Automation para Estados do TBSM
34. Regras de status recebidos baseadas em texto do TBSM116
35. As Autorizações e as Funções para Executar as Tarefas do System Automation for Multiplatforms 125

Sobre este guia

Este guia explica como implementar e usar os recursos de recuperação automatizados baseados em política que são fornecidos pelo IBM Tivoli System Automation for Multiplatforms (System Automation for Multiplatforms).

O System Automation for Multiplatforms fornece alta disponibilidade para recursos em clusters do AIX (no IBM System p), em clusters do Linux[®] (no IBM System x, System z, System i e System p) e em clusters do Windows (no IBM System x).

Quem deve usar este guia

Este guia é destinado a administradores e operadores de sistemas que desejam usar os recursos de automação e failover do System Automation for Multiplatforms.

Onde Encontrar Informações Adicionais

A biblioteca Tivoli System Automation é composta dos livros a seguir, incluindo esta publicação, descrevendo Tivoli System Automation para Multiplataformas:

- Guia do Administrador e do Usuário do System Automation for Multiplatforms, SC34-2698-01
- Tivoli System Automation para Multiplataformas Guia de Instalação e Configuração , SC34-2699-01
- Tivoli System Automation para Multiplataformas Referência Guide, SC43-2646-01
- Tivoli System Automation para Multiplataformas High Availability Policies Guide, SC34-2660-01

Você pode fazer download da documentação completa em

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

A biblioteca do Tivoli System Automation contém os seguintes manuais, incluindo este, que descreve o System Automation Application Manager:

- System Automation Application Manager Administrator's and User's Guide, SC34-2701-00
- System Automation Application Manager Guia de Instalação e Configuração , SC34-2702-00
- System Automation Application Manager Referência and Problem Determination Guide, SC34-2703-00

É possível fazer download dos manuais em:

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

A página inicial do IBM Tivoli System Automation contém informações úteis atualizadas, incluindo links de suporte e downloads para pacotes de manutenção. Você localizará a página inicial do IBM Tivoli System Automation em:

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

Convenções

As seguintes convenções de realce são utilizadas neste manual:

Tabela 1. Convenções de destaque usadas neste manual	
Negrito	Identifica comandos, sub-rotinas, palavras-chave, arquivos, estruturas, diretórios e outros itens cujos nomes são predefinidos pelo sistema. Além disso, identifica objetos gráficos, como botões, etiquetas e ícones, selecionados pelo usuário.

Tabela 1. Convenções de destaque usadas neste manual (continuação)	
Itálico	Identifica parâmetros cujos nomes ou valores reais devem ser fornecidos pelo usuário.
monoespaçame nto	Identifica exemplos de valores de dados específicos, exemplos de texto semelhantes ao texto que pode ser exibido, exemplos de partes de código do programa semelhantes às que podem ser gravadas por um programador, mensagens do sistema ou informações que devem ser realmente digitadas.

Este manual utiliza símbolos para mostrar recursos, grupos de recursos, equivalências e relacionamentos. Os símbolos utilizados são:

	ResourceGroup
	Equivalency
C	fixed Resource
0	floating Resource
	Relationship

Figura 1. Símbolos Utilizados neste Guia

ISO 9000

Sistemas com qualidade registrada pelo ISO 9000 foram utilizados no desenvolvimento e na fabricação deste produto.

Informações relacionadas ao RSCT

As seguintes publicações do IBM Reliable Scalable Cluster Technology (RSCT) estão disponíveis no CD do System Automation for Multiplatforms:

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

Para obter informações adicionais sobre o RSCT, consulte IBM Cluster systems.

Para obter mais informações, consulte Linux on IBM zSeries e S/390: High Availability for z/VM and Linux IBM Redpaper.

Como Obter Publicações

As publicações do System Automation for Multiplatforms também estão disponíveis (válidas logo após o lançamento) nestes Web sites:

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

Como Entrar em Contato por E-mail

Se você quiser entrar em contato conosco por e-mail, envie seus comentários para eservdoc@de.ibm.com

O Que Há de Novo Nesta Liberação

Obtenha uma visão geral rápida sobre os novos recursos do System Automation for Multiplatforms versão 4.1.0.

Operações melhoradas na linha de comandos com o novo comando samcc

O System Automation for Multiplatforms versão 4.1.0.2 inclui um novo comando samcc, que pode ser usado como Operations Console na interface da linha de comandos. Para obter informações adicionais, consulte.

Suporte à plataformas adicionais

O System Automation for Multiplatforms versão 4.1.0.1 suporta as novas plataformas a seguir:

- SUSE SLES 12 (64 bits)
- Red Hat RHEL 7 (64 bits)
- Ubuntu 14.04 (64 bits): System x, Power Systems (somente Little Endian)

O System Automation for Multiplatforms versão 4.1.0.2 suporta as novas plataformas a seguir:

- Red Hat RHEL 7.1 no Power Systems Little Endian (64-bit)
- O System Automation for Multiplatforms versão 4.1.0.3 suporta as novas plataformas a seguir:
- AIX 7.2

O System Automation for Multiplatforms versão 4.1.0.4 suporta as novas plataformas a seguir:

• Ubuntu 16.04 (64 bits): System x, Power Systems (somente Little Endian).

Para obter informações adicionais, consulte *Guia de instalação e configuração do System Automation for Multiplatforms*.

O System Automation for Multiplatforms versão 4.1.0.5 suporta as novas plataformas a seguir:

- SUSE SLES 15 (64 bits)
- Ubuntu 18.04 (64 bits): System x, Power Systems (somente Little Endian).

System Automation for Multiplatforms versão 4.1.0.5 inclui suporte para:

• SAP Netweaver 7.5.3 ENSA2.

System Automation for Multiplatforms versão 4.1.0.6 suporta as seguintes novas plataformas:

- Red Hat RHEL 8 (64 bits)
- Ubuntu 20.04 (64 bits): System x, Power Systems (apenas Little Endian)

System Automation for Multiplatforms versão 4.1.0.6 inclui suporte para:

- Incluído o suporte do SAP NetWeaver para o S/4HANA 1809
- Incluído o suporte do SAP NetWeaver para o S/4HANA 1909
- Suporte incluído para Oracle 19c
- Suporte incluído para SAP HANA 2.0 SPS 04 Revisão 046
- O System Automation for Multiplatforms versão 4.1.0.7 suporta as seguintes novas plataformas:
- AIX 7.2 TL5
- O System Automation for Multiplatforms versão 4.1.0.7 inclui suporte para:
- Incluído suporte do SAP NetWeaver para S/4HANA 2020
- Incluído suporte para SAP HANA 2.0 SPS 05 Revisão 050

Política de alta disponibilidade melhorada para o SAP

A política de alta disponibilidade do SAP Central Services está disponível como um recurso opcional do System Automation for Multiplatforms, que é vendido separadamente. Essa política de alta disponibilidade do SAP Central Services agora está adaptada à tecnologia do SAP.

O usuário pode iniciar e parar a pilha do SAP NetWeaver usando a interface com o usuário do SAP sem interferir com a política do System Automation. O SAP Software Update Manager pode atualizar a solução Netweaver sem a necessidade de desativar o System Automation durante o processo de atualização.

As opções de configuração do SAP suportadas: suporte de pilha Java, ABAP e DUAL para failover do SAP Central Services. Além disso, as seguintes opções de configuração são suportadas:

- Servidor de aplicativos (reinicialização no local do servidor de aplicativos primário e adicional)
- Failover do roteador SAP
- Failover de SAP Web Dispatcher
- Iniciar após o suporte da dependência ao banco de dados
- O System Automation for Multiplatforms versão 4.1.0.2 inclui suporte para:
- SAP HANA System Replication failover

A versão do kernel SAP suportada é 7.20 ou superior.

Para obter informações adicionais, consulte System Automation for Multiplatforms High Availability Policies Guide.

Reunindo informações sobre falhas do aplicativo

O programa samwhy é uma ferramenta simples e de fácil uso que oferece a detecção de falhas do aplicativo e sua análise para aplicativos que são controlados pelo System Automation. samwhy ajuda o operador a entender o que aconteceu e fornece uma explicação sobre por que o System Automation reagiu dessa forma.

Para obter informações adicionais, consulte System Automation for Multiplatforms Reference Guide.

A alta disponibilidade do adaptador de automação de ponta a ponta está simplificada

Uma política de automação extra ou um endereço IP virtual não é mais necessário.

Para obter informações adicionais, consulte Guia de instalação e configuração do System Automation for Multiplatforms.

Execute o adaptador de automação de ponta a ponta com um usuário não raiz

Por padrão, o adaptador de automação de ponta a ponta é executado com um usuário raiz. Agora o adaptador também pode ser configurado para executar com um usuário não raiz.

Para obter informações adicionais, consulte Guia de instalação e configuração do System Automation for Multiplatforms.

Capítulo 1. Planejamento

O planejamento inclui tarefas, como avaliar sua infraestrutura atual e assegurar que seus sistemas tenham os pré-requisitos necessários.

Planejamento da Instalação

Antes de instalar o System Automation for Multiplatforms em seus ambientes AIX e Linux, você deve assegurar que possui os pré-requisitos corretos.

Sobre Esta Tarefa

Empacotando

O System Automation for Multiplatforms pode ser adquirido na IBM[®] como um pacote de mídia ou transferido por download de um site de download de distribuição de software IBM.

DVD do Produto

Conteúdo do DVD do produto System Automation for Multiplatforms versão 4.1.

Sobre Esta Tarefa

DVDs separados com as seguintes etiquetas contêm scripts e pacotes de software para cada plataforma e a arquitetura correspondente:

- Tivoli System Automation para Multiplataformas 4.1 Linux on System x, Linux on POWER e Linux on System z
- Tivoli System Automation para Multiplataformas 4.1 AIX

Para instalar o System Automation for Multiplatforms, use o script de instalação listado na coluna direita da tabela abaixo.

Tabela 2. Versões do DVD do produto		
Sistema operacional	Etiqueta do DVD do produto	script de instalação
Linux	Tivoli System Automation para Multiplataformas v4.1 - Linux on System x, Linux on POWER e Linux on System z	SAM4100MPLinux/installSAM
AIX	Tivoli System Automation para Multiplataformas v4.1 - AIX	SAM4100MPAIX/installSAM

Distribuição Eletrônica

Se preferir a distribuição eletrônica à entrega no DVD, após comprar o System Automation for Multiplatforms, é possível fazer download dos archives apropriados da web usando a URL fornecida.

Linux

Tabela 3. Archive para plataformas Linux	
Nome do Archive	Descrição
SA MP 4.1 Linux.tar	Este é o archive utilizado para instalar o produto. Para extrair o archive, é necessário o GNU tar 1.13 ou mais recente. Utilize o comando tar xf para extrair o archive. Após extrair os arquivos, você localizará o script de instalação installSAM no seguinte diretório: SAM4100MPLinux

AIX

Tabela 4. Archive para plataformas AIX	
Nome do Archive	Descrição
SA MP 4.1 AIX.tar	Este é o archive utilizado para instalar o produto. Utilize o comando tar xf para extrair o archive. Após extrair os arquivos, você localizará o script de instalação installSAM no seguinte diretório: SAM4100MPAIX

Pré-requisitos

Certifique-se de preencher os requisitos de software e de hardware para o System Automation for Multiplatforms.

Pré-requisitos em sistemas AIX

- É necessária a autoridade de administrador para instalar o System Automation for Multiplatforms.
- Uma versão de 32 bits do Java 7, Java 7.1 ou Java 8 é necessária com os seguintes níveis mínimos de atualização de serviço:
 - Java 7.0 SR8: pacote AIX Java7.jre/Java7.sdk 7.0.0.145
 - Java 7.1 SR2: pacote AIX Java71.jre/Java71.sdk 7.1.0.25
 - Java 8.0 SR0: pacote AIX Java8.jre/Java8.sdk 8.0.0.507
 - System Automation for Multiplatforms Fixpack Versão 4.1.0.6 suporta o Java 8 SR6 FP15: pacote AIX Java8.jre/Java8.sdk 8.0.6.15
- System Automation for Multiplatforms Fixpack Versão 4.1.0.6 no AIX, o RSCT 3.2.5.2 será instalado. Os níveis TL a seguir do AIX são suportados somente com esse fixpack:
- AIX 7.1 TL 5
- AIX 7.2 TL 2
- AIX 7.2 TL 3
- AIX 7.2 TL 4

Pré-requisitos em Sistemas Linux

Os seguintes pré-requisitos devem ser atendidos antes que o System Automation for Multiplatforms possa ser instalado em um sistema Linux:

- O pacote a seguir é necessário em cada sistema RedHat v7.1:
- perl-Sys-Syslog
- O seguinte pacote é necessário em cada sistema RedHat v8:
 - perl-Net-Ping

- A autoridade raiz é necessária para instalar o System Automation for Multiplatforms.
- Algumas bibliotecas de 32 bits devem ser instaladas em cada sistema RedHat 6, mesmo se um kernel de 64 bits estiver em execução, antes que o System Automation for Multiplatforms possa ser instalado. Essas bibliotecas estão contidas nos pacotes do RPM Package Manager a seguir:
- 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
- O System Automation for Multiplatforms Fixpack Versão 4.1.0.6 suporta: Java 8 SR6 FP15: pacote Linux Java8.jre/Java8.sdk 8.0.6.15

Pacotes RSCT

Durante a instalação do System Automation for Multiplatforms no AIX, os níveis dos pacotes de RSCT que são requeridos pelo System Automation for Multiplatforms são verificados com relação aos níveis de pacotes de RSCT já instalados com o sistema operacional, e os pacotes ausentes ou os níveis mais altos de pacotes de RSCT são instalados, se necessário. Sob certas circunstâncias, você pode precisar instalar manualmente níveis mais altos de determinados pacotes de RSCT. Por exemplo, se o pacote básico de RSCT não estiver instalado e o nível do pacote principal de RSCT instalado for maior que o nível dos pacotes de RSCT fornecido com o System Automation for Multiplatforms, a instalação do pacote básico de RSCT pode falhar devido aos pré-requisitos de RSCT que não estão sendo atendidos. É necessário fazer download e instalar os conjuntos de arquivos de RSCT apropriados a partir do centro de serviços do AIX para assegurar que todos os pacotes RSCT instalados estejam no mesmo nível.

O System Automation for Multiplatforms Versão 4.1.0.0 inclui o RSCT nível 3.1.5.3 (APAR IV52893).

O System Automation for Multiplatforms Version 4.1.0.6 inclui o RSCT nível 3.2.5.3 (o S.O. Linux de 64 bits), nível RSCT 3.1.5.16 (S.O Linux de 32 bits) e RSCT nível 3.2.5.2 (S.O. AIX).

Requisitos para ambientes virtuais como KVM ou VMWare

Como as máquinas virtuais frequentemente não têm uma forma confiável para manter o controle de tempo, CPUs com Contador de registro de data e hora são suscetíveis a problemas de sincronização. Para evitar problemas de sincronização de tempo, configure uma sincronização de tempo apropriada, por exemplo, NTP, para nós que estão em execução em ambientes virtuais.

Verificando Pré-requisitos

Descubra como executar uma verificação de pré-requisitos.

Sobre Esta Tarefa

Conclua as seguintes etapas:

- 1. Efetue login como root ou com autoridade equivalente.
- 2. Se você fez download do arquivo tar da Internet, extraia o arquivo:

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

Se você recebeu o produto em um DVD, monte o DVD e altere para o diretório onde o DVD está montado.

3. Insira o seguinte comando:

- Linux: cd SAM4100MPLinux
- AIX: cd SAM4100MPAIX

Para obter informações sobre as plataformas suportadas, consulte <u>"Plataformas Suportadas" na</u> página 5

4. Para iniciar a verificação de pré-requisitos, emita o seguinte comando:

./prereqSAM

Geralmente, você não especifica nenhuma das opções que estão disponíveis para o comando **prereqSAM**. Para obter uma descrição detalhada do comando, consulte *Tivoli System Automation for Multiplatforms Reference Guide*.

5. Quando a verificação estiver concluída, verifique o seguinte arquivo de log para obter informações sobre pré-requisitos ausentes:

/tmp/prereqSAM.<#>.log

A tag <#> é um número; o número mais alto identifica o arquivo de log mais recente.

6. Se o sistema não tiver passado na verificação de pré-requisitos, corrija qualquer problema antes de iniciar a instalação.

Pré-requisitos de Instalação

Sobre Esta Tarefa

Antes de iniciar a instalação, você deve preencher estes requisitos:

- É necessário ter propriedade de administrador para instalar o System Automation for Multiplatforms no sistema.
- Um shell Korn deve ser instalado em todas as plataformas do S.O., exceto nas plataformas de S.O. SUSE, nas quais deve-se instalar um shell Korn MirBSD (mksh).
- Perl será necessário para usar a interface da linha de comandos do System Automation for Multiplatforms, incluindo os comandos nativos de RSCT. A interface da linha de comandos é instalado por padrão nos sistemas Linux ou AIX como parte do sistema operacional. Se você estiver usando o System Automation for Multiplatforms em um idioma diferente do inglês, uma versão especial de Perl pode ser necessária. Devido a problemas conhecidos com o Perl 5.8.0 e como ele manipula os códigos de idiomas codificados por UTF-8, alguns caracteres podem não ser exibidos adequadamente. O problema pode ocorrer em sistemas com Perl 5.8.0 instalado, se você usar um código de idioma codificado por UTF-8. Quando versões anteriores ou subsequentes do Perl ou locales não codificados UTF-8 são utilizados, esse problema não ocorre.

Se você optar por fazer upgrade do Perl versão 5.8.0 em uma distribuição do Linux, processe as etapas a seguir:

- 1. Faça download da fonte do Perl 5.8.1.
- 2. Extraia o arquivo em qualquer diretório usando -xvf.
- 3. Compile e instale no sistema UTF-8, consultando as instruções fornecidas com os arquivos transferidos por download.
- 4. Altere o link simbólico, que está apontando para o diretório da versão do Perl que é usada pelo System Automation for Multiplatforms

Altere o link de:

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

Para o diretório onde a nova versão do Perl é instalada:

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

- Certifique-se de que os diretórios /usr/sbin e /opt tenham pelo menos 100 MB de espaço livre e que o diretório /var também forneça pelo menos 100 MB de espaço livre.
- Em qualquer nó em que o adaptador de automação de ponta a ponta estiver configurado para execução, pelo menos 128 MB de RAM devem estar disponíveis.
- Durante a instalação do System Automation for Multiplatforms no AIX, os níveis dos pacotes de RSCT que são necessários para o System Automation for Multiplatforms são verificados com relação aos níveis de pacotes de RSCT já instalados com o sistema operacional. Os pacotes ausentes ou os níveis mais altos dos pacotes de RSCT são instalados, se necessário. Sob certas circunstâncias, você pode precisar instalar manualmente níveis mais altos de determinados pacotes de RSCT. Por exemplo, se o pacote básico de RSCT não estiver instalado e o nível do pacote principal de RSCT instalado for maior que o nível dos pacotes de RSCT fornecidos com o System Automation for Multiplatforms, a instalação do pacote básico de RSCT pode falhar devido aos pré-requisitos de RSCT não serem atendidos. É necessário fazer download e instalar os conjuntos de arquivos de RSCT apropriados a partir do centro de serviços do AIX para assegurar que todos os pacotes RSCT instalados estejam no mesmo nível.
- Para outros requisitos específicos do sistema operacional, veja <u>Relatórios de compatibilidade de</u> produto de software.
- Para idiomas que estão usando o conjunto de caracteres de byte duplo (DBCS), o buffer de diálogo do Telnet deve ser suficientemente grande para assegurar que longas mensagens sejam exibidas adequadamente. Caso contrário, aumente o buffer de diálogo Telnet.
- Em algumas distribuições RHEL, o ambiente SELinux é ativado por padrão. Certifique-se de que o ambiente SELinux seja desativado para que o System Automation for Multiplatforms funcione corretamente.

Plataformas Suportadas

Descubra quais plataformas são suportados pelo System Automation for Multiplatforms.

Sobre Esta Tarefa

O System Automation for Multiplatforms suporta os ambientes UNIX a seguir:

- Linux on System z
- Linux on System x
- Linux on Power
- Ubuntu on System x⁵
- Ubuntu on Power⁵
- AIX
- O System Automation for Multiplatforms é executado em:
- Todas as máquinas IBM Systems que executam Linux.
- Máquinas IBM System p que executam AIX.

O System Automation for Multiplatforms é executado sob:

- VMware on IBM System x (exceto servidores baseados em Intel IA64) e qualquer outro servidor baseado em Intel de 32 bits, servidor baseado em AMD Opteron (64 bits) ou servidor baseado em Intel EM64T (64 bits). A migração ativa de sistemas usando o vMotion é suportada (consulte <u>"Suporte ao</u> VMware vMotion" na página 7).
- RHEV-H versão 4.3, versão do hypervisor KVM 5.4 ou superior em todas as distribuições suportadas do Linux na migração em tempo real do IBM System x. de sistemas não é suportada.

A tabela a seguir lista as versões de sistemas operacionais suportados.

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

Tabela 5. Plataformas UNIX e Linux suportadas do System Automation for Multiplatforms				
	IBM System x ¹	IBM System z	Power Systems	Power Systems (Little Endian)
SUSE SLES 12 (64 bits) ⁴	x	х		x
SUSE SLES 15 (64 bits) ⁷	x	х		x
Red Hat RHEL 7 (64 bits)	x ⁴	x ⁴	x ⁴	x ⁵
Red Hat RHEL 8 (64 bits) ⁸	x	x		x
Ubuntu 18.04 LTS (64 bits) ⁷	х			x
Ubuntu 20.04 LTS (64 bits) ⁸	х			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			

Todos os níveis de SP das versões do SUSE e versões do Red Hat suportados listados acima também são suportados, a menos que uma das notas a seguir indique um requisito mínimo mais específico.

Nota:

- 1. System x significa System x (exceto servidores baseados em Intel IA64) e qualquer outro servidor baseado em Intel de 32 bits ou servidor baseado em AMD Opteron (64 bits) ou servidor baseado em Intel EM64T (64 bits).
- 2. São suportados o zSystems versão z15 e o pSystems versão p9.
- 3. Todos os níveis futuros/novos de SP do Linux (SUSE e RHEL) são suportados, se forem suportados pelos pacotes RSCT empacotados (consulte "Pré-requisitos" na página 2 para obter mais detalhes) com este fix pack e são compatíveis com versões anteriores com o nível de SP qualificado com este fix pack.
- 4. O suporte à plataforma é introduzido com o fix pack 4.1.0.1.
- 5. O suporte à plataforma foi introduzido com o fix pack 4.1.0.2.
- 6. O suporte à plataforma foi introduzido com o fix pack 4.1.0.4.
- 7. O suporte à plataforma foi introduzido com o fix pack 4.1.0.5.
- 8. O suporte à plataforma é introduzido com fix pack 4.1.0.6.
- 9. A partir do fix pack 4.1.0.7, foi introduzido o suporte para plataforma..

Para obter informações adicionais, consulte <u>"Instalando em novos sistemas operacionais" na página 37</u> na página 34.

Interfaces de Rede Suportadas

Sobre Esta Tarefa

Todas as plataformas suportam as interfaces de rede 10 Megabit Ethernet, Fast Ethernet e Gigabit Ethernet. Além disso, a plataforma System z também suporta HiperSockets, CTC e VM Guest LAN.

Suporte para Sistemas de Arquivos de Rede

O System Automation for Multiplatforms suporta network file systems no Linux on POWER, Linux on System x, Linux on System z e AIX.

Os sistemas de arquivos de rede não são coletados. Para automatizar um network file system, use recursos IBM.AgFileSystem definidos pelo usuário.

Restrição:

- Network file systems de classe IBM. AgFileSystem podem ser automatizados e monitorados com sucesso somente se o usuário root do sistema de importação tiver acesso de gravação para o sistema de arquivos.
- O uso em cascata de sistemas de arquivos não é possível:

Com o System Automation for Multiplatforms, é possível definir um servidor NFS altamente disponível, em que os sistemas de arquivos exportados são automatizados como recursos de classe IBM.AgFileSystem que residem em uma mídia de disco compartilhado. O próprio servidor NFS é automatizado como um recurso de classe IBM.Application que pode flutuar em sistemas que têm acesso à mídia de disco compartilhado. Quando um sistema adicional importar os sistemas de arquivos de rede, no entanto, os sistemas de arquivos importados ainda não devem existir como recursos IBM.AgFileSystem definidos pelo usuário no sistema de importação, caso contrário, o monitoramento dos sistemas de arquivos falhará e os recursos entrarão em OpState 3 (FAILED OFFLINE).

Requisitos de Suporte do Live Partition Mobility

Sobre Esta Tarefa

Com o AIX Nível 6100-00-01 (ou superior) instalado nos servidores POWER6 de origem e de destino, o recurso Live Partition Mobility pode ser usado para migrar uma LPAR em execução como um nó do System Automation for Multiplatforms. O estado ou a operação do cluster do System Automation for Multiplatforms não é afetado. O cluster está configurado para usar as configurações de pulsação padrão. Nesse caso, o efeito nos servidores de aplicativos é uma breve interrupção de operações durante a migração. Não é necessário reiniciar o System Automation for Multiplatforms ou os servidores de aplicativos.

Certifique-se de que o período de interrupção durante o Live Partition Mobility não cause eventos de cluster indesejáveis. Podem ocorrer eventos de cluster indesejáveis, se muitas pulsações do nó estiverem ausentes durante o período médio de interrupção. Nesse caso, libere as configurações de pulsação durante o Live Partition Mobility.

Outra maneira de minimizar a chance de eventos de cluster indesejáveis durante a movimentação de uma LPAR é parar o domínio do mesmo nível de maneira forçada, antes do início da movimentação com stoprpdomain -f, ou seja, sem parar os aplicativos gerenciados pelos serviços de cluster. Após a conclusão da movimentação, reinicie o domínio do mesmo nível.

Restrição: O desempatador de disco não é suportado pelo SCSI virtual, que é um pré-requisito do Live Partition Mobility.

Suporte ao VMware vMotion

Sobre Esta Tarefa

Com uma configuração do VMware vSphere com diversos servidores ESX gerenciados por um vCenter Server, o recurso vMotion pode ser usado para migrar convidados de produção em execução como um nó do System Automation for Multiplatforms. A migração não afeta o estado ou operação do cluster do System Automation for Multiplatforms, desde que o cluster esteja configurado para usar configurações de pulsação padrão. Nesse caso, o efeito nos servidores de aplicativos em execução sob controle do System Automation for Multiplatforms é uma breve interrupção das operações durante a migração. Nem o System Automation for Multiplatforms nem os servidores de aplicativos terão que ser reiniciados.

Certifique-se de que o período de interrupção durante o vMotion não cause eventos de cluster indesejáveis. Ocorrerão eventos de cluster indesejáveis se muitas pulsações do nó estiverem ausentes durante o período médio de interrupção. Nesse caso, libere as configurações de pulsação durante o vMotion.

Outra maneira de minimizar a chance de eventos de cluster indesejáveis durante a movimentação de um convidado virtual é parar o domínio do mesmo nível de maneira forçada, antes do início da movimentação com stoprpdomain -f, ou seja, sem parar os aplicativos gerenciados pelos serviços de cluster. Após a conclusão da movimentação, reinicie o domínio do mesmo nível.

O System Automation for Multiplatforms suporta servidores vMotion for ESX e ESXi com a versão 3.5 ou superior e os seguintes sistemas operacionais guest:

- RHEL 6 (x86-64 ou x86-32)
- SLES 12 ou 15 (x86-64)
- RHEL 7 ou 8 (x86-64)
- Ubuntu 16.04, 18.04 ou 20.04 (x86-64)

Limitações: O System Automation for Multiplatforms não suporta o vMotion de nós que usam armazenamento compartilhado, pois o vMotion não suporta volumes de armazenamento (discos) reais ou virtuais compartilhados.

Suporte a imagem de sistema único e realocação de convidado em tempo real do z/VM

O z/VM 6.2 introduz suporte a Imagem de sistema único (SSI), que é uma tecnologia de armazenamento em cluster de multissistema. É possível armazenar em cluster até 4 imagens do z/VM usando Imagem de sistema único. SSI facilita compartilhamento de recurso entre os membros no cluster. É possível mover um convidado ativo do Linux on System z para outro sistema z/VM sem uma indisponibilidade do convidado. Esse recurso é chamado de Live Guest Relocation (LGR) e é suportado somente para convidados do Linux on System z.

Para entender os conceitos e recursos de SSI e LGR do z/VM, consulte <u>An Introduction to z/VM Single</u> System Image (SSI) e Live Guest Relocação (LGR) (SG24-8006).

Se o nível de requisito do z/VM estiver instalado nos sistemas de origem e de destino, o recurso Live Guest Relocation do z/VM pode ser usado para realocar um sistema convidado z/VM Linux. Se o nível requisito do System Automation for Multiplatforms estiver instalado no sistema convidado Linux, realocar esse sistema convidado não afeta o estado ou operação do cluster do System Automation for Multiplatforms se as configurações de pulsação padrão estiverem configuradas. Para um aplicativo gerenciado pelo System Automation for Multiplatforms, o processo de realocação é uma breve suspensão das operações. Reinicialização não é necessária para o System Automation for Multiplatforms e o aplicativo.

Valide se o período de suspensão durante Live Guest Relocation não causa eventos de cluster indesejados. Eventos de cluster indesejados ocorrem se um número configurado de pulsações estiver ausente do nó que sofrer uma suspensão durante Live Guest Relocation. Se o teste mostrar que o período médio de suspensão pode causar a perda de muitas pulsações, as configurações de pulsação devem ser relaxadas durante o tempo de Live Guest Relocation. Para minimizar muito a chance de eventos de cluster indesejados enquanto um sistema convidado z/VM é realocado, pare o domínio do mesmo nível de maneira forçada antes que a realocação seja iniciada usando **stoprpdomain -f**. Por exemplo, sem parar os aplicativos que são gerenciados pelos serviços de cluster. Na conclusão bem-sucedida da realocação, reinicie o domínio do mesmo nível usando o comando **startrpdomain**.

Requisitos

• System Automation for Multiplatforms versão 3.2.2.4 (ou superior)

• z/VM versão 6.2

Limitações

O desempatador de disco de ECKD e o desempatador de SCSI PR não podem ser usados com Live Guest Relocation, pois os convidados que retém uma reserva em um disco não podem ser realocados.

Preparando a Instalação

O System Automation for Multiplatforms está contido em vários pacotes que devem ser instalados em cada nó do cluster que você deseja automatizar. O tipo de pacote e o conteúdo dependem do sistema operacional em que o System Automation for Multiplatforms está sendo instalado.

Iniciando a Configuração

Execute as seguintes configurações iniciais:

• Em todos os nós, configure e exporte a variável de ambiente CT_MANAGEMENT_SCOPE para 2 (escopo de domínio do mesmo nível) para todos os usuários do System Automation for Multiplatforms: export CT_MANAGEMENT_SCOPE=2

Para configurar a variável permanentemente, configure-a e exporte-a no perfil.

Em sistemas SLES, é possível criar scripts em /etc/profile.d com o seguinte conteúdo:

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

• Certifique-se de que a variável de ambiente LANG esteja configurada com um dos códigos de idioma suportados para o usuário root. Para configurar a variável de ambiente, use o comando:

export LANG=xx_XX

xx_XX denota um dos idiomas suportados.

Para obter uma lista de idiomas e códigos de idioma suportados, consulte <u>"Idiomas e Códigos de Idioma</u> Suportados" na página 25.

Carregamento em Nós

O System Automation for Multiplatforms requer que alguns de seus subsistemas sejam processados constantemente no nó para assegurar que os serviços de cluster estejam funcionando corretamente (por exemplo, pulsação e comunicação entre os subsistemas). Se isso não for possível, o System Automation poderá acionar métodos de proteção de recursos críticos no caso desses subsistemas não poderem se comunicar dentro de um curto período de tempo. Este mecanismo de proteção eventualmente conduz a uma reinicialização do nó no qual este problema ocorre.

Para evitar uma reinicialização do sistema indesejada, o carregamento de E/S e de troca constante deve ser inferior a 10%.

Para obter informações adicionais sobre os métodos de proteção de recursos críticos, consulte o *Tivoli System Automation for Multiplatforms Administrator's and User's Guide*.

Número de Nós em um Cluster

Linux

O número máximo de nós em um cluster é 32.

AIX

O número máximo de nós em um cluster é 130.

Nota:

- 1. Os pacotes de software devem estar disponíveis nos nós em que você deseja instalar o System Automation for Multiplatforms. Por exemplo, é possível montar o DVD em um PC e usar o FTP para transferir os arquivos para o nó, ou instalar os pacotes através de um Network File System compartilhado.
- 2. Para assegurar que os pacotes de software sejam instalados e desinstalados corretamente, use os scripts do System Automation for Multiplatforms, **installSAM** e **uninstallSAM**. Eles também executam tarefas de verificação de requisitos, de instalação e migração de licença.
- 3. Com exceção dos pacotes de idiomas, todos os pacotes são necessários para que o System Automation funcione. A partir do System Automation for Multiplatforms 4.1, não é mais possível desinstalar o pacote RSCT rsct.opt.storagerm sem desinstalar o produto inteiro.

Planejando o novo suporte de plataforma

A partir do fix pack 4.1.0.1, o System Automation for Multiplatforms introduz diferentes pacotes de instalação para ambientes de linguagem de 32 bits e 64 bits.

Os pacotes correspondentes também são fornecidos para todos os seguintes fix packs 4.1.0.x. Ambos os pacotes têm o mesmo código base.

- O primeiro pacote 4.1.0-TIV-SAMP-Linux-FPxxxx contém a compilação do produto System Automation for Multiplatforms para ambientes de linguagem de 32 bits. Esses ambiente de linguagem de 32 bits são requeridos pelo System Automation for Multiplatforms nos sistemas operacionais Linux RHEL 6.
- O segundo pacote 4.1.0-TIV-SAMP-Linux64-FPxxxx contém a compilação do produto System Automation for Multiplatforms para ambientes de linguagem de 64 bits. Esses ambiente de linguagem de 64 bits são requeridos pelo System Automation for Multiplatforms nos sistemas operacionais Linux RHEL 7/8, SLES 12/15 e Ubuntu 16.04/18.04/20.04

Não é possível usar o segundo pacote para os sistemas operacionais Linux RHEL 6. O System Automation for Multiplatforms 4.1.0.0 ou inferior não é suportado no SLES 12/15, RHEL 7/8 e Ubuntu 16.04/18.04/20.04.

Planejamento para uma Infraestrutura de Rede Altamente Disponível

Entenda a complexidade e planeje a configuração de uma rede altamente disponível.

A figura a seguir mostra uma infraestrutura de rede no Linux.



Figura 2. Problemas ao planejar uma rede de alta disponibilidade

Cada dispositivo de rede estático configurado é identificado por uma entrada na tabela de roteamento. O algoritmo de rota escolhe a primeira rota correspondente fora dessa tabela. Neste exemplo, o dispositivo eth1 no nó lnxcm1 falha. Como eth1 é a primeira entrada na tabela de roteamento, o nó não pode enviar pacotes fora da rede, embora exista outra interface de rede em funcionamento eth0.

Considere as seguintes perguntas antes de iniciar o planejamento de sua rede de alta disponibilidade:

- 1. De que tipo de rede de alta disponibilidade você precisa?
 - É necessário mover um ServiceIP de uma interface para outra no mesmo nó?
 - É necessário alternar para outro nó que tenha uma interface funcional na sub-rede necessária?
- 2. É possível implementar sub-redes IP adicionais ou você usa uma infraestrutura de rede existente?
- 3. Você trabalha apenas no escopo de nossos nós de cluster ou pode implementar serviços de rede em outros nós fora do cluster de automação?
- 4. Qual hardware de rede você possui?

Dependendo de como respondeu às perguntas, talvez você queira escolher uma das seguintes configurações para desenvolver sua própria estratégia de rede de alta disponibilidade.

Planejamento para Dispositivos de Armazenamento

Usando Dispositivos de Armazenamento de Caminho Único

O suporte para dispositivos de armazenamento de caminho único é diferente, dependendo do seu ambiente operacional.

AIX

É fornecido suporte completo para dispositivos de armazenamento de caminho único:

• Recursos IBM. AgFileSystem coletados podem ser automatizados.

Os recursos IBM. AgFileSystem são coletados se forem do tipo jfs ou jfs2 e residirem em entidades de armazenamento que são coletadas por elas mesmas (entidades de armazenamento de classe IBM.LogicalVolume, IBM.VolumeGroup, IBM.Disk).

- Recursos IBM.AgFileSystem definidos pelo usuário podem ser automatizados, por exemplo, sistema de arquivos de rede.
- A reserva SCSI-2 é suportada.

Limitações:

- Sem faixa
- Recursos IBM. AgFileSystem definidos pelo usuário podem ser automatizados somente se o disco que está hospedando o sistema de arquivos tiver o mesmo nome de dispositivo em todos os nós do cluster.

Linux on POWER e Linux on System x

É fornecido suporte limitado:

• Recursos IBM.AgFileSystem coletados podem ser automatizados.

Recursos IBM.AgFileSystem são coletados se forem do tipo ext2, ext3 ou reiserfs e residirem em entidades de armazenamento que sejam, por sua vez, coletadas (entidades de armazenamento de classe IBM.LogicalVolume, IBM.Partition, IBM.VolumeGroup, IBM.Disk).

• Recursos IBM.AgFileSystem definidos pelo usuário podem ser automatizados, por exemplo, sistema de arquivos de rede.

Limitações:

- O suporte para reserva SCSI é limitado. Desempenhe uma operação de reserva de disco para verificar se a reserva SCSI está disponível.
- Recursos IBM. AgFileSystem definidos pelo usuário podem ser automatizados somente se o disco que está hospedando o sistema de arquivos tiver o mesmo nome de dispositivo em todos os nós do cluster.

Linux on System z

Dispositivos fornecidos pelo mapeador de dispositivos ou md em si são coletados como recursos IBM. Disk somente se um volume físico tiver sido criado no dispositivo md usando o comando **pvcreate**.

Limitações:

- Somente recursos IBM. AgFileSystem definidos pelo usuário ou recursos IBM. AgFileSystem que residem em dispositivos fornecidos pelo mapeador de dispositivos ou md coletados podem ser automatizados. A coleta de recurso para outros discos não é suportada. Mesmo se a coleta de outros discos obtiver êxito, os recursos coletados não poderão ser automatizados.
- Recursos IBM. AgFileSystem definidos pelo usuário podem ser automatizados somente se o disco que está hospedando o sistema de arquivos tiver o mesmo nome de dispositivo em todos os nós do cluster.
- A reserva SCSI não é suportada.

Usando Dispositivos de Armazenamento com Caminhos Múltiplos

Dependendo do seu ambiente, o suporte para dispositivos de armazenamento com caminhos múltiplos pode ter algumas restrições.

AIX

É fornecido suporte completo para dispositivos de armazenamento SPIO e MPIO:

• Recursos IBM.AgFileSystem coletados podem ser automatizados.

Recursos IBM. AgFileSystem são coletados se forem do tipo jfs ou jfs2 e residirem em entidades de armazenamento que são por sua vez coletadas (entidades de armazenamento de classe IBM.LogicalVolume, IBM.VolumeGroup, IBM.Disk).

- Recursos IBM.AgFileSystem definidos pelo usuário podem ser automatizados (por exemplo, sistemas de arquivos de rede).
- A reserva SCSI-2 é suportada para os dispositivos de armazenamento SPIO e MPIO utilizando a unidade RDAC (Redundant Disk Array Controller).

Nota: Este driver está disponível apenas para as famílias IBM TotalStorage DS4k e DS6k.

Limitações:

- Sem faixa
- Recursos IBM. AgFileSystem definidos pelo usuário podem ser automatizados somente se o disco que está hospedando o sistema de arquivos tiver o mesmo nome de dispositivo em todos os nós do cluster.

Linux on POWER e Linux on System x

O suporte total está disponível para dispositivos de armazenamento de E/S de caminho único (SPIO) e para dispositivos de armazenamento de E/S com caminhos múltiplos (MPIO), com drivers de dispositivo Redundant Disk Array Controller (RDAC), bem como dispositivos md e fornecidos pelo mapeador de dispositivos.

• Recursos IBM.AgFileSystem coletados podem ser automatizados.

Recursos IBM.AgFileSystem são coletados se forem do tipo ext2, ext3 ou reiserfs e residirem em entidades de armazenamento que sejam, por sua vez, coletadas (entidades de armazenamento de classe IBM.LogicalVolume, IBM.Partition, IBM.VolumeGroup, IBM.Disk).

- Recursos IBM. AgFileSystem definidos pelo usuário podem ser automatizados (por exemplo, sistemas de arquivos de rede).
- A reserva SCSI-2 é suportada para discos coletados do driver RDAC.
- Linux RAID (dispositivos fornecidos por /dev/device mapper ou md) é suportado.
- Discos gerenciados pelo mapeador de dispositivos são suportados.

Limitações:

- Sistemas de arquivos criados em dispositivos fornecidos pelo mapeador de dispositivos ou md sem usar o LVM não são coletados; eles podem ser automatizados somente usando recursos IBM.AgFileSystem definidos pelo usuário.
- Dispositivos fornecidos pelo mapeador de dispositivos ou md em si são coletados como recursos IBM.Disk somente se um volume físico tiver sido criado no dispositivo md usando o comando **pvcreate**.
- A reserva SCSI-2 não é suportada para drivers não RDAC ou para os próprios dispositivos fornecidos pelo mapeador de dispositivos ou md.
- Recursos IBM. AgFileSystem definidos pelo usuário podem ser automatizados somente se o disco que está hospedando o sistema de arquivos tiver o mesmo nome de dispositivo em todos os nós do cluster.
- EVMS não é suportado, o qual inclui quaisquer Grupos de Volume/Volumes Lógicos criados ou gerenciados pelo EVMS.
- Para o SLES 12/15 e o RHEL 7/8, há suporte para a coleta de entidades de armazenamento de classe IBM.Disk, IBM.VolumeGroup, IBM.LogicalVolume, IBM.Partition e IBM.AgFileSystem. Os sistemas de arquivos poderão ser automatizados apenas se as limitações para dispositivos fornecidos pelo mapeador de dispositivos ou md listadas acima forem atendidas.

Linux on System z

Dispositivos fornecidos pelo mapeador de dispositivos ou md em si são coletados como recursos IBM.Disk somente se um volume físico tiver sido criado no dispositivo de bloco fornecido usando o comando pvcreate. Isso não depende da tecnologia de disco subjacente, ECKD ou SCSI.

Limitações:

- Somente recursos IBM. AgFileSystems definidos pelo usuário ou recursos IBM. AgFileSystems que residem em dispositivos fornecidos pelo mapeador de dispositivos ou md coletados podem ser automatizados. A coleta de recurso para outros discos não é suportada. Mesmo se a coleta de outros discos obtiver êxito, os recursos coletados não poderão ser automatizados.
- Recursos IBM. AgFileSystems definidos pelo usuário podem ser automatizados somente se o disco que está hospedando o sistema de arquivos tiver o mesmo nome de dispositivo em todos os nós do cluster.
- A reserva SCSI não é suportada.

Usando Interfaces de Rede

É possível instalar uma configuração de alta disponibilidade com dois nós em um cluster, cada um com duas interfaces de rede.

Antes de iniciar essa configuração, tenha em mente que não é possível ter mais de uma interface de rede estática configurada na mesma sub-rede IP. Cada endereço IP é responsável por uma entrada na tabela de roteamento de kernel. Se houver duas interfaces na mesma sub-rede, haverá duas rotas para a mesma sub-rede. Se a interface que criou a primeira entrada falhar, a comunicação para essa sub-rede é interrompida mesmo se houver outra interface, que ainda pode se comunicar.

Duas Redes Separadas Fisicamente, ServiceIP Movido entre os Nós

Tabela 6. Configuração de rede para um cluster de dois nós com interfaces de rede			
Recurso	Nome	Dispositivo	IP
Nó do cluster	lnxcm1	eth0 eth1	9.152.172.1/24 192.168.1.1/24
Nó do cluster	lnxcm2	eth0 eth1	9.152.172.2/24 192.168.1.2/24
Roteador	gw	eth0	9.152.172.254/24
ServiceIP	-	-	9.152.172.3/24

Aplica-se a seguinte configuração de rede:



Figura 3. Dois Nós, Duas Interfaces, Duas Redes Separadas Fisicamente

A comunicação do cluster conta agora com duas redes: a 192.168.1.0 e a 9.152.172.0. Se houver falha em uma interface de rede, o cluster não será interrompido.

- A rede 9.152.172.0 representa a rede para o serviço de TI altamente disponível.
- A rede 192.168.1.0 torna a comunicação interna do cluster mais confiável.

Como somente a rede do ServiceIP está conectada ao gateway, uma falha da interface eth0 no lnxcm1 fará com que a mecanização mova o ServiceIP para a interface eth0 no outro nó lnxcm2. Em consequência da separação física das duas redes, não é possível mover o ServiceIP da eth0 para a eth1 no mesmo nó.

A política de amostra do System Automation for Multiplatforms é igual à mostrada na Figura 7 na página 19.

Tabela 7. Vantagens e desvantagens de uma configuração de dois nós com interfaces de rede		
Vantagem	Desvantagem	
Configuração fácil.	O ServiceIP é movido apenas entre os nós.	
Redundância na comunicação do cluster.		

Três redes lógicas em uma rede física, mover ServiceIP entre as interfaces de rede

Outra configuração de rede é necessária para não apenas mover o ServiceIP entre os nós no cluster, mas também entre as interfaces dentro de um nó.

Uma rede lógica separada para cada interface de um nó é necessária, além de uma rede adicional para o ServiceIP. Escolher uma rede existente (uma de eth0 ou eth1) pode causar problemas de roteamento. Certifique-se de conectar todas as interfaces à mesma rede física. Isso permite que cada interface contenha os endereços de todas as redes lógicas.

Aplica-se a seguinte configuração de rede:

Tabela 8. Configuração de rede para três redes lógicas em uma rede física			
Recurso	Nome	Dispositivo	IP
Nó do cluster	lnxcm1	eth0 eth1	192.168.1.1/24 192.168.2.1/24
Nó do cluster	lnxcm2	eth0 eth1	192.168.1.2/24 192.168.2.2/24
Roteador	gw	eth0	9.152.172.254/24
ServiceIP	-	-	9.152.172.3/24



Figura 4. Dois Nós, Duas Interfaces, Uma Rede Física

- A rede 9.152.172.0 representa a rede para o serviço de TI altamente disponível.
- A rede 192.168.1.0 representa a primeira rede de comunicação interna do cluster.
- A rede 192.168.2.0 representa a segunda rede de comunicação interna do cluster.

Amostra de política do System Automation for Multiplatforms:

```
lnxcm1# mkequ NetInt
IBM.NetworkInterface:eth0:lnxcm1,eth1:lnxcm1,eth0:lnxcm2,eth1:lnxcm2
lnxcm1# mkrsrc IBM.ServiceIP Name="SIP" IPAddress="9.152.172.3"
NetMask="255.255.255.0" NodeNameList="{'lnxcm1', 'lnxcm2'}"
lnxcm1# mkrg rg
lnxcm1# addrgmbr -g rg IBM.ServiceIP:SIP
lnxcm1# mkre1 -p dependson -S IBM.ServiceIP:SIP -G IBM.Equivalency:NetInt
```

Tabela 9. Vantagens e desvantagens de uma configuração de rede para três redes lógicas em uma rede física

Vantagem	Desvantagem
Configuração fácil.	3 redes lógicas em 1 rede física.
Redundância na comunicação do cluster.	Tráfego de 3 redes em um 1 meio físico.

Tabela 9. Vantagens e desvantagens de uma configuração de rede para três redes lógicas em uma rede física (continuação)

Vantagem	Desvantagem
ServiceIP pode ser movido entre interfaces e nós.	

Duas Redes Separadas Fisicamente, Roteamento Dinâmico e VIPA

Uma descrição detalhada dessa configuração está além do escopo desse manual. Basicamente, o ServiceIP é designado a uma rede virtual no kernel de um nó do cluster. O roteamento dinâmico em todos os nós do cluster e no gateway garante que uma rota para o ServiceIP esteja estabelecida.

Tabela 10. Configuração de rede de duas redes fisicamente separadas IP Recurso Nome Dispositivo Nó do cluster lnxcm1 eth0 9.152.170.1/24 eth1 9.152.171.1/24 Nó do cluster lnxcm2 eth0 9.152.170.2/24 eth1 9.152.171.2/24 Roteador gw eth0 9.152.170.254/24 eth1 9.152.171.254/24 ServiceIP 9.152.172.3/24 _ _ gw



Aplica-se a seguinte configuração de rede:

Figura 5. Duas Redes Separadas Fisicamente, Roteamento Dinâmico e VIPA

Tabela 11. Vantagens e desvantagens para uma configuração de rede de duas redes fisicamente separadas

,	
Vantagem	Desvantagem
Não há dependência com o dispositivo de rede física.	Configuração complicada.
Conceito de se localizar dinamicamente o melhor meio para um host (endereço IP)	Roteamento dinâmico necessário.
Não há necessidade de mover o ServiceIP entre as interfaces.	A configuração não está restrita aos nós do cluster, o gateway também precisa suportar o roteamento dinâmico.

Ligação de Interface

Várias interfaces de rede física estão ligadas a um dispositivo de rede lógica. O sistema operacional precisa suportar esse recurso com um driver de dispositivo de ligação especial. Consulte a documentação de seu sistema operacional para saber como configurar a ligação de interface no sistema. Certifique-se de que você configure ligação de alta disponibilidade (alta disponibilidade) e assegure que suas placas da interface de rede suportem o mecanismo de detecção de falha da interface que seu driver de ligação requer.

Tabela 12. Configuração de rede para interfaces de rede física ligadas			
Recurso	Nome	Dispositivo	IP
Nó do cluster	lnxcm1	eth0 eth1	9.152.172.1/24 9.152.172.1/24
Nó do cluster	lnxcm2	eth0 eth1	9.152.172.2/24 9.152.172.2/24
Roteador	gw	eth0	9.152.172.254/24
ServiceIP	-	-	9.152.172.3/24

Aplica-se a seguinte configuração de rede:



Figura 6. Interfaces de Rede Ligadas a um Dispositivo de Rede Lógica

Tabela 13. Vantagens e desvantagens de uma configuração de rede para interfaces de rede física ligadas		
Vantagem	Desvantagem	
Configuração fácil.	O sistema operacional precisa suportar a ligação de interface.	
Redundância na comunicação do cluster.	O hardware da interface de rede pode precisar suportar a detecção de defeito da interface (por exemplo, monitoramento de link MII).	
Não há necessidade de mover o ServiceIP entre os dispositivos no mesmo nó.		

Usando uma Interface Ethernet

É possível configurar uma configuração de alta disponibilidade com dois nós em um cluster, cada um com uma interface Ethernet separada.

É fornecida a seguinte configuração de rede:

Tabela 14. Configuração de rede de um cluster de dois nós com interfaces Ethernet			
Recurso	Nome	Dispositivo	IP
Nó do cluster	lnxcm1	eth0	9.152.172.1/24
Nó do cluster	lnxcm2	eth0	9.152.172.2/24
Roteador	gw	eth0	9.152.172.254/24
ServiceIP	-	-	9.152.172.3/24



Figura 7. Dois Nós, Uma Interface

Nessa configuração, a comunicação do cluster e a apresentação do serviço de TI altamente disponível utilizam o mesmo caminho de comunicação, a rede 9.152.172.0.

A mecanização pode designar o ServiceIP na interface eth0 no lnxcm1 ou na interface eth0 no lnxcm2. Se uma interface falhar, a automação moverá o ServiceIP para o outro nó. Portanto, isso satisfaz a política que requer a designação do ServiceIP em uma interface de rede em execução.

Nesta configuração, a falha de uma interface de rede levará a uma interrupção na comunicação do cluster com todos os problemas descritos em Guia do Administrador e do Usuário do System Automation for Multiplatforms. Se a comunicação for interrompida conforme mostrado em <u>Figura 8 na página 20</u>, o desempatador decidirá qual nó continuará com a automação. Se o desempatador estiver reservado pelo nó lnxcm1, então, nenhuma interface de rede online estará disponível no nó lnxcm1 para designar o ServiceIP.



Figura 8. Dois Nós, Uma Interface – Falha na Interface

Neste exemplo, a rede 9.152.172.0 atende dois objetivos:

1. A representação da rede para o serviço de TI altamente disponível.

2. A utilização para comunicação interna do cluster.

Amostra de política do System Automation for Multiplatforms:

```
lnxcm1# mkequ NetInt IBM.NetworkInterface:eth0:lnxcm1,eth0:lnxcm2
lnxcm1# mkrsrc IBM.ServiceIP Name="SIP"
IPAddress="9.152.172.3"
NetMask="255.255.255.0"
NodeNameList="{'lnxcm1', 'lnxcm2'}"
Inxcm1# mkrg rg
Inxcm1# addrgmbr -g rg IBM.ServiceIP:SIP -G IBM.Equivalency:NetInt
```

Tabela 15. Vantagens e desvantagens de um cluster de dois nós com interfaces Ethernet	
Vantagem	Desvantagem
A configuração é simples.	Cada problema de comunicação leva à divisão do cluster.

Tabela 15. Vantagens e desvantagens de um cluster de dois nós com interfaces Ethernet (continuação)		
Vantagem	Desvantagem	
Menos hardware de rede necessário.	O ServiceIP é movido apenas entre os nós.	
Capítulo 2. Instalando

A instalação ou upgrade do System Automation for Multiplatforms envolve preparar o sistema e executar um conjunto de tarefas que são específicas de seu ambiente.

Fazendo Upgrade

É possível fazer upgrade do System Automation for Multiplatforms a partir de uma versão Try & Buy para uma versão completa ou de uma versão em execução para a liberação mais recente.

Fazendo Upgrade de uma Versão Try & Buy para uma Versão Completa do Produto

A versão Try & Buy do System Automation for Multiplatforms está instalada e você comprou a versão completa do produto. Então, você recebe outra cópia da mídia de instalação, que contém o arquivo de licença para a licença completa.

Sobre Esta Tarefa

O arquivo de licença está no meio de instalação no subdiretório license. Para executar o upgrade da licença, insira:

samlicm -i <license_file_name>

Para exibir a licença, insira:

samlicm -s

Após fazer upgrade da licença, verifique se quaisquer atualizações do System Automation for Multiplatforms estão disponíveis e instale as atualizações.

Fazendo Upgrade de uma Versão Anterior à Versão 4.1

É possível fazer upgrade para a versão 4.1 de versões anteriores do produto.

Sobre Esta Tarefa

Ao fazer upgrade do System Automation for Multiplatforms a partir de uma versão anterior à versão 4.1, observe os comentários a seguir:

Configuração de adaptador silenciosa

Se estiver usando o utilitário de configuração cfgsamadapter em modo silencioso para definir as configurações do adaptador de automação de ponta a ponta, certifique-se de gerar um novo arquivo de propriedades de entrada silencioso no novo nível de liberação. As configurações do adaptador de automação são configuradas no modo silencioso quando você inicia o utilitário cfgsamadapter usando a opção - s. Antes de poder executar qualquer configuração silenciosa, gere um novo arquivo de propriedades de entrada abrindo o utilitário cfgsamadapter com as opções - s [-g | -gr], em vez de usar um arquivo de propriedades de entrada existente.

Console de operações removido

O console de operações e o editor de políticas não estão contidos na versão 4.1. Ainda é possível usar o console de operações para operar domínios de primeiro nível e o editor de políticas que é fornecido pelo System Automation for Multiplatforms até a versão 3.2.2 para manter as políticas.

Instalando o System Automation for Multiplatforms

É possível instalar o System Automation for Multiplatforms em seu ambiente, ou fazer upgrade de uma versão anterior do produto.

Sobre Esta Tarefa

Os seguintes tópicos explicam como instalar ou fazer upgrade do System Automation for Multiplatforms em ambientes AIX ou Linux.

Instalação inicial

Se desejar executar uma instalação inicial do System Automation for Multiplatforms, veja "Executando a instalação" na página 24.

Instalação existente

Se uma versão anterior do System Automation for Multiplatforms já estiver instalada, deve-se executar algumas etapas antes de poder instalar a nova versão do System Automation for Multiplatforms. Para obter informações adicionais sobre como migrar para uma nova versão do produto, veja "Migrando o Domínio de Automação do Sistema" na página 27.

Executando a instalação

Use um script de instalação para instalar o System Automation for Multiplatforms.

Sobre Esta Tarefa

O script de instalação executa as ações a seguir:

- Uma verificação de pré-requisito completa para verificar se todos os pré-requisitos estão disponíveis e no nível necessário. Se o sistema não passar na verificação, a instalação não será iniciada e você deverá fornecer os pré-requisitos ausentes antes de reiniciar a instalação. Consulte <u>"Verificando Pré-</u>requisitos " na página 3
- Instale o System Automation for Multiplatforms, incluindo o adaptador de automação de ponta a ponta.

Para evitar reiniciar a instalação, é possível iniciar a verificação de pré-requisitos separadamente antes de iniciar a instalação.

Se um domínio do mesmo nível IBM Reliable Scalable Cluster Technology (RSCT) existir, assegure que o nó no qual você está executando o script esteja offline no domínio. Caso contrário, a instalação será cancelada.

Instale o produto, incluindo o adaptador de automação:

- 1. Efetue login como root ou com autoridade equivalente.
- 2. Se você transferiu por download o arquivo .tar da Internet, extraia-o:

tar -xvf <arquivo_tar>

Se você recebeu o produto em um DVD, monte o DVD e altere para o diretório onde o DVD está montado.

- 3. Insira o seguinte comando:
 - Linux: cd SAM4100MPLinux
 - AIX:cd SAM4100MPAIX
- 4. Execute o script de instalação:

```
./installSAM
```

Geralmente, não é necessário especificar nenhuma das opções disponíveis para o comando installSAM. A instalação padrão instala os pacotes para todos os idiomas suportados. Se não desejar instalar todos os idiomas e desejar somente o idioma inglês, será possível especificar a opção

--nonls. Para obter uma descrição detalhada do comando **installSAM**, consulte *Tivoli System Automation for Multiplatforms Reference Guide* .

5. Leia as informações no contrato de licença e as informações sobre licença que são exibidas. É possível rolar para avançar linha por linha com a tecla Enter e página por página com a barra de espaço, o que é semelhante à opção "mais" no UNIX. Quando tiver rolado até a parte inferior do arquivo de informações sobre licença e desejar aceitar os termos do contrato de licença, digite 'y'. Qualquer outra entrada cancela a instalação.

A instalação também será cancelada se nenhum arquivo de licença for localizado.

6. Após a aceitação do contrato de licença, o programa de instalação verifica os pré-requisitos para verificar se eles estão disponíveis e no nível necessário.

Se o sistema não passar na verificação, a instalação não será iniciada e você deverá fornecer os pré-requisitos ausentes antes de reiniciar a instalação.

As informações sobre os resultados da verificação de pré-requisitos estão disponíveis no arquivo de log /tmp/installSAM.<#>.log.

Se o sistema tiver passado na verificação, o produto, incluindo o adaptador de automação, será instalado.

7. Verifique o seguinte arquivo de log para obter informações sobre a instalação:

/tmp/installSAM.<#>.log

O símbolo hash <#> é um número; o número mais alto identifica o arquivo de log mais recente.

As entradas no arquivo de log possuem os seguintes prefixos:

prereqSAM

Entradas que são gravadas durante a verificação de pré-requisitos.

installSAM

Entradas que são gravadas durante a instalação do produto.

8. Para localizar quais pacotes foram instalados, inspecione /tmp/installSAM.<#>.log, em que <#> é o número mais alto na lista de logs localizados.

Instalando a Licença do Produto

O System Automation for Multiplatforms requer a instalação de uma licença válida do produto em cada sistema no qual estiver sendo executado.

Sobre Esta Tarefa

A licença está contida no meio de instalação no subdiretório 'license'. A instalação da licença é executada durante o processo de instalação do produto. Se a licença não foi instalada com sucesso, execute o seguinte comando para instalar a licença:

```
samlicm -i license_file
```

Para exibir a licença, emita:

samlicm -s

Para obter uma descrição detalhada do comando, consulte *Tivoli System Automation for Multiplatforms Reference Guide* .

Idiomas e Códigos de Idioma Suportados

Se desejar usar o System Automation for Multiplatforms em um idioma diferente do inglês, descubra quais idiomas e códigos de idiomas são suportados.

Sobre Esta Tarefa

Linux

O <u>Tabela 16 na página 26</u> mostra as combinações de idiomas e códigos de idioma que são suportados para o System Automation for Multiplatforms em sistemas Linux para exibir mensagens traduzidas. Novas versões de sistemas operacionais Linux podem não suportar toda a codificação listada. A codificação UTF-8 é sempre suportada.

UTF-8 Idioma ISO-8859-1 EUC/GBK Euro GB18030/BIG5 de_DE.UTF-8 Alemão de DE, de_DE@euro de DE.ISO-8859-1 Espanhol es_ES.UTF-8 es_ES, es_ES@euro es_ES.ISO-8859-1 Francês fr_FR.UTF-8 fr_FR, fr_FR@euro fr_FR.ISO-8859-1 Italiano it_IT.UTF-8 it IT, it_IT@euro it_IT.ISO-8859-1 Japonês ja_JP.eucJP ja_JP.UTF-8 Coreano ko_KR.UTF-8 ko_KR.eucKR Português do pt_BR pt_BR.UTF-8 Brasil Chinês zh_CN.UTF-8 zh_CN.GBK, zh_CN.GB18030 simplificado zh_CN.GB2312 Chinês zh_TW.UTF-8 zh_TW.Big5, zh_TW tradicional

Tabela 16. Idiomas e códigos de idiomas suportados pelo System Automation for Multiplatforms em sistemas Linux.

AIX

A tabela a seguir mostra as combinações de idiomas e códigos de idiomas que são suportadas para o System Automation for Multiplatforms no AIX para exibir mensagens traduzidas.

Tabela 17. Idiomas e códigos de idioma suportados pelo Tivoli System Automation em sistemas AIX				
Idioma	UTF-8	ISO-8859-1	EUC/GBK	SJIS/GB18030/ BIG5
Alemão	DE_DE	de_DE		
Espanhol	ES_ES	es_ES		
Francês	FR_FR	fr_FR		
Italiano	IT_IT	it_IT		
Japonês	JA_JP		ja_JP	Ja_JP
Coreano	KO_KR		ko_KR	
Português do Brasil	PT_BR	pt_BR		
Chinês simplificado	ZH_CN		zh_CN	Zh_CN

Tabela 17. Idiomas e códigos de idioma suportados pelo Tivoli System Automation em sistemas AIX (continuação)

Idioma	UTF-8	ISO-8859-1	EUC/GBK	SJIS/GB18030/ BIG5
Chinês tradicional	ZH_TW		zh_TW	Zh_TW

Migrando o Domínio de Automação do Sistema

É possível migrar para o System Automation for Multiplatforms versão 4.1 se uma versão mais antiga já estiver instalada.

Sobre Esta Tarefa

Antes que seja possível migrar um ou mais nós para um nível mais novo, certifique-se de que esteja familiarizado com as características a seguir:

- O processo de migração inicia quando qualquer nó dentro do cluster ativo é atualizado para o nível de código superior.
- É sempre possível atualizar para um nível de código superior. A migração descendente não é possível.
- O processo de migração será concluído apenas quando o número da versão ativa for igual ao número mais alto da versão de código instalada. Até esse ponto, níveis de código diferentes podem coexistir.
- A partir da versão 4.1, tornar o adaptador de automação de ponta a ponta altamente disponível não requer mais uma política de automação. Para obter informações adicionais, consulte <u>"Migrando um</u> Adaptador de Automação de Ponta a Ponta Altamente Disponível" na página 30.

Realizando a Migração de um Domínio Inteiro

Durante a migração, o domínio não está disponível. Para minimizar o tempo de inatividade, você pode executar uma verificação de pré-requisitos antes de iniciar a migração real.

Sobre Esta Tarefa

Para obter informações adicionais, consulte "Verificando Pré-requisitos " na página 3.

Migrar um domínio inteiro:

- 1. Certifique-se de que todos os recursos estejam offline:
 - a. Verifique se o adaptador de automação de ponta a ponta está em execução:

samadapter status

Se estiver em execução, pare o Adaptador de Automação:

samadapter stop

b. Pare todos os grupos de recursos online, definindo seus atributos NominalState como offline:

chrg -o Offline <resource-group-name>

2. Pare o domínio se ele estiver online:

stoprpdomain <domain-name>

3. No AIX, insira o comando a seguir após o cluster ser interrompido e antes da instalação ser iniciada:

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

- 4. Execute o script ./installSAM a partir do diretório de instalação no DVD do produto ou a partir da entrega eletrônica extraída em todos os nós. Para obter informações adicionais sobre o script installSAM, veja "Executando a instalação" na página 24.
- 5. Inicie o domínio:

startrpdomain <domain-name>

- 6. Verifique os níveis de código com o comando lssrc –ls IBM.RecoveryRM (consulte a amostra em "Verificando o Número da Versão Instalada e o Número da Versão Ativa" na página 29). Todos os nós têm o novo nível de código instalado, mas o nível de código ativo é o anterior.
- 7. Para ativar a nova versão, continue com "Concluindo a Migração" na página 29.

Migrando Nó por Nó

A migração nó por nó é suportada somente quando você migrar a partir do System Automation for Multiplatforms V2.3 ou superior. Migrar os nós de um domínio um a um tem a vantagem de que o System Automation for Multiplatforms permanece disponível durante a migração.

Sobre Esta Tarefa

Para obter informações adicionais sobre como minimizar tempo de inatividade, veja <u>"Verificando Pré-</u>requisitos " na página 3.

Execute uma migração nó por nó:

1. Exclua o nó da automação para garantir que os recursos que devem ser mantidos disponíveis sejam movidos para outro nó no domínio do mesmo nível:

samctrl -u a <node>

Nota: O comando pode ser executado por um período de tempo considerável até que todas as operações de movimentação sejam concluídas.

2. Pare o nó a partir de outro nó no domínio e verifique se ele foi parado:

stoprpnode <node>; lsrpnode

- 3. Para atualizar o nó, execute o script ./installSAM a partir do diretório de instalação no CD do produto ou a partir da entrega eletrônica extraída. Para obter informações adicionais sobre o script installSAM, veja "Executando a instalação" na página 24.
- 4. Inicie o nó:

startrpnode <node>

5. Inclua o nó atualizado na automação novamente:

samctrl -u d <node>

- 6. O nó atualizado pode agora unir-se ao domínio existente. Use o comando lssrc -ls IBM. RecoveryRM (consulte a amostra em <u>"Verificando o Número da Versão Instalada e o Número</u> <u>da Versão Ativa" na página 29</u>) para exibir a versão instalada e a versão ativa do produto. Os recursos do novo código não são ativados até que o número da versão ativa do System Automation for Multiplatforms seja igual ao número mais alto da versão do System Automation for Multiplatforms instalada no cluster. Não é possível usar esses novos recursos de código até que todos os nós sejam atualizados.
- 7. Repita as etapas 1-6 para outros nós do cluster.
- 8. Para ativar a nova versão, continue com "Concluindo a Migração" na página 29.

Verificando o Número da Versão Instalada e o Número da Versão Ativa

Após o upgrade, os novos recursos ainda não estarão ativados. Os níveis de código anterior e novo podem coexistir até que a migração esteja concluída.

Sobre Esta Tarefa

O comando **lssrc** -ls **IBM.RecoveryRM** mostra o número da versão ativa AVN e o número da versão instalada IVN do produto. Quando IVN e AVN forem iguais, a migração estará concluída. Saída:

```
: IBM.RecoveryRM
Subsystem
PTD
                    : 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
                           : d4b7e876c (4b7e876c)
   Our CVN
   Total Node Count
   Joined Member Count : 2
   Startup Quorum Count : 2
Startup Quorum Count : 1
Operational Curr
   Operational Quorum State : HAS_QUORUM
   In Config Quorum : TRUE
In Config State : TRUE
   Replace Config State : FALSE
```

Figura 9. Verificando os números das versões ativa e instalada

Para ativar a nova versão, continue com "Concluindo a Migração" na página 29.

Concluindo a Migração

Verifique se a migração foi executada com sucesso.

Sobre Esta Tarefa

Verifique e conclua a migração:

- 1. Certifique-se de que o domínio tenha sido iniciado e que todos os nós do domínio estejam online.
- 2. Emita o comando **lsrpdomain** para exibir a versão do RSCT que está ativa no domínio do mesmo nível, e o status da versão combinada:

```
NameOpStateRSCTActiveVersionMixedVersionsTSPortGSPortSA_DomainOnline2.5.5.1Yes1234712348
```

3. Emita o comando **1srpnode** para exibir qual versão do RSCT está instalada nos nós. Lembre-se de que todos os nós devem estar online:

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

4. Se o domínio de mesmo nível RSCT estiver em execução no modo de versão combinada (MixedVersions = Yes) e todos os nós forem atualizados para a nova liberação, atualize a versão ativa de RSCT executando a ação RSCT CompleteMigration em um dos nós. Antes de poder executar a ação, revise os procedimentos de preparação de migração de RSCT no IBM RSCT Administration Guide. Para atualizar o RSCTActiveVersion, certifique-se de que todos os nós estão online. Insira o comando a seguir em um dos nós:

runact -c IBM.PeerDomain CompleteMigration Options=0

Para verificar se a versão de RSCT ativa está atualizada, insira o comando lsrpdomain novamente:

NameOpStateRSCTActiveVersionMixedVersionsTSPortGSPortSA_DomainOnline2.5.5.1No1234712348

- 5. Execute o comando **samctrl** -**m** para ativar os novos recursos e concluir a migração. Para obter informações adicionais sobre o comando, consulte *System Automation for Multiplatforms Reference Guide*.
- 6. Se a migração tiver sido feita a partir do System Automation for Multiplatforms release 3.1, você deve ajustar o valor do atributo OperationalFlags, inserindo o seguinte comando em um dos nós:

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

Para exibir o valor real desse atributo, insira:

lsrsrc -c IBM.CHARMControl

Os recursos do novo código estarão ativos se o valor de ActiveVersion e InstalledVersion do System Automation for Multiplatforms for igual para todos os nós.

Migrando um Adaptador de Automação de Ponta a Ponta Altamente Disponível

Descubra como fazer upgrade de um adaptador de automação de ponta a ponta altamente disponível para a versão 4.1.

Iniciando com o System Automation for Multiplatforms versão 4.1, uma política de automação não é mais necessária para tornar o adaptador de automação de ponta a ponta altamente disponível. No Windows, esta implementação já estava disponível antes da versão 4.1 e agora está disponível para todos os outros sistemas operacionais.

System Automation for Multiplatforms versão 3.2 ou inferior:

O <u>Figura 10 na página 31</u> mostra o ambiente no qual o adaptador de automação de ponta a ponta operava em clusters do UNIX e Linux.



Figura 10. Ambiente do adaptador de automação de ponta a ponta em clusters do UNIX e Linux antes da versão 4.1

System Automation for Multiplatforms versão 4.1:

O Figura 11 na página 31 mostra o ambiente no qual o adaptador opera a partir da versão 4.1.



Figura 11. Ambiente do adaptador de automação de ponta a ponta disponível com versão 4.1

A partir da versão 4.1, o adaptador de automação está conectado ao nó principal do System Automation. A infraestrutura de cluster certifica que o System Automation for Multiplatforms principal e o adaptador estejam sempre disponíveis. Nenhuma política de automação adicional é necessária para tornar o adaptador altamente disponível. O endereço IP virtual, que é um recurso crítico do System Automation não é mais necessário neste cenário.

Alterar a implementação de alta disponibilidade para o adaptador de automação de ponta a ponta tem as seguintes implicações, se você fizer upgrade do nó do cluster, conforme descrito em <u>"Migrando Nó por</u> Nó" na página 28.

A implementação antiga está ativa durante o processo de migração

Se a migração ainda não estiver concluída, existem versões diferentes do código ativo em diferentes nós no cluster. Durante esse tempo, a antiga implementação de alta disponibilidade ainda está ativa. A nova implementação se torna ativa assim que a versão ativa é configurada para a versão 4.1.0.0 (ou superior). Para obter informações adicionais, veja <u>"Concluindo a Migração" na página 29</u>

A configuração de política de automação ainda é possível durante o processo de migração

Uma política de automação não é mais necessária para tornar o adaptador altamente disponível. No entanto, a implementação antiga ainda é suportada se você não tiver concluído uma migração nó por nó. As tarefas de configuração de política de automação do adaptador ainda estão disponíveis e são suportadas durante o processo de migração. A documentação dessas tarefas de configuração foi removida. Se ainda precisar inspecionar a descrição dessas tarefas, consulte a documentação para a versão anterior do produto.

Nota: Se desejar modificar a configuração de alta disponibilidade durante uma migração nó por nó, certifique-se de executar o utilitário de configuração em um nó do cluster que esteja online. A razão é que o número da versão ativa não pode ser determinado em um nó offline. A implementação antiga da configuração de alta disponibilidade do adaptador não está disponível em um cluster offline ou em um nó offline. Mesmo se o número da versão ativa for inferior a 4.1.0.0.

Antes de concluir a migração para a versão 4.1, verifique todas as suas políticas de automação para um domínio inteiro e migração nó por nó. As políticas de automação podem conter recursos que estão relacionados à alta disponibilidade do adaptador de automação de ponta a ponta. Remova todos esses recursos:

- Verifique qual prefixo do recurso é usado quando você configura a automação do adaptador. O prefixo padrão é samadapter-.
- Remova todos os relacionamentos, recursos e grupos de recursos que têm um nome que comece com o prefixo.
- Se você estiver usando o formato xml para definir suas políticas, remova todos os relacionamentos, recursos e grupos de recursos que têm um nome que comece com o prefixo dos arquivos xml.

Ações necessárias após ter concluído a migração

Se o adaptador estiver em execução enquanto a migração do cluster é iniciada, o adaptador será interrompido e não iniciado novamente após a migração ser concluída.

Execute as etapas de migração manual a seguir antes de poder iniciar o adaptador:

- 1. Execute o utilitário de configuração cfgsamadapter para alterar o nome do host do adaptador ou endereço IP. Selecione o nome do host local de cada nó do cluster como padrão ou especifique um nome do host distinto ou endereço IP.
- Se selecionar o padrão para o host do adaptador, faça a réplica da configuração para os outros nós no cluster. Caso contrário, configure explicitamente um nome do host ou endereço IP em cada nó do cluster.

Agora, é possível iniciar o adaptador. É possível usar o diálogo de configuração conforme descrito em Guia do Administrador e do Usuário do System Automation for Multiplatforms ou usar o comando samadapter start.

Continue usando a antiga implementação de alta disponibilidade do adaptador

Em alguns casos raros, pode não ser possível usar a nova implementação de alta disponibilidade do adaptador. Por exemplo, se desejar impor que o adaptador seja executado apenas em um

subconjunto dos nós disponíveis no cluster. Este cenário é possível com a política de automação anterior. Mas, com a nova abordagem, o adaptador pode ser executado em qualquer nó do cluster.

Nesse caso, você tem a oportunidade de impor que a política de automação é ainda usada para tornar o adaptador altamente disponível se você estiver usando a versão 4.1. Mesmo se você já estiver executando um cluster usando a abordagem nova ou antiga, é possível alternar para a outra respectiva abordagem. Os cenários a seguir são suportados:

1. Continue a usar a implementação antiga ao migrar para a versão 4.1.

Se você migrar seu cluster de uma versão anterior à 4.1 para a versão 4.1, a nova implementação de alta disponibilidade do adaptador está ativada. Se desejar usar a implementação antiga em vez disso, execute as etapas a seguir depois que você atualizou o código do produto para a versão 4.1 em todos os nós do cluster:

- a. Edite o arquivo de propriedades de configuração /etc/opt/IBM/tsamp/sam/cfg/ sam.adapter.properties e altere o valor do parâmetro use-adapter-ha-policy de false para true em cada nó no cluster.
- b. Emita o comando **samctrl** -m.

2. Alternando para a nova implementação do adaptador de alta disponibilidade após concluir a migração.

Se você migrou seu cluster de uma versão anterior à 4.1 para a versão 4.1 e seguiu o procedimento que está descrito para o cenário 1 acima, você ainda está usando a antiga implementação de alta disponibilidade do adaptador. Se você, então, deseja alternar para a nova implementação de alta disponibilidade do adaptador, execute as etapas a seguir:

- a. Pare o domínio, inserindo o comando **stoprpdomain**.
- b. Edite o arquivo de propriedades de configuração /etc/opt/IBM/tsamp/sam/cfg/ sam.adapter.properties e altere o valor do parâmetro use-adapter-ha-policy de true para false em cada nó no cluster.
- c. Inicie o domínio, inserindo o comando **startrpdomain**.

3. Alternando de volta para a antiga implementação de alta disponibilidade do adaptador após concluir a migração.

Se você concluir a migração de seu cluster de uma versão anterior à 4.1 para a versão 4.1 sem seguir o procedimento que está descrito para o cenário 1 acima, você está usando a nova implementação de alta disponibilidade do adaptador. O mesmo é verdadeiro se você seguiu o procedimento descrito para o cenário 2. Se você, então, deseja alternar de volta para a antiga implementação de alta disponibilidade do adaptador, execute as etapas a seguir:

- a. Pare o adaptador inserindo o comando **samadapter stop**.
- b. Edite o arquivo de propriedades de configuração /etc/opt/IBM/tsamp/sam/cfg/ sam.adapter.properties e altere o valor do parâmetro use-adapter-ha-policy de false para true em cada nó no cluster.
- c. Inicie o utilitário de configuração inserindo o comando cfgsamadapter e conclua as tarefas a seguir:
 - i) Na janela principal do diálogo de configuração, clique em Configurar.
 - ii) Clique em Salvar para salvar as mudanças na configuração. Em seguida, a entrada do publicador EEZ que é necessária para a implementação antiga é incluída no arquivo de propriedades de configuração /etc/Tivoli/tec/samPublisher.conf em qualquer caso. Isso é necessário porque a entrada do publicador pode ser removida pelo adaptador quando ele usa a nova implementação de alta disponibilidade do adaptador.
 - iii) Na janela principal do diálogo de configuração, clique em **Replicar** e propague as mudanças de configuração para os outros nós no cluster.
 - iv) Na janela principal do diálogo de configuração, clique em **Definir** para ativar a política de alta disponibilidade do adaptador novamente. Ela é removida pelo System Automation for Multiplatforms durante a execução do comando **samctrl** -m.

d. Inicie o adaptador inserindo o comando **samadapter start**.

4. Usando a antiga implementação de alta disponibilidade do adaptador em um cluster novo versão **4.1.0.0**.

Se você executar uma instalação inicial da versão 4.1.0.0, você está usando a nova implementação de alta disponibilidade do adaptador. Se desejar usar a antiga implementação de alta disponibilidade do adaptador em vez disso, execute as etapas a seguir:

- a. Pare o adaptador inserindo o comando **samadapter stop**.
- b. Edite o arquivo de propriedades de configuração /etc/opt/IBM/tsamp/sam/cfg/ sam.adapter.properties e altere o valor do parâmetro use-adapter-ha-policy de false para true em cada nó no cluster.
- c. Inicie o utilitário de configuração inserindo o comando **cfgsamadapter** e conclua as tarefas a seguir:
 - i) Na janela principal do diálogo de configuração, clique em Configurar.
 - ii) Na guia Automação, configure a política de alta disponibilidade do adaptador.
 - iii) Clique em **Salvar** para salvar as mudanças na configuração.
 - iv) Na janela principal do diálogo de configuração, clique em **Replicar** e propague as mudanças de configuração para os outros nós no cluster.
 - v) Na janela principal do diálogo de configuração, clique em **Definir** para ativar a política de alta disponibilidade do adaptador.

d. Inicie o adaptador inserindo o comando **samadapter start**.

Cenários 3 e 4 referem-se à tarefa **Definir** e a guia **Automação**. A documentação correspondente está removida na versão 4.1. Se ainda precisar inspecionar a descrição dessas tarefas, consulte a documentação para a versão anterior do produto.

Pós-instalação

Para poder obter os dados de depuração, deve-se configurar o criador de logs do sistema.

Sobre Esta Tarefa

Após instalar o System Automation for Multiplatforms no AIX, você deve concluir a seguinte tarefa:

Configurar o criador de logs do sistema no AIX

O criador de logs do sistema não está configurado por padrão. As mensagens são gravadas para o log de erros.

Para poder obter os dados de depuração, você deve configurar o criador de logs do sistema no arquivo /etc/syslog.conf. Quando fizer as mudanças necessárias, você deve reciclar o syslogd com o comando **refresh** -**s syslogd**. O local do arquivo de log é definido em /etc/ syslog.conf.

Nenhuma ação adicional é necessária no caso do Linux.

Tornando Grupos de Volumes Compartilhados com Capacidade de Concorrência Aprimorada no AIX

Se seus grupos de volumes compartilhados não tiverem capacidade simultânea aprimorada, quando um nó travar, os discos serão bloqueados e o nó remoto não será capaz de acessar o disco. Para evitar essa situação, conceda ao grupo de volumes compartilhados a capacidade simultânea aprimorada.

Sobre Esta Tarefa

Nota:

1. Certifique-se de que o pacote bos.clvm.enh esteja instalado em seu sistema.

2. O System Automation for Multiplatforms suporta grupos de volumes com capacidade de concorrência no modo não concorrente ao usar recursos de classes IBM. AgFileSystem ou IBM. VolumeGroup dentro da política. O System Automation for Multiplatforms não suporta o modo simultâneo de grupos de volumes simultâneos aprimorados e o sistema de arquivos contido como recursos dentro da política. O suporte para grupos de volumes simultâneos aprimorados pode ser fornecido explicitamente por um provedor de política usando recursos IBM. Application para gerenciar o sistema de arquivos na parte superior dos grupos de volumes simultâneos aprimorados.

Antes de tornar o grupo de volumes com capacidade de concorrência aprimorada, use o comando lsvg para visualizar informações sobre o grupo de volumes compartilhados:

# lsvg vgERSTZ0			
VOLUMĚ GROUP:	vgERSTZ0	VG IDENTIFIER:	
00c31bfe00004c00000	00118c2f1ead2		
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

Para tornar um grupo de volumes apto ao aprimoramento simultâneo usando SMIT:

1. Insira o seguinte comando:

smitty vg

Texto semelhante ao seguinte é exibido:

Set Characteristics of a Volume Group Change a Volume Group		
* VOLUME GROUP name * Activate volume group AUTOMATICALLY	vgERSTZ0 no	+
at system restart? * A QUORUM of disks required to keep the volume group op-line 2	yes	+
Convert this VG to Concurrent Capable?	enhanced concurrent	

2. Pressione ENTER.

Para conceder ao grupo de volumes capacidade simultânea aprimorada a partir da linha de comandos, insira:

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

Após conceder ao grupo de volumes capacidade simultânea aprimorada, o comando lsvg retorna informações semelhantes à saída de exemplo a seguir:

# lsvg vgERSTZ0			
VOLUMĚ GŘOUP:	vgERSTZ0	VG IDENTIFIER:	
00c31bfe00004c000000	00118c2f1ead2		
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:	Θ
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	<pre>size (Dynamic):</pre>	256 kilobyte(s)	AUTO SYNC:	no
НОТ	SPARE:	no	BB POLICY:	relocatable

Procedimento de Retrocesso

Siga as etapas descritas para retroceder a instalação para a liberação anterior.

Sobre Esta Tarefa

Para retroceder o System Automation for Multiplatforms para a liberação anterior, execute as etapas a seguir:

1. Salve a política de automação:

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

2. Altere todos os grupos de recursos para offline. Como alternativa, se não desejar afetar os recursos, pare o domínio:

stoprpdomain -f domain_name

- Remova o domínio se também for necessário retroceder o nível de RSCT. Caso contrário, coloque o domínio offline.
- 4. O System Automation for Multiplatforms pode ser retrocedido executando o comando ./installSAM --forceAll. O comando instala o System Automation for Multiplatforms e o distribuível RSCT onde installSAM está localizado, independentemente da versão que já está instalada.
- 5. Se você tiver removido o domínio, crie o domínio novamente. Caso contrário, inicie o domínio inserindo startrpdomain -w domain_name.
- 6. Se o domínio tiver sido criado novamente, será possível reaplicar a política salva inserindo sampolicy -a file.xml.

Desinstalando

É possível remover o System Automation for Multiplatforms de seus ambientes AIX e Linux com um procedimento documentado.

Sobre Esta Tarefa

Considere as sugestões a seguir antes de iniciar o procedimento de desinstalação:

- Utilize o script **uninstallSAM** fornecido para seu sistema operacional para desinstalar o System Automation for Multiplatforms. Por exemplo, execute **./uninstallSAM** a partir do diretório de instalação, para assegurar uma desinstalação correta do produto.
- Antes de desinstalar, sempre salve sua configuração com o comando sampolicy –s. Para obter informações adicionais sobre como salvar uma configuração do System Automation for Multiplatforms, consulte *Tivoli System Automation for Multiplatforms Administrator's and User's Guide*.

A descrição do comando **sampolicy** no System Automation for Multiplatforms Reference Guide.

• O comando **uninstallSAM** remove todas as informações de configuração definidas para o domínio. Por essa razão, você nunca deve usar **uninstallSAM** se pretende fazer upgrade para uma nova versão.

Para desinstalar o System Automation for Multiplatforms, execute as etapas a seguir:

- 1. Assegure-se de que o domínio esteja offline:
 - Para verificar se um domínio está online, execute o seguinte comando:

lsrpdomain

• Para parar o domínio, execute o seguinte comando:

stoprpdomain <domain>

2. Desinstale o produto com o script uninstallSAM, disponível no diretório /opt/IBM/tsamp/sam/ uninst/:

./uninstallSAM

Geralmente, não é necessário especificar nenhuma das opções disponíveis para o comando uninstallSAM. Para obter uma descrição detalhada do comando, consulte System Automation for Multiplatforms Reference Guide.

O Redhat Package Manager assegura que RSCT e SRC não sejam desinstalados com o System Automation for Multiplatforms, caso CSM ou GPFS esteja instalado no mesmo Linux do sistema. CFM ou GPFS também usa os pacotes de RSCT e do System Resource Controller (SRC). Mensagens do Redhat Package Manager indicam essa condição.

3. Verifique o arquivo de log a seguir para obter informações sobre a desinstalação:

/tmp/uninstallSAM.<#>.log

O símbolo hash <#> indica um número. O número mais alto identifica o arquivo de log mais recente.

4. Para verificar quais pacotes foram desinstalados, inspecione /tmp/uninstallSAM.<#>.log, em que <#> é o número mais alto dos arquivos de log que você pode localizar.

Nota: O comando uninstallSAM exclui todas as configurações que estão armazenadas em /etc/opt/IBM/tsamp/sam também.

Instalando em novos sistemas operacionais

O suporte de novos sistemas operacionais pode ser apresentado com um fix pack 4.1.0.<f>, em que <f> é o respectivo número de fix pack

Uma instalação do System Automation for Multiplatforms 4.1.0.0, conforme descrito em <u>"Instalando o</u> System Automation for Multiplatforms" na página 24, é possível somente no conjunto de plataformas e versões de sistemas operacionais que são inicialmente suportadas para este nível de liberação versão 4.1. No entanto, suporte para plataformas adicionais ou versões do sistema operacional podem ser incluídos com os fix packs em um momento posterior. Isso é chamado de "novo suporte de plataforma" a seguir. Se desejar instalar um fix pack em um sistema operacional já suportados, faça upgrade de sua instalação.

Para verificar qual novo suporte de plataforma é apresentado com o fix pack, veja <u>"Plataformas</u> Suportadas" na página 5.

Se suporte a novo sistema operacional for introduzido com um fix pack, este fix pack deve ser instalado como uma instalação inicial em vez de uma instalação de upgrade. Portanto, é necessário copiar o arquivo de licença 4.1 para o diretório SAM410<f>MP<platform>/license antes de iniciar a instalação do fix pack. Execute as etapas a seguir:

1. Obtenha um arquivo de licença do System Automation for Multiplatforms que esteja contido em uma das entregas da liberação 4.1:

DVD do Produto

Use um dos DVDs listados em <u>"DVD do Produto" na página 1</u> para obter a licença. Localize o arquivo de licença chamado sam41.lic no diretório SAM4100MP<platform>/license.

Distribuição Eletrônica

Use um dos archives listados em <u>"Distribuição Eletrônica" na página 1</u> para obter a licença. Extraia o archive. Na árvore de diretórios expandida, localize o arquivo de licença chamado sam41.lic no diretório SAM4100MP<platform>/license.

 Extraia o archive do fix pack 4.1.0.<f> que contém o suporte de novos sistemas operacionais, conforme descrito em <u>"Instruções de uso para archives específicos da plataforma" na página 39</u>. Na árvore de diretórios expandida, o diretório SAM410<f>MP<platform>/license está vazio.

- 3. Copie o arquivo de licença obtido na etapa 1 para o diretório SAM410<f>MP<platform>/license da árvore de diretórios expandida do fix pack.
- 4. Inicie a instalação do System Automation for Multiplatforms, conforme descrito em <u>"Executando a instalação" na página 24</u>. O programa de instalação executa uma instalação inicial do produto no novo sistema operacional.

Migração do SLES 12 para o SLES 15 ou do RHEL 6 para o RHEL 7/8

É possível migrar do SLES 12 para SLES 15, do RHEL 6 para o RHEL 7/8 ou do RHEL 7 para o RHEL 8 com os clusters existentes do System Automation for Multiplatforms.

Execute as seguintes etapas para migrar seu cluster:

- 1. Salve a política usando o comando sampolicy -s. Pare os recursos e remova o domínio.
- 2. Instale a plataforma de S.O. de destino SLES 15, RHEL 7 ou RHEL 8 em todos os nós do cluster.
- 3. Instale o pacote System Automation for Multiplatforms que suporta o SLES 15 e o RHEL 7/8: 4.1.0-TIV-SAMP-Linux64-FP000x. Para obter mais informações, consulte <u>Instalando em novos sistemas</u> operacionais.
- 4. Crie o domínio novamente e ative a política: sampolicy -a

Nota:

- 1. O recurso de migração Nó por Nó é suportado apenas para fazer upgrade do nível do produto System Automation for Multiplatforms, mas não para fazer upgrade da versão do sistema operacional.
- 2. Não há suporte para ter um domínio com níveis mistos de sistema operacional, por exemplo SLES 12/15 ou RHEL 6/7/8.
- 3. Os ambientes de linguagem de 32 bits e de 64 bits não podem ser usados no mesmo domínio.

Instalando fix packs de serviço

Instalando serviço significa aplicar fix packs de serviço corretivo à liberação 4.1 do System Automation for Multiplatforms ou fazer upgrade do nível de liberação do software a partir da liberação 4.1. Esses fix packs de serviço são chamados de fix packs do produto.

Sobre Esta Tarefa

Os fix packs do produto estão disponíveis para o System Automation for Multiplatforms nos seguintes formatos:

Linux

Archives no formato .tar compactado.

AIX

Archives no formato .tar compactado.

Obtendo Fix Packs

Sobre Esta Tarefa

Para obter informações adicionais, consulte a página do produto System Automation for Multiplatforms.

Archives para fix packs do produto podem ser transferidos por download a partir do <u>System Automation</u> for <u>Multiplatforms Support Portal</u>. Faça download do archive em um diretório temporário. Geralmente, há um archive disponível para cada sistema operacional. Para obter informações adicionais sobre as convenções de nomenclatura que se aplicam aos archives do fix pack do produto, consulte <u>"Convenções</u> de Nomenclatura do Archive" na página 39.

Convenções de Nomenclatura do Archive

Saiba mais sobre a sintaxe dos nomes de archive.

Sobre Esta Tarefa

Os archives para fix packs do produto para o System Automation for Multiplatforms possuem a seguinte sintaxe:

4.1.0-TIV-SAMP-<platform>-FP<fix_pack_number>.<archive_type> contém o service fix pack para o System Automation for Multiplatforms.

Explicação:

<platform>

Sistema operacional no qual o System Automation for Multiplatforms está instalado.

<fix_pack_number> Número do fix pack.

<archive_type>

tar.gzoutar.Z.

Exemplo:

O archive tar.Z que é usado para instalar o fix pack 1 para System Automation for Multiplatforms 4.1.0 em sistemas operacionais AIX:

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

Instruções de uso para archives específicos da plataforma

Saiba mais sobre como fazer download e instalar o fix pack.

Sobre Esta Tarefa

As tabelas listam os archives, que você pode fazer download para aplicar serviço para os sistemas operacionais Linux e AIX. Para cada archive, siga as instruções específicas listadas na coluna **Descrição**.

Linux

Tabela 18. Archive para sistemas operacionais Linux		
Nome do Archive	Descrição	
4.1.0-TIV-SAMP-Linux- FP <fix_pack_number>.tar.gz</fix_pack_number>	Use o comando tar -zxf para descompactar e extrair o archive. Depois de extrair o archive, o script de instalação installSAM é armazenado em: SAM41 <maintenance_level>MPLinux/ installSAM</maintenance_level>	

A partir do fix pack 4.1.0.1, o suporte para mais versões de sistema operacional foi introduzido conforme descrito em <u>"Plataformas Suportadas" na página 5</u>. Essas versões de sistemas operacionais não suportam mais um modo de compatibilidade de 32 bits. A tabela a seguir descreve o archive do System Automation for Multiplatforms que contém a entrega de serviço de 64 bits correspondente. Para obter informações adicionais, consulte <u>"Instalando em novos sistemas operacionais" na página 37</u>.

Tabela 19. Archive para sistemas operacionais Linux de 64 bits

Nome do Archive	Descrição
4.1.0-TIV-SAMP-Linux64- FP <fix_pack_number>.tar.gz</fix_pack_number>	Use o comando tar -zxf para descompactar e extrair o archive. Depois de extrair o archive, o script de instalação installSAM é armazenado em: SAM41 <maintenance_level>MPLinux64/ installSAM</maintenance_level>

AIX

Tabela 20. Archive para sistemas operacionais AIX		
Nome do Archive	Descrição	
4.1.0-TIV-SAMP-AIX- FP <fix_pack_number>.tar.Z</fix_pack_number>	Use o comando uncompress para descompactar o archive, em seguida, use o comando tar -xf para extrair o archive. É possível localizar o script de instalação installSAM depois de extrair o archive: SAM41 <maintenance_level>MPAIX/installSAM</maintenance_level>	

Instalando serviço para o System Automation for Multiplatforms

Instalar um serviço significa fazer upgrade do System Automation for Multiplatforms do release 4.1. Portanto, a liberação 4.1 deve ser instalada antes de qualquer serviço poder ser aplicado.

Sobre Esta Tarefa

Antes de iniciar:

- Os fix packs do produto são sempre acumulativos.
- Você deve ter autoridade de administrador para instalar um fix pack do produto.
- Ao transferir por download os archives do site de suporte do System Automation for Multiplatforms (consulte <u>"Obtendo Fix Packs" na página 38</u>), descompacte o archive do fix pack do produto em um diretório temporário. Para obter informações sobre como descompactar o archive para seu sistema operacional, veja "Instruções de uso para archives específicos da plataforma" na página 39.
- Faça backup da configuração do sistema antes de instalar o fix pack do serviço. Para obter informações adicionais, consulte *Tivoli System Automation for Multiplatforms Administrator's and User's Guide*.
- Para minimizar o tempo de inatividade, você pode executar uma verificação de pré-requisitos antes de iniciar a instalação. Para obter informações adicionais, consulte <u>"Verificando Pré-requisitos " na página</u> <u>3</u>.

Execute as seguintes etapas em cada nó do domínio do mesmo nível:

- 1. Verifique se quaisquer recursos estão online no nó para o qual deseja executar serviço:
 - Se houver recursos online e eles precisarem ser mantidos disponíveis, exclua o nó da automação:

samctrl -u a <nó>

O System Automation for Multiplatforms para os recursos no nó e, se possível, reinicie-os em um nó diferente no domínio do mesmo nível.

- Se os recursos não precisarem ser mantidos disponíveis durante o serviço, coloque os grupos de recursos offline.
- 2. Pare o nó a partir de outro nó no domínio e verifique se ele foi parado:

stoprpnode <nó>; lsrpnode

- 3. Após receber os archives, extraia-os. Eles criam uma estrutura de diretório com o diretório-raiz SAM41mf MP, em que mf significa nível de modificação e nível de correção.
- 4. Instale o fix pack do serviço com o script installSAM. Para obter informações detalhadas sobre o script, consulte "Executando a instalação" na página 24.
- 5. Inicie o nó:

startrpnode <nó>

6. Se você excluiu o nó na etapa 2, inclua-o na automação:

samctrl -u d <nó>

- 7. Se precisar que os grupos de recursos estejam online, mantenha-os online. Caso contrário, atrase essa etapa até que o último nó do domínio do mesmo nível receba serviço.
- 8. Após todos os nós serem atendidos, execute as etapas descritas em <u>"Concluindo a Migração" na</u> página 29. As mudanças entram em vigor no domínio inteiro e a versão correta é mostrada.

Desinstalando o Serviço

Para desinstalar um fix pack, é necessário desinstalar o produto completo.

Sobre Esta Tarefa

Para desinstalar o System Automation for Multiplatforms, siga as instruções em <u>"Desinstalando" na</u> página 36.

Depois que a desinstalação estiver concluída, é preciso reinstalar o System Automation for Multiplatforms e o nível de serviço necessário (nível do fix pack).

Instalando o recurso extended disaster recovery (xDR)

Atualmente, as empresas e os negócios dependem de soluções de recuperação após falhas para recuperar dados críticos. Para solucionar esse problema, o System Automation for Multiplatforms suporta o GDPS/PPRC Multiplatform Resiliency on System z (xDR).

Sobre Esta Tarefa

Geographically Dispersed Parallel Sysplex (GDPS) é uma solução de disponibilidade de aplicativos e de recuperação de desastre que é altamente customizada para funcionar com seu ambiente z/OS. Isso fornece recuperação de desastres e de falha a partir de um único ponto de controle e assegura a consistência dos dados. Para obter informações adicionais sobre o GDPS, consulte a publicação IBM Redbooks*GDPS Family - An Introduction to Concepts and Capabilities,* que pode ser transferida por download em IBM Redbooks.

O System Automation for Multiplatforms estende GDPS/PPRC para sistemas Linux que estão em execução no System z. Ele fornece uma solução de recuperação de desastre coordenada para sistemas que estão em execução no

- zSeries, incluindo o z/OS
- Linux on System z sob o z/VM
- · Linux on System z em execução nativa na LPAR

Pacote xDR

O código do recurso xDR está incluído como parte do produto System Automation for Multiplatforms. Não será possível usar a função correspondente, a menos que tenha instalado uma licença separada para ativar o código.

Sobre Esta Tarefa

Você poderá obter a licença quando pedir o recurso xDR. O nome do arquivo de licença é sam41XDR.lic:

DVD

Instale o recurso xDR a partir do DVDSystem Automation for Multiplatforms v4.1 -xDR para Linux on System z. O arquivo de licença está disponível no diretório SAM4100FeatXDR/license.

Distribuição Eletrônica

Se você obtiver o recurso xDR por meio de distribuição eletrônica, localizará o arquivo de licença no arquivo de distribuição eletrônica CIVG7ML.txt. Esse arquivo é idêntico ao próprio arquivo de licença. Renomeie ou copie o arquivo de distribuição eletrônica para sam41XDR.lic.

Pré-requisitos de xDR

Para poder instalar a licença do recurso xDR, você deve instalar o produto base System Automation for Multiplatforms.

Sobre Esta Tarefa

xDR é suportado somente no Linux on System z.

As seguintes distribuições Linux são suportadas para xDR:

- xDR para Linux no System z em execução no z/VM[®] requer um dos seguintes sistemas operacionais:
 - SUSE SLES 12 (64 bits)
 - SUSE SLES 15 (64 bits)
 - Red Hat RHEL 6 (64 bits)
 - Red Hat RHEL 7 (64 bits)
 - Red Hat RHEL 8 (64 bits)
- O xDR para Linux on System z executando nativo em LPAR usando discos ECKD [™] requer um dos seguintes sistemas operacionais:
 - SUSE SLES 12
 - SUSE SLES 15

Nota:

- Se deseja usar a função de xDR, versões específicas do z/VM, Linux on System z, GDPS e System Automation for Multiplatforms devem ser instaladas. Para obter informações detalhadas sobre a função disponível e as versões requeridas, consulte os manuais do GDPS. O System Automation for Multiplatforms suporta apenas o xDR para Linux on System z.
- 2. As convenções de nomenclatura xDR requerem que os nomes dos clusters e os nós não excedam 32 caracteres. Os nomes de clusters e de nós não podem conter pontos (.) ou traços (-) e não devem ser idênticos. Para o xDR, os nomes de cluster não fazem distinção de maiúsculas e minúsculas. Para usar o xDR, o System Automation for Multiplatforms deve ser customizado conforme descrito nos manuais do GDPS.
- 3. Inglês é o único idioma suportado por xDR e GDPS.

Instalando a licença do recurso xDR

Use o comando **samlicm** para instalar a licença.

Sobre Esta Tarefa

O arquivo de licença deve estar acessível a partir do sistema em que o System Automation for Multiplatforms está instalado. Copie o arquivo sam41XDR.lic para um local em que ele esteja acessível quando você iniciar o **samlicm**.

Instale a licença:

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

Verifique se a licença do recurso foi instalada com sucesso:

samlicm -s

O nome do recurso xDR aparece como valor do campo Anotação do produto na saída do comando. Por exemplo:

```
...
Product ID: 101
Anotação do Produto: SA para MP xDR para Linux on System z
...
```

Para obter informações adicionais sobre o comando **samlicm**, veja System Automation for Multiplatforms *Reference Guide*.

Fazendo Upgrade do Recurso xDR de uma Versão Inferior à 4.1

A partir da versão 4.1, a licença do recurso xDR é instalada em um diretório de destino diferente.

Sobre Esta Tarefa

Se você atualizar o recurso xDR a partir de uma versão inferior à 4.1, a licença do recurso xDR instalado anteriormente será removida. Instale novamente a licença do recurso, conforme descrito em <u>"Instalando a licença do recurso xDR" na página 42</u>. É possível usar o arquivo de licença da versão do System Automation for Multiplatforms a partir da qual você atualizou o código do produto. Ou é possível usar o arquivo de licença da versão para a qual você atualizou.

Começando com a versão 4.1, o xDR for Linux on System z[®] em execução no z/VM[®] suporta apenas que o armazenamento de todos os nós de proxy esteja permanentemente bloqueado. Clientes que estão atualmente usando um cluster de proxy de nó duplo com a opção de bloquear o armazenamento para o proxy principal devem migrar executando o script enableErpd. O bloqueio do armazenamento deverá ser feito ao incluir o comando LOCK no arquivo boot.local ou rc.local dos dois nós do proxy. Para obter informações adicionais, consulte os manuais do GDPS.

Desinstalando o recurso xDR

Sobre Esta Tarefa

Não há nenhum procedimento de desinstalação específico definido para o recurso xDR. Ele é desinstalado implicitamente na instalação do System Automation for Multiplatforms.

Instalando a política de alta disponibilidade do SAP

O recurso de política de alta disponibilidade do SAP Central Services está incluído como parte do System Automation for Multiplatforms, mas requer uma licença separada.

O recurso da política de alta disponibilidade do SAP está incluído como parte do System Automation for Multiplatforms, mas requer uma licença separada.

Para obter informações adicionais sobre como instalar o recurso de política de alta disponibilidade do SAP, consulte System Automation for Multiplatforms High Availability Policies Guide.

Capítulo 3. Configurando

Após ter instalado o System Automation for Multiplatforms com sucesso, processe tarefas de configuração que dependem de componentes e funções do System Automation for Multiplatforms que você requer.

Nota: Você precisa de um servidor X11 para usar o diálogo de configuração do adaptador de automação. A versão de 32 bits dos pacotes de instalação do X11 é necessária para executar o diálogo de configuração. Em alguns sistemas operacionais Linux, esses pacotes estão contidos na mídia de distribuição, mas não fazem parte da instalação padrão. Certifique-se de que a versão de 32 bits dos pacotes de instalação do X11 esteja instalada.

Também é possível configurar o adaptador de automação em modo silencioso, usando um arquivo de propriedades de entrada. Se não houver um servidor X11 disponível, a configuração silenciosa será o único método suportado nesse sistema. Para obter informações adicionais, consulte <u>"Configurando no</u> Modo Silencioso" na página 82.

Configurando o comportamento de automação do sistema

É possível gerenciar e controlar o System Automation for Multiplatforms, alterando um conjunto de atributos que afetam o comportamento do produto.

É possível iniciar ou parar a função de automação, definir períodos de tempo limite e excluir nós de automação, por exemplo, para fins de manutenção.

É possível modificar os atributos a seguir:

TimeOut

Especifica o valor de tempo limite, em segundos, para uma operação de controle de início que é executada pelo System Automation for Multiplatforms. Quando o período limite expirar, a operação será repetida se o RetryCount não for excedido.

RetryCount

Número de vezes que uma operação de controle pode ser tentada novamente, se falhar ou atingir o tempo limite.

Automation

Sinalizador para ativar ou desativar a mecanização por parte do System Automation for Multiplatforms.

ExcludedNodes

Lista de nós em que o System Automation for Multiplatforms ativamente afasta ou pára recursos. Pode ser utilizado, por exemplo, para fins de manutenção.

ResourceRestartTimeOut

Período de tempo, em segundos, que o System Automation for Multiplatforms espera para reiniciar recursos, que estavam em um nó com falha em outro nó.

TraceLevel

O nível de rastreio pode ser usado para controlar o número de entradas de rastreio gravadas. O valor máximo de 255 resulta em rastreio detalhado, enquanto o valor O suprime a gravação de várias classes de entradas de rastreio. Baixar o nível de rastreio é aconselhável para políticas de automação com muitos recursos.

É possível listar os valores atuais dos atributos com o comando **lssamctrl**. Os atributos são alterados com o comando **samctrl**. Para obter informações adicionais, consulte *IBM Tivoli System Automation for Multiplatforms Reference* para obter uma listagem e uma descrição desses comandos.

TimeOut e RetryCount

O atributo TimeOut é sempre usado em conjunto com o atributo RetryCount:

TimeOut

Especifica quanto tempo o System Automation for Multiplatforms aguardará uma ação do gerenciador de recursos.

RetryCount

Especifica o número de possíveis tentativas de operação de controle que o System Automation for Multiplatforms faz dentro do período de TimeOut se a operação de controle não for bem-sucedida. Em geral, se a primeira tentativa não for bem-sucedida, as chances de que funcionará na segunda ou demais tentativas são muito baixas.

Iniciar operações

O cronômetro de operações é iniciado quando o System Automation for Multiplatforms envia a primeira operação de controle de início de recurso para um recurso. Depois que o cronômetro é iniciado, existem três possibilidades:

- O recurso é alterado para o estado desejado (on-line ou off-line) dentro do período do tempo limite. Neste caso, nenhuma ação adicional é acionada porque o recurso está no estado desejado pelo System Automation for Multiplatforms.
- 2. O recurso rejeita a operação de controle de início dentro do período limite. O que acontece em seguida depende do código da rejeição:
 - Se ele indicar que o erro é recuperável, o System Automation for Multiplatforms continuará a emitir operações de controle de início para o recurso. Cada tentativa de operação de controle é contada. Quando o valor de RetryCount é excedido, o System Automation for Multiplatforms pára de emitir operações de controle adicionais.
 - Se o erro não for recuperável, o recurso entrará em um estado de problema. Se isso acionará, ou não, ações adicionais de automação dependerá do tipo do recurso para o qual a operação de início foi emitida:
 - Se um recurso fixo for afetado, nenhuma ação adicional será acionada.
 - Se a operação de controle foi emitida para um constituinte de um recurso flutuante e esse constituinte estiver no estado Off-line ou Off-line com Falha, o System Automation for Multiplatforms tentará emitir as operações de controle para outro constituinte do recurso.
 Observe que o constituinte que rejeitou a operação de controle permanecerá em um estado de erro irrecuperável até que você emita uma operação de reconfiguração para ele.
- 3. O recurso não alcança o estado desejado (on-line) dentro do período do tempo limite. Neste caso, o System Automation for Multiplatforms primeiro emite uma operação de reconfiguração para o recurso e aguarda até que ela tenha sido aceita e o recurso esteja off-line. Em seguida, o System Automation for Multiplatforms emite outra operação de controle de início para o recurso. Cada tentativa de operação de controle é contada e o System Automation for Multiplatforms pára de emitir operações de controle quando o RetryCount é excedido ou quando o tempo limite máximo (TimeOut * RetryCount) expira, o que ocorrer primeiro.

Quando o System Automation for Multiplatforms pára de emitir operações de controle para um recurso fixo ou para um constituinte de um recurso flutuante, o OpState do recurso é configurado para off-line com falha. Isso indica que o recurso não é mais utilizável e que uma intervenção manual é necessária para corrigir a causa da falha. Depois que o problema for resolvido, o recurso deverá ser reconfigurado com o comando RMC **resetrsrc**.

Observe que o contador de novas tentativas é sempre reconfigurado quando o recurso alcança seu estado desejado porque nenhum limite é implementado. Isso significa, por exemplo, que um recurso que é iniciado, permanece on-line durante um curto período de tempo e, então, pára novamente, será reiniciado pelo System Automation for Multiplatforms em um loop.

Os valores padrão são:

- TimeOut = 60
- RetryCount = 3

Você usa o comando **samctrl -t Timeout** para alterar o valor de TimeOut e o comando **samctrl -r Retry_count** para alterar o valor de RetryCount.

A classe IBM. Application fornece seu próprio valor de tempo limite. Se você incluir um recurso da classe IBM. Application em um grupo, o valor geral de TimeOut não será usado para esse recurso. Como valor de TimeOut para esse membro do grupo, o maior valor do atributo StartCommandTimeout ou MonitorCommandPeriod (que são atributos do recurso IBM. Application) será usado.

Operações de parada

O cronômetro de operações é iniciado quando o System Automation for Multiplatforms envia pela primeira vez uma operação de controle de parada de recurso para um recurso. Depois que o cronômetro for iniciado, existem três possibilidades:

- 1. O recurso é alterado para o estado desejado (off-line) dentro do período do tempo limite. Nenhuma ação adicional é acionada.
- 2. O recurso rejeita o controle de parada dentro do período do tempo limite. O que acontece em seguida depende do código da rejeição:
 - Se ele indicar que o erro é recuperável, o System Automation for Multiplatforms emitirá outra operação de controle de parada no recurso.
 - Se o erro não for recuperável, o recurso entrará em um estado de problema. A intervenção manual é requerida para retirar o recurso do estado problemático.
- 3. O recurso não alcança o estado desejado (off-line) dentro do período do tempo limite. Nesse caso, o System Automation for Multiplatforms primeiro emite uma operação de reconfiguração para o recurso e aguarda até que o recurso alcance seu estado desejado (off-line).

Automation

Essa sinalização indica se a função de automação do System Automation for Multiplatforms está ativada ou não. Se a automação estiver desativada, o System Automation for Multiplatforms para de enviar operações de controle. O estado dos recursos permanece inalterado.

O valor padrão é o modo AUTO, o que significa que automação está ativada.

Utilize o comando **samctrl** -M F para ativar a mecanização e o comando **samctrl** -M T para desativar a mecanização.

ExcludedNodes

Lista de nós em que o System Automation for Multiplatforms para todos os recursos e os move para outro nó, se possível.

Por exemplo, você tem o recurso flutuante A, que pode ser executado em quatro nós, node05, node06, node07 e node08. Ele é um membro do grupo de recursos RG_A. Após colocar o grupo online, ele será iniciado no node05. Se você incluir o node05 na lista de nós excluídos, o System Automation for Multiplatforms para o recurso no node05. O recurso é reiniciado em um dos outros nós.

Cuidado: Se você excluir um nó e um ou mais membros obrigatórios de um grupo não puder ser reiniciado em outro nó, o grupo inteiro poderá ser interrompido.

Por padrão, a lista está vazia, o que significa que todos os nós no domínio do mesmo nível podem ser utilizados.

Use **samctrl** -**u a** para incluir um ou mais nós na lista de nós excluídos. **samctrl** -**u d** para excluir nós dessa lista. **samctrl** -**u r** para substituir nós na lista.

ResourceRestartTimeout

O valor de ResourceRestartTimeout especifica o tempo, em segundos, que o System Automation for Multiplatforms espera antes de reiniciar recursos que estão em um nó com falha e diferente. Recursos no nó com falha podem ser limpos antes que os recursos sejam movidos para outro sistema. O valor padrão é 5 segundos.

Especifique o valor de tempo limite de reinício do recurso com o comando samctrl -o.

Você pode especificar o nível de rastreio com o comando **samctrl** -1 . O TraceLevel determina o número de entradas de rastreio que são gravadas. O valor padrão é 127. O valor máximo de 255 resulta em rastreio detalhado. Se o valor for configurado para 0, diversas classes de entradas de rastreio não serão gravadas. Reduzir o nível de rastreio é aconselhável para políticas de automação com muitos recursos.

Exemplos

Para listar os parâmetros de controle atuais do System Automation for Multiplatforms, utilize o comando **lssamctrl**.

Informações de controle do System Automation for Multiplatforms:

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

Para incluir o nó node05 na lista de nós excluídos, insira:

samctrl -u a node05

Para configurar o parâmetro RetryCount para 5, insira:

samctrl -r 5

Configurando o desempatador

Configure um desempatador para ambientes em cluster com um número par de nós.

O System Automation for Multiplatforms requer que a maioria dos nós esteja online no domínio para iniciar ações de automação. Se o domínio consistir em um número par de nós, pode ocorrer que exatamente metade dos nós do domínio esteja Online. Nesse caso, o System Automation usa um desempatador para decidir o estado do quorum, que determina se ações de automação podem ser iniciadas (HAS_QUORUM) ou se nenhuma ação de automação é possível (PENDING_QUORUM, NO_QUORUM).

Configure um desempatador de disco compartilhado, como ECKD ou SCSI usando a classe de recurso **IBM.TieBreaker**. Além disso, dois desempatadores são predefinidos, operator e fail. O desempatador operator fornece um resultado indeterminado quando ocorre um empate e fica a cargo do administrador para resolver o empate por meio da concessão ou negação do quorum operacional. Quando ocorre um empate e um desempatador do tipo Fail está ativo, a tentativa de reservar o desempatador sempre é negada. O tipo de desempatador padrão está configurado para Operator.

Implementações adicionais de um desempatador podem ser incluídas usando o tipo de desempatador **EXEC**. O System Automation for Multiplatforms fornece uma rede e um desempatador do NFS como implementações adicionais do desempatador.

Liste o tipo de desempatador disponível:

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

Saída:

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

Liste o nome do desempatador:

lsrsrc IBM.TieBreaker

Saída:

```
Resource Persistent Attributes for: IBM. TieBreaker
        resource 1:
                                = "FAIL"
            Name
                               = "FAIL"
            Туре
                               = ""
            DeviceInfo
                               = ""
            ReprobeData
            ReleaseRetryPeriod = 0
            HeartbeatPeriod
                               = 0
            PreReserveWaitTime = 0
            PostReserveWaitTime = 0
            NodeInfo
                                = {}
        resource 2:
                               = "Operator"
            Name
                               = "Operator"
= ""
            Туре
            DeviceInfo
                                = ""
            ReprobeData
            ReleaseRetryPeriod = 0
            HeartbeatPeriod = 0
            PreReserveWaitTime = 0
            PostReserveWaitTime = 0
                              = {}
            NodeInfo
resource 3:
                               = "myTieBreaker"
= "SCSI"
           Name
           Туре
                             = "ID=0 LUN=0 CHAN=0 HOST=2"
           DeviceInfo
                               = ""
           ReprobeData
           ReleaseRetryPeriod = 0
           HeartbeatPeriod = 5
PreReserveWaitTime = 0
           PostReserveWaitTime = 0
           NodeInfo
                               = {}
resource 4:
                              = "mytb"
= "EXEC"
           Name
           Туре
           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"
```

Embora seja possível definir vários recursos do desempatador na classe de recurso IBM. TieBreaker, somente um deles pode estar ativo no cluster ao mesmo tempo. Insira o comando a seguir para listar o desempatador que está ativo no cluster:

lsrsrc -c IBM.PeerNode OpQuorumTieBreaker

Saída:

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

Configure o desempatador ativo:

chrsrc -c IBM.PeerNode OpQuorumTieBreaker="Operator"

Insira o comando a seguir para conceder ou negar o quorum operacional quando o desempatador for Operator:

runact -c IBM.PeerDomain ResolveOpQuorumTie Ownership=1 (0 to deny)

Nota: Para evitar condições de disputa, o desempatador operator deve ser negado para o subcluster perdedor. Em seguida, o desempatador operator pode ser concedido ao subcluster, que deve continuar.

Desempatador de disco compartilhado

Configure um desempatador de disco em um cluster que tenha um número par de nós. O disco desempatador é compartilhado entre todos os nós do cluster.

Um disco pode ser usado como recurso desempatador usando a classe de recurso IBM. TieBreaker. Caso apenas metade do número de nós esteja online em um subdomínio, o System Automation for Multiplatforms tenta reservar o disco do desempatador usando a função de reserva ou liberação. Se a reserva for bem-sucedida, o subdomínio obtém o quorum e o System Automation for Multiplatforms pode continuar a automatizar recursos. A reserva do disco é liberada quando outro nó se associa ao domínio, de forma que mais da metade dos nós esteja online nesse domínio.

Nota: Ao definir o desempatador, certifique-se de que o disco especificado para o recurso IBM. TieBreaker não seja usado também para armazenar sistemas de arquivos.

Os três exemplos a seguir mostram como usar um desempatador com um dispositivo ECKD, SCSI ou DISK. O desempatador não precisa ser formatado ou particionado.

Configuração do desempatador de ECKD para um cluster de dois nós

Configure um desempatador de ECKD no Linux on System z.

Se os nós estiverem em execução sob o z/VM, veja <u>"Desempatador do ECKD em ambientes z/VM" na</u> página 59 para obter implicações de configuração adicionais com relação à definição de um dasd ECKD a ser usado como desempatador.

O tipo de desempatador de ECKD é específico para Linux on System z. Se deseja criar um objeto desempatador de ECKD, é necessário configurar o atributo de atributo de recurso persistente DeviceInfo para indicar o número do dispositivo ECKD. Esse tipo de desempatador usa um mecanismo de reserva ou liberação e precisa ser novamente reservado periodicamente para reter a reserva. Por essa razão, também é possível especificar o atributo de recurso persistente HeartbeatPeriod quando você cria um desempatador desse tipo. O atributo de recurso persistente HeartbeatPeriod define o intervalo em que a solicitação de reserva é inserida novamente.

Colete as informações do sistema a seguir (Linux kernel 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 FFFFFFF

 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

Para o Linux kernel v2.6, use o comando **lscss** em vez de o comando cat /proc/subchannels. Execute as etapas a seguir para usar o desempatador:

1. Crie um objeto de recurso desempatador em IBM. TieBreaker class. DeviceInfo mostra o número do dispositivo ECKD. Ele pode ser obtido no arquivo /proc/dasd/devices.

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

<pre>node01:~ # lsrsrc IBM.TieBre Resource Persistent Attribut resource 1.</pre>	eaker tes for: IBM.TieBreaker
Namo	- "Operator"
Type	= "Operator"
DovicoInfo	- ""
PoproboData	
Repropedata	=
ReleaseRellyPeriod	= 0
	= 0
	= 0
PostReservewaltlime	= 0
Nodelnio	= 15
resource 2:	
Name	
Type	= "Fail"
Deviceinio	=
ReprobeData	= ""
ReleaseRetryPeriod	= 0
HeartbeatPeriod	$= \Theta$
PreReserveWaitTime	= 0
PostReserveWaitTime	= 0
NodeInfo	= {}
resource 3:	
Name	= "myTieBreaker"
Туре	= "ECKD"
DeviceInfo	= "ID=50de"
ReprobeData	= ""
ReleaseRetryPeriod	$= \Theta$
HeartbeatPeriod	= 5
PreReserveWaitTime	= 0
PostReserveWaitTime	= 0
NodeInfo	= -53

2. Altere o atributo OpQuorumTieBreaker na classe IBM. PeerNode para um dos objetos de recurso do desempatador.

Reinicializando um nó manualmente

Se um nó de um cluster de dois nós for reinicializado, o nó da reinicialização pode voltar rapidamente. A reinicialização pode interromper o método do desempatador e causar uma reinicialização indesejada do nó remanescente. Se um nó que pertence a um cluster precisar ser reinicializado manualmente, use o comando **halt -nf** em vez de **reboot -nf**.

Interromper manualmente uma reserva de disco

Se o nó que reserva um desempatador estiver inativo e não puder ser reinicializado, o acesso manual ao nó de funcionamento será necessário para interromper a reserva e assumi-la nesse nó.

 O disco do desempatador pode ser ainda conectado ao nó em funcionamento, desde que esse nó não tenha sido reinicializado no tempo médio:

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) em (94: 8) é dasdc: ativo em blocksize: 4096,601020 blocks, 2347 MB O disco do desempatador pode ser compartimentado se esse nó for reinicializado e não puder mais reconhecer o disco do desempatador:

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

Para interromper a reserva do disco do desempatador, insira o comando /usr/sbin/rsct/bin/tb_break:

tb_break -t ECKD /dev/dasdc

O disco do desempatador agora está reservado pelo nó funcional.

Nota: Se o comando **tb_brk** não funcionar na primeira vez, insira-o novamente.

Configuração do desempatador de SCSI para um cluster de dois nós

Configure um desempatador de SCSI no Linux on System x ou Linux on POWER.

Este tipo de desempatador de SCSI é específico do Linux on System x e Linux on POWER. Se desejar criar um objeto desempatador de SCSI, deve-se especificar o dispositivo de SCSI com o atributo de recurso persistente DeviceInfo. Se a configuração do SCSI for diferente em diferentes nós no cluster, também será possível usar o atributo de recurso persistente NodeInfo para refletir essas diferenças. Esse tipo de desempatador usa um mecanismo de reserva/liberação e deve ser novamente reservado periodicamente para reter a reserva. Ao criar um desempatador desse tipo, também é possível especificar o atributo de recurso persistente HeartbeatPeriod. O atributo de recurso persistente HeartbeatPeriod define o intervalo no qual a solicitação de reserva é emitida novamente.

Os dispositivos SCSI no Linux podem ser identificados por quatro valores de número inteiro para os atributos HOST, CHAN, ID e LUN:

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

Normalmente, esses parâmetros são idênticos em cada nó do cluster. Por exemplo, para node1 e node2, os parâmetros são HOST=0 CHAN=0 ID=4 LUN=0.

Nesse caso, use o comando a seguir para criar o objeto desempatador:

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

Os quatro valores também podem ser diferentes para nós diferentes (mesmo se o dispositivo de destino for igual). Nesse caso, use o campo NodeInfo além do campo DeviceInfo.

Utilize os quatro valores inteiros a partir da saída do comando:

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

Para o disco sdf os valores dos atributos do identificador de SCSI são HOST=2, CHAN=2, ID=4, LUN=0. Por exemplo, um dispositivo SCSI está conectado a dois nós que são chamados node1 e node2 e tem os identificadores de SCSI a seguir:

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

Crie o objeto desempatador usando DeviceInfo para especificar valores de atributos comuns e NodeInfo para especificar valores de atributos específicos do nó:

mkrsrc IBM.TieBreaker Name=scsi Type=SCSI DeviceInfo="ID=4 LUN=0" NodeInfo='{["node1", "HOST=0 CHAN=0"], ["node2", "HOST=2 CHAN=2"]}' O System Automation for Multiplatforms manipula DeviceInfo e NodeInfo a ponto de mesclar essas duas cadeias: primeiro DeviceInfo e, em seguida, NodeInfo. Por exemplo, para o node1 a sequência mesclada é:

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

Essa sequência é analisada.

Além disso, qualquer palavra-chave duplicada é permitida e a última será usada. Portanto, o mesmo comando pode ser especificado como

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

Essa simplificação pode ser útil já que, na maioria dos casos, o ID de SCSI é o mesmo para muitos nós.

Interromper manualmente uma reserva de disco

Se o nó que reserva um desempatador estiver desativado e não puder ser reiniciado, o acesso manual ao nó de funcionamento será necessário para liberar o disco do desempatador de SCSI. Para liberar um disco, execute o comando **tb_break [-f] HOST CHAN ID LUN**, por exemplo:

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

Configuração do desempatador do AIX DISK para um cluster de dois nós

Configure um desempatador do AIX DISK em sistemas AIX.

O tipo de desempatador do DISK é específico do AIX. Se deseja criar um objeto desempatador do DISK, é necessário configurar o atributo de recurso persistente DeviceInfo para indicar o nome do dispositivo AIX. O nome do dispositivo AIX deve especificar um disco físico SCSI ou semelhante ao SCSI que seja compartilhado por todos os nós do domínio do mesmo nível.

Discos físicos que são conectados via Fibre Channel, iSCSI e Serial Storage Architecture podem servir como desempatador do DISK. Discos rígidos IDE não suportam o protocolo SCSI e não podem funcionar como um desempatador do DISK. Os volumes lógicos também não podem funcionar como desempatador do DISK. Esse tipo de desempatador usa um mecanismo de reserva ou liberação e precisa ser novamente reservado periodicamente para reter a reserva. Por essa razão, também é possível especificar o atributo de recurso persistente HeartbeatPeriod quando você cria um desempatador desse tipo. O atributo de recurso persistente HeartbeatPeriod define o intervalo em que a solicitação de reserva é inserida novamente.

Use o comando a seguir para listar cada volume físico conhecido no sistema juntamente com seu nome de disco físico:

lspv

É exibida uma saída semelhante à seguinte:

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

Use o comando **1sdev** para verificar se um disco é um disco SCSI ou semelhante ao SCSI. Esse disco é um candidato adequado para um desempatador de disco. Por exemplo:

lsdev -C -l hdisk1

É exibida uma saída semelhante à seguinte:

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

Para servir como disco do desempatador, o disco deve ser compartilhado por todos os nós do domínio do mesmo nível. Verifique o ID do volume físico retornado pelo comando **1spv** para determinar se o disco está compartilhado entre os nós. Na saída anterior do comando **1spv**, o ID do volume físico está listado

na segunda coluna; o ID do volume para o hdisk1 é 000069683404ed54. O AIX se lembra de todos os discos que estão conectados ao sistema e os discos que são listados pelo comando **1spv** não podem mais ser conectados. Se esse disco tiver sido movido para outro sistema, ele pode aparecer como se o disco estivesse compartilhado, mas ele não está mais conectado ao sistema original.

Certifique-se de que o disco no qual os recursos IBM. TieBreaker estão armazenados não armazenem sistemas de arquivos também. Se os nós do cluster compartilharem mais de um disco, pode ser difícil determinar qual disco é o disco do desempatador e qual é usado para dados do aplicativo. A saída do comando **1sdev** mostra o endereço SCSI que está associado ao disco. (Na saída anterior do comando **1sdev**, o endereço SCSI está listado na terceira coluna; o endereço SCSI para o hdisk0 é 10-60-00-0,0). Essas informações ajudam você a identificar o disco correto se souber o endereço do disco antes de sua instalação.

Após determinar o nome do dispositivo, use o comando mkrsrc para definir o objeto desempatador:

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

Verificando a capacidade de reserva de SCSI

O desempatador depende da reserva de SCSI-2, que não é necessariamente suportada em cada combinação de configuração de armazenamento e driver. Para verificar se a configuração suporta a reserva de SCSI-2, RSCT fornece o utilitário **disk_reserve** que deve ser iniciado com seu caminho completo /usr/sbin/rsct/bin/disk_reserve.

O desempatador funciona corretamente se o disco do desempatador puder ser reservado e desbloqueado a partir do nó e se o disco não puder ser reservado a partir de um nó enquanto ele estiver bloqueado por outro nó.

Uso:

```
/usr/sbin/rsct/bin/disk_reserve [-1 | -u | -b] [-h] [-v] [-f] [-d sdisk_name]
/usr/sbin/rsct/bin/disk_reserve [-1 | -u | -b] [-h] [-v] [-f] [-g sg_device_name]
```

- h exibe este texto de ajuda
- -v verbose
- -f reserva após quebra (para a opção -l ou -b)
- -d sdisk_name disco para operar, por exemplo /dev/sdb
- -1 bloquear (reserva)
- -u desbloquear (liberar)
- -b-break
- -g sg_device_name , por exemplo /dev/sg1

Exemplos:

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

Interromper manualmente uma reserva de disco

Se o nó que reserva um desempatador estiver desativado e não puder ser reiniciado, o acesso manual ao nó de funcionamento será necessário para liberar o disco do desempatador de SCSI. Para liberar o disco, use o comando **tb_break**, por exemplo:

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

A seguir está um exemplo para um disco que não satisfaz os critérios para servir como um disco do desempatador. Insira o comando **1spath**, por exemplo:

lspath -l hdisk2 lspath: 0514-538 Não pode executar a função solicitada porque o dispositivo especificado não suporta vários caminhos.

Saída de amostra:

#lspath -l hdisk2 Ativado hdisk2 fscsi0 Com Falha hdisk2 fscsi0 Com Falha hdisk2 fscsi0 Com Falha hdisk2 fscsi0 Com Falha hdisk2 fscsi0 Ativado hdisk2 fscsi0 hdisk2 fscsi0 Ativado hdisk2 fscsi1 Ativado Com Falha hdisk2 fscsi1 Com Falha hdisk2 fscsi1 Com Falha hdisk2 fscsi1 Com Falha hdisk2 fscsi1 Ativado hdisk2 fscsi1 hdisk2 fscsi1 Ativado

Esta saída de amostra mostra que o disco não suporta a reserva de SCSI-2 e não pode ser usado como um desempatador.

Reserva persistente da SCSI para o desempatador de disco

É possível configurar um desempatador de disco para usar reserva persistente da SCSI no AIX e Linux for System x. A partir do System Automation for Multiplatforms versão 3.2.1.3, essa funcionalidade está estendida para incluir o Linux for System z.

Desempatador de SCSI-3 no AIX

Por padrão, o desempatador do tipo DISK no AIX depende da reserva ou liberação de SCSI-2, que não é necessariamente suportada por cada combinação de armazenamento em disco e configuração do driver SCSI. Geralmente, soluções de virtualização de armazenamento, como o SAN Volume Controller não suporta a reserva de SCSI-2. Nesses ambientes, o sistema operacional AIX pode ser configurado para transformar comandos de reserva ou liberação de SCSI-2 para comandos de reserva persistente de SCSI-3.

Use o comando a seguir para configurar reserva ou liberação de SCSI-2 para transformação de reserva persistente de SCSI-3 no AIX:

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

<pv_name>

O nome do volume físico no sistema AIX a ser usado para o desempate.

<unique_key>

É uma chave numérico arbitrária que é exclusiva para cada nó no cluster.

Execute esse comando em cada sistema peer remoto do domínio e especifique uma chave exclusiva diferente em cada sistema. Para descobrir se um disco SCSI a ser usado para o desempatador DISK suporta essa abordagem, execute

lsattr -El <pv_name>

Procure os atributos PR_key_value e reserve_policy. Se os atributos não puderem ser ajustados conforme descrito nos parágrafos anteriores, verifique os drivers de dispositivo ausentes em <u>Conexão de</u> host para SDDPCM no AIX.

Discos em blades POWER em um ambiente zBX podem ser definidos somente como Unidade de disco SCSI virtual. Eles não podem ser configurados para suportar reserva ou liberação de SCSI-2 ou

reserva persistente de SCSI-3. Portanto, esses discos não podem ser usados como desempatador de disco.

Desempatador SCSIPR no Linux for System x

O System Automation for Multiplatforms versão 3.2.1.2 introduziu o desempatador de tipo SCSIPR, que é específico para o Linux no System x. Ele é suportado no RHEL 7, RHEL 8, SLES 12 e SLES 15.

O desempatador SCSIPR usa reservas persistentes SCSI-3 em um dispositivo de armazenamento em disco SCSI como mecanismo de desempate. Se uma situação de empate na qual o domínio do mesmo nível for particionado em dois subdomínios e cada subdomínio contiver exatamente metade dos nós definidos, o subdomínio, que é capaz de obter uma reserva persistente exclusiva do dispositivo de armazenamento em disco SCSI compartilhado, obtém o quorum operacional.

Pré-requisitos

O dispositivo de armazenamento disco SCSI a ser usado pelo desempatador SCSIPR deve suportar o protocolo de reserva persistente SCSI-3 com tipo de reserva Write Exclusive Registrants Only. Esse dispositivo deve ser compartilhado por todos os sistemas no domínio do mesmo nível e todos os sistemas devem ser capazes de reservar o dispositivo usando o protocolo de reserva persistente SCSI-3.

O desempatador SCISPR usa o utilitário sg_persist. Use os comandos a seguir para verificar se ele já está instalado em todos os sistemas do domínio do mesmo nível:

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

Se o utilitário sg_persist ainda não estiver instalado, é necessário instalar o pacote Linux apropriado:

• RHEL 7, RHEL 8, SLES 12 e SLES 15: sg3_utils*.rpm

Definição

Ao criar um desempatador do tipo SCSIPR, use o atributo de recurso persistente DeviceInfo para especificar o dispositivo de armazenamento em disco SCSI a ser usado pelo desempatador. Se a configuração de SCSI for diferente entre os sistemas de domínio do mesmo nível, use o atributo de recurso persistente NodeInfo para refletir essas diferenças.

O desempatador SCSIPR usa um mecanismo de reserva ou liberação e precisa ser novamente reservado periodicamente para conter a reserva. Por essa razão, especifique o atributo de recurso persistente HeartbeatPeriod ao criar um desempatador deste tipo. O atributo de recurso persistente HeartbeatPeriod define o intervalo em que a reserva é tentada novamente.

Nota: Ao definir recursos do desempatador, esteja ciente de que o disco no qual os recursos IBM. Tiebreaker estão armazenados não é usado também para armazenar sistemas de arquivos.

Use uma das opções a seguir para identificar o dispositivo de armazenamento disco SCSI a ser usado pelo desempatador no atributo de recurso persistente DeviceInfo:

- 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>

Exemplo:

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

Verificação

Execute as etapas a seguir em todos os sistemas peer remotos para verificar se todos os sistemas suportam o desempatador SCSIPR corretamente com o dispositivo de armazenamento disco SCSI escolhido:

• Reserve o dispositivo de disco usando o comando **tb_break**:

```
/usr/sbin/rsct/bin/tb_break -1 -t SCSIPR <DeviceInfo device specification for this system>
```

Esse comando deve ser capaz de reservar o dispositivo de disco com sucesso.

• Tente reservar o mesmo dispositivo de disco usando o comando **tb_break** em todos os outros sistemas de domínio do mesmo nível:

/usr/sbin/rsct/bin/tb_break -1 -t SCSIPR <DeviceInfo device specification for this system>

Esse comando deve falhar ao reservar o dispositivo de disco porque ele já está exclusivamente reservado pelo primeiro sistema.

• Libere o dispositivo de disco usando o comando tb_break:

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

Esse comando deve ser capaz de liberar o dispositivo de disco com sucesso.

Verificando se uma reserva está retida:

Use o comando a seguir para verificar se uma reserva está retida no dispositivo de armazenamento disco SCSI:

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

Exemplo: nenhuma reserva está retida:

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

Exemplo: reserva está retida:

```
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
```

Quando você reservar um dispositivo de disco, cada sistema peer remoto usa seu identificador de nó RSCT como chave de reserva. Um identificador de nó RSCT do sistema peer remoto pode ser exibido usando o comando **/usr/sbin/rsct/bin/lsnodeid**. Se um dispositivo de armazenamento disco SCSI é reservado pelo desempatador SCSIPR, é possível determinar o sistema que está mantendo a reserva. Determine a chave de reserva atual e compare-a ao identificador de nó RSCT de sistemas peer remotos.

Dividindo uma reserva:

Se um sistema peer remoto atualmente retém uma reserva no dispositivo de armazenamento disco SCSI, é possível interromper essa reserva a partir de outro sistema peer remoto. Use o comando a seguir para dividir de forma forçada uma reserva existente e obter uma nova reserva:

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

Desempatador SCSIPR no Linux for System z

A partir do System Automation for Multiplatforms versão 3.2.1.3 o tipo de desempatador SCSIPR foi introduzido para uso com o Linux no System z. Ele é suportado no SLES 12 e no SLES 15.

O desempatador SCSIPR usa reservas persistentes SCSI-3 em um dispositivo de armazenamento em disco SCSI como mecanismo de desempate. Se uma situação de empate na qual o domínio do mesmo nível for particionado em dois subdomínios e cada subdomínio contiver exatamente metade dos nós definidos, o subdomínio, que é capaz de obter uma reserva persistente exclusiva do dispositivo de armazenamento em disco SCSI compartilhado, obtém o quorum operacional.

Pré-requisitos

O dispositivo de armazenamento disco SCSI a ser usado pelo desempatador SCSIPR deve suportar o protocolo de reserva persistente SCSI-3 com tipo de reserva Write Exclusive Registrants Only. Esse dispositivo deve ser compartilhado por todos os sistemas no domínio do mesmo nível e todos os sistemas devem ser capazes de reservar o dispositivo usando o protocolo de reserva persistente SCSI-3. O desempatador SCISPR usa o utilitário sg_persist. Use os comandos a seguir para verificar se ele já está instalado em todos os sistemas do domínio do mesmo nível:

which sg_persist
rpm -qf /usr/bin/sg_persist

Se o utilitário sg_persist ainda não estiver instalado, é necessário instalar o pacote Linux apropriado:

• RHEL 7, RHEL 8, SLES 12 e SLES 15: sg3_utils*.rpm

O disco que funciona como desempatador deve ter uma virtualização do identificador de porta N ativada. Caso contrário, cada reserva é executada em nome do CEC inteiro, a caixa física do zSeries, em vez de uma única partição lógica nesse CEC. Para obter informações adicionais sobre virtualização do identificador de porta N no zSeries, consulte:

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

Definição

Ao criar um desempatador do tipo SCSIPR, use o atributo de recurso persistente DeviceInfo para especificar o dispositivo de armazenamento em disco SCSI a ser usado pelo desempatador. Se a configuração de SCSI for diferente entre os sistemas de domínio do mesmo nível, use o atributo de recurso persistente NodeInfo para refletir essas diferenças.

O desempatador SCSIPR usa um mecanismo de reserva ou liberação e precisa ser novamente reservado periodicamente para conter a reserva. Por essa razão, especifique o atributo de recurso persistente HeartbeatPeriod ao criar um desempatador deste tipo. O atributo de recurso persistente HeartbeatPeriod define o intervalo em que a reserva é tentada novamente.

Nota: Ao definir recursos do desempatador, esteja ciente de que o disco no qual os recursos IBM. Tiebreaker estão armazenados não é usado para armazenar sistemas de arquivos.

Use uma das opções a seguir para identificar o dispositivo de armazenamento disco SCSI a ser usado pelo desempatador no atributo de recurso persistente DeviceInfo:

- 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>

Exemplo:

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

Execute as etapas a seguir em todos os sistemas peer remotos para verificar se todos os sistemas suportam o desempatador SCSIPR corretamente com o dispositivo de armazenamento disco SCSI escolhido:

• Reserve o dispositivo de disco usando o comando tb_break:

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

Esse comando deve ser capaz de reservar o dispositivo de disco com sucesso.

• Tente reservar o mesmo dispositivo de disco usando o comando tb_break em todos os outros sistemas de domínio do mesmo nível:

/usr/sbin/rsct/bin/tb_break -1 -t SCSIPR <DeviceInfo device specification for this system>

Esse comando deve falhar ao reservar o dispositivo de disco porque ele já está exclusivamente reservado pelo primeiro sistema.

• Libere o dispositivo de disco usando o comando tb_break:

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

Esse comando deve ser capaz de liberar o dispositivo de disco com sucesso.

Verificando se uma reserva está retida:

Use o comando a seguir para verificar se uma reserva está retida no dispositivo de armazenamento disco SCSI:

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

Exemplo: nenhuma reserva está retida:

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

Exemplo: reserva está retida:

```
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
```

Quando você reservar um dispositivo de disco, cada sistema peer remoto usa seu identificador de nó RSCT como chave de reserva. Um identificador de nó RSCT do sistema peer remoto pode ser exibido usando o comando **/usr/sbin/rsct/bin/lsnodeid**. Se um dispositivo de armazenamento disco SCSI é reservado pelo desempatador SCSIPR, é possível determinar o sistema que está mantendo a reserva determinando a chave de reserva. Compare a chave de reserva a todo identificador de nó de RSCT dos sistemas peer remotos.

Dividindo uma reserva:

Se um sistema peer remoto retém uma reserva no dispositivo de armazenamento disco SCSI, é possível interromper essa reserva a partir de outro sistema peer remoto. Use o comando a seguir para dividir de forma forçada uma reserva existente e obter uma nova reserva:

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

Desempatador do ECKD em ambientes z/VM

No Linux on System z[®], um ECKD[™] DASD pode ser usado como recurso desempatador.

O desempatador do ECKD usa a função de reserva e liberação, o que pode levar a etapas de configuração adicionais. Um ECKD DASD reservado não pode ser acessado pelo z/VM[®]. Portanto, z/VM não pode conectar ou mudar para online esse dispositivo que está reservado por outro sistema. Como solução alternativa para essa situação, um conjunto de ações de configuração é necessário. O requisitos correspondentes são explicados nas seções a seguir.

Requisitos do ECKD DASD para domínios executados em um único sistema z/VM

Se todos os nós do domínio do System Automation forem convidados do mesmo sistema z/VM, as definições a seguir serão necessárias para o ECKD DASD:

- Um MiniDisk de pacote completo definido.
- Se cache do MiniDisk for usado, seu valor deve estar definido para off.
- O ECKD DASD está compartilhado entre ambos os convidados no sistema z/VM.

Requisitos do ECKD DASD para domínios que abrangem dois sistemas z/VM

Se os nós do domínio do System Automation forem convidados de dois sistemas z/VM diferentes, as definições a seguir serão necessárias para o ECKD DASD:

- O disco do desempatador precisa ser definido como um disco DEVNO em uma instrução MiniDisk no perfil do usuário (nenhum MiniDisk, nenhum MiniDisk fullpack, nenhum DASD dedicado ou conectado)
- O disco ECKD (DEVNO) é compartilhado entre ambos os nós.
- O ECKD DASD não deve ser um sistema que está conectado quando o z/VM for ativado para IPL

Efetuar logon nos convidados Linux mostra a conexão de dispositivo a seguir, um dispositivo virtual (291 no exemplo) com o endereço real (4a82 no exemplo). O dispositivo torna-se compartilhado no exemplo com o comando cp set shared on 4a82. O dispositivo precisa ser compartilhado em ambos os lados.

```
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
```

Caso um dos sistemas z/VM seja encerrado, o ECKD DASD é reservado pelo convidado Linux sobrevivente no outro sistema z/VM. Do lado sobrevivente, é possível ver a saída a seguir:

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

Após iniciar o sistema z/VM novamente, o DASD 4A82 ainda está offline e não pode ser configurado online, pois ainda está reservado pelo outro sistema. Um tempo limite de 20 a 30 minutos ocorre em vez disso.

A recomendação é iniciar o Linux no z/VM reiniciado sem o DASD do desempatador. Isto será bemsucedido, desde que o DASD não seja necessário para iniciar o Linux. Após o Linux ser iniciado, o System Automation iniciará automaticamente no convidado do Linux e, em seguida, o Linux unirá novamente o domínio do System Automaton de modo automático. A reserva do ECKD DASD é liberada. É possível ativar o dispositivo do disco do desempatador (4a82 no exemplo). Confirme o comando **share** e vincule o endereço virtual do disco do desempatador (291 neste exemplo) no novo sistema ativado para IPL. Insira o comando **chccwdev** -e 291 no Linux reiniciado. Após esse comando ser concluído, tudo está ativo e em execução. Nenhuma interação adicional no Linux sobrevivente será necessária.

Todos os comandos necessários são comandos CP. Portanto, um script que processa esses comandos usando o VMCP poderá ser gravado para automatizar a restauração do Linux com falha.

Para o exemplo, o script poderá conter os comandos a seguir:

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

O System Automation reconhece o novo DASD definido automaticamente.

Desempatador de rede

O desempatador de rede fornece uma alternativa para os desempatadores baseados em disco e em operador. Ele utiliza um IP externo (instância de rede) para resolver a situação de empate.

Há várias situações nas quais o uso de um desempatador de rede é mais apropriado, por exemplo:

- Um disco compartilhado para ser usado como um desempatador de disco não está disponível.
- A capacidade de se comunicar com instâncias fora do cluster tem a prioridade mais alta.

Exemplo: A função principal de um servidor da web é entregar páginas da web a clientes fora do cluster. Para tornar esse serviço altamente disponível, o desempatador não deve conceder acesso a um nó que não seja capaz de se comunicar com instâncias fora do cluster.

Utilize o desempatador de rede somente para domínios em que todos os nós estejam na mesma sub-rede IP. Ter os nós em diferentes sub-redes IP aumenta a probabilidade de que os dois nós possam executar ping no desempatador de rede, enquanto não podem se comunicar entre si. Além disso, o endereço IP de gateway padrão não deverá ser utilizado se estiver virtualizado pela infra-estrutura de rede. Escolha um endereço IP, que pode ser acessado apenas por meio de um caminho único a partir de cada nó no domínio.

Na configuração padrão, o desempatador de rede faz duas tentativas de executar ping no endereço IP do desempatador de rede. Esse número padrão de pings pode ser muito baixo em ambientes virtualizados ou em ambientes com uma conexão de rede lenta ou não confiável. Para esses ambientes, é possível aumentar o número de pings que são executados pelo desempatador de rede até no máximo nove. Em seguida, é possível assegurar um resultado correto da operação de reserva do desempatador.

Requisitos para o desempatador de rede

Para assegurar a função do desempatador de rede, a instância de IP externo deve estar acessível a partir de todos os nós no cluster altamente disponível. Além disso, a instância de IP externa deve ser capaz de responder a solicitações de repetição do ICMP (ping). Se você instalar uma regra de firewall, que bloqueia o tráfego do ICMP entre os nós do cluster e a instância de IP externa, o desempatador de rede não funcionará. Nesta situação, os nós do cluster podem não se comunicar com seus peers (divisão de cluster), mas os dois subclusters são capazes de acessar a instância de IP externa. Geralmente, o IP assegura que se os dois subclusters podem atingir o gateway externo, eles também podem se comunicar com seus peers. Se essa regra não puder ser assegurada, por exemplo, devido a configurações do firewall, você não poderá usar o desempatador de rede.

A tabela a seguir mostra as vantagens e desvantagens de desempatadores de rede e de disco:

Tabela 21. Comparação dos Desempatadores com Base na Rede e com Base no Disco			
Desempatador baseado em rede	Desempatador baseado em disco		
 +: Sem dependência de hardware. +: Avalia a disponibilidade da comunicação. 	 +: Desempatador mais seguro. O hardware assegura que somente uma instância (nó) seja capaz de obter o desempatador. 		
 -: Se a instância IP externa não estiver disponível no caso de uma divisão do cluster, nenhum subcluster obterá quorum. 	 -: Se houver uma perda na comunicação, esse desempatador poderá conceder acesso a um n que não é capaz de se comunicar com instância 		
 -: Pode haver condições de erro em que ocorra uma situação de empate, mas mais de um nó consegue se comunicar. Nesse caso, ambos os subclusters são capazes de obter o desempatador. 	fora do cluster.		

Configurando um desempatador de rede

Defina um desempatador de rede como um recurso IBM. TieBreaker do tipo EXEC. Para obter informações adicionais sobre um desempatador EXEC, veja a documentação de RSCT. Os arquivos executáveis do desempatador de rede samtb_net e samtb_net6 estão no diretório /usr/sbin/rsct/ bin. Na implementação atual, as opções a seguir devem ser especificadas como pares de key=value durante a criação do desempatador EXEC RSCT:

Address=<IP address>

Endereço da instância IP externa, que é usada para resolver a situação de empate. Em uma rede IPv6, especifique um endereço em formato IPv6. Não use os nomes de DNS. O DNS não pode funcionar corretamente se ocorrerem problemas de comunicação, o que é geralmente o caso durante divisões do cluster. Endereço é uma opção obrigatória, não há nenhum valor padrão.

Log=<1/0>

Especifique 1 se desejar que o desempatador de rede grave logs no recurso de log do sistema (syslog). Caso contrário, especifique 0.

Count=<number>

Número de solicitações de repetição de ICMP, que são enviadas ao quorum de solicitação. Se o primeiro pedido obtiver uma resposta, nenhum outro pedido será enviado. O valor padrão é 2. O intervalo de valor permitido é 1 a 9. Aumente o valor para Contagem para ambientes virtuais ou ambientes com uma conexão de rede lenta ou não confiável.

Dependendo da versão de IP, há diferentes arquivos executáveis do desempatador de rede que você deve usar ao definir o desempatador.

O comando a seguir cria um novo desempatador de rede para um endereço IPv4:

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

O comando a seguir cria um novo desempatador de rede para um endereço IPv6:

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

Ative o desempatador de rede da seguinte forma:

chrsrc -c IBM.PeerNode OpQuorumTieBreaker="mynetworktb"

Use o comando **chrsrc** para manipular a definição do desempatador de rede. Por exemplo, se você deseja aumentar o valor do número de pings, insira os comandos a seguir:

```
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"
```

Para excluir a definição do desempatador, use o comando **rmrsrc**.

Comportamento de reserva de um desempatador de rede

Quando um nó reserva um desempatador, o desempatador não fica mais disponível e não pode ser reservado por nenhum outro nó. Essa abordagem não é viável para um desempatador de rede. Portanto, o comportamento de reserva de um desempatador de rede é diferente da seguinte forma.

Após uma tentativa de reserva mal sucedida, nenhuma outra reserva será possível até que o nó junte-se novamente ao cluster. Um arquivo é gravado em /var/ct/, que indica que uma reserva falhou. Se esse arquivo estiver presente, um comando de reserva para um desempatador sempre falhará. Um processo adicional é bifurcado, que observa o quorum e remove o arquivo de bloqueio se o nó tiver se juntado novamente ao domínio.

O arquivo de amostra a seguir foi criado pelo desempatador de rede como resultado de uma operação de reserva do desempatador com falha para a instância de IP externo 123.456.789.1. Ele contém o registro de data e hora da operação de reserva com falha.

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

Configurando um recurso desempatador para o desempatador de rede

Este tópico descreve as opções de configuração do desempatador que precisam ser consideradas quando você define um desempatador de rede.

PostReserveWaitTime=30

O PostReserveWaitTime define o atraso entre o momento em que o desempatador é reservado com sucesso e o momento em que o quorum é concedido. Um nó que reserva o desempatador de rede não obtém um quorum operacional até que o PostReserveWaitTime seja passado. Especifique um valor de 30 segundos para fornecer tempo suficiente de indisponibilidade. Esse tempo é necessário para que os nós detectem que o outro nó está offline e para restaurar imediatamente a comunicação. Nesse caso, ambos os nós podem reservar o desempatador de rede. Devido ao tempo de espera mais longo, a comunicação entre os nós é restabelecida e a chance de ambos os nós obterem quorum e iniciarem recursos em paralelo é minimizada.

HeartbeatPeriod=30

Após uma reserva bem-sucedida, ConfigRM começa a chamar periodicamente a operação de pulsação do desempatador. Para manter o carregamento do sistema baixo durante uma divisão de cluster, aumente o tempo entre as pulsações do desempatador ou até mesmo desligue a pulsação configurando HeartbeatPeriod para 0.

Revisando os logs do sistema de um desempatador de rede

A seguir é mostrado o conteúdo de um log do sistema de amostra para um cenário de erro do desempatador de rede em um cluster de dois nós (nó n1 e nó n2).

No Figura 12 na página 63, é possível ver os logs do sistema de um cluster de dois nós (nó n1 e nó n2). Para o cenário de erro, assume-se que não há recursos críticos em execução em ambos os nós. Um problema na rede interrompe todos os caminhos de comunicação disponíveis entre os peers, mas um peer (n2) ainda é capaz de se comunicar com seu gateway (123.456.789.1). Após algum tempo, a comunicação é restabelecida e ambos os nós podem se associar ao cluster.



Figura 12. Logs do sistema de cluster de dois nós

desempatador do NFS

O desempatador do NFS resolve situações de empate que são baseadas em arquivos de reserva que estão armazenados em um servidor NFS v4. O servidor NFS pode ser usado para vários clusters do

System Automation for Multiplatforms. Se o mesmo servidor for usado para vários desempatadores do NFS, cada desempatador precisa de um arquivo de reserva com um nome exclusivo.

Não é possível que, em uma situação de divisão de cluster, mais de um nó tenha quorum ou quorum pendente a qualquer momento. Se o nó que obteve o quorum falhar posteriormente, outros nós tentarão automaticamente obter o quorum que é baseado no protocolo de desafiador-defensor.

O servidor NFS pode estar em qualquer sistema que suporte executar o NFS v4. Se você utilizar um servidor NFS compatível com a v4.1 ou o padrão pNFS mais novo para desempatadores do System Automation for Multiplatforms, certifique-se de que os recursos de replicação e failover do servidor NFS estejam desativados. Use o servidor NFS somente para propósitos do desempatador do System Automation for Multiplatforms.

Bibliotecas do cliente NFS v4 devem ser instaladas em todos os nós do cluster do System Automation for Multiplatforms.

Um cenário de exemplo para usar um desempatador do NFS é uma configuração de três sites. Dois sites hospedam um conjunto de clusters de dois nós e o desempatador deve estar no terceiro site. Um desempatador de disco não pode ser usado, pois ele requer uma configuração de SAN que não esteja necessariamente cruzando todos os três sites. Também não é possível fazer quaisquer suposições sobre a topologia de rede. Nenhum dispositivo de rede no terceiro site pode ser escolhido como o endereço de destino para o desempatador de rede. Nesse caso, o terceiro site pode ser usado para hospedar o servidor NFS v4 que é usado como desempatador.

Se o servidor de quorum NFS estiver inativo ou não acessível em uma situação de divisão de cluster, os nós do cluster não obterão quorum. Essa situação é semelhante a um desempatador de disco, em que nenhum nó obterá quorum se o dispositivo de disco tiver falhado ou estiver inacessível. Certifique-se de que o servidor de quorum NFS esteja permanentemente em execução e funcione de forma confiável.

O System Automation monta o sistema de arquivos NFS em vários estágios para os nós do cluster, mas não periodicamente.

Initialize

A montagem é estabelecida quando o desempatador NFS está configurado como o desempatador ativo, durante a operação Initialize. O mesmo acontece durante a inicialização do domínio ou do nó. Se isso falhar, o nó talvez não seja capaz de se associar ao domínio.

Reserve

Durante a operação Reserve, antes de o arquivo de reserva ser acessado, a montagem NFS é verificada e (r)estabelecida, se necessário.

Terminate

O sistema de arquivos NFS é desmontado durante a operação Terminate, que é executada quando o desempatador NFS não é mais o desempatador ativo ou quando o domínio/nó é interrompido.

O System Automation for Multiplatforms monta o sistema de arquivos NFS em vários estágios nos nós do cluster, mas não periodicamente:

- Inicialmente, a montagem é estabelecida quando o desempatador NFS é configurado como o desempatador ativo durante a operação Initialize ou a inicialização do domínio ou do nó. Se a montagem falhar, o nó talvez não seja capaz de se associar ao domínio.
- Durante a operação Reserve antes de o arquivo de reserva ser acessado, a montagem NFS é verificada e (r)estabelecida, se necessário.

O sistema de arquivos NFS é desmontado durante a operação Terminate, que é executada quando o desempatador NFS não é mais o desempatador ativo ou quando o domínio ou o nó é interrompido.

Nota: A existência do arquivo de reserva é essencial no caso de uma divisão do cluster e a exclusão do arquivo de reserva pode fazer com que os dois nós em um cluster tenham o quorum concedido. Use um esquema de nomenclatura para esses arquivos que permita uma associação direta entre o arquivo de reserva e o cluster, usando o arquivo de reserva. Por exemplo, NFS_reserve_file_SAP_HA_sapnode1_sapnode2_D0_NOT_REMOVE indica claramente o propósito do arquivo, o nome do cluster e os nomes dos nós que usam o arquivo de reserva. Se o arquivo tiver sido excluído, ative o desempatador operator padrão, crie o arquivo novamente e, em seguida, ative o

desempatador do NFS novamente. Para obter informações adicionais sobre o desempatador do operador, consulte "Configurando o desempatador" na página 48.

Ativando o Servidor NFS no Linux

Descubra como ativar o suporte ao NFS v4 se você estiver executando o System Automation for Multiplatforms no Linux.

Ative o suporte ao NFS v4:

1. Inclua a seguinte linha em /etc/exports para o sistema de arquivos do servidor de quorum:

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

O nome do diretório </your/quorumserverDir> é um exemplo. É possível usar qualquer nome de diretório. Certifique-se de que apenas um caminho seja exportado com fsid=0.

- Crie um diretório <quorum_server_directory> e configure sua máscara de bits de permissão como a+rwxt.
- 3. Pode ser necessário incluir as seguintes linhas em /etc/fstab para montar os sistemas de arquivos rpc_pipefs e nfsd automaticamente:

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

b.nfsd /proc/fs/nfsd nfsd defaults 0 0

- 4. Pode ser necessário reiniciar o servidor para que as mudanças nos arquivos config no diretório /etc sejam aplicadas. Consulte a documentação da distribuição do Linux para obter detalhes adicionais.
- 5. Verifique se os diretórios /var/lib/nfs/v4recovery/e/var/lib/nfs/ rpc_pipefs/ foram criados. Dependendo da distribuição usada, pode ser necessário carregar o módulo de kernel NFS, executando o comando modprobe nfs.
- 6. Dependendo da distribuição que você usa, os daemons são iniciados de maneira diferente. Por exemplo, pode ser necessário digitar /etc/init.d/idmapd start ou service idmapd start para iniciar o daemon rpc.idmapd. Os seguintes daemons devem ser iniciados:
 - a.rpc.idmapd
 - b.rpc.gssd
 - c.rpc.nfsd
- 7. Atualize a lista de exportação executando o comando exportfs -r.
- 8. Verifique se os daemons rpc.nfsd e rpc.idmapd estão ativos e em execução.
 - a. rpc.nfsd: Use o comando ps -ef | grep nfsd para verificar se um processo com o nome nfsd está ativo e em execução.
 - b.rpc.idmapd:Useocomandops -ef | grep rpc.idmapd
 - c. Use o comando rpcinfo -p para verificar as versões de todos os programas RPC registrados.

O ID do NFS v4 para o daemon de mapeamento rpc.idmapd é necessário para execução no nó do System Automation for Multiplatforms que está executando o desempatador do NFS. Consulte a documentação das distribuições sobre como iniciar o daemon idmapd.

Para verificar se um nó do System Automation for Multiplatforms pode acessar corretamente o servidor NFS, insira o comando a seguir:

mount -t nfs4 <nfs_server_name>:/<quorum_directory_name>/<local_directory>

A instalação será verificada com sucesso se o comando de montagem for bem-sucedido e se for possível criar arquivos no diretório do NFS v4 montado.

Se a operação de montagem não for bem-sucedida, corrija sua instalação com a ajuda da documentação do sistema operacional.

Consulte a documentação de sua distribuição Linux para obter detalhes adicionais.

Ativando o Servidor NFS no AIX

Descubra como ativar suporte ao NFS v4 se você estiver executando o System Automation for Multiplatforms on AIX.

Certifique-se de que os daemons relacionados ao NFS v4 estejam iniciados no servidor NFS:

- 1. Verifique se os daemons relacionados ao NFS v4 estão iniciados em seu servidor com o comando lssrc -g nfs.
- 2. Inicie o servidor NFS executando os comandos a seguir se o servidor NFS ainda não estiver iniciado:

```
a.mknfs
```

```
b.chnfsdom <your_nfs_domain_name>
```

- c.startsrc -s nfsrgyd
- 3. Crie um diretório <quorum_server> e configure sua máscara de bits de permissão como a+rwxt.
- 4. Exporte esse diretório para clientes NFS v4 com o comando mknfsexp -v 4 -d <quorum_server> [-h <host>].
- 5. É possível restringir a lista de hosts que têm permissão para montar o diretório por razões de segurança. Restrinja a lista de hosts a todos os nós do System Automation for Multiplatforms que usam o servidor NFS, especificando a opção - h.

Inicie e configure os daemons relacionados a NFS, que são necessários no cliente NFS, executando o comando mknfs. No caso de o servidor NFS usado estar em execução no Linux, você pode ver a mensagem de erro a seguir no log do sistema após um desempatador do NFS ser inicializado:

vmount: operation not permited

O servidor NFS Linux NFS verifica se a porta para o cliente NFS é uma porta reservada. Caso você receba uma mensagem de erro, execute o comando a seguir em cada sistema AIX no qual o desempatador do NFS é executado.

nfso -p -o nfs_use_reserved_ports=1

Para verificar se um nó do System Automation for Multiplatforms pode acessar corretamente o servidor NFS, insira:

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

A instalação será verificada com sucesso se o comando de montagem for bem-sucedido e se for possível criar arquivos no diretório do NFS v4 montado.

Se a operação de montagem não for bem-sucedida, corrija sua instalação com a ajuda da documentação do sistema operacional.

Configurando o desempatador do NFS

Defina um desempatador de rede como um recurso IBM. TieBreaker do tipo EXEC.

O executável samtb_nfs do desempatador do NFS está no diretório /usr/sbin/rsct/bin. Na implementação atual, as opções a seguir devem ser especificadas como pares de key=value durante a criação do desempatador executável RSCT:

nfsQuorumServer

O nome do host do servidor NFS v4 usado. Esta opção é obrigatória.

localQuorumDirectory

O diretório que é usado pelo desempatador do NFS no nó do System Automation for Multiplatforms. O diretório é criado automaticamente, se não existir. Se esta opção não for especificada, o diretório padrão /var/ct/nfsTieBreaker/ será usado.

remoteQuorumDirectory

O diretório, que é exportado pelo nfsQuorumServer e usado pelo desempatador do NFS do System Automation for Multiplatforms. Se esta opção não for especificada, o padrão / será usado.

nfsOptions

As opções que são usadas para o comando de montagem. Use a opção padrão conforme documentado em "Opções de Montagem NFS Padrão" na página 68.

É necessário substituir todos os caracteres '=' por '::' e todos os caracteres ', ' por '..'. Por exemplo, vers::4..fg..soft..retry::1..timeo::10 é transformado em vers=4, fg, soft, retry=1, timeo=10 antes da opção de montagem ser passada para o comando de montagem do sistema operacional.

Se nfsOptions não for especificado, as opções de montagem padrão são:

AIX

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

Linux

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

reserveFileName

O nome do arquivo que é criado pelo desempatador do NFS no remoteQuorumDirectory do nfsQuorumServer para armazenar informações relacionadas ao desempatador. Esta opção é obrigatória.

Se diversos clusters estiverem usando o mesmo servidor NFS v4 para o desempatador NFS, certifique-se de que cada cluster esteja usando um reserveFileName distinto. Se dois clusters estiverem usando o mesmo arquivo de reserva, um subcluster pode perder quorum de forma desnecessária em uma situação de divisão de cluster. Para se certificar de que os nomes de arquivos de reserva são exclusivos, é possível considerar um esquema de nomenclatura que usa o nome do cluster e pelo menos alguns dos nomes do nó do cluster.

Log

Usado para ativar ou desativar informação de log de gravação para syslog.

- Log=0: Nenhuma informação de log é reunida.
- Log=1: Informações importantes são gravadas no syslog.
- · Log=2: São produzidas informações em nível de rastreio e depuração
- O valor padrão é 1.

HeartbeatPeriod

Após uma reserva bem-sucedida, ConfigRM começa a chamar periodicamente a operação de pulsação do desempatador. Para o desempatador do NFS, especifique um valor maior que 15.

PostReserveWaitTime

PostReserveWaitTime define o atraso entre a reserva bem-sucedida do desempatador e o quorum de tempo que é concedido. Um nó que reserva o desempatador de não obtém um quorum operacional até que PostReserveWaitTime seja passado. Para o desempatador do NFS, PostReserveWaitTime deve ser igual a 15.

Para criar um desempatador do NFS myNFSTiebreaker no servidor NFS my.nfs.server.com com localQuorumDirectory /my/quorumServer, nível de log 2 e padrões para as outras opções, o comando a seguir poderá ser usado:

```
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'
```

Quando o desempatador do NFS for ativado, uma lógica de validação assegura que o servidor NFS funcione conforme o esperado.

Os erros de configuração a seguir não podem ser detectados pela lógica de validação:

- Se HeartbeatPeriod for menor que 15.
- Se reserveFileName não for exclusivo para o servidor NFS v4 usado.
- Se PostReserveWaitTime não é igual a 15.

Para obter informações adicionais sobre um desempatador EXEC, consulte a documentação de RSCT.

Opções de Montagem NFS Padrão

As seguintes opções de montagem são usadas:

rw

Especifica que o diretório montado é acessível para leitura e gravação.

soft

Retorna um erro caso o servidor não possa ser acessado.

intr

Permite sinais de interrupção.

noac

Os atributos de arquivo não são armazenados em cache. Força a solicitação de gravação do cliente a ser síncrona.

fg

Executa o comando de montagem e falha se o comando de montagem não for bem-sucedido.

retry=0

O sistema é encerrado imediatamente se um comando de montagem falhar.

Se você usar outras opções de montagem, não haverá garantia de que em todos os casos o desempatador do NFS ainda funcionará.

Proteção de tempo limite para as operações do desempatador do NFS

É importante assegurar que as operações do desempatador EXEC não sejam interrompidas pelas razões a seguir:

- Operações baseadas em RSCT, como **lsrsrc**, **lsrpnode** e **lssam** são bloqueadas enquanto operações do desempatador são executadas.
- Se uma operação de reserva em um nó com um recurso crítico em execução for interrompida, o nó permanecerá em PENDING_QUORUM enquanto outro nó pode ser capaz de atingir HAS_QUORUM. Em seguida, um recurso crítico está online em vários nós no cluster simultaneamente.

O desempatador do NFS tem dois processos definidos. Um processo do trabalhador e um segundo processo que ativa o cronômetro e para o trabalhador se ele não concluir no período de tempo limite:

- samtb_nfs_worker: Executa as operações do desempatador real.
- samtb_nfs: Inicializa um cronômetro e, em seguida, executa samtb_nfs_worker a partir de um encadeamento bifurcado. Se samtb_nfs_worker for finalizado no período de tempo limite, samtb_nfs sai com o código de retorno samtb_nfs_worker. Se samtb_nfs_worker não terminar dentro do período de tempo limite, o manipulador de alarme assegura que samtb_nfs_worker está interrompido e grava uma mensagem de erro no syslog e termina com -1 (FAILED).

Os valores de tempo limite a seguir são usados:

Operação Reserve

13 após a divisão do cluster.

Operação Validate

60 segundos no tempo de definição do desempatador.

Operação Initialize

20 segundos após um nó ser reinicializado durante inicialização do cluster.

Todas as outras operações

15 segundos.

Cloud Tie Breaker

A solução Cloud Tie Breaker resolve situações de empate de contêiner reservado, que são armazenamentos no Amazon Web Services (S3). O Cloud Tie Breaker suporta apenas cluster de dois nós e tipo de armazenamento AWS do contêiner.

Configurando o desempatador de nuvem

A solução do desempatador de nuvem resolve as situações de empate do contêiner reservado, que são armazenadas no Amazon Web Services (S3). O Cloud Tie Breaker suporta apenas cluster de dois nós e tipo de armazenamento AWS do contêiner.

O desempatador de nuvem usa o armazenamento em nuvem externo para reter o estado do desempatador e fornece várias vantagens, como evitar situações de split brain, facilidade de uso em nuvem, facilidade de virtualização da rede.

O desempatador de nuvem é especificado por um par de chaves de acesso e chaves secretas, que são usadas para acessar o armazenamento em nuvem. O serviço do desempatador de nuvem deve estar acessível a partir de cada nó no cluster.

O serviço de armazenamento do desempatador de nuvem consiste em contêineres e objetos contidos dentro desses contêineres.

Os nomes de contêiner devem ser exclusivos porque o namespace do contêiner é compartilhado por todos os usuários do serviço de armazenamento. O nome de um contêiner não pode ser designado a outro contêiner até que o contêiner existente seja excluído. Os contêineres possuem listas de controle de acesso, que são usadas para autenticar a conexão com a nuvem a partir do nó. A propriedade de exclusividade do contêiner dentro do serviço de nuvem assegura que apenas um nó do cluster de dois nós possa adquirir o dispositivo desempatador. Isso evita a possibilidade de desenvolver situações de split brain.

Isso representa uma configuração de nuvem desempatadora com dois nós (nodeha01 e nodeha02) em um cluster, que têm acesso a um armazenamento compartilhado no Amazon Web Services (S3). Os dois nós têm permissões de leitura e gravação na nuvem, para que cada nó possa criar um contêiner no armazenamento e possa criar um objeto desempatador no contêiner. Em caso de uma situação de split brain, o nó que tem a propriedade do container terá recursos QUORUM e o nó continuará a funcionar no cluster.

Configurando o desempatador de nuvem

Primeiro, defina um desempatador de nuvem como um recurso IBM. TieBreaker do tipo EXEC. Para obter informações adicionais sobre um desempatador EXEC, consulte a documentação do RSCT. É possível localizar o arquivo de configuração do desempatador samtb_cld no diretório /usr/sbin/ rsct/bin. O script no arquivo de configuração cria um contêiner no local remoto, ou seja, no Amazon Web Services (S3). Ele também ajuda a excluir o contêiner e a manter a propriedade do contêiner. O nó, que possui o contêiner, terá o quorum e o trabalho como o membro Ativo do cluster durante uma situação de split brain.

Para configurar um desempatador de nuvem, conclua os procedimentos a seguir.

- 1. "Criando contas do AWS" na página 69
- 2. "Buscando chave de acesso e chave secreta a partir do AWS" na página 70
- 3. "Configurando o desempatador de cluster na nuvem" na página 71

Criando contas do AWS

Crie duas contas de armazenamento em nuvem. As contas devem ter permissão para criar e excluir contêineres. É possível se inscrever para o Amazon Web services (AWS) Simple Storage Service (S3).

Para criar contas de armazenamento em nuvem no AWS S3, conclua as etapas a seguir.

1. Clique no seguinte link:

Amazon Web Services (AWS) Simple Storage Service (S3). O navegador redireciona para a página inicial do AWS.

- 2. Clique no botão Criar uma conta do AWS.
- 3. Insira detalhes pessoais no formulário exibido para criar uma conta. E clique no botão Continuar.
- 4. Insira detalhes do gateway de pagamento. Depois que os detalhes do gateway de pagamento forem validados, sua conta se tornará ativa.

Buscando chave de acesso e chave secreta a partir do AWS

Cada nó usa uma conta do AWS distinta para acessar o armazenamento em nuvem compartilhado. Recupere a chave de acesso e a chave secreta de ambas as contas a partir do website de serviço de armazenamento em nuvem. Coloque as informações de chave de acesso em cada máquina.

Para buscar a chave de acesso e a chave secreta a partir do AWS, conclua as etapas a seguir.

- 1. Efetue login no console do AWS.
- 2. Na página inicial, clique em seu nome da conta e, em seguida, clique em Minhas credenciais de segurança.
- 3. Clique no botão Criar nova chave de acesso. Após clicar no botão, o navegador avisa para fazer download da chave de acesso e da chave secreta.
- 4. Faça download e salve a chave de acesso e a chave secreta. Nomeie a chave secreta como Node1.secret e a chave de acesso como Node1.access.
- 5. Da mesma forma, faça download e salve a chave de acesso e a chave secreta de outra conta. Nomeie a chave secreta como Node2.secret e a chave de acesso como Node2.access.

Posicionamento de chaves

Cada conta está associada a um par de chave de acesso e chave secreta. O par de chaves deve ser colocado nos nós em que o desempatador deve ser configurado. As chaves de acesso e secretas devem ser colocadas nos arquivos acessíveis à raiz em cada um dos dois nós.

O exemplo a seguir mostra o formato de nomenclatura dos arquivos. O conteúdo dos arquivos segue de maneira natural e direta a nomenclatura do arquivo.

Tabela 22. Nome de arquivos em um cluster de dois nós		
No. S.	Nome de arquivos no cluster de dois nós	
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	

Em um cluster de dois nós, os arquivos são nomeados da seguinte forma:

Assegure-se de que todos os quatro arquivos estejam presentes em cada um dos dois nós no cluster e que sejam legíveis para a raiz.

Validação de ambiente

Com o Perl, e a chave de acesso e a chave secreta instaladas em cada nó, é possível validar a configuração do desempatador de nuvem. Execute o comando a seguir no primeiro nó com privilégios de administrador:

/usr/sbin/rsct/bin/samtb_cld

Qualquer erro indica que os pré-requisitos estão ausentes. Corrija quaisquer erros e, em seguida, execute novamente o comando de validação acima. Você não deverá prosseguir até que a validação seja feita sem erro.

Da mesma forma, valide o outro nó.

Configurando o desempatador de cluster na nuvem

Depois de validar o recurso do desempatador de nuvem e assegurar-se de que ele esteja configurado corretamente em cada um dos dois nós no cluster, execute a sequência de três comandos a seguir em qualquer nó com privilégios de administrador.

Nota: É necessário executar esses comandos apenas uma vez em qualquer nó do cluster.

Execute o seguinte comando:

export CT_MANAGEMENT_SCOPE=2

Execute o comando a seguir com privilégios de administrador para criar um recurso desempatador e para nomear o objeto CloudTB1:

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

Execute o comando a seguir para configurar o desempatador ativo para o cluster atual. Esse comando configura o objeto desempatador recém-criado denominado CloudTB1 como o desempatador ativo:

chrsrc -c IBM.PeerNode OpQuorumTieBreaker=CloudTB1

Assegure-se de que os três comandos sejam executados sem erro. Após a execução dos comandos acima, o cluster de dois nós tem um desempatador de tipo 'cloud'. Execute o comando a seguir para validar a configuração do desempatador:

lsrsrc -c IBM.PeerNode OpQuorumTieBreaker

A saída deve ser semelhante à tela a seguir:

Essa saída indica que o desempatador recém-criado CloudTB1 está ativo no cluster.

Determinação e Análise de Problema

O exemplo a seguir mostra um conteúdo de log do sistema de amostra para um cenário de erro de quebra de amarração desempatador em nuvem em um cluster de dois nós com os logs de nodeha01.

O desempatador de nuvem efetua login nas entradas nativas de recurso SYSLOG definidas afixadas com o seguinte rótulo:

1 samtb_cld

Por exemplo, se o recurso SYSLOG estiver armazenando dados no arquivo /var/log/messages nessa máquina, será possível ver todas as entradas registradas pelo desempatador de nuvem executando o comando a seguir:

cat /var/log/messages | grep samtb_cld

As entradas de maior interesse são aquelas que indicam que o quórum foi atingido. Você deverá ver mensagens semelhantes à tela a seguir no SYSLOG, especificamente em casos em que o desempatador de nuvem é capaz de adquirir o dispositivo de quorum:

```
Feb 19 15:59:03 nodeha01 samtb_cld[7203]:
*****INF0: tryReserve: returning 0
Feb 19 15:59:03 nodeha01 samtb_cld[7203]:
*****INF0: op=reserve rc=0 log=1
Feb 19 15:59:03 nodeha01 samtb_cld[7203]:
*****INF0: 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
```

Substituindo o Quorum Operacional

Substitua o estado de quorum operacional se não houver nós suficientes para alguma vez atingir um quorum operacional.

Para remover nós do cluster, pelo menos um nó do cluster deve estar online para iniciar o comando **rmrpnode**. O quorum operacional é necessário para executar esse comando. Se não houver nós suficientes para atingir o quorum operacional, não será possível ajustar o tamanho do cluster para restabelecer o quorum.

Se, por qualquer motivo, a função de quorum operacional precisar ser desativada, o atributo persistente OpQuorumOverride deverá ser configurado para 1:

chrsrc -c IBM.PeerNode OpQuorumOverride=1

Nesse caso , o Estado do quorum operacional sempre será HAS_QUORUM e a proteção de recurso não estará mais assegurada.

Configurando o Adaptador de Automação de Ponta a Ponta

Se desejar integrar um domínio do System Automation for Multiplatforms no ambiente de automação de ponta a ponta do System Automation Application Manager, deve-se configurar o adaptador de automação.

Para integrar um domínio do System Automation for Multiplatforms ao ambiente de automação de ponta a ponta do System Automation Application Manager, as condições a seguir se aplicam:

- Nomes de objetos do System Automation for Multiplatforms. Por exemplo, nomes de grupos, nomes de recursos e descrições não devem conter os caracteres a seguir:
 - ": Aspas duplas
 - ': Aspas simples
 - ; : Ponto e vírgula
 - \$: Sinal de dólar
 - /:Barra
- Nomes de domínios do System Automation for Multiplatforms devem ser exclusivos dentro do escopo de domínios de automação que se conectam ao mesmo gerenciador de automação de ponta a ponta.

Figura 13 na página 73 mostra o ambiente no qual o adaptador de automação de ponta a ponta opera e o que precisa ser configurado para o adaptador de automação de ponta a ponta:



Figura 13. Visão geral do ambiente do adaptador de automação de ponta a ponta em um cluster do System Automation for Multiplatforms

Para integrar um domínio do System Automation for Multiplatforms no ambiente de automação de ponta a ponta do System Automation Application Manager, o produto System Automation Application Manager deve ser instalado. Para obter mais informações sobre o gerenciamento de automação de ponta a ponta, consulte o *Guia do Administrador e do Usuário do System Automation for Multiplatforms*.

Iniciando o diálogo de configuração do adaptador de automação de ponta a ponta

Use o comando cfgsamadapter para iniciar o diálogo de configuração.

Sobre Esta Tarefa

Nota:

- 1. O utilitário cfgsamadapter é um aplicativo do X Window System e deve ser usado a partir de uma estação de trabalho com recursos do servidor do X Window System. Os pacotes de instalação do X11 é necessária para executar o diálogo de configuração. Em alguns sistemas operacionais, esses pacotes estão contidos na mídia de distribuição, mas não fazem parte da instalação padrão.
 - Instale a versão de 32 bits dos pacotes de instalação do X11 nos sistemas operacionais AIX e Linux, em que a versão de 32 bits do System Automation for Multiplatforms está instalado.
 - Instale a versão de 64 bits dos pacotes de instalação do X11 nos sistemas operacionais Ubuntu e Linux, em que a versão de 64 bits do System Automation for Multiplatforms está instalado.
- Nos sistemas AIX, o requisito a seguir deve ser atendido para a instalação do adaptador de automação de ponta a ponta: O pacotes de SSL/SSH devem ser instalados e o subsistema sshd deve estar em execução para poder concluir a tarefa Replicação da configuração do adaptador.
- 3. Também é possível configurar o adaptador de automação de ponta a ponta em modo silencioso, usando um arquivo de propriedades de entrada. Se não houver um servidor X11 disponível, a configuração silenciosa será o único método suportado nesse sistema. Para obter informações adicionais, consulte "Configurando no Modo Silencioso" na página 82.

4. Para usar o diálogo de configuração, efetue logon no sistema com o ID do usuário root ou deve-se ter acesso de gravação aos diretórios /etc/opt/IBM/tsamp/sam/cfg e /etc/Tivoli.

Insira o comando **cfgsamadapter** para iniciar o diálogo de configuração do adaptador Tivoli System Automation. A janela principal do diálogo é exibida:

🍰 Tivoli System Autor	mation for Multiplatforms Adapter Configuration
Adapter configu	ration
Configure	Configure the automation adapter
Replicate	Replicate configuration files to other nodes in the domain
Control	Control the automation adapter and event or data publishers
	Done Help

Figura 14. Janela principal do diálogo de configuração do adaptador de automação de ponta a ponta

Tarefas de configuração:

- 1. Configure o adaptador de automação de ponta a ponta (consulte a página <u>"Definindo as Configurações</u> do Adaptador de Automação" na página 74)
- 2. Replique os arquivos de configuração do adaptador de automação de ponta a ponta para outros nós (consulte a página <u>"Replicando os Arquivos de Configuração do adaptador de automação de ponta a</u> ponta" na página 81)
- 3. Controle o adaptador de automação e publicadores de eventos ou dados. Inicie ou pare o adaptador de automação de ponta a ponta, o publicador de eventos Tivoli Netcool/OMNIbus ou o publicador de dados do relatório. Para obter informações adicionais sobre o adaptador e os publicadores, veja Guia do Administrador e do Usuário do System Automation for Multiplatforms.

Definindo as Configurações do Adaptador de Automação

Na janela principal do diálogo de configuração, clique em **Configurar** para exibir as guias de configuração descritas nas seções a seguir.

Sobre Esta Tarefa

Guia do adaptador

Use a guia Adaptador para configurar o host do adaptador.

Campos e controles na guia Adaptador:

Nome do Host ou Endereço IP

Nome do host do nó em que o adaptador é executado. O nome do host local é usado como valor padrão. Se desejar usar um valor diferente do nome do host local, limpe a caixa de seleção **Usar nome do host local** para ativar o campo de entrada para edição. Por exemplo, se você estiver usando uma segunda rede.

Impacto na replicação do arquivo de configuração: Se você usar o nome do host local, a função **Replicar** assegura que o respectivo nome do host local seja usado em cada nó de destino de replicação. Se você especificar um nome do host ou endereço IP diferente, a função **Replicar** replicará este valor para os outros nós no cluster. Neste caso, configure o host do adaptador em cada nó separadamente, se não desejar que o mesmo valor seja usado em todos os nós. Para obter informações adicionais, consulte <u>"Replicando os Arquivos de Configuração do adaptador de</u> automação de ponta a ponta" na página 81.

Número da porta de solicitações

Especifique o número da porta na qual o adaptador atende solicitações do host de gerenciamento de automação de ponta a ponta. A porta padrão é 2001.

Local do conjunto de políticas

Especifique o nome do caminho qualificado do diretório que contém os arquivos de políticas XML. Se você estiver usando o System Automation Application Manager para ativar uma política de automação do System Automation for Multiplatforms, o conjunto de políticas será necessário. Definir e criar o diretório do conjunto de políticas em todos os nós do cluster. Esse parâmetro é opcional.

Clique em Avançado para especificar o comportamento de tempo de execução do adaptador:

Retardo de Parada do Adaptador

Defina o período de tempo medido em segundos. A parada do adaptador será atrasada nesse período de tempo para permitir que o adaptador entregue adequadamente o evento de saída do domínio. O valor-padrão é 5. É possível aumentar o valor em sistemas lentos. O valor varia entre 3 e 60 segundos.

Intervalo de Atividades do Contato Remoto

Defina o período de tempo que é medido em segundos após o qual o adaptador parará se ele não tiver sido contatado pelo host de gerenciamento de automação de ponta a ponta. O host contata periodicamente o adaptador para verificar se ele ainda está em execução. O valor-padrão é 360. Se um valor diferente de 0 for especificado, o intervalo deverá ser um múltiplo do intervalo de verificação.

Quando o valor estiver configurado como 0, o adaptador será executado continuamente e nunca será interrompido.

Intervalo de Novas Tentativas do Contato Inicial

Defina o período de tempo medido em minutos. O adaptador tenta nesse período de tempo entrar em contato com o host de gerenciamento de automação de ponta a ponta até que seja bem-sucedido ou o tempo especificado decorra. O valor padrão é 0, o que significa que o adaptador tenta entrar em contato com o host de gerenciamento de automação de ponta a ponta indefinidamente.

Ativar armazenamento em cache de eventos EIF

Selecione essa caixa de seleção para ativar o armazenamento em cache de eventos.

Intervalo de Tentativas de Reconexão do EIF

Defina o período de tempo medido em segundos. O adaptador irá esperar antes de tentar restabelecer a conexão com o host de gerenciamento de automação de ponta a ponta após a conexão ter sido interrompida. O valor-padrão é 30.

Guia Host que Usa o Adaptador

Use a guia Host que Usa o Adaptador para configurar o host do gerenciador de automação de ponta a ponta ao qual o adaptador se conecta.

Campos na guia Host que Usa o Adaptador:

Nome do host ou endereço IP

O nome ou o endereço IP do host em que o gerenciador de automação de ponta a ponta é executado.

Host alternativo

Um valor para esse campo é opcional. Se você definiu uma configuração de recuperação de desastre com dois sites diferentes para o System Automation Application Manager, o gerenciador de automação de ponta a ponta poderá ser executado em qualquer site. Para suportar essa configuração, especifique também o nome do host ou endereço IP do segundo site. No caso de uma comutação de site do Application Manager, isso assegurará que o adaptador seja alternado diretamente para a nova instância ativa do gerenciador de automação de ponta a ponta como o destino para enviar eventos.

Número da Porta de Eventos

A porta na qual o gerenciador de automação de ponta a ponta recebe eventos do adaptador de automação. O número da porta especificado aqui deve corresponder ao número da porta especificado como o número da porta do evento ao configurar o domínio do gerenciador de automação de ponta a ponta. A porta padrão é 2002.

Nota: Se a comunicação entre o adaptador de automação de ponta a ponta e o host de gerenciamento de automação de ponta a ponta usar IPv6, as seguintes restrições serão aplicadas.

Para a comunicação do adaptador com o host que usa o adaptador:

- 1. Se um nome de host IPv6 for especificado na configuração do host de gerenciamento de automação de ponta a ponta, o servidor DNS deverá ser configurado para retornar apenas registros IPv6.
- 2. Se o servidor DNS estiver configurado para retornar registros IPv4 e IPv6, apenas o endereço IPv4 será usado. Caso deseje usar IPv6, especifique explicitamente o endereço IPv6 em vez do nome do host na configuração do host de gerenciamento de automação de ponta a ponta.

Para a comunicação do host de gerenciamento de automação de ponta a ponta com o adaptador:

- 1. Se um nome do host IPv6 for especificado na configuração do host do adaptador, o servidor DNS deverá ser configurado para retornar apenas registros IPv6.
- 2. Se o servidor DNS estiver configurado para retornar registros IPv4 e IPv6, apenas o endereço IPv4 será usado. Caso queira usar IPv6, especifique explicitamente o endereço IPv6 em vez de o nome do host na configuração do host do adaptador.

Use o comando host -n -a <nome_do_host_ipv6> para verificar os registros de consulta do DNS.

Guia Relatório

Use a guia Relatório para definir as configurações para coletar dados do relatório no banco de dados do System Automation Application Manager.

Após configurar o banco de dados de relatório, é necessário iniciar o publicador de dados do relatório.

Nota:

- 1. A função de relatório, como a geração de relatórios, é fornecida como parte do produto System Automation Application Manager até a versão 3.2.2.
- 2. Certifique-se de desativar o relatório antes de desinstalar o System Automation Application Manager do host de gerenciamento de automação de ponta a ponta.

Instalações do banco de dados local do System Automation Application Manager são descartadas durante a desinstalação. Nesse caso, pare o publicador de dados do relatório.

Para iniciar ou parar o publicador de dados do relatório, consulte *Guia do Administrador e do Usuário do System Automation for Multiplatforms* ou use os comandos a seguir:

samctrl -e JDBC or samctrl -d JDBC

Se desejar coletar dados do relatório no banco de dados DB2 do System Automation Application Manager, selecione a caixa de seleção **Ativar coleta de dados do relatório**. Caso contrário, cancele a seleção da caixa de seleção, que desativa os campos de entrada nessa guia.

Campos na guia Relatório:

Nome ou endereço IP do servidor DB2

O nome do host ou o endereço IP do servidor DB2 que hospeda o banco de dados de dados do relatório. A função de relatório real, como a geração de relatórios, é fornecida como parte do produto System Automation Application Manager. O servidor DB2 deve ser o mesmo sistema no qual o banco de dados DB2 do System Automation Application Manager está localizado.

Se você omitir esse valor, o valor que você especifica para o host do System Automation Application Manager na guia **Host usando adaptador** é usado como o padrão. Se estiver usando um DB2 remoto para o banco de dados do System Automation Application Manager, especifique o nome do host ou endereço IP desse sistema DB2 remoto.

Nota: Se o servidor DB2 for executado no z/OS, certifique-se de que o arquivo db2jcc_license_cisuz.jar esteja disponível em cada nó em seu cluster do System Automation for Multiplatforms. Esse arquivo contém a licença para se conectar ao DB2 no z/OS a partir do sistema não z/OS.

É possível localizar esse arquivo no diretório do WebSphere Application Server que é usado para o System Automation Application Manager. Procure na seguinte árvore de diretórios o arquivo:

<WAS_INSTALL_ROOT>/deploytool/itp/plugins

Copie o arquivo para o diretório /opt/IBM/tsamp/sam/lib em cada nó no cluster do System Automation for Multiplatforms. Certifique-se de que você tenha um contrato de licença do DB2.

Servidor DB2 alternativo

Um valor para esse campo é opcional. Se você definiu um configuração de recuperação de desastre com dois sites diferentes para o System Automation Application Manager, o gerenciador de automação de ponta a ponta poderá ser executado em qualquer site. Para suportar essa configuração, especifique o nome do host ou endereço IP do System Automation Application Manager no segundo site neste campo. No caso de uma alternação de site do Application Manager, o adaptador alterna automaticamente para a nova instância ativa do gerenciador de automação de ponta a ponta como o destino para dados do relatório coletados. Os valores de todas as configurações a seguir são usados para ambos os servidores DB2. Se o banco de dados estiver no mesmo sistema que o gerenciador de automação de ponta a ponta, especifique o mesmo valor que você usou para o host alternativo do System Automation Application Manager que está usando o adaptador.

Se estiver usando um DB2 remoto para o banco de dados do System Automation Application Manager, deixe este campo vazio.

Nota: Se você especificar um servidor DB2 alternativo, será necessário configurar o recurso Nova Rota do Cliente Automática do DB2. Em seguida, a função de relatório é ativada para sempre alimentar os dados do relatório para a instância primária do DB2 HADR. Consulte a documentação do DB2 para obter uma descrição de como configurar este recurso.

Exemplo:

O DB2 HADR é configurado para o banco de dados eautodb nos dois hosts lnxcm5x e lnxcm6x. A porta do DB2 é 50000 nos dois hosts. Para configurar a Nova Rota do Cliente Automática para os dois hosts, execute os seguintes comandos:

• No lnxcm5x:

db2 update alternate server for database eautodb using host name ${\tt lnxcm6x}$ port 50001

• No lnxcm6x:

db2 update alternate server for database eautodb using host name $\tt lnxcm5x$ port 50001

Nome do banco de dados DB2

O nome do banco de dados DB2 do System Automation Application Manager, em que os dados do relatório estão armazenados.

Nome do esquema do DB2

O nome do esquema que é usado para as tabelas de banco de dados em que os dados do relatório são armazenados. Altere o valor desse parâmetro somente se o banco de dados DB2 do System Automation Application Manager estiver em um sistema z/OS. Você pode precisar controlar o nome do esquema para identificar exclusivamente as tabelas de banco de dados na sua instalação do DB2.

Porta do DB2

O número da porta que é usado para acessar o banco de dados DB2 do System Automation Application Manager, em que os dados do relatório são armazenados. A porta padrão é 50001.

ID do Usuário

O ID do usuário que é usado para acessar o banco de dados DB2 do System Automation Application Manager, em que os dados do relatório são armazenados.

Senha

A senha que é usada para acessar o banco de dados DB2 do System Automation Application Manager, em que os dados do relatório são armazenados.

Clique em Alterar para alterar a senha.

Nota: Assegure que você atualize a senha configurada sempre que a senha do banco de dados DB2 for alterada. Se a senha configurada não corresponder à senha do banco de dados DB2, os eventos não são gravados no banco de dados.

Guia Publicação de Eventos

Use a guia **Publicação de eventos** para definir configurações para publicar eventos EIF no Tivoli Netcool/ Omnibus.

Controles e campos na guia Publicação de eventos:

Publicação de eventos do OMNIbus

Ativar publicação de eventos EIF do OMNIbus

Selecione esta caixa de seleção se desejar que os eventos EIF sejam enviados para o host no qual o OMNIbus Probe for Tivoli EIF está em execução. Se a caixa de seleção não for selecionada, todos os outros campos nesta guia serão desativados. Se você ativar ou desativar a publicação de eventos EIF, certifique-se de iniciar ou parar o publicador de eventos correspondente. Para iniciar ou parar o publicador de eventos EIF, consulte *Guia do Administrador e do Usuário do System Automation for Multiplatforms* ou use os seguintes comandos:

samctrl -e TEC or samctrl -d TECs

Nota: Por razões de compatibilidade, como alternativa, um servidor e porta do Tivoli Enterprise Console ainda podem ser configurados.

Servidor de eventos

Nome do Host ou Endereço IP

O nome do host ou endereço IP do host onde o OMNIbus Probe for Tivoli EIF está em execução. É possível especificar até oito valores, que são separados por vírgulas. O primeiro local é o servidor de eventos principal, enquanto outros são servidores secundários a serem usados na ordem especificada quando o servidor principal está inativo.

Número da Porta

O número da porta que é usado pelo OMNIbus Probe for Tivoli EIF para atender eventos EIF. Se você usar o mapeamento de porta, será possível especificar 0 como o número da porta.

Filtro de eventos

Publique eventos EIF que são causados por:

Mudanças na configuração de relacionamentos

Selecione essa caixa de seleção se desejar que todos os eventos EIF causados por inclusão, remoção e mudança de relacionamentos a serem enviados para o servidor de eventos. Caso contrário, os eventos de mudança na configuração para relacionamentos são filtrados.

Mudanças na configuração de recursos

Selecione essa caixa de seleção se desejar que todos os eventos EIF causados por inclusão, remoção e mudança de recursos sejam enviados para o servidor de eventos. Caso contrário, os eventos de mudança na configuração para recursos são filtrados.

Incluindo e removendo solicitações

Selecione essa caixa de seleção se desejar que os eventos EIF causados por inclusão e remoção de solicitações a serem enviados para o servidor de eventos. Caso contrário, os eventos para incluir e remover solicitações serão filtrados.

Mudanças de status de recurso

Selecione essa caixa de seleção se desejar que os eventos EIF relacionados a mudanças de status do recurso sejam enviados para o servidor de eventos. Caso contrário, todos os eventos de mudança de status do recurso são filtrados. Dependendo da gravidade, selecione um dos botões de opções para definir quais eventos de mudança de status são publicados.

Definindo filtros adicionais:

Os filtros de eventos que podem ser ativados ou desativados nesta guia são os filtros predefinidos que estão incluídos com o System Automation for Multiplatforms. Se deseja definir filtros adicionais, modifique manualmente o arquivo de propriedades de configuração correspondente:

/etc/Tivoli/TECPublisher.conf

Se desejar editar um filtro predefinido, inclua um filtro e desative o filtro predefinido. Se as mudanças na configuração forem aplicadas pelo utilitário de configuração cfgsamadapter, quaisquer filtros incluídos serão preservados.

Guia Segurança

Use a guia **Segurança** para configurar a segurança da interface entre o host que usa o adaptador e o host de gerenciamento de ponta a ponta.

Selecione **Ativar SSL** se desejar usar o protocolo Secure Socket layer (SSL) para a comunicação entre o adaptador de automação e o host que usa o adaptador. Se marcada, os seguintes campos de entrada deverão ser preenchidos.

Controles e campos na guia Segurança:

Truststore

Nome do arquivo de armazenamento confiável que é usado para SSL. O nome do arquivo pode conter diversos caracteres de ponto. Clique em **Pesquisar** para selecionar um arquivo.

Keystore

Nome do arquivo keystore é usado para SSL. O nome do arquivo pode conter diversos caracteres de ponto. Clique em **Pesquisar** para selecionar um arquivo.

Senha do Keystore

Arquivo de senha do armazenamento de chave. Clique em Alterar para alterar a senha.

Nota: Se o truststore estiver em um arquivo diferente do keystore, as senhas para os arquivos deverão ser idênticas.

Alias de certificado

O nome alternativo do certificado a ser usado pelo servidor.

Forçar Autenticação do Usuário

Selecione a caixa de seleção **Forçar Autenticação do Usuário** para permitir a autenticação do usuário com o Pluggable Access Module (PAM).

Se você usar o System Automation Application Manager para manter também as políticas XML do System Automation for Multiplatforms, será necessário ativar **Aplicar autenticação do usuário**.

Serviço PAM

Nome do serviço Pluggable Access Module que determina quais verificações são feitas para validar os usuários, dependendo do sistema operacional em que o adaptador está em execução.

- Para qualquer distribuição SUSE Linux, um arquivo no diretório /etc/pam.d
- Para qualquer distribuição RedHat Linux, uma entrada no arquivo /etc/pam.conf
- Para o AIX, uma entrada no arquivo /etc/pam.conf

Guia Criador de Logs

Use a guia Criador de Logs para especificar as configurações para criação de log, rastreio e Primeira Captura de Dados com Falha. É possível alterar as configurações permanente ou temporariamente.

A guia Criador de Logs exibe os valores que estão configurados atualmente no arquivo de configuração.

Na guia Criador de Logs, é possível executar as seguintes tarefas:

Alterar as configurações permanentemente

Execute essas etapas:

- 1. Faça as mudanças necessárias na guia.
- 2. Clique em Salvar.

Resultados: As configurações no arquivo de configuração são atualizadas. Reinicie o adaptador para que as mudanças entrem em vigor.

Alterar as configurações temporariamente

Execute estas etapas depois de assegurar-se de que o adaptador esteja em execução:

- 1. Faça as mudanças necessárias na guia.
- 2. Clique em Aplicar.

Resultados: As novas configurações entram em vigor imediatamente. Elas não são armazenadas no arquivo de configuração. Se o adaptador não estiver em execução, você receberá uma mensagem de erro.

Reverter para as configurações permanentes

Se você tiver alterado as configurações temporariamente, execute as seguintes etapas para reverter para as configurações permanentes definidas no arquivo de configuração, ou quando não tiver certeza de quais configurações estão ativas atualmente para o adaptador:

- 1. Chame o diálogo de configuração e abra a guia Criador de Logs. A guia Criador de Logs exibe os valores que estão configurados atualmente no arquivo de configuração.
- 2. Clique em Aplicar para ativar as configurações.

Resultados: As configurações entram em vigor imediatamente. Se o adaptador não estiver em execução, você receberá uma mensagem de erro.

Controles e campos na guia Criador de logs:

Tamanho máximo do arquivo de log/rastreio

O uso máximo de disco em KB que um arquivo de log pode atingir. Se o limite for atingido, outro arquivo de log será criado. O número máximo de arquivos de log é dois, o que significa que o arquivo menos recente será sobrescrito após ambos os arquivos serem preenchidos. O tamanho máximo do arquivo padrão é 1024 KB.

Nível de criação de log de mensagem

Selecione o **Nível de criação de log de mensagem**, dependendo da gravidade das mensagens que deseja registrar.

Nível de criação de logs de rastreio

Selecione o **Nível de criação de log de rastreio,** dependendo da gravidade dos incidentes que você deseja que sejam registrados.

Nível de gravação da primeira captura de dados com falha (FFDC)

Selecione o nível de registro FFDC, dependendo da gravidade dos incidentes para o qual você deseja que dados FFDC sejam coletados.

Espaço em disco máximo da primeira captura de dados com falha (FFDC)

Especifique o espaço máximo em disco em bytes usado pelos rastreios de FFDC, que são gravados no diretório de rastreio de FFDC. O espaço padrão é de 10485760 bytes (10 MB).

Política de espaço excedido da primeira captura de dados com falha (FFDC)

Selecione uma das opções:

Ignorar

Emita um aviso, mas não aplique a limitação de espaço em disco de FFDC.

Exclusão automática

Excluir automaticamente os arquivos FFDC para aplicar a limitação de espaço em disco de FFDC. Esse é o valor padrão da política de espaço excedido.

Suspender

Pare as ações adicionais de FFDC até que o espaço em disco seja liberado manualmente.

Modo de filtro de ID de mensagem da primeira captura de dados com falha (FFDC)

Selecione uma das opções:

Intermediário

Todos os eventos de log com mensagens que estiverem especificados na lista de IDs de mensagens passam pelo filtro e os dados de FFDC são gravados. Esse é o modo de filtro padrão.

Bloquear

Todos os eventos de log com mensagens que estiverem especificados na lista de IDs de mensagens são bloqueados.

Lista de IDs de mensagem da primeira captura de dados com falha (FFDC)

Os IDs de mensagem que controlam para quais eventos de log os dados de FFDC são gravados, dependendo do modo de filtro. A comparação de IDs de mensagem faz distinção entre maiúsculas e minúsculas. Cada ID de mensagem deve ocorrer em uma nova linha. Caracteres curinga, por exemplo, *E para todas as mensagens de erro, são permitidos.

Salvando a Configuração

Clique em **Salvar** na janela de configuração para salvar as mudanças nos arquivos de configuração do adaptador.

Sobre Esta Tarefa

Se houver entradas ausentes ou um valor estiver fora do intervalo, por exemplo, um número da porta, será exibida uma mensagem de erro. Após conclusão bem-sucedida, a janela de status de atualização da configuração aparece, mostrando a lista de arquivos de configuração e seus status de atualização. Reinicie o adaptador para que as mudanças sejam efetivadas.

Replicando os Arquivos de Configuração do adaptador de automação de ponta a ponta

Replique os arquivos de configuração do adaptador de automação de ponta a ponta para outros nós no domínio.

Sobre Esta Tarefa

Clique em **Replicar** na janela principal do diálogo de configuração (veja <u>"Iniciando o diálogo de</u> configuração do adaptador de automação de ponta a ponta " na página 73). A janela **Replicar arquivos de configuração** é exibida.

Distribua (replique) os arquivos de configuração do adaptador de automação para os nós restantes no domínio do mesmo nível RSCT:

- 1. Selecione os arquivos de configuração que você deseja replicar ou clique em **Selecionar todos** para selecionar todos os arquivos de configuração da lista.
 - Se (1) o arquivo sam. adapter.ssl.properties estiver entre os arquivos selecionados e (2) os arquivos de armazenamento confiável e keystore SSL que você configurou na guia **Segurança** da configuração de adaptador existirem no nó de origem de replicação, esses arquivos de armazenamento confiável e keystore são replicados.
 - Assegure que o diretório onde os arquivos estão no nó de origem de replicação também exista em todos os nós de destino.
- 2. Clique em **Selecionar todos** abaixo da lista de nós de destino de replicação para assegurar que a configuração do adaptador seja idêntica em todos os nós.
- 3. Digite o ID do usuário e a senha dos nós de destino para os quais você deseja replicar os arquivos.
- 4. Inicie a replicação clicando em **Replicar**.

A replicação pode demorar um pouco. Enquanto os arquivos estão sendo replicados, o botão **Replicar** é indentado e esmaecido. Quando a replicação é concluída, o status de replicação de cada arquivo de configuração é exibido.

Tornando o Adaptador de Automação de Ponta a Ponta Altamente Disponível

Se o cluster do Tivoli System Automation consistir em mais de um nó, o adaptador de automação de ponta a ponta deverá ser mantido altamente disponível.

Sobre Esta Tarefa

A comunicação com o Operations Console do System Automation Application Manager permanece ativa durante indisponibilidades do nó ou manutenção do nó no cluster.

Conforme ilustrado em <u>"Configurando o Adaptador de Automação de Ponta a Ponta" na página 72,</u> o adaptador de automação está conectado ao nó principal do System Automation. A infraestrutura de cluster assegura que o principal esteja sempre disponível e, portanto, o adaptador também está implicitamente sempre disponível no nó principal. Não é necessária configuração de política de automação para tornar o adaptador altamente disponível a partir da versão 4.1.0.0 do System Automation for Multiplatforms.

Configurando no Modo Silencioso

É possível configurar o adaptador de automação de ponta a ponta usando a configuração silenciosa.

Na ferramenta de configuração no modo silencioso, é possível configurar o adaptador de automação de ponta a ponta sem iniciar o diálogo de configuração. Nesse caso, você não precisa ter uma sessão do X Window disponível.

Configure o adaptador de automação de ponta a ponta editando valores de parâmetro de configuração em um arquivo de propriedades associado. Se você usar o modo de configuração silenciosa, você não precisa ter uma sessão do X Window disponível.

Deve-se primeiro iniciar a ferramenta de configuração para gerar um arquivo de propriedades de entrada do modo silencioso processar uma atualização da configuração. Para obter informações adicionais, consulte "Configurando o Adaptador de Automação de Ponta a Ponta" na página 72.

Trabalhando no Modo Silencioso

Saiba mais sobre as tarefas principais se você trabalhar no modo de configuração silenciosa.

Para usar a ferramenta de configuração no modo silencioso, é necessário seguir estas etapas para cada componente que você deseja configurar:

- 1. Gerar ou localizar os arquivos de propriedades de entrada no modo silencioso. Consulte <u>"Arquivo de</u> Propriedades de Entrada no Modo Silencioso" na página 83.
- 2. Editar os valores de parâmetros no arquivo. Consulte <u>"Editando o Arquivo de Propriedades de Entrada"</u> na página 84.
- 3. Inicie a ferramenta de configuração no modo silencioso para atualizar os arquivos de configuração de destino, veja "Iniciando a configuração silenciosa" na página 83.
- 4. Se a ferramenta de configuração não for concluída com sucesso, lide com os erros que forem relatados (veja "Saída no Modo Silencioso" na página 84) e inicie a ferramenta de configuração novamente.

Para algumas tarefas, nenhum suporte à configuração silenciosa está disponível. Se você não deseja usar os diálogos de configuração, deve-se processar essas tarefas manualmente. Para obter informações adicionais, consulte "Tarefas de Configuração a Serem Executadas Manualmente" na página 82.

Tarefas de Configuração a Serem Executadas Manualmente

Algumas tarefas de configuração que são chamadas no modo de diálogo clicando no botão de comando correspondente na janela da barra de ativação não são suportadas no modo de configuração silenciosa.

Se não desejar usar o diálogo de configuração, será necessário executar as seguintes tarefas manualmente:

1. Replicar os arquivos de configuração

Se o domínio do System Automation for Multiplatforms consistir em mais de um nó, replique manualmente os arquivos de configuração do adaptador de automação de ponta a ponta para os outros nós no domínio do System Automation for Multiplatforms. Replique os arquivos de configuração, executando a ferramenta de configuração no modo silencioso com arquivos de propriedades de entrada idênticos em cada nó no domínio.

2. Controlar o adaptador de automação e publicadores

- Use o comando samadapter {start|stop} para iniciar ou parar o adaptador de automação de ponta a ponta.
- Use o comando samctrl {-e|-d} TEC para iniciar ou parar o publicador de eventos do Tivoli Netcool/OMNIbus.
- Use o comando samctrl {-e|-d} JDBC para iniciar ou parar o publicador de dados do relatório.

Iniciando a configuração silenciosa

Use o comando **cfgsamadapter** -**s** para iniciar a configuração silenciosa.

Inicie a configuração silenciosa para o adaptador de automação de ponta a ponta:

- Para usar a ferramenta de configuração do adaptador do System Automation em modo silencioso, deve-se ter acesso de gravação aos diretórios /etc/opt/IBM/tsamp/sam/cfg e /etc/Tivoli.
- Insira o comando cfgsamadapter -s

Para obter informações adicionais sobre o comando cfgsamadapter, veja *Tivoli System Automation para Multiplataformas Referência*.

Arquivo de Propriedades de Entrada no Modo Silencioso

Gere um arquivo de propriedades de entrada no modo silencioso a partir de valores que estão atualmente configurados. Use o arquivo para modificar definições de configuração no modo silencioso.

Gere os arquivos de propriedades de entrada no modo silencioso a partir de valores que estão definidos atualmente nos arquivos de configuração de destino correspondentes. As vantagens são:

- É possível gerar arquivos de propriedades imediatamente após a instalação e antes de começar a customizar.
- Se você customizar com o diálogo de configuração e no modo silencioso, é possível primeiro gerar um arquivo de entrada atualizado antes de aplicar as mudanças no modo silencioso
- É possível recuperar-se com facilidade da exclusão acidental do arquivo de propriedades de entrada no modo silencioso

Para gerar um arquivo de propriedades de entrada do modo silencioso, use uma das opções a seguir quando você iniciar a configuração silenciosa:

-g

Gere o arquivo de propriedades de entrada somente se ele não existir.

-gr

Gere o arquivo de propriedades de entrada e substitua-o se ele existir.

-l location

O arquivo de propriedades de entrada para a configuração silenciosa está no diretório especificado com *location*. Se -1 for omitido, o arquivo de propriedades de entrada está no diretório padrão /etc/opt/IBM/tsamp/sam/cfg.

Tabela 23. Arquivos de propriedades de entrada gerados		
Comando de configuração	Arquivo de propriedades de entrada silenciosa	
cfgsamadapter -s -g -gr	/etc/opt/IBM/tsamp/sam/cfg/ silent.samadapter.properties	
cfgsamadapter -s -g -gr -l location	<i>location</i> /silent.samadapter.properties	

Capítulo 3. Configurando 83

Se você atualizar as definições de configuração no modo silencioso, o arquivo de propriedades silencioso será usado como entrada para a tarefa de atualização. Se desejar que o utilitário de configuração recupere o arquivo de entrada de um local diferente do diretório /etc/opt/IBM/tsamp/sam/cfg, use a opção **-1** *location*.

Editando o Arquivo de Propriedades de Entrada

Modifique os valores no arquivo de propriedades de entrada para alterar a configuração no modo silencioso.

Os arquivos de propriedades de entrada gerados para cada um dos componentes contêm pares de palavra-chave/valor do parâmetro de configuração. Para facilitar o máximo possível alternar entre os modos e minimizar erros ao editar o arquivo de propriedades, a estrutura, a terminologia e o texto que é usado no arquivo de propriedades do modo silencioso idêntico à estrutura, terminologia e texto do diálogo de configuração.

Os nomes de guias, por exemplo, **Adaptador**, ou botões, por exemplo, **Avançado. . .**, no diálogo de configuração são usados como identificadores no arquivo de propriedades, por exemplo:

Cada nome de campo no diálogo de configuração, por exemplo, **Número da porta de solicitação**, está contido no arquivo de propriedades. Uma breve descrição e a palavra-chave para esse campo é incluída, por exemplo:

```
#
# ... Número da porta de solicitações
# Porta do adaptador de automação para receber solicitações do host usando
# o adaptador
adapter-request-port=2001
#
```

Para editar o arquivo de propriedades, localize a palavra-chave associada ao valor que você deseja alterar e sobrescrever o valor.

Se você configurar o valor de uma palavra-chave necessária para em branco ou comentar a palavrachave, o valor que é definido no arquivo de configuração de destino permanecerá inalterado.

Nota:

- 1. Se uma palavra-chave for especificada várias vezes, o valor da última ocorrência no arquivo será usado.
- 2. Cada valor deve ser especificado em uma única linha.

Saída no Modo Silencioso

Inspecione a saída que é gerada pela ferramenta de configuração no modo silencioso.

Iniciar a ferramenta de configuração no modo silencioso leva à saída que corresponde mais estritamente à saída que é exibida pelo diálogo de configuração. Os tipos a seguir de saída podem ser gerados:

Nenhuma atualização

Não há atualizações de configuração a serem salvas. Todos os parâmetros em todos os arquivos de configuração de destino já correspondem aos parâmetros de entrada silenciosa especificados. Nenhum erro foi detectado ao verificar os parâmetros de entrada silenciosa. Se houver informações adicionais disponíveis ou forem detectadas condições de aviso, as informações e avisos serão relatados. Se os avisos forem relatados, a ferramenta de configuração emitirá o código de retorno "1" em vez de "0". Pode ser necessário observar esse comportamento, quando você iniciar a configuração silenciosa, por exemplo, em um shell script.

Conclusão bem-sucedida

Pelo menos um dos arquivos de configuração de destino é atualizado e todos os arquivos de configuração e seus status de atualização são listados. Nenhum erro é detectado ao verificar os parâmetros de entrada silenciosa. Se houver informações adicionais disponíveis ou forem detectadas condições de aviso, as informações e avisos serão relatados. Se os avisos forem relatados, a ferramenta de configuração emitirá o código de retorno "1" em vez de "0". Você pode precisar observar esse comportamento ao iniciar a configuração silenciosa, por exemplo, em um shell script.

Conclusão malsucedida

Nenhum arquivo de configuração de destino é atualizado. Quaisquer erros detectados ao verificar os parâmetros de entrada silenciosa são relatados. A ferramenta de configuração termina quando o código de retorno "2" é retornado.

Geração do arquivo de propriedades de entrada silenciosa

Os valores dos arquivos de configuração de destino são usados para gerar o arquivo de entrada. Nenhum arquivo de configuração de destino é atualizado.

Erro irrecuperável

As mensagens de erro que indicam a razão do erro são relatadas. A ferramenta de configuração termina quando o código de retorno maior que "2" é retornado.

Detectando Falhas da Interface de Rede

Se você estiver executando um cluster de um único nó ou de dois nós, mais configuração é necessária para detectar falhas da interface de rede.

O software de cluster tenta periodicamente entrar em contato com cada interface de rede no cluster. Se a tentativa de contato com uma interface falhar em um nó de um cluster de dois nós, a interface correspondente no outro nó também será sinalizada como offline. Ela é sinalizada como offline porque não recebe uma resposta de seu peer.

Para evitar esse comportamento, o software de cluster deve ser configurado para entrar em contato com uma instância de rede fora do cluster. Você pode usar o gateway padrão da sub-rede na qual a interface se encontra.

Em cada nó, crie o seguinte arquivo:

```
/var/ct/cfg/netmon.cf
```

Cada linha desse arquivo contém o nome do sistema ou o endereço IP da instância de rede externa. Endereços IP podem ser especificados em formato de número com decimal.

Exemplo de um arquivo netmon.cf:

```
#Este é o gateway padrão para todas as interfaces na sub-rede 192.168.1.0
192.168.1.1
# Este é o gateway padrão para todas as interfaces na sub-rede 192.168.2.0
gw.de.ibm.com
```

Usando Ethernet on Power Systems virtualizado

A decisão sobre o estado dos adaptadores de rede é tomada com base em se qualquer tráfego de rede pode ser visto no adaptador local. Por exemplo, se o adaptador local ou remoto está quebrado. O tráfego de rede é refletido pela contagem de bytes de entrada da interface.

Se o Virtual I/O (VIO) estiver envolvido, o teste se tornará não confiável, pois não é possível distinguir se o tráfego de entrada vem do servidor ou cliente VIO. A LPAR não é capaz de distinguir um adaptador virtual de um adaptador real. Para abordar esse problema, a biblioteca netmon suporta até 32 destinos para cada adaptador de rede local. Se for possível executar ping em qualquer um destes destinos, o adaptador local será considerado como ativo. Os destinos podem ser especificados no arquivo netmon.cf com a palavra-chave !REQD.

```
!REQD <owner><target>
```

- ! REQD: Valor de sequência. Nenhum espaço extra. Sempre no início de uma linha.
- <owner>: Especifica a interface. O <owner> monitora o adaptador e determina o status que é baseado em se ele pode executar ping de qualquer um dos destinos que estão definidos em uma linha abaixo do <owner>. O <owner> pode ser especificado como um nome do host, um endereço IP ou um nome da interface. Caso o nome do host ou o endereço IP seja especificado, ele deve fazer referência ao nome inicial ou endereço IP. Nenhum alias de serviço é permitido. Se o nome do host for especificado, ele deverá ser resolvido para um endereço IP ou a linha será ignorada. A palavra-chave !ALL especifica todos os adaptadores.
- <target>: O endereço IP ou o nome do host em que você deseja que o <owner> tenha ping. Um destino de nome do host deve ser resolvido para um endereço IP a ser usado para entradas netmon.cf .

Executando no Linux on System z sob z/VM

Além de criar o arguivo netmon.cf, desative a transmissão para todos os grupos de comunicação quando estiver executando o System Automation for Multiplatforms no Linux on System z em um ambiente z/VM. O mecanismo de pulsação RSCT executa um ping de transmissão de tempos em tempos, especialmente quando um adaptador de interface de rede não está disponível. O propósito deste recurso é descobrir se o adaptador de interface de rede que envia esse ping de transmissão ainda está operacional. Verifique se outros sistemas respondem a esse ping de transmissão ou não. Esse recurso não será necessário se o arquivo netmon. cf estiver configurado corretamente. Nesse caso, há outros adaptadores de interface de rede conhecidos que devem ser verificador para disponibilidade. Embora um ping de transmissão em um sistema independente não represente um problema de desempenho, ele terá um impacto negativo no desempenho, se os sistemas estiverem em execução em um ambiente z/VM. O impacto no desempenho ocorre, porque todos os outros sistemas que estão em execução no z/VM e no mesmo segmento de rede (mesma rede IP e máscara de rede) respondem a esta solicitação de ping de transmissão. Como resultado, mesmo os sistemas guest da VM que estão inativos e atualmente transferidos da memória principal para a secundária são carregados no z/VM apenas para responder a este ping. Dependendo do número de sistemas convidados que estão em execução no z/VM, o desempenho de todo o sistema z/VM pode diminuir.

Para evitar um impacto negativo no desempenho, aplique as mudanças de configuração a seguir:

• Obtenha todos os grupos de comunicação do cluster:

‡ lscomg

• Desative a transmissão para todos os grupos de comunicação:

```
# chcomg -x b <communication group> ...
```

Por exemplo:

chcomg -x b CG1

• Use o comando **1scomg** novamente para verificar se a transmissão está desativada.

Ativando a Pulsação de Disco

É possível ativar a pulsação de disco para assegurar a integridade de dados em ambientes em cluster.

A pulsação de disco diminui a probabilidade de uma divisão de cluster, pois é capaz de distinguir entre uma falha de rede e uma falha do nó.

Uma falha de rede ocorrerá se a conexão de rede entre os nós e de um nó com o disco compartilhado falhar, conforme mostrado em Figura 15 na página 87.



Storage Area Network (SAN)

Figura 15. Falha de rede em um cenário de dois nós com um disco compartilhado

Uma falha de nó ocorre se um nó não estiver mais acessível, conforme mostrado em Figura 16 na página 87.



Storage Area Network (SAN)

Figura 16. Falha do nó em um cenário de dois nós com um disco compartilhado

Se uma divisão de cluster puder ser evitada, nenhuma proteção de recurso crítico será necessária. Os sistemas não precisam ser reinicializados. Os problemas de integridade de dados também são evitados.

Caso ocorra uma divisão de cluster, os nós que perderam acesso ao disco de pulsação também perdem acesso aos dados vitais. A proteção de recurso crítico serve para evitar distorção de dados. A pulsação de

disco pode relaxar as regras de proteção de recurso crítico, já que os nós sem acesso ao disco não podem alterar dados.

Nota:

- 1. A pulsação de disco pode ser ativada somente quando o domínio do mesmo nível já estiver online.
- 2. A pulsação de disco pode ser definida somente entre dois nós. Para mais de dois nós, cada par deverá estar conectado separadamente.

Localize um volume físico adequado, um volume lógico ou um dispositivo de caminhos múltiplos no Linux. Os dados neste volume são apagados. Crie um recurso de interface de pulsação com

```
CT_MANAGEMENT_SCOPE=2
mkrsrc IBM.HeartbeatInterface attributes [Force=0|1]
```

Atributos

Nome

Nome arbitrário com no máximo 36 caracteres.

DeviceInfo

ID do disco ou do volume válido:

- /dev/hdisk: discos brutos
- LVID: volumes lógicos
- MPATH: dispositivos com caminhos múltiplos
- PVID: volumes físicos

CommGroup

Nome da instância em IBM. CommunicationGroup. É criado se o parâmetro Force for 1.

NodeNameList

Par de nós nestas interfaces de pulsação, como {'node1','node2'}.

MediaType

2 (disco)

Para cada sinal de heartbeat, um grupo de comunicação é criado. Isso também é verdadeiro para a pulsação convencional baseada em rede. O grupo de comunicação é criado junto com o dispositivo de pulsação. O grupo de comunicação pode ser ajustado de forma semelhante aos grupos baseados em rede. PingGracePeriodMilliSec não pode ser alterado para pulsação de disco.

Execute as tarefas a seguir para verificar a configuração de pulsação do disco:

- Na configuração da instalação do sistema, certifique-se de que o disco, que é usado para a pulsação de disco não está reservado por nenhum nó peer.
- A pulsação de disco pode ser testada usando os comandos a seguir.

```
dhb_read -p <device-name> -t  # run it on a sender side
dhb_read -p <device-name> -r  # run it on a receiving side
```

Para verificação completa, execute os comandos novamente, trocando o nó do remetente e do destinatário. Se esse teste não funcionar, ele pode não ser suportado devido à reserva de disco ou à instalação ou configuração do sistema não é compatível.

· Verifique se as chamadas do sistema a seguir entre os nós funcionam corretamente:

open("<dev>", 0_RDWR|0_DIRECT), pread() and pwrite();

Protegendo Recursos Críticos (Comutador de Segurança)

Ative o Comutador de segurança (DMS) em seu ambiente de alta disponibilidade.

Em um ambiente de alta disponibilidade, é essencial que no máximo uma instância de um recurso crítico esteja em execução. Um exemplo típico de um recurso crítico é o acesso de gravação para um disco

compartilhado. Quando o acesso de gravação for concedido a mais de um nó por vez, isso resulta em corrupção absoluta da estrutura do sistema de arquivos.

Os algoritmos de quorum do RSCT ConfigRM impedem que esse cenário aconteça, se ConfigRM, HATS e HAGS recebem recursos do sistema suficientes para executar seus cálculos. O DMS terá efeito se esses componentes de infraestrutura de RSCT não puderem mais ser confiáveis para manipular recursos críticos, por exemplo, devido à escassez de processo ou bloqueios. O DMS precisa ser acessado periodicamente dentro de um determinado período de tempo. Se o acesso falha, o kernel do sistema operacional aciona um reinício imediato do sistema para impedir que um recurso crítico seja iniciado duas vezes.

Em sistemas Linux, essa função é implementada usando a chamada de reboot e halt do sistema e um módulo softdog. No AIX, o driver de dispositivo haDMS é usado para esse propósito.

Valores de Quorum Operacional

Se recursos críticos estiverem ativos em um subcluster que perdeu quorum, ConfigRM decidirá de que maneira o sistema pode ser interrompido. Seis métodos de proteção diferentes podem ser configurados pelo atributo CritRsctProtMethod em cada nó.

A tabela a seguir lista quais métodos de finalização do sistema são representados por qual valor do atributo CritRsctProtMethod.

Tabela 24. Métodos de proteção de quorum operacional		
Significado	Valor	
Reconfiguração brusca e reinicialização do sistema operacional (padrão)	1	
Parar o sistema operacional	2	
Reconfiguração brusca e reinicialização do sistema operacional com sync	3	
Parada com sync	4	
Sem proteção. O sistema continua em operação	5	
Sair e reiniciar subsistemas RSCT	6	

Ativando o Suporte IPv6

Para usar o IPv6 com o System Automation, você deve configurar seu sistema operacional para IPv4 e IPv6. Operações de cluster RSCT normais usam conexões IPv4, mas recursos IBM.ServiceIP podem ser definidos para usar endereços IPv6.

Sobre Esta Tarefa

Para ativar o suporte IPv6 no RSCT e o System Automation for Multiplatforms, execute o seguinte comando:

```
chrsrc -c IBM.NetworkInterface IPv6Support=1
```

O comando **chrsrc** cria mais recursos IBM.NetworkInterface para interfaces ativadas para IPv6 também. Agora há dois recursos IBM.NetworkInterface por interface física: um para IPv4 e outro para IPv6. Para obter exemplos de como criar recursos IBM.ServiceIP com endereços IPv6, veja Guia do Administrador e do Usuário do System Automation for Multiplatforms. Um novo atributo da classe IBM.ServiceIP denominado Netprefix é definido para uso com o IPv6.

Configurando o adaptador de automação com uma conta de usuário não raiz

Por padrão, o adaptador de automação de ponta a ponta do System Automation for Multiplatforms é executado com um usuário raiz. Saiba como o adaptador pode ser configurado para executar com um usuário não raiz.

Antes de configurar o adaptador com um usuário não raiz, instale e configure o adaptador com a conta do usuário raiz:

- Crie e inicie o domínio do System Automation.
- Configure o adaptador com o utilitário cfgsamadapter.
- Configure a conectividade SSL com o System Automation Application Manager (opcional).
- Verifique a função do adaptador com o console de operações do System Automation Application Manager.

Processar essas etapas antecipadamente assegura que as etapas para configuração não raiz do adaptador devem ser processadas somente uma vez.

A configuração não raiz para o adaptador envolve as etapas a seguir:

- 1. Execute as preparações de segurança específicas do sistema operacional, por exemplo, a criação de um usuário e grupo dedicados para o adaptador. Consulte <u>"Configurando a segurança para sistemas operacionais específicos" na página 90</u> para uma descrição das ações correspondentes que devem ser processadas manualmente.
- 2. Altere a propriedade do grupo e as permissões de determinados arquivos e diretórios que foram criados pela instalação padrão. Configure as permissões apropriadas do System Automation e do RSCT para o usuário do adaptador. As ações que estão relacionadas a essa etapa são executadas automaticamente usando o script setupAdapterNonRoot.sh. Todas as ações que são processadas pelo script são descritas no tópico <u>"Executando o script de configuração do adaptador do usuário não raiz" na página 92.</u>

Configurando a segurança para sistemas operacionais específicos

Saiba mais sobre as preparações de segurança específicas do sistema operacional que são obrigatórias antes de poder ativar o script setupAdapterNonRoot.sh. Execute as ações descritas nesta seção em todos os nós do cluster.

Criando uma conta do usuário e do grupo

A mesma conta do grupo e do usuário deverá ser criada em cada nó do cluster. Elas são passadas como parâmetros de entrada para o script setupAdapterNonRoot.sh.

Crie um grupo que é o grupo primário para a conta do usuário do adaptador. O nome do grupo sagroup é usado na seção a seguir. Qualquer outro nome também é valido. sagroup é usado quando você modifica a propriedade do grupo de vários arquivos e diretórios do System Automation for Multiplatforms, concedendo direitos de acesso à conta do usuário do adaptador. Com o System Automation for Multiplatforms versão 4.1.0.4 ou superior, o grupo também pode ser criado pelo script 'setupAdapterNonRoot.sh' ao usar a nova opção '**--manage-group**'.

Crie a conta do usuário para executar o adaptador usando o ID de grupo sagroup como o grupo primário para o usuário. O nome de usuário samadapt é usado na seção a seguir. A conta do usuário samadapt pode ser uma conta do usuário técnico que não se destina ao uso em um shell de login. Uma senha não é necessária nesse caso. Assegure-se de que o diretório inicial do usuário exista e que possua os direitos de acesso corretos.

O usuário samadapt pode ser um administrador ou operador do System Automation for Multiplatforms. É necessário seguir as instruções que são fornecidas em <u>Capítulo 5, "Protegendo ", na página 121</u> para configurar os direitos apropriados. Para um operador, designe a função sa_operator. Para um administrador, designe a função sa_admin. Com a função sa_operator, o adaptador pode iniciar e parar recursos e grupos de recursos e, com a função sa_admin, ele pode ativar e desativar adicionalmente as políticas.

Nota: Se você deseja ativar usuários não raiz adicionais para a administração e operação do System Automation, consulte <u>Capítulo 5, "Protegendo ", na página 121</u>. Utilize o grupo sagroup também para esses usuários.

Etapas de configuração se a autenticação do usuário estiver ativada

As etapas de configuração adicionais são necessárias caso a autenticação do usuário com os Pluggable Authentication Modules (PAMs) esteja ativada na configuração do adaptador de automação.

Específico do Linux (SLES)

A conta do usuário samadapt deve ser incluída no ID do grupo de sombra, permitindo que o samadapt leia o arquivo /etc/shadow, que contém os usuários e suas senhas criptografadas. O arquivo /etc/shadow possui a propriedade root: shadow com as configurações de permissão padrão de 640 bits. O acesso a /etc/shadow é necessário para permitir a autenticação do usuário do PAM (Pluggable Access Module) a partir de uma conta de usuário não raiz. Isso acontece quando o PAM é usado para verificar as credenciais do usuário para acessar o domínio do System Automation for Multiplatforms do mecanismo de automação ou console de operações do System Automation Application Manager.

específico do AIX

A conta do usuário samadapt deve ser incluída no ID do grupo security, permitindo que o samadapt use função do PAM e acesso ao diretório /etc/security. Isso é necessário para verificar as credenciais do usuário ao acessar o domínio do System Automation for Multiplatforms a partir do mecanismo de automação ou console de operações do System Automation Application Manager. Além disso, as configurações da ACL devem ser modificadas para o arquivo /etc/security/ password.

No AIX, o arquivo /etc/security/passwd contém as contas do usuário e suas senhas criptografadas. O arquivo /etc/security/passwd tem a propriedade de root:security com as configurações de permissão padrão de 600 bits. Essa configuração nega acesso da conta do usuário samadapt, mesmo se for um membro do grupo de segurança. O acesso pode ser concedido ao modificar as ACLs no arquivo, evitando a modificação dos bits de propriedade e de permissão.

As ACLs podem ser modificadas utilizando os utilitários acledit ou aclget/aclput. Saída de exemplo:

Mescle essas mudanças a outras modificações aplicadas anteriormente.

Ative a conta do usuário samadapter a ser usada pelo System Automation Application Manager

Se a autenticação do usuário do adaptador de automação estiver ativada e você desejar usar a conta do usuário samadapt para acessar o cluster do System Automation for Multiplatforms a partir do System Automation Application Manager, será preciso configurar uma senha para este ID do usuário. É possível especificar suas credenciais para acessar um domínio de automação de primeiro nível no utilitário de configuração cfgeezdm. Ou é possível usar as credenciais para acessar o domínio a partir do console de operações do System Automation Application Manager.

Executando o script de configuração do adaptador do usuário não raiz

Execute o script setupAdapterNonRoot.sh para as ações restantes para a configuração do adaptador não raiz.

O script está no diretório /opt/IBM/tsamp/sam/bin. Antes de executar o script, as seguintes condições devem ser atendidas:

- Se você fizer upgrade do System Automation for Multiplatforms a partir de uma versão anterior à 4.1 para a versão 4.1, todos os nós no cluster serão atualizados para a nova versão. A migração do cluster está concluída. O comando samctrl -m é executado com sucesso.
- · O adaptador foi interrompido.
- Com o System Automation for Multiplatforms versão 4.1.0.3 ou anterior, certifique-se de que as etapas manuais descritas em "Configurando a segurança para sistemas operacionais específicos" na página 90 sejam concluídas com sucesso.
- O cluster do System Automation é definido, mas não é necessário parar o cluster. As etapas de configuração não interferem com as operações de cluster.

Execute o script setupAdapterNonRoot.sh em todos os nós do cluster.

Há versões diferentes desse script com base na versão do produto instalado, que diferem na funcionalidade e nos pré-requisitos necessários. As informações de uso e a saída de amostra a seguir se aplicam ao script incluído no System Automation for Multiplatforms da versão 4.1.0.0 até a versão 4.1.0.3:

Nome

setupAdapterNonRoot.sh - configures end-to-end automation adapter to run with a non-root user account

Synopsis setupAdapterNonRoot.sh [-x] userName [groupName]

Descrição Script to configure the end-to-end automation adapter to run with a non-root user account. It adapts group ownerships and permissions, as well as RSCT security definitions.

Options

-x Set ACL permissions for the sa_admin role. Optional, if omitted, the default is to set ACL permissions for the sa_operator role.

Parameters

userName - the name of the user account that the adapter should run as groupName - the name of the primary group of the adapter user account

Exit Codes

0 all configurations completed successfully

1 at least one configuration task failed - see print out for details

2 prerequisites not satisfied - see print out for details

Execute o script como um usuário com permissões raiz:

Verificação de pré-requisitos

Verifica se um cluster e a conta do usuário existem e se o adaptador de automação foi interrompido. Também é verificado se o grupo especificado é o grupo primário da conta do usuário.

Alterando as propriedades e as permissões do grupo

Diversas propriedades e permissões de arquivos e diretórios precisam ser alteradas, pois são criadas inicialmente somente para acesso de usuário raiz. Para obter informações adicionais, consulte "Alterando as propriedades e as permissões do grupo" na página 94.

Nota: O script altera o grupo proprietário do arquivo /etc/ibm/tivoli/common/cfg/ log.properties. Esse arquivo também pode ser utilizado por outros produtos Tivoli. Se um desses produtos também for executado com uma conta de usuário não raiz, assegure-se de que o arquivo log.properties ainda seja legível para esses produtos.

Configurando as permissões apropriadas do System Automation e do RSCT

Para permitir que a conta do usuário não raiz samadapt use o RSCT Resource Management Control (RMC), deve-se conceder permissões usando o arquivo /var/ct/cfg/ctrmc.acls. Para obter

informações adicionais, consulte <u>"Configurando as permissões apropriadas do System Automation</u> e do RSCT" na página 95.

Adaptando a configuração do adaptador de automação

O usuário não raiz e o grupo são incluídos nas propriedades de configuração do adaptador. Para obter informações adicionais, consulte <u>"Adaptando a configuração do adaptador de automação" na página</u> 96.

Saída de amostra:

```
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.
      As informações de uso e a saída de amostra a seguir se aplicam ao script incluído no System Automation
      for Multiplatforms 4.1.0.4 e superior:
```

ynopsis: setupAdapterNonRoot.sh [-h] [local] [manage-group] [-x sa-admin][-g group <groupname>] userName</groupname>	
Descrição Script to configure the end-to-end automation adapter to run with a non-root user account. It adapts group ownerships and permissions, as well as RSCT security definitions.	
arameters userName - the name of the user account that is used to start the adapter.	
ixit Codes 0 all configurations completed successfully 1 at least one configuration task failed 2 prerequisites not satisfied	
ptions: -h Print this help. -g orgroup <groupname> The name of the primary group for the specified user account. (default: group name = sagroup)</groupname>	
iocai Run script only on local node. Upcional, se omitido, o padrao e executar mudanças	5

```
em todos os nós do cluster.

--manage-group Criar um grupo UNIX local (caso o grupo não exista) e incluir um usuário

especificado neste grupo.

Set group as primary group for the user. Se omitido, o padrão é não fazer

nenhuma mudança no grupo e no usuário.

-x or -sa-admin Configurar permissões de ACL para a função sa_admin. Opcional e, se omitido, o

padrão é configurar permissões de ACL para a função sa_operator.
```

Execute o script como um usuário com permissões raiz:

Verificação de pré-requisitos

Verifica se um cluster e a conta do usuário existem e se o adaptador de automação foi interrompido. Também é verificado se o grupo especificado é o grupo primário da conta do usuário.

Alterando as propriedades e as permissões do grupo

Diversas propriedades e permissões de arquivos e diretórios precisam ser alteradas, pois são criadas inicialmente somente para acesso de usuário raiz. Para obter informações adicionais, consulte "Alterando as propriedades e as permissões do grupo" na página 94.

Nota: O script altera o grupo proprietário do arquivo /etc/ibm/tivoli/common/cfg/ log.properties. Esse arquivo também pode ser utilizado por outros produtos Tivoli. Se um desses produtos também for executado com uma conta de usuário não raiz, assegure-se de que o arquivo log.properties ainda seja legível para esses produtos.

Configurando as permissões apropriadas do System Automation e do RSCT

Para permitir que a conta do usuário não raiz samadapt use o RSCT Resource Management Control (RMC), deve-se conceder permissões usando o arquivo /var/ct/cfg/ctrmc.acls. Para obter informações adicionais, consulte <u>"Configurando as permissões apropriadas do System Automation</u> e do RSCT" na página 95.

Adaptando a configuração do adaptador de automação

O usuário não raiz e o grupo são incluídos nas propriedades de configuração do adaptador. Para obter informações adicionais, consulte <u>"Adaptando a configuração do adaptador de automação" na página</u> 96.

```
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
```

Alterando as propriedades e as permissões do grupo
O script setupAdapterNonRoot. sh aplica várias mudanças à propriedade em grupo de arquivos e diretórios do System Automation for Multiplatforms usando o grupo sagroup. Nenhum arquivo que possua IDs de usuários será alterado. As permissões de acesso também são alteradas no nível do grupo, se necessário.

As mudanças que são feitas no sistema de arquivos:

- Ativar o adaptador para ler ou gravar seu diretório de cache /var/opt/IBM/tsamp.
- Alterar as permissões e a propriedade do arquivo /etc/ibm/tivoli/common/cfg/ log.properties. Ele contém o local do diretório comum do Tivoli, que é usado pelo adaptador.
- Conceder acesso de leitura, gravação ou operação para o diretório comum do Tivoli. O nome do diretório é armazenado no arquivo /etc/ibm/tivoli/common/cfg/log.properties. O diretório padrão é /var/ibm/tivoli/common.
- Permitir leitura dos arquivos de configuração do adaptador nos diretórios /etc/opt/IBM/ tsamp/sam/cfg e /etc/Tivoli/tec.
- Conceder acesso ao conjunto de políticas do adaptador. O local pode ser configurado com a ferramenta cfgsamadapter. O diretório padrão é: /etc/opt/IBM/tsamp/sam/policyPool.
- Altere o grupo dos arquivos binários do adaptador em /opt/IBM/tsamp/sam/bin, /usr/sbin/ rsct/bin e seus arquivos JAR relacionados em /opt/IBM/tsamp/sam/lib.

Para obter detalhes adicionais veja a origem do script setupAdapterNonRoot.sh.

Configurando as permissões apropriadas do System Automation e do RSCT

Para permitir que a conta de usuário não raiz samadapt execute o RSCT Resource Management Control (RMC), o script setupAdapterNonRoot.sh concede permissões, usando o arquivo /var/ct/cfg/ ctrmc.acls. O uso do script com o System Automation da versão 4.1.0.4 ou superior também ajusta o arquivo /var/ct/cfg/ctsec_map.global

Para obter informações adicionais sobre a segurança de RSCT, consulte o manual RSCT Technical Reference. O manual é empacotado junto com o System Automation distribuível.

O ctrmc.acls é composto por vários blocos (sub-rotinas), que descrevem a permissão de acesso para uma classe de recurso do RSCT. Além disso, o conteúdo da sub-rotina DEFAULT é anexado a todas as outras sub-rotinas. A sub-rotina é usada como um padrão para as classes de recursos de RSCT que não têm sua própria sub-rotina em ctrmc.acls. Para conceder acesso às classes de recursos de RSCT para a conta do usuário não raiz do adaptador, a sub-rotina DEFAULT é modificada assim.

O exemplo a seguir do Linux SLES mostra as entradas que são incluídas na sub-rotina ctrmc DEFAULT:

DEFAULT root@LOCALHOST * rw LOCALHOST * r none:clusteruser * r // added by preprpnode none:root * rw // added by preprpnode

As novas entradas são do tipo userid@RSCT-nodeid:

userid

A conta do usuário não raiz que está preparada para executar o adaptador.

RSCT-nodeid

O RSCT nodeid está contido no arquivo /var/ct/cfg/ct_node_id em cada nó do cluster.

Uma entrada é incluída para cada nó do cluster na parte superior da sub-rotina DEFAULT, elas têm precedência sobre as entradas menos específicas existentes.

É possível descobrir que a sub-rotina DEFAULT para sistemas operacionais AIX é muito maior do que o exemplo do Linux. Mas as mudanças que são feitas são exatamente as mesmas.

O arquivo ctsec_map.global é usado para mapear usuários de sistema local para os usuários do RSCT. O conteúdo é o seguinte:

```
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
```

Após a conclusão da modificação do ctrmc.acls (e, se aplicável, ctsec_map.global), o RSCT RMC é acionado para ler novamente o arquivo. Isso é feito executando o comando:

refresh -s ctrmc

Após executar o script setupAdapterNonRoot.sh, verifique os conteúdos do ctrmc.acls (e, se aplicável, applicable ctsec_map.global) em busca de modificações apropriadas.

Adaptando a configuração do adaptador de automação

Quando o adaptador é iniciado, ele precisa conhecer o usuário não raiz e o grupo.

Portanto, o script setupAdapterNonRoot.sh certifica-se de que o arquivo de propriedades de configuração do adaptador /etc/opt/IBM/tsamp/sam/cfg/sam.adapter.properties contém os parâmetros a seguir:

```
non-root-user=samadapt
non-root-group=sagroup
```

Serviço e Manutenção

Se você instalar um fix pack ou incluir nós no cluster, as etapas para aplicar a configuração não raiz do adaptador deverão ser repetidas parcialmente.

Cenários e as etapas que devem ser repetidas.

Instalando Fix Packs

A instalação dos fix packs do System Automation for Multiplatforms pode substituir as propriedades e permissões de arquivos e grupos correspondentes no diretório /opt/IBM/tsamp/sam.

Execute o script setupAdapterNonRoot. sh novamente em cada nó logo após a instalação de um fix pack no nó. Especifique os mesmos parâmetros de entrada para o script assim como para sua chamada inicial.

Incluindo novos nós

Inclua um nó no cluster usando os comandos preprpnode e addrpnode.

Execute as etapas descritas em <u>"Configurando a segurança para sistemas operacionais específicos"</u> na página 90 no novo nó após incluir o nó no cluster. Execute o script setupAdapterNonRoot.sh conforme descrito em <u>"Executando o script de configuração do adaptador do usuário não raiz" na página 92</u> em todos os nós do cluster (antigos e novos). Especifique os mesmos parâmetros de entrada para o script assim como para sua chamada inicial nos nós do cluster antigo.

Alterando o ID do usuário do adaptador não raiz

Se desejar alterar o ID do usuário que é usado para a configuração do adaptador não raiz, remova a configuração existente. Em seguida, é possível definir a configuração para o novo usuário.

Remova a configuração existente executando o script setupAdapterNonRoot.sh com os parâmetros a seguir. Para o System Automation for Multiplatforms versão 4.1.0.0 – 4.1.0.3, use:

setupAdapterNonRoot.sh -x root

Em seguida, execute o script novamente com os novos ID do usuário e grupo desejados.

Para o System Automation for Multiplatforms versão 4.1.0.4 ou superior, use:

```
AIX:
setupAdapterNonRoot.sh -g system root
Linux:
setupAdapterNonRoot.sh -g root root
```

Em seguida, execute o script novamente com os novos ID do usuário e grupo desejados.

Removendo a configuração do adaptador não raiz

Remova a configuração do adaptador não raiz ao reconfigurar todas as permissões e autorizações para a raiz.

Execute o script setupAdapterNonRoot.sh com os parâmetros a seguir:

Para o System Automation for Multiplatforms versão 4.1.0.0 – 4.1.0.3, use:

```
AIX:
setupAdapterNonRoot.sh -x root system
Linux:
setupAdapterNonRoot.sh -x root root
```

Para o System Automation for Multiplatforms versão 4.1.0.4 ou superior, use:

AIX: setupAdapterNonRoot.sh -g system root Linux: setupAdapterNonRoot.sh -g root root

Limitações

As limitações estão relacionadas aos problemas que podem surgir quando você acessar as políticas XML no conjunto de políticas do System Automation for Multiplatforms. Limitações podem ocorrer quando você replicar os arquivos de configuração em outros nós no cluster.

Iniciando o adaptador com uma política ativa que não é legível pela conta de usuário não raiz

Quando a política é carregada a partir de um arquivo de políticas XML, o nome e o local desse arquivo podem ser exibidos se você inserir o comando lssamctrl a partir de um shell de comando em um dos nós do cluster. O local do arquivo de políticas não precisa ser o conjunto de políticas porque o comando sampolicy - a pode utilizar arquivos de políticas a partir de qualquer local.

```
node:~ # lssamctrl
Exibindo Informações de Controle do SAM:
SAMControl:
TimeOut = 60
RetryCount
                        = 3
Automation
                        = Auto
ExcludedNodes
                        = {}
ResourceRestartTimeOut = 5
ActiveVersion = [3.2.2.2, Mon Apr 8 15:49:33 2013]
EnablePublisher
                        = Desativado
TraceLevel = 31
ActivePolicy = [/etc/opt/IBM/tsamp/sam/policyPool/nonRootAdapter-testuser-2.xml,20130415143902+0200,0]
CleanupList = {}
PublisherList = {}
```

Caso esse arquivo de políticas XML exista, mas não esteja legível para a conta de usuário não raiz. Em seguida, o adaptador falha ao iniciar corretamente nesse nó e a conexão com o System Automation Application Manager não é estabelecida.

Resolução: Modifique a permissão do arquivo de política XML ou mova o arquivo para o conjunto de políticas.

Ler e ativar as políticas do System Automation for Multiplatforms a partir do conjunto de políticas. Isto não será possível se samadapt tiver a função de operador.

Para ativar uma política de automação nova ou alterada a partir do console de operações do System Automation Application Manager, o ID do usuário samadapt deve ter permissão para ler o arquivo XML correspondente no conjunto de políticas. As políticas XML que tiverem configurações de bit de propriedade ou de permissão inadequadas não serão exibidas nos diálogos de seleção de política do console de operações.

Resolução: As etapas de configuração não raiz ajustam propriedade e permissão para os arquivos de políticas XML existentes. Assegure que os arquivos de políticas XML armazenados no conjunto de políticas posteriormente, por exemplo, ao salvar as políticas com o comando sampolicy -s, tenham as permissões apropriadas.

Replicando arquivos de configuração

Replique os arquivos de configuração de outros nós no cluster usando a função **Replicar** do utilitário cfgsamadapter. Alguns dos arquivos substituídos possuem permissões de gravação configuradas apenas para o ID do usuário raiz. Portanto, é possível executar a função **Replicar** apenas se você usar o ID do usuário raiz.

Resolução: Execute setupAdapterNonRoot.sh nos nós de destino de replicação imediatamente após a replicação ser concluída. Especifique os mesmos parâmetros de entrada para o script assim como para sua chamada inicial. Como uma alternativa para usar a função **Replicar**, execute cfgsamadapter para executar as mesmas mudanças na configuração explicitamente em cada nó do cluster.

Capítulo 4. Integrando

O System Automation for Multiplatforms integra outros aplicativos Tivoli para fornecer uma solução abrangente. A integração de aplicativos Tivoli e seu ambiente requer tarefas de configuração específicas para adaptação à sua infraestrutura existente.

As configurações necessárias para as seguintes integrações são descritas:

- Encaminhar eventos do System Automation for Multiplatforms para o IBM Tivoli Enterprise Console (TEC).
- Encaminhar eventos do System Automation for Multiplatforms para o IBM Tivoli Netcool/OMNIbus.
- Enriqueça visualizações de TBSM com informações de recursos e eventos do System Automation for Multiplatforms.

Consoles de Eventos

O System Automation for Multiplatforms envia eventos EIF para o Tivoli Enterprise Console (TEC) ou Tivoli Netcool/OMNIbus (OMNIbus). TEC e OMNIbus são aplicativos de gerenciamento de eventos baseados em regras que usam um servidor central para processar eventos recebidos.

Eles coletam alarmes e eventos de uma variedade de origens:

- Aplicativos Tivoli
- Aplicativos de parceiros Tivoli
- · Aplicativos de cliente
- · Network management platforms
- Sistemas de banco de dados relacional

Para o IBM Tivoli System Automation para Multiplataformas , um evento é gerado e encaminhado para o console de eventos do TEC ou do OMNIbus nos seguintes casos:

- A configuração do IBM Tivoli System Automation para Multiplataformas ou o estado de um recurso automatizado é alterado.
- São encontrados problemas.

Se desejar usar eventos do System Automation com o Tivoli Business Service Manager (TBSM), você deve encaminhar eventos para o OMNIbus.

O IBM Tivoli System Automation para Multiplataformas pode produzir os seguintes tipos de eventos:

Classe de eventos / Grupo de Alertas	Descrição	
SystemAutomation_Resource_Status_Change	Status de um recurso automatizado alterado.	
SystemAutomation_Resource_Configuration_Change	Um novo recurso automatizado foi incluído ou um recurso existente foi excluído ou modificado.	
SystemAutomation_Relationship_Configuration_Change	Um novo relacionamento foi incluído ou um relacionamento existente foi excluído ou modificado.	
SystemAutomation_Domain_Status_Change	 O status do domínio foi alterado. Por exemplo: O gerenciador de automação ou o adaptador de automação do domínio inicia ou para. Uma nova política de automação é ativada. 	

Tabela 25. Tipos de classes de eventos do System Automation Application Manager

Tabela 25. Tipos de classes de eventos do System Automation Application Manager (continuação)		
Classe de eventos / Grupo de Alertas	Descrição	
SystemAutomation_Request_Configuration_Change	Uma nova solicitação é emitida em um recurso automatizado ou uma solicitação existente é cancelada.	

Os tópicos a seguir descrevem como configurar o IBM Tivoli System Automation para Multiplataformas e os consoles de eventos para ativar o encaminhamento de eventos para o TEC ou o OMNIbus:

- Configurar o OMNIbus para ser usado com o IBM Tivoli System Automation para Multiplataformas : "Tivoli Netcool/OMNIbus" na página 100
- Configurar o TEC para ser usado com o IBM Tivoli System Automation para Multiplataformas : <u>"Tivoli</u> Enterprise Console" na página 108.

Depois de preparar o console de evento de sua escolha, você deve ativar a geração de evento, conforme descrito em "Ativando a geração de evento" na página 108.

Tivoli Netcool/OMNIbus

Os tópicos nesta seção descrevem como configurar o IBM Tivoli Netcool/OMNIbus para encaminhar eventos do System Automation para o console de evento do OMNIbus. Essa configuração do OMNIbus também é um pré-requisito para a integração do IBM Tivoli System Automation para Multiplataformas com o Tivoli Business Service Manager.

Pré-requisitos

Como o System Automation for Multiplatforms usa eventos do Tivoli Event Integration Facility (EIF) para comunicação, os seguintes componentes são necessários:

- IBM Tivoli Netcool/OMNIbus (OMNIbus)
- OMNIbus Probes Library for Nonnative Base
- OMNIbus Probe for Tivoli EIF (EIF Probe). Essa análise pode receber eventos EIF enviados do System Automation e encaminhá-los para o ObjectServer.

As seguintes versões mínimas são necessárias:

- OMNIbus Probe for Tivoli EIF V.9.0
- IBM Tivoli Netcool/OMNIbus 7.2.1

Nota: Se estiver executando o IBM Tivoli Netcool/OMNIbus V7.2.1, instale a Correção Provisória 3 (7.2.1.5-IF0003). Se estiver executando o IBM Tivoli Netcool/OMNIbus V7.3 ou superior, não serão necessários fix packs adicionais.

Instale e configure esses componentes de acordo com a documentação disponível no <u>IBM Tivoli Netcool/</u> OMNIbus Knowledge Center.

Variáveis de ambiente

\$NCHOME

Refere-se ao diretório inicial do Netcool no qual os pacotes são instalados. Diretório padrão no Linux: /opt/IBM/tivoli/netcool.

\$OMNIHOME

A variável \$OMNIHOME é usada para fornecer suporte legado para scripts, aplicativos de terceiros e análises que continuam a usar a variável de ambiente \$OMNIHOME. \$OMNIHOME refere-se a \$NCHOME/ omnibus.

Campos de Eventos no Banco de Dados do OMNIbus

A tabela OMNIbus alerts.status será estendida com as novas colunas a seguir para reter as informações específicas do System Automation for Multiplatforms. Elas serão preenchidas no arquivo de regras OMNIbus específico do System Automation for Multiplatforms ao processar um evento.

Tabela 26. Atributos de status do System Automation for Multiplatforms usados em eventos de mudança de status de recurso (alerts.status)		
Nome do Atributo	Тіро	Descrição
SADesiredState	varchar(16)	Estado Desejado que reflete o objetivo de automação de um recurso automatizado. Valores possíveis:
		Pending Online
		• Offline
		• NoChange
		Isso significa que o objetivo de automação do recurso não pode ser alterado por um operador
SAObservedState	varchar(16)	O estado atual observado de possíveis valores de um recurso automatizado:
		• Unknown
		Pending Online
		• Offline
		• Iniciando
		• Parando
		NotApplicable
		Nota: Corresponde a c_status_observed em eventos TEC.
SAOperationalState	varchar(255)	Lista de valores de estados operacionais que fornece informações de granularidade mais baixa sobre o estado atual do recurso. Para obter uma lista de possíveis valores, consulte o arquivo SystemAutomation.baroc.
		Nota: Corresponde a c_status_operational em eventos TEC.
SACompoundState	varchar(16)	Estado composto que indica se o recurso está funcionando conforme desejado ou se encontrou um erro. Valores possíveis:
		• Ok
		• Aviso
		• erro
		• Fatal
		Nota: Corresponde a c_status_compound em eventos TEC.

Tabela 27. Identificação do recurso, do domínio, do evento (alerts.status)		
SADomainName	varchar(64)	Nome do Domínio de Automação. Parte da chave de recursos para identificar um recurso.
		Nota: corresponde a sa_domain_name en eventos re

Tabela 27. Identificação do recurso, do domínio, do evento (alerts.status) (continuação)		
SAResourceName varchar(255)	Nome do recurso. Esse é um nome de recurso composto que consiste no próprio nome de recurso concatenado com a classe de recurso e, opcionalmente, com o nó do recurso. A ordem das partes do nome e do caractere separador depende do produto System Automation de envio.	
		<class_name>:<resource_name>:<node_name></node_name></resource_name></class_name>
		Para SA z/OS:
		<resource_name>:<class_name>:<node_name></node_name></class_name></resource_name>
	Nota: <node_name> será configurado apenas se existir. Para referências de recursos do System Automation Application Manager, o nome de nó contém o nome do domínio de automação de primeiro nível referenciado. Corresponde a sa_resource_name em eventos TEC.</node_name>	
SAEventReason	varchar(255)	Motivos do evento. Um evento pode ter diversos motivos de evento no evento TEC. Exemplos de motivos de evento:
		StatusCommonObservedChanged
		ConfigurationDeleted
		PreferredMemberChanged
		Nota: Corresponde a sa_event_reason em eventos TEC.
SAReferencedResourc e	varchar(255)	Para referências de recursos de ponta a ponta do System Automation Application Manager, ele contém a chave de recursos referenciada.

Tabela 28. Outros atributos usados em eventos de mudança de status do recurso (alerts.status)		
SAExludedFromAutomation	varchar(16)	Sinalizador que indica se o recurso foi excluído da automação (isto é, a automação foi suspensa). Usado em eventos de mudança de status do recurso. Valores possíveis:
		NotExcluded
		• Excluded
		Nota: Corresponde a sa_flag_excluded em eventos TEC.
SADesiredRole	varchar(16)	Função desejada. Usado para referências de replicação que indicam a direção da replicação de armazenamento desejada (apenas SA AM). Usado em eventos de mudança de status do recurso.
		Nota: Corresponde a sa_role_desired em eventos TEC.
SAObservedRole	varchar(16)	Função observada. Usado para referências de replicação que indicam a direção da replicação de armazenamento observada (apenas SA AM). Usado em eventos de mudança de status do recurso.
		Nota: Corresponde a sa_role_observed em eventos TEC.

Tabela 29. Eventos de mudança de status do domínio (alerts.status)		
SADomainState	varchar(16)	Status do domínio de automação, os valores possíveis são:
		• Pending Online
		• Offline
		• Unknown
		Nota: Corresponde a sa_domain_state em eventos TEC.
SACommunicationState	varchar(32)	Esse estado reflete a conexão e o estado de disponibilidade do domínio, se o domínio estiver conectado ao System Automation Application Manager. Valores possíveis:
		• Ok
		AsyncTimeout
		AsyncMissedEvent
		• SyncFailed
		 SyncFailedAndAsyncMissedEvent
		 SyncFailedAndAsyncTimeout
		• DomainHasLeft
		Nota: Corresponde a sa_communication_state em eventos TEC.

Além dos novos campos para eventos do System Automation, os campos existentes a seguir serão configurados no arquivo de regras para eventos do System Automation durante o processamento de eventos.

Tabela 30. Campos existentes do arquivo de regras para eventos do System Automation		
Nome do Atributo	Descrição	
Gerente	Nome descritivo da análise que coletou e encaminhou o alarme para o ObjectServer. Valor para eventos do SA: tivoli_eif on <host name="">.</host>	
Agente	Nome descritivo do gerenciador que gerou o evento. Valor para eventos do System Automation for Multiplatforms: SystemAutomation .	
Nó	Identifica o nome do host de onde vem o evento.	
AlertGroup	Identifica o tipo de evento emitido pelo System Automation. Consulte a <u>Tabela 25 na</u> página 99 para obter uma lista de possíveis classes de eventos.	
AlertKey	Chave descritiva que indica o recurso que acionou o evento. Para eventos de recursos, ele contém a chave de recursos formatada como o token de origem do System Automation, por exemplo, EEZResourceKey, DN={DB2Cluster}, NN={}, RN={db2rs}, RC={IBM.Applicat ion}. Para eventos de domínios, ele contém o nome de domínio formatado como o Token de Origem do System Automation, por exemplo, EEZDomain, DN={Db2Cluster}	

Tabela 30. Campos existentes do arquivo de regras para eventos do System Automation (continuação)		
Nome do Atributo	Descrição	
Gravidade	Indica o nível de gravidade do evento. Para eventos de recursos, o estado composto do recurso determina o nível de gravidade. A cor do evento na lista de eventos é controlada pelo valor da gravidade:	
	• 0: Claro	
	• 1: Indeterminado	
	• 2: Aviso	
	• 3: Menor	
	• 4: Grave	
	• 5: Crítico	
	Consulte a seção <u>"Estado Composto para Mapeamento de Gravidade" na página 104</u> .	
Resumo	Resumo do texto que descreve o evento.	
Serviço	Nome do serviço afetado por esse evento. Corresponde ao campo SAResourceName.	
Identificador	Identificador que identifica exclusivamente a origem do problema e controla a deduplicação do ObjectServer. O ObjectServer usa a deduplicação para garantir que informações de evento geradas da mesma origem não sejam duplicadas na lista de eventos. Os eventos repetidos são identificados usando-se o atributo Identificador e armazenados como um único evento para reduzir a quantidade de dados no ObjectServer. Para eventos do System Automation, o campo Identificador é configurado como AlertKey + ":" + AlertGroup. Portanto, o console de eventos sempre exibe o último evento do mesmo recurso e AlertGroup.	
Classe	A classe exclusiva para eventos do System Automation. O valor é 87725 (Tivoli System Automation).	
ExtendedAttr	Contém pares nome-valor de atributos específicos internos adicionais do System Automation, para os quais não existe nenhuma coluna dedicada na tabela alerts.status.	

Além dos atributos armazenados na tabela alerts.status do OMNIbus, informações extras são gravadas na tabela alerts.details . Por exemplo, para eventos de domínio, o nome do produto e a versão do produto de automação correspondentes ao domínio são armazenados na tabela alerts.details.

Estado Composto para Mapeamento de Gravidade

Para eventos que contêm um valor de SACompoundState, por exemplo, todos os eventos de mudanças de estado do recurso, a tabela de mapeamento a seguir é usada:

Tabela 31. Estado composto para mapeamento de gravidade do OMNIbus		
SACompoundState	Campo Gravidade do OMNIbus	
Fatal	5 (Crítico)	
erro	4 (Grave)	
Aviso	3 (Menor)	
ОК	1 (Indeterminado)	

Para outros eventos que não contêm o valor de SACompoundState, por exemplo, eventos de solicitação ou eventos de domínio, o campo de gravidade do EIF é usado para determinar a gravidade do OMNIbus.

Tabela 32. Mapeamento de Gravidade EIF para OMNIbus		
Gravidade do EIF	Campo Gravidade do OMNIbus	
60 (FATAL)	5 (Crítico)	
50 (CRÍTICO)	5 (Crítico)	
40 (MENOR)	4 (Grave)	
30 (AVISO)	3 (Menor)	
20 (INOFENSIVO)	2 (Aviso)	
Else	1 (Indeterminado)	

Nota: O valor da Gravidade de EIF do evento EIF original pode ser localizado no campo ExtendedAttr de um evento.

Configurando o OMNIbus para Processar Eventos do System Automation

A configuração do OMNIbus envolve a atualização do banco de dados do OMNIbus e a ativação do arquivo de regras.

Atualizando o Banco de Dados do OMNIbus

O banco de dados do ObjectServer do OMNIbus inclui a tabela alerts.status que contém todos os campos que são mostrados e selecionados por uma lista de eventos.

Sobre Esta Tarefa

Para eventos do System Automation for Multiplatforms, as colunas adicionais descritas em <u>"Campos</u> <u>de Eventos no Banco de Dados do OMNIbus" na página 101</u> precisam ser criadas na tabela alerts.status.

O arquivo sa_db_update.sql cria as novas colunas na tabela alert.status. A classe de eventos usada para eventos do Tivoli System Automation também foi criada. O System Automation for Multiplatforms usa a classe de eventos 87725 para seus eventos. A classe é usada para associar ferramentas, como a ferramenta de ativação no contexto, a um tipo específico de evento.

Insira o seguinte comando no servidor OMNIbus:

UNIX:

\$OMNIHOME/bin/nco_sql -server NCOMS -username root < sa_db_update.sql</pre>

Windows:

%NCHOME%\bin\redist\isql -S NCOMS -U root < sa_db_update.sql</pre>

Insira sua senha quando solicitado.

É possível localizar o arquivo sa_db_update.sql no DVD do produto System Automation for Multiplatforms no diretório /integration.

Nota: A classe de eventos 87725 é predefinida no OMNIbus Versão 7.3.1 ou superior. Se executar o script sa_db_update.sql usando o OMNIbus Versão 7.3.1, você receberá a seguinte mensagem de erro:

```
ERRO=Tentativa de inserir linha duplicada na linha 2 da instrução 'insert into alerts.conversions values ( 'Class87725','Class',87725,'Tivoli System Automation' );...'
```

Essa mensagem de erro pode ser ignorada.

Verifique se as colunas específicas e a classe de eventos do SA foram incluídas com êxito no OMNIbus:

1. Abra a janela Administrador do Netcool/OMNIbus usando o comando nco_config .

- 2. Na janela Administrador do Netcool/OMNIbus, selecione o botão do menu Sistema.
- 3. Clique em **Bancos de Dados**. A área de janela Bancos de Dados é aberta.
- 4. Selecione a tabela alerts.status. A área de janela da tabela alerts.status é aberta.
- 5. Verifique se as seguintes colunas estão listadas:
 - 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. Na janela Administrador do Netcool/OMNIbus, selecione o botão do menu Visual.
- 7. Clique em **Classes**. A área de janela Classes é aberta.
- 8. Verifique se a classe com o ID 87725 e a etiqueta Tivoli System Automation está listada na tabela.

Ativando arquivo de regras

Um arquivo de regras do OMNIbus define como a análise processará dados de eventos para criar um alerta. Para cada alerta, o arquivo de regras também cria um identificador que identifica exclusivamente a origem do problema.

Sobre Esta Tarefa

O probe for Tivoli EIF usa um arquivo de regras padrão chamado tivoli_eif.rules. O System Automation for Multiplatforms envia o arquivo de regras específico tivoli_eif_sa.rules do System Automation. Esse arquivo precisa ser incluído no tivoli_eif.rules padrão usando uma instrução include. O arquivo de regras tivoli_eif_sa.rules processa um evento do EIF recebido pela análise para o Tivoli EIF se o campo de evento source contiver o valor System Automation.

O arquivo padrão tivoli_eif.rules está no sistema em que a análise para o Tivoli EIF está instalada no diretório a seguir:

```
Windows: %OMNIHOME%\probes\<os_dir>\tivoli_eif.rules
UNIX: $OMNIHOME/probes/<os_dir>/tivoli_eif.rules
```

Execute as seguintes etapas para ativar o arquivo tivoli_eif_sa.rules:

- 1. Copie o arquivo tivoli_eif_sa.rules, que está no diretório /integration no CD do produto System Automation for Multiplatforms, para o sistema em que a análise do OMNIbus para o Tivoli EIF está instalada. Como diretório de destino, escolha o diretório em que o arquivo tivoli_eif.rules está localizado.
- 2. Ative o arquivo de regras tivoli_eif_sa.rules enviado. Edite o arquivo tivoli_eif.rules usado no probe for Tivoli EIF e inclua uma instrução include para o arquivo tivoli_eif_sa.rules.

O conteúdo de tivoli_eif.rules parecerá diferente, dependendo do tipo de instalação do OMNIbus que você tem:

a. Se você usar uma instalação do OMNIbus independente:

Abra o arquivo tivoli_eif.rules em um editor de texto e inclua a instrução include depois do bloco switch(\$source):

b. Se você fizer a integração com o Tivoli Business Service Manager (TBSM) e usar a versão do OMNIbus que é fornecida com o TBSM:

Abra o arquivo tivoli_eif.rules em um editor de texto e inclua a instrução include no bloco em que os arquivos de regras predefinidas estão incluídos. Procure a linha # Include customer rules which would override any previous rules.e inclua a instrução include do tivoli_eif_sa.rules antes desta linha:

```
4F4F4F
 #### Tratar de Eventos TEC
 4‡4‡4‡
 include "tec_event.rules"
 ⋬╞⋬╞⋬╞
 #### Tratar de Eventos Z
 41:41:41:
 # include "zos_event.rules"
 414144
 ### Tratar de eventos definidos pelo usuário Z.
 4⊧4⊧4⊧
 # include "zos_event_user_defined.rules"
 4F4F4F
 #### Tratar da designação de identidade Z.
 4|=4|=4|=
 # include "zos_identity.rules"
 4#4#4#
 ### Tratar de eventos EE (Event Enablement).
 4⊧4⊧4⊧
 # include "tivoli_eif_ee.rules"
include "tivoli_eif_sa.rules"
 # Incluir regras do cliente que substituiriam regras anteriores.
 # include "customer_override.rules"
```

3. Pare a análise do EIF.

:

:

- No Windows: Selecione Painel de Controle > Ferramentas Administrativas > Serviços. Na lista de serviços, clique duas vezes na Análise do EIF e, em seguida, clique em Parar.
- No UNIX: Insira o seguinte comando na linha de comandos

```
$OMNIHOME/bin/nco_pa_stop -process <probe_name>
```

- 4. Reinicie a análise do EIF.
 - No Windows: Na lista de serviços, clique duas vezes em **OMNIbus EIF Prob**e e, em seguida, clique em **Iniciar**
 - No UNIX: Insira o seguinte comando na linha de comandos:

\$OMNIHOME/bin/nco_pa_start -process <probe_name>

Nota:

 É possível testar suas mudanças no arquivo de regras usando a ferramenta de verificação de sintaxe nco_p_syntax entregue com o servidor OMNIbus. Use o arquivo de regras raiz tivoli_eif.rules. Os arquivos incluídos são verificados automaticamente.

Exemplo:

\$0MNIHOME/probes/nco_p_syntax -rulesfile \$0MNIHOME/probes/linux2x86/tivoli_eif.rules

2. Se desejar que a Análise seja forçada a ler o arquivo de regras novamente sem perder eventos, insira o comando a seguir:

kill -HUP <pid>

pid é o ID do processo de análise. É possível determinar o pid usando o comando nco_pa_status.

Tivoli Enterprise Console

É possível configurar o Tivoli Enterprise Console[®] para encaminhar eventos do System Automation para o TEC.

Configurando o TEC para Processar Eventos do System Automation

A linguagem de programação Basic Recorder of Objects in C (BAROC) é usada para definir a estrutura de eventos e suas propriedades. Essas definições são armazenadas em arquivos com a extensão .baroc. O arquivo baroc para eventos do System Automation chama-se SystemAutomation.baroc e fica localizado no diretório /usr/sbin/rsct/samples/tec/SystemAutomation.baroc após a instalação. Para preparar o TEC para ser usado com o System Automation for Multiplatforms, importe, compile, carregue e ative o arquivo baroc do TEC, SystemAutomation.baroc, no servidor do TEC. Para obter informações adicionais, consulte o IBM Tivoli Enterprise Console Rule Builder's Guide, GC32–0669.

Ativando a geração de evento

Se desejar enviar eventos para o TEC ou o OMNIbus, ative o encaminhamento de eventos no System Automation for Multiplatforms.

Sobre Esta Tarefa

Ative e configure a função de geração e encaminhamento de evento do EIF ativando o publicador do TEC. Execute as etapas a seguir:

- 1. Configure a publicação de eventos usando o utilitário de configuração cfgsamadapter. Para obter informações adicionais sobre como configurar a publicação de eventos, consulte <u>"Guia Publicação de Eventos"</u> na página 78.
- 2. Ative o publicador em cada nó no cluster do System Automation for Multiplatforms. Por padrão, o publicador está desativado. É possível ativar o publicador usando o diálogo de configuração Guia do Administrador e do Usuário do System Automation for Multiplatforms ou usando o comando samctrl, conforme descrito em <u>"Ativando o Publicador Usando a Interface da Linha de Comandos" na página 109.</u>
- 3. Configure um novo código de idioma para as mensagens de eventos do TEC, se não desejar usar o código de idioma do sistema padrão.

Ativando o Publicador Usando a Interface da Linha de Comandos

É possível usar a interface da linha de comandos (CLI) do System Automation for Multiplatforms ou o diálogo de configuração cfgsamadapter para controlar o publicador.

Sobre Esta Tarefa

Esta seção descreve como controlar o publicador usando a CLI. Se desejar usar o diálogo de configuração cfgsamadapter, consulte *Guia do Administrador e do Usuário do System Automation for Multiplatforms*.

A função Publicador está desativada por padrão. Para consultar o status do publicador, emita o seguinte comando:

node1:/usr/sbin/rsct/samples/tec # lssamctrl

São exibidas as seguintes informações de controle do Tivoli System Automation:

```
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
                      = 31
   TraceLevel
   ActivePolicy
CleanupList
                       = []
                       = {}
    PublisherList
                         = {}
```

Para ativar o publicador TEC, emita este comando em qualquer nó:

node1:/usr/sbin/rsct/samples/tec # samctrl -e TEC

Para desativar o publicador TEC, emita este comando em qualquer nó:

node1:/usr/sbin/rsct/samples/tec # samctrl -d TEC

Para ativar todos os publicadores definidos, emita este comando em qualquer nó:

node1:/usr/sbin/rsct/samples/tec # samctrl -e P

Para desativar todos os publicadores definidos, emita este comando em qualquer nó:

```
node1:/usr/sbin/rsct/samples/tec # samctrl -d P
```

Configurando um Novo Código de Idioma para Mensagens de Eventos do TEC ou OMNIbus

Sobre Esta Tarefa

As mensagens de eventos do TEC ou OMNIbus estão sempre no idioma que é o código de idioma do sistema padrão no nó onde o System Automation for Multiplatforms principal está em execução.

Nota: Os nomes de recursos em mensagens de eventos do TEC ou OMNIbus podem estar corrompidos se o usuário criou os recursos (mkrg, mkrsrc) em um shell com um código de idioma diferente do código de idioma do sistema padrão, ou o programa do terminal tiver uma tradução do conjunto de caracteres diferente da definida no código de idioma de shell. Para resolver esse problema, os códigos do idioma do sistema e do shell devem ter configurações idênticas e a conversão de caracteres do programa do terminal precisa ser configurada adequadamente. Se o código do idioma do shell for alterado e os recursos já tiverem sido criados com a configuração antiga do código do idioma do shell, todos os recursos deverão ser excluídos e precisarão ser recriados com o novo código do idioma do shell.

Se o usuário optar por ajustar o código de idioma do sistema padrão de acordo com suas configurações de shell preferidas, essa alteração precisará ser feita em todos os nós do cluster. Para isso, desempenhe o seguinte:

- 1. Pare o cluster usando o comando **stoprpdomain**.
- 2. Edite o arquivo que contém o código de idioma do sistema padrão, configure os valores apropriados e salve o arquivo.

SUSE Linux

Arquivo: /etc/sysconfig/language

Palavras-chave: RC_LANG="<NewLocale>"

Substitua <NewLocale> por sua configuração do código de idioma.

ROOT_USES_LANG="yes"

Todas as palavras-chave iniciadas por RC_LC_ devem ser configuradas para sequências vazias "", por exemplo RC_LC_ALL= "".

Execute /etc/SUSEconfig para aplicar as mudanças a seu sistema. Também é possível utilizar a ferramenta de configuração do sistema yast2 sysconfig para aplicar as alterações.

RedHat Linux

Arquivo:/etc/sysconfig/i18n

Palavras-chave: LANG="<NewLocale>"

Substitua <NewLocale> por sua configuração do código de idioma.

AIX

Arquivo: /etc/environment

Palavras-chave: LANG="<NewLocale>"

Substitua <NewLocale> por sua configuração do código de idioma.

- 3. Reinicialize o sistema.
- 4. Repita as etapas em todos os nós no cluster.
- 5. Inicie o cluster usando o comando **startrpdomain**.

Tivoli Business Service Manager (TBSM)

O TBSM entrega as informações em tempo real que são necessárias para responder a alertas com eficiência e de acordo com os requisitos de negócios, e, opcionalmente, para atender aos acordos de nível de serviço (SLAs).

As ferramentas do TBSM permitem construir um modelo de serviço que é integrado com alertas do IBM Tivoli Netcool®/OMNIbus[™] ou, opcionalmente, com dados de uma origem de dados SQL.

O servidor de Dados do TBSM analisa eventos do IBM Netcool/OMNIbus ObjectServer ou dados de SQL para correspondências com regras de status recebidas configuradas para seus modelos de serviço. Se os dados de correspondência alterarem o status de serviço, o status do modelo de serviço do TBSM será alterado adequadamente. Quando um status de serviço é alterado, o TBSM envia eventos de serviço correspondentes de volta para o ObjectServer.

O Discovery Library Toolkit permite criar objetos de serviço do TBSM usando dados de arquivos Discovery Library Adaptor (DLA) ou do IBM Tivoli Application Dependency Discovery Manager.

O console do TBSM fornece uma interface gráfica com o usuário (GUI) em execução no Tivoli Integrated Portal (TIP) que permite vincular logicamente serviços e necessidades de negócios no modelo de serviço. O modelo de serviço fornece ao operador uma visualização de como um corporativo está executando em um determinado momento ou como o corporativo executou em um determinado período de tempo.

A figura a seguir mostra a arquitetura básica para TBSM:



Figura 17. Arquitetura Básica para TBSM

Principais Componentes

Tivoli Integrated Portal

O Tivoli Integrated Portal permite a interação e a transmissão segura de dados entre produtos Tivoli através de um portal comum. É possível ativar de um aplicativo para outro e dentro da mesma visualização de painel para pesquisar diferentes aspectos do corporativo gerenciado.

Tivoli Netcool/OMNIbus

O TBSM monitora o Tivoli Netcool/OMNIbus ObjectServer para eventos recebidos. O ObjectServer coleta eventos de análises, monitores e de outros aplicativos, como o IBM Tivoli Monitoring. Use o TBSM para criar modelos de serviço que respondam aos dados recebidos nos eventos recebidos. Por exemplo, os dados de eventos recebidos podem alterar o status de um serviço ou iniciar o rastreamento de uma violação de SLA em potencial.

Tivoli Netcool/Webtop (OMNIbus Web GUI)

Netcool/Webtop é o console do navegador do Netcool/OMNIbus e o TBSM usa os componentes do Netcool/Webtop para exibir eventos relacionados a modelos de serviço. O Active Event List (AEL) e o portlet Service Details no TBSM são componentes do Netcool/Webtop e são instalados como parte do TBSM. O Tivoli Integrated Portal também inclui componentes do Netcool/Webtop.

Servidor de Painel do TBSM

O servidor de Painel do TBSM gerencia o console do TBSM e se comunica com o Servidor de Dados do TBSM para suportar a criação e a visualização de modelos de serviço por meio de consoles conectados do TBSM. Conforme os usuários do console visualizarem partes do modelo de serviço, o servidor de painel adquirirá e manterá os status de serviços do servidor de dados.

Servidor de Dados do TBSM

O Servidor de Dados do TBSM monitora o ObjectServer e os bancos de dados externos em relação a dados que afetam os status dos serviços configurados no console do TBSM ou com a ferramenta de linha de comandos radshell. O servidor calcula os status desses serviços aplicando regras nos dados externos. Seus modelos de serviço e as regras são armazenados no banco de dados do TBSM.

Integrando o System Automation for Multiplatforms

Os aplicativos de negócios consistem geralmente em diferentes componentes de middleware, vêm com multicamadas e são executados em plataformas heterogêneas. O Tivoli Business Service Manager (TBSM)

fornece informações de funcionamento sobre o aplicativo com multicamadas. O TBSM também monitora acordos de nível de serviço (SLA) com base em informações vindas de várias origens. O Netcool/OMNIbus é usado para coletar todos os eventos relacionados à paisagem do aplicativo de negócios e o TBSM usa esses eventos para determinar os status dos aplicativos de negócios.

O System Automation for Multiplatforms automatiza dependências de início ou parada em paisagens de aplicativos de negócios, fornece operação comum, recuperação automática em situações de falha e obtém um status de disponibilidade agregada. O System Automation for Multiplatforms e o System Automation for z/OS tornam componentes individuais do aplicativo de negócios altamente disponíveis, por exemplo, um banco de dados crítico.

O System Automation for Multiplatforms pode ser usado para integrar-se a TBSM, aprimorando visualizações de serviço de TBSM com dados de eventos do System Automation. O System Automation for Multiplatforms entrega um modelo de serviço de TBSM que contém regras pré-configuradas sobre como mapear estados do System Automation para instâncias de serviço de TBSM.

Pré-requisitos

Antes de iniciar, instale e configure os seguintes produtos e teste a instalação:

- Configure e ative o encaminhamento de eventos para o OMNIbus para eventos do System Automation for Multiplatforms. Para obter informações adicionais, veja <u>"Configurando o OMNIbus para Processar</u> Eventos do System Automation" na página 105 e <u>"Ativando a geração de evento" na página 108</u>.
- Tivoli Business Service Manager (TBSM) V4.2.1 ou superior
- Atualize o esquema do Netcool OMNIbus ObjectServer para TBSM.
 - Se você já tiver um servidor OMNIbus, importe os arquivos de esquema tbsm_db_update.sql e ClearServiceDeps.auto.
 - Se o OMNIbus for instalado com o TBSM, o instalador do TBSM executará as atualizações de esquema necessárias.

É possível localizar informações específicas do produto TBSM no TivoliBusiness Service Manager. Para obter informações adicionais sobre a instalação do produto, consulte <u>Tivoli Business Service Manager</u> Knowledge Center.

Configurando o TBSM

Sobre Esta Tarefa

Para simplificar o processo de definição e configuração de serviços no TBSM, modelos de serviços podem ser definidos para instâncias de serviços com comportamento comum. Em vez de definir cada um dos serviços e suas dependências individualmente, um modelo pode ser criado para um tipo de serviço e, em seguida, designado a serviços aplicáveis.

As instâncias de serviço representam os serviços reais que são designados a um modelo. O modelo define como um serviço responderá a dados recebidos e os status de outros serviços. Serviços do mesmo tipo devem ser designados a um modelo comum. Isso permite usar as mesmas regras de modelo para avaliar os status de diversos serviços.

Ao designar um modelo a um serviço, você identifica o serviço com o modelo. Os modelos eliminam a necessidade de se criar as mesmas regras para um tipo de serviço mais de uma vez.

Modelo de serviço para o TBSM

O System Automation for Multiplatforms fornece um modelo de serviço de TBSM que é usado para recursos do System Automation, que são exibidos em uma árvore de serviço de TBSM.

Sobre Esta Tarefa

O modelo de serviço é denominado EEZ_SystemAutomationResource. Ele fornece

- Uma regra de status de entrada que é denominada SACompoundState, que usa eventos de mudança de estado, que vêm de recursos do System Automation for Multiplatforms para determinar o estado geral de serviços.
- Regras de status de recebimento baseadas em texto que exportam o estado observado do System Automation e outros estados específicos do System Automation de um recurso, para que possam ser usadas em visualizações de TBSM. Para obter informações adicionais sobre como usar as regras de status de recebimento baseadas em texto, veja <u>"Customizando Visualizações do TBSM para Incluir</u> Informações do System Automation" na página <u>116</u>.

O modelo de serviço EEZ_SystemAutomationResource contém uma regra de status de recebimento denominada SACompoundState, que determina o estado geral de um serviço. Se o modelo de serviço tiver sido designado para uma instância de serviço específica, os eventos de mudança de estado do recurso que são do System Automation for Multiplatforms influenciarão o estado geral do serviço. Eventos são associados a uma instância de serviço se o AlertKey no evento corresponder ao AlertKey definido como identificador para a instância de serviço.

O TBSM possui três estados gerais disponíveis: Inválido, Marginal e Bom. O mapeamento a seguir é definido na regra SACompoundState para mapear eventos de mudança de estado de recurso do System Automation para um estado geral de TBSM para uma instância de serviço:

Tabela 33. Mapeamento de Eventos de Mudança de Estado de Recurso do System Automation para Estados do TBSM

Gravidade do Evento	Estado do TBSM
5 (Crítico)	Inválido (Vermelho)
4 (Grave)	Inválido (Vermelho)
3 (Menor)	Marginal (Amarelo)
1 (Indeterminado)	Bom (Verde)

Como há um mapeamento de um para um do estado composto de um recurso para a gravidade do evento, o estado composto do System Automation determina diretamente o estado do TBSM. Para obter informações adicionais sobre o mapeamento do estado composto para a gravidade do evento, veja "Estado Composto para Mapeamento de Gravidade" na página 104.

Definindo um Modelo de Serviço do System Automation no TBSM

Sobre Esta Tarefa

O modelo EEZ_SystemAutomationResource é necessário para usar eventos do System Automation no TBSM. Importe o modelo EEZ_SystemAutomationResource para o TBSM da seguinte forma:

- 1. Copie o arquivo EEZ_SystemAutomationResource.radsh do diretório /integration do CD do produto System Automation for Multiplatforms para um diretório temporário em que o servidor de dados do TBSM esteja instalado.
- 2. Abra um prompt de comandos no sistema do servidor de dados do TBSM. Vá para o diretório em que você copiou EEZ_SystemAutomationResource.radsh e emita o seguinte comando:

• UNIX:

cat EEZ_SystemAutomationResource.radsh |
\$TBSM_HOME/bin/rad_radshell

• Windows:

```
type EEZ_SystemAutomationResource.radsh |
%TBSM_HOME%\bin\rad_radshell
```

O modelo de serviço fornecido pelo System Automation for Multiplatforms está agora definido no TBSM.

Definindo o Acionador no Netcool/OMNIbus

Sobre Esta Tarefa

No ObjectServer do OMNIbus, um novo evento de mudança de estado de um recurso substitui o evento anterior (deduplicação de evento).

Por padrão, TBSM processa um evento deduplicado somente quando o valor do campo **Gravidade** é alterado. Nesses casos, TBSM processa os eventos deduplicados e atualiza o status de serviço. Uma mudança de status é possível para um recurso, que atualiza os campos de status que são usados nas regras de status de recebimento baseadas em texto que estão contidas no modelo de serviço EEZ_SystemAutomationResource. Mas o valor da gravidade não é alterado porque o estado composto do recurso não altera. Defina um acionador no OMNIbus para garantir que o TBSM atualize os serviços também nesses casos.

O arquivo sa_db_tbsm_update.sql é usado para definir o acionador que é denominado update_tbsm_service_on_sa_events no OMNIbus. Esse acionador garante que o TBSM reprocesse os eventos se um dos estados usados nas regras de status recebidos baseadas em texto for alterado, mesmo que o valor da gravidade não seja alterado. Sempre que você quiser usar as regras de status recebidos baseadas em texto incluídas no modelo de serviço EEZ_SystemAutomationResource , crie essa definição de acionador.

Insira o seguinte comando no servidor OMNIbus para definir o acionador:

UNIX:

\$OMNIHOME/bin/nco_sql -server NCOMS -username root < sa_db_tbsm_update.sql</pre>

Windows:

%NCHOME%\bin\redist\isql -S NCOMS -U root < sa_db_tbsm_update.sql</pre>

Insira o ID do usuário e a senha quando solicitado.

sa_db_tbsm_update.sql está incluído com o System Automation for Multiplatforms e pode ser localizado no diretório / integration no DVD do produto.

Integrando recursos do System Automation e TBSM

Sobre Esta Tarefa

Se desejar incluir recursos do System Automation em uma árvore de serviço de TBSM, é necessário criar manualmente uma instância de serviço em TBSM e, em seguida, designar o modelo de serviço do System Automation. Isso é descrito em "Designando o Modelo de Serviço a uma Instância de Serviço" na página <u>114</u>. Isso também deverá ser feito se você quiser enriquecer instâncias de serviço já existentes em uma árvore de serviço do TBSM com informações de eventos do System Automation.

Nota: Se você também estiver usando o System Automation Application Manager, poderá usar seu Discovery Library Adapter para criar instâncias de serviço automaticamente para recursos gerenciados pelo System Automation Application Manager.

Designando o Modelo de Serviço a uma Instância de Serviço

Um modelo de serviço consiste em regras que podem ser aplicadas para instâncias de serviços. Um modelo pode ser usado para mais de uma instância. Para designar o modelo EEZ_SystemAutomationResource a um serviço, é possível identificar o serviço com o modelo.

Sobre Esta Tarefa

Continue como a seguir:

- 1. Identifique os serviços usando o modelo EEZ_SystemAutomationResource para tornar as regras de status recebidos definidas disponíveis para esses serviços.
 - a. No portlet **Service Navigation**, selecione o **Nome do serviço** ao qual deseja designar o modelo de serviço EEZ_SystemAutomationResource específico do System Automation.
 - b. Selecione a guia Editar serviço no Editor de serviço para editar o serviço.
 - c. Selecione a guia Modelos. É possível ver as duas listas a seguir:
 - Modelos Disponíveis: Exibe todos os modelos os quais você tem permissão para designar à instância de serviço selecionada.
 - Modelos Selecionados: Exibe todos os modelos designados ao serviço.
 - d. Para designar o modelo do System Automation a um serviço, selecione o modelo
 EEZ_SystemAutomationResource na lista de Modelos Disponíveis. Clique no botão de seta
 >> para mover o modelo para a lista Modelos selecionados.
- 2. Configure os valores do **Campo de Identificação** para este serviço. TBSM usa os campos de identificação para mapear eventos recebidos para uma instância de serviço.
 - a. Selecione a guia Editar Serviço.
 - b. Selecione a guia Campos de Identificação, que fornece as regras definidas no modelo EEZ_SystemAutomationResource e os valores do campo de identificação necessários para mapear um evento para a instância de serviço selecionada. As regras contidas no modelo EEZ_SystemAutomationResource usam o atributo do evento AlertKey como identificador. Por padrão, o valor de cada campo de identificação é o valor inserido no campo Nome do Serviço.
 - c. Insira o valor de atributo AlertKey correto que corresponde ao serviço selecionado. O AlertKey deve conter a chave de recursos exclusiva do System Automation formatada como CDM SourceToken. A estrutura é definida como esta:

```
EEZResourceKey,DN={DomainName},NN={NodeName},
RN={ResourceName},RC={ResourceClass}
```

Você pode considerar abrir um dos eventos do recurso e copiar e colar o valor do AlertKey do evento para evitar erros de digitação. Exemplos de valores válidos do AlertKey:

Recurso

Recurso constituinte ou fixo que é exibido por lssam como IBM.Application:db2rs:saxb32c.

AlertKey:

```
EEZResourceKey,DN={DB2Cluster},NN={saxb32c},RN={db2- rs},
RC={IBM.Application}
```

Mover grupo

```
Recurso flutuante. O domínio DB2Cluster é exibido por lssam como:
IBM.Application:db2-rs
```

AlertKey:

```
EEZResourceKey,DN={DB2Cluster},NN={},RN={db2- rs},
RC={IBM.Application}
```

Grupo de Recurso

O domínio é DB2Cluster, que é exibido por lssam como: IBM.ResourceGroup:DB2.

AlertKey:

```
EEZResourceKey,DN={DB2Cluster},NN={},RN={DB2},
RC={IBM.ResourceGroup}
```

d. Clique em Salvar para aplicar suas mudanças.

Sempre que novos eventos de mudança de estado do System Automation for Multiplatforms forem recebidos para o serviço que correspondam ao AlertKey especificado, TBSM irá agora processar as regras de status recebidas e alterar, potencialmente, o estado geral do serviço com base na gravidade do evento.

Customizando Visualizações do TBSM para Incluir Informações do System Automation

Sobre Esta Tarefa

O modelo de serviço EEZ_SystemAutomationResource contém regras de status de recebimento baseadas em texto que recuperam o Estado observado do System Automation e outros estados específicos do System Automation de um recurso. Essas informações podem ser usadas em Visualizações de TBSM para enriquecer instâncias de serviços com informações vindas do System Automation for Multiplatforms.

Tabela 34. Regras de status recebidos baseadas em texto do TBSM				
Nome da Regra	Descrição			
SAObservedStateValue	Recupera o campo SAObservedState de um evento de mudança de status do recurso.			
	Valores possíveis:			
	• Unknown			
	Pending Online			
	• Offline			
	• Iniciando			
	• Parando			
	• NotApplicable			
SADesiredStateValue	Recupera o campo SADesiredState de um evento de mudança de status do recurso.			
	Valores possíveis:			
	Pending Online			
	• Offline			
	 NoChange (ou seja, o objetivo de automação do recurso não pode ser alterado por um operador) 			
SAOperationalStateValue	Recupera o campo SAOperationalStateValue de um evento de mudança de status do recurso. Lista de valores do Estado Operacional, fornecendo informações mais refinadas sobre o estado atual do recurso. Para obter uma lista de possíveis valores, consulte o arquivo SystemAutomation.baroc.			

As seguintes regras de status recebidos baseadas em texto estão disponíveis:

Tabela 34. Regras de status recebidos baseadas em texto do TBSM (continuação)			
Nome da Regra	Descrição		
SACompoundStateValue	Recupera o campo SACompoundStateValue de um evento de mudança de status do recurso. Estado Composto que indica se o recurso está funcionando conforme desejado ou se encontrou um erro. Valores possíveis:		
	• Ok		
	• Aviso		
	• erro		
	• Fatal		
SAExcludedFromAutomationValue	Recupera o campo SAExcludedFromAutomationValue de um evento de mudança de status do recurso. Sinalizador que indica se o recurso foi excluído da automação (isto é, a automação foi suspensa).		
	Valores possíveis:		
	NotExcluded		
	• Excluded		

Incluindo Colunas para Informações Adicionais do System Automation em uma Árvore de Serviços do TBSM

Sobre Esta Tarefa

É possível modificar as colunas de árvores customizadas exibidas no TBSM no

- Portlet Service Navigation
- Portlet Service Tree

O portlet Service Navigation padrão tem três colunas:

- Estado
- Hora
- Eventos

É possível modificar, excluir e incluir três colunas com o **Editor do modelo de árvore**. O **Editor do modelo de árvore** está disponível a partir da barra de ferramentas **Serviços** no portlet **Service Navigation**. É possível incluir um novo modelo de árvore no portlet **Service Navigation**. Para cada coluna customizada, use o **Editor do modelo de árvore** para especificar os dados de regra que você deseja exibir na coluna.

Incluindo colunas:

Esse recurso pode ser usado para incluir colunas para qualquer uma das regras de status recebidos baseadas em texto fornecidas definidas pelo modelo EEZ_SystemAutomationResource. Por exemplo, é possível definir uma coluna que exiba o Estado Observado atual vindo do System Automation de cada instância de serviço que tenha o modelo EEZ_SystemAutomationResource designado. Execute as etapas a seguir:

- 1. Clique no botão **Editor de Modelo de Árvore** na barra de ferramentas do portlet Service Navigation.
- 2. Selecione o modelo de árvore que você deseja modificar na lista suspensa **Nome do Modelo de Árvore**.
- 3. Clique no botão Incluir Nova Coluna de Árvore na seção Configuração da Coluna.
- 4. Digite o nome que deseja usar no campo em branco da nova coluna, por exemplo, "Estado da Disponibilidade".

- 5. Ajuste a posição e a largura da coluna, conforme apropriado
- 6. Na **seção Seleção do Modelo de Serviço**, selecione o modelo EEZ_SystemAutomationResource.
- 7. No **Mapeamento de Regra do Modelo de Serviço**, selecione o modelo EEZ_SystemAutomationResource na lista de Modelos Ativos.
- 8. Para cada regra que você quiser exibir em uma coluna da árvore de serviço, selecione a caixa de seleção **Exibir** e escolha uma coluna na caixa suspensa para exibir o valor de saída. Neste exemplo, selecione a caixa de seleção **Exibir** do atributo @SA0bservedStateValue e escolha a coluna **Estado de Disponibilidade** na caixa suspensa dessa linha.
- 9. Clique em **OK** para salvar as mudanças no modelo da árvore.

A figura a seguir mostra uma captura de tela do editor de modelo de árvore. Uma nova coluna **Estado de disponibilidade** é incluída, mostrando o Estado observado de automação do sistema:

2 T	Free Tem	plate Editor - Mozilla Firefox			
	saxb33e	https://saxb33e:16316/ibm/sla/rad/Templa	teTreeEd	tor. faces	☆
					^
1		Tree Template Name: ServiceInst	tance	×	
6	Column Co	onfiguration 💛			
Г		-			_
	1. 4	🖞 🛅 🧗 🦉 🗖 Enable Static	Sizing f	or Tree Template	
		,			
		State 🗲 🕂		Availability State	~
ŀ	<				>
s	ervice Te	mplate Selection 送			
Iг					
	BSM_Ap	pLogicalGrouping		Selected Templates	~
	BSM_Ap BSM_Ap	pServer pServerCluster		BSM_DB2DatabaseServer BSM_HTTP	
	BSM_Ap	pServerGroup		BSM_WebsphereServer	
	BSM_Ap	plicationCluster		EEZ_SystemAutomationResource	
	BSM_Ba BSM_Bri	idge			
	BSM_Bu BSM_CI	sinessApplication CS		▼	
s	ervice Te	mplate Rule Mapping 💛			
Ιr					
	A etime Te	BSM_HTTP BSM_WebsphereServer		<u>^</u>	
	Active re	DefaultTag			
	Available	Attributes	esource		
	Display	Attribute Name	Type	Columo Disolay Name	
		serviceStatusImage	default	State	~
		@SAObservedStateValue	8	Availability State	~
		slaStatusImage	default	Time	~
		rawEventsImage	default	Events	~
		@SAExcludedFromAutomationValue	8	Automation Suspended	~
		@SAOperationalStateList	8	Operational States	~
		@SADesiredStateValue	8	Desired State	~
		@SACompoundStateValue	۲		~
		@SACompoundState	۲		~
_					
	2				Cancel
	•				
Done					

Figura 18. Editor de modelo de árvore

Para visualizar a Árvore de Serviços atualizada, atualize o portlet Service Navigation. A nova coluna ocorre agora mostrando a saída da regra de status recebido que você selecionou.

Nota: É necessário criar novos eventos de mudança de status do recurso para atualizar as informações de estado exibidas no TBSM. Eventos antigos não são processados novamente.

Usando o editor de políticas do TBSM:

Opcionalmente, é possível formatar valores de colunas usando o editor de políticas do TBSM. Por exemplo, exiba os valores de Estado Observado do SA em cores diferentes. Continue como a seguir:

- 1. Clique no botão **Editor de Modelo de Árvore** na barra de ferramentas do portlet Service Navigation.
- 2. Escolha o modelo de árvore que você deseja modificar na lista suspensa Nome do Modelo de Árvore.
- 3. Clique no botão **Editar Política...** para abrir a política que exibe valores de colunas. A política chamada GetTreeColumnValue é aberta no editor de políticas:



Figura 19. Editor de Modelo de Árvore do TBSM

4. Modifique a política. O fragmento de código a seguir serve como exemplo de como alterar a cor dos valores de saída baseados em texto. Neste exemplo, assume-se que uma coluna chamada "Estado de Disponibilidade" tenha sido definida mostrando a saída da Regra SAObservedState. Dependendo do valor do estado observado, o fragmento de política retorna o valor em uma cor diferente:

```
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>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 = 'Stopping') {
        VALUE = '<font color="blue"> <b>Stopping</b></font>';
        if (value = 'Starting') {
        VALUE = '<font color="blue"> <b>Starting</b></font>';
        if (value = 'Starting') {
        VALUE = '<font color="blue"> <b>Starting</b></font>';
        if (value = 'Starting') {
        VALUE = '<font color="blue"> <b>Starting</b></font>';
        if (value = 'Starting') {
        VALUE = '<font color="blue"> <b>Starting</b></font>';
        if (value = 'Starting') {
        VALUE = '<font color="blue"> <b>Starting</b></font>';
        if (value = 'Starting') {
        VALUE = '<font color="blue"> <b>Starting</b></font>';
        if (value = 'Starting') {
        VALUE = '<font color="blue"> <b>Starting</b></br>
```

5. Salve a política modificada

Capítulo 5. Protegendo

A proteção do ambiente do System Automation for Multiplatforms envolve configurar conexões Secure Socket Layer (SSL) e proteger os ambientes em cluster contra acesso não autorizado.

É possível configurar a segurança não root para a interface da linha de comandos do System Automation for Multiplatforms em sistemas AIX e Linux.

Em sistemas Linux e AIX, por padrão, apenas o usuário root tem a autoridade necessária para concluir tarefas operacionais no System Automation for Multiplatforms e para alterar a política de automação do System Automation for Multiplatforms, enquanto todos os outros usuários possuem apenas acesso de leitura.

Gerenciando Autorização para Usuários que Acessam o Cluster

O conceito de segurança do System Automation for Multiplatforms é baseado no componente RMC do RSCT, que implementa a autorização de segurança com um arquivo de lista de controle de acesso (ACL). Especificamente, o RMC usa o arquivo de ACL em um determinado nó para determinar as permissões que um usuário deve ter para acessar classes de recursos e suas instâncias de recursos. Como os gerenciadores de recursos do System Automation são implementados internamente como um aplicativo RMC, o mesmo conjunto de regras de controle da ACL deve ser usado para permitir que usuários não raiz gerenciem (definam, indefinam ou alterem) as classes de recursos relacionadas ao System Automation (IBM.ResourceGroup, IBM.ManagedRelationship, IBM.Equivalency, IBM.ManagedResource, IBM.CHARMControl, IBM.Application e IBM.ServiceIP) e iniciem e parem os grupos de recursos correspondentes.

Para obter informações detalhadas sobre como configurar os arquivos de ACL do RMC, consulte as seguintes seções no IBM RSCT Administration Guide:

- "Managing user access to resources using RMC ACL files" no Capítulo 4 ("Managing and monitoring resources using RMC and resource managers")
- "Configuring the global and local authorization identity mappings" no Capítulo 7 ("Understanding and administering cluster security services")

Configurando IDs do Usuário não Root para a Interface da Linha de Comandos

O suporte de autorização de segurança RSCT e RMC gerencia o acesso de usuário com base em classes de recursos individuais e em nós únicos, por exemplo, o acesso de usuário pode ser restrito a uma classe de recurso RMC específica em um determinado nó no cluster. Esse nível de configuração de autorização é complexo e requer um claro entendimento da natureza de cada classe de recurso RMC individual.

Portanto, você deve criar funções para um operador do System Automation for Multiplatforms e um administrador do System Automation for Multiplatforms com configurações gerais que permitem que usuários não root gerenciem todas as classes de recursos a partir de qualquer nó que esteja definido no cluster. Use o seguinte procedimento para criar estas duas funções:

- sa_admin para um administrador
- sa_operator para um operador

As funções são descritas em mais detalhes na seção: <u>http://www.ibm.com/support/knowledgecenter/en/</u>SSRM2X_4.1.0/com.ibm.samp.doc_4.1/sampugbug_limit_non-root.html

O System Automation for Multiplatforms versão 4.1.0.4 ou superior fornece o script samnonrootuser para a execução da configuração desse usuário não raiz. O script requer um usuário existente e, em seguida, ajusta as permissões de arquivo e os arquivos ACL para definir o usuário como 'sa_admin' ou como 'sa_operator'.

Se a versão do System Automation instalado for anterior à 4.1.0.4, a configuração manual descrita abaixo precisará ser realizada:

Para criar as funções, execute as seguintes etapas (observe que é necessária a autoridade de administrador). Este exemplo mostra os comandos que devem ser executados em um ambiente Linux:

1. Crie os IDs do usuário que estão autorizados a gerenciar o System Automation for Multiplatforms em todos os nós:

```
# /usr/sbin/useradd ernie
# /usr/sbin/useradd bert
```

2. Crie um grupo para os IDs do usuário em todos os nós:

```
# /usr/sbin/groupadd sagroup
```

3. Inclua o grupo nos IDs do usuário em todos os nós:

```
# /usr/sbin/usermod -G sagroup ernie
# /usr/sbin/usermod -G sagroup bert
```

Nota: Assegure-se de configurar a seguinte variável de ambiente para todos os usuários do System Automation for Multiplatforms em todos os nós (escopo de domínio de ponto):

CT_MANAGEMENT_SCOPE=2

É possível configurar a variável permanentemente, se você configurá-la no perfil do usuário.

4. Altere a propriedade do grupo do arquivo /var/ct/IBM.RecoveryRM.log.

O arquivo é usado para controlar o histórico do System Automation for Multiplatforms. Todos os comandos que modificam os recursos do gerenciador de automação (IBM.RecoveryRM) são registrados nesse arquivo.

Por padrão, o arquivo é de propriedade do grupo de usuários root:

-rw-r--r-- 1 root root 204 Oct 4 22:00 /var/ct/IBM.RecoveryRM.log

Altere a propriedade do grupo para sagroup:

/bin/chgrp sagroup /var/ct/IBM.RecoveryRM.log

Altere a permissão de arquivo para 664:

Nota: Se o arquivo /var/ct/IBM. RecoveryRM.log não existir após a instalação inicial do System Automation for Multiplatforms, será possível criar um arquivo simulado executando o comando /usr/bin/touch:

/usr/bin/touch /var/ct/IBM.RecoveryRM.log

5. Modifique o arquivo /var/ct/cfg/ctsec_map.global em todos os nós.

Você deve incluir as seguintes entradas para os IDs do usuário ernie e bert no arquivo de mapeamento de identidade de autorização global RSCT (/var/ct/cfg/ctsec_map.global) em cada nó no cluster. Inclua as novas entradas acima da entrada para o usuário clusteruser:

```
unix:ernie@<cluster>=sa_operator
unix:ernie@<any_cluster>=sa_operator
unix:bert@<cluster>=sa_admin
unix:bert@<any_cluster>=sa_admin
unix:bert@<iw>=sa_admin
```

```
unix:*@*=clusteruser
```

O arquivo é utilizado para mapear um ID de usuário local em um nó para um ID de usuário global dentro do domínio do System Automation for Multiplatforms. No exemplo, o ID do usuário local ernie é mapeado para o ID do usuário global sa_operator, e o ID do usuário local bert é mapeado para o ID do usuário global sa_admin.

É possível autorizar mais IDs de usuários locais para o System Automation for Multiplatforms, incluindo linhas neste arquivo de mapeamento global (em todos os nós), e mapeando-os para o operador ou administrador de função desejado.

Nota: Se o arquivo //var/ct/cfg/ctsec_map.global não existir em um nó, copie o arquivo padrão /usr/sbin/rsct/cfg/ctsec_map.global para o diretório /var/ct/cfg e inclua as novas entradas no arquivo /var/ct/cfg/ctsec_map.global. Não remova qualquer entrada do arquivo /var/ct/cfg/ctsec_map.global que exista no arquivo padrão que você copiou. Os arquivos /var/ct/cfg/ctsec_map.global em todos os nós dentro do cluster devem ser idênticos. Sempre inclua novos IDs para usuários não root acima das entradas para o usuário clusteruser.

6. Modifique o arquivo /var/ct/cfg/ctrmc.acls em todos os nós. Deve-se incluir as entradas a seguir para os IDs de usuário global sa_operator e sa_admin no arquivo ACL do RMC (/var/ct/cfg/ctrmc.acls) em cada nó no cluster, além de remover a linha que começa com LOCALHOST, por exemplo:

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 // anexar esta linha para saoperator

7. Quando tiver concluído as modificações necessárias, execute o seguinte comando em cada nó no cluster para ativar as mudanças:

/usr/bin/refresh -s ctrmc

- 8. Mudanças adicionais que precisam usar os comandos **sampolicy** e ***samadapter**:
 - a. Acesso aos arquivos de configuração:

/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. Acesso aos arquivos de log:

/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. Acesso aos arquivos de configuração no diretório /etc. Se não houver nenhum diretório /etc/opt/IBM/tsamp/sam/cfg, crie-o utilizando

/bin/mkdir -p /etc/opt/IBM/tsamp/sam/cfg

Em seguida, configure as permissões apropriadas:

/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. Ajustes opcionais necessários para trabalhar com o pacote sam.policies: Políticas predeterminadas para vários aplicativos são fornecidas no pacote de instalação sam.policies, que pode ser transferido por download a partir de IBM Integrated Service Management Library.

- 10. Para permitir que um usuário que tem a função sa_admin configure estas políticas predeterminadas, as permissões e a propriedade do diretório /usr/sbin/rsct/sapolicies devem ser alteradas após a instalação do pacote sam.policies em todos os nós:
 - # chmod -R 2775 /usr/sbin/rsct/sapolicies
 # chgrp -R sagroup /usr/sbin/rsct/sapolicies

Quando tiver concluído as etapas com sucesso, os usuários locais ernie e bert poderão executar tarefas operacionais do System Automation for Multiplatforms, como emitir solicitações de início e parada em recursos e o usuário local bert também poderá executar tarefas administrativas do System Automation for Multiplatforms, como definir e modificar políticas.

Autorização Padrão Modificada para Usuários não Root que Usam o RSCT Nível 2.5.4.0 ou Superior

A partir do RSCT nível 2.5.4.0 (AIX 6 e Linux), foi introduzida uma mudança que impede que usuários não root executem comandos para listar recursos. As permissões apropriadas serão configuradas automaticamente se um novo domínio for criado.

Se você migrar um domínio existente para esse nível de RSCT, as permissões apropriadas para executar comandos, como lssam ou lsrg -m, não serão automaticamente configuradas para usuários não root. Dependendo de seu nível de RSCT, escolha as ações apropriadas para ajustar a configuração:

O nível de RSCT é igual ou superior a 2.5.5.2 (AIX 6 e Linux:

Crie outro domínio que ajusta implicitamente a configuração. Não inicie o novo domínio. É possível removê-lo posteriormente.

Como alternativa, ou se o nível de RSCT for inferior a 2.4.13.2:

Use os seguintes comandos para ajustar a configuração em todos os nós como usuário root:

1. Edite o arquivo /usr/sbin/rsct/cfg/ctsec_map.global e inclua o seguinte conteúdo, se ele não existir:

unix:*@*=clusteruser

2. Crie um arquivo /tmp/addacl e inclua o seguinte conteúdo:

DEFAULT none:clusteruser * r

3. Ajuste o arquivo acl executando o seguinte comando:

/usr/sbin/rsct/install/bin/chrmcacl -a < /tmp/addacl</pre>

4. Atualize o subsistema ctrmc para que as mudanças entrem em vigor:

refresh -s ctrmc

Os usuários não root agora podem usar comandos, como lssam ou lsrg -m, da mesma forma que faziam com níveis anteriores de RSCT.

Limitações da Configuração de Segurança de não Root

Sobre Esta Tarefa

A lista a seguir resume as limitações da configuração de segurança de não root:

• Um usuário comum não pode visualizar o conteúdo do arquivo de rastreio do gerenciador de recursos RMC (por exemplo, o rastreio do daemon IBM. RecoveryRMd).

Todos os dameons do Gerenciador de Recursos RMC usam o utilitário da biblioteca de estrutura RMC para criar arquivos de rastreio e imagens principais no diretório /var/ct/<cluster>. Como esses

gerenciadores de recurso podem ser iniciados apenas por um superusuário (ID do usuário root) através do comando **/usr/bin/startsrc**, os arquivos que são criados pertencem ao ID do usuário root.

Todos os usuários não root não podem coletar informações de depuração e rastreio usando o comando **/usr/sbin/rsct/bin/ctsnap**.

Para permitir que usuários não root coletem dados de rastreios ou de depuração ctsnap ou ambos, um mecanismo como "sudo" deve ser implementado para esses usuários e comandos.

- Os comandos a seguir podem ser iniciados apenas com autoridade root, porque eles usam a criação de log do Tivoli, que funcionará corretamente apenas se os arquivos de log forem mantidos com direitos de root:
 - O comando **sampolicy**.
 - O comando **samadapter** para iniciar o adaptador de automação de ponta a ponta.
 - O comando **samlicm** para instalar ou fazer upgrade de uma licença.
- A granularidade dos objetos ACL é baseada nas classes de recurso e não nos recursos. Isso significa que um usuário comum tem permissão para modificar os recursos de uma classe de recurso, ou não, mas não é possível conceder ou negar as permissões com base no recurso, por exemplo, um administrador de banco de dados não pode ter autorização apenas para os recursos de banco de dados.
- A função "sa_operator" pode modificar os recursos, alterando os valores de atributo para os recursos. Esse é um resultado da permissão "s", que é necessária para emitir os pedidos do System Automation for Multiplatforms. Sem a permissão "s", os usuários que possuem essa função não conseguiriam executar nenhuma tarefa útil. Com a permissão "s", eles têm permissão para configurar e alterar atributos.

A tabela a seguir mostra a função ou a autoridade que é necessária para executar as tarefas típicas do System Automation for Multiplatforms.

Tarefa	Autoridade	Funções	Permissões			
Instalação do produto e da licença do produto	root	Administrador do Sistema	Instalar e fazer upgrade do System Automation for Multiplatforms e da licença do produto.			
Gerenciamento do Cluster	root / sa_admin	Administrador do Sistema / Administrador do System Automation for Multiplatforms	Definindo, iniciando, parando e monitorando os clusters e os Gerenciadores de Recursos RMC individuais			
Definição de recurso e definição de política do System Automation for Multiplatforms	root / sa_admin	Administrador do Sistema / Administrador do System Automation for Multiplatforms	Definindo, removendo, alterando recursos e configurando as políticas de automação			
Operação de Automação	root / sa_admin / sa_operator	Administrador do Sistema / Administrador e Operador do System Automation for Multiplatforms	Emitindo o pedido On-line e Off-line e reconfigurando e monitorando os grupos de recursos e os recursos individuais			

Tabela 35. As Autorizações e as Funções para Executar as Tarefas do System Automation for Multiplatforms Tabela 35. As Autorizações e as Funções para Executar as Tarefas do System Automation for Multiplatforms (continuação)

Tarefa	Autoridade	Funções	Permissões	
Coletando dados de rastreio e depuração para determinação de problemas	root	Administrador do Sistema	Acesso a todos os arquivos de rastreio do aplicativo (log) e do sistema. (consulte a lista de limitações)	
Configuração de Segurança	root	Administrador do Sistema	Definir, alterar e remover a configuração de segurança descrita nesta seção.	
Configuração do Adaptador	root / sa_admin	Administrador do Sistema / Administrador do System Automation for Multiplatforms	Definindo, alterando e removendo a configuração da automação de ponta a ponta	

Protegendo a Conexão com o Adaptador de Automação de Ponta a Ponta Usando SSL

Configure o Secure Socket Layer (SSL) em seu ambiente para comunicação entre o Servidor de automação de ponta a ponta do System Automation Application Manager e o Adaptador de automação de ponta a ponta do System Automation for Multiplatforms.

Sobre Esta Tarefa

Este tópico descreve como proteger a conexão entre o Servidor System Automation Application Manager e o adaptador de automação de ponta a ponta. A conexão entre o Servidor System Automation Application Manager e o adaptador de automação é uma comunicação bidirecional e todas as consultas e ações são protegidas com a criptografia SSL. O envio de eventos EIF do adaptador de automação para o Servidor System Automation Application Manager não é segura. Para obter informações adicionais sobre como proteger esta conexão, consulte o *Guia de Configuração e Instalação do IBM Tivoli System Automation Application Manager*.

Gerar Keystore e Truststore com Chaves SSL Públicas e Privadas

Sobre Esta Tarefa

Gere os seguintes arquivos:

- Truststore: Contém as chaves públicas do Application Manager e dos adaptadores FLA.
- Keystore do Application Manager: Contém a chave privada do Application Manager.
- Keystore do Adaptador: Gere um por adaptador. Contém a chave privada de um adaptador FLA.

A <u>Figura 20 na página 127</u> mostra uma visão geral dos componentes, arquivos e etapas envolvidas na geração de arquivos. A seguir, o termo *operations console* refere-se ao System Automation Application Manager operations console.

Operations Console Server



Figura 20. Geração de Keystore e Truststore usando SSL

Gere o truststore e o keystore executando as etapas a seguir. As chaves expiram depois de 25 anos com a validade padrão configurada como 9125. Certifique-se de que a passphrase tenha pelo menos 6 caracteres. Os números das etapas estão relacionados aos números na Figura 20 na página 127. Os valores usados são amostras ou valores-padrão.

1. Configurar variáveis:

```
# java keytool from the console de operações 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. Gerar keystore com chaves públicas e privadas do adaptador de automação:

```
${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. Gerar keystore com chaves públicas e privadas do operations console:

-dname "cn=SAAM Server, ou=Tivoli System Automation, o=IBM, c=US" \
-keystore "\${0C_CONFIG_DIR}/ssl/sam.ssl.operationsconsole.keystore.jks"

4. Exportar arquivo de certificado com a chave pública do adaptador de automação:

```
${JAVA_KEYTOOL} -export -alias samadapter \
    -file ${0C_CONFIG_DIR}/ssl/samadapter.cer -storepass ${PASSPHRASE} \
    -keystore "${0C_CONFIG_DIR}/ssl/sam.ssl.adapter.keystore.jks"
```

5. Exportar arquivo de certificado com a chave pública do operations console:

```
${JAVA_KEYTOOL} -export -alias eezoperationsconsole \
    -file "${OC_CONFIG_DIR}/ssl/eezoperationsconsole.cer" -storepass ${PASSPHRASE} \
    -keystore "${OC_CONFIG_DIR}/ssl/sam.ssl.operationsconsole.keystore.jks"
```

6. Gerar truststore de chaves autorizadas e importar o certificado com a chave pública do adaptador de automação:

```
${JAVA_KEYTOOL} -import -noprompt -alias samadapter \
    -file "${0C_CONFIG_DIR}/ssl/samadapter.cer" -storepass ${PASSPHRASE} \
    -keystore "${0C_CONFIG_DIR}/ssl/sam.ssl.authorizedkeys.truststore.jks"
```

7. Gerar truststore de chaves autorizadas e importar o certificado com a chave pública do operations console:

```
{JAVA_KEYTOOL} -import -noprompt -alias samoperationsconsole \
        -file "${0C_CONFIG_DIR}/ssl/samoperationsconsole.cer" -storepass ${PASSPHRASE} \
        -keystore "${0C_CONFIG_DIR}/ssl/sam.ssl.authorizedkeys.truststore.jks"
```

 Excluir arquivo de certificado do adaptador de automação. O arquivo de certificado não é mais necessário no tempo de execução:

rm \${OC_CONFIG_DIR}/ssl/samadapter.cer

9. Excluir arquivo de certificado do operations console. O arquivo de certificado não é mais necessário no tempo de execução:

```
rm ${OC_CONFIG_DIR}/ssl/samoperationsconsole.cer
```

Ativar a Segurança SSL em Configurações do Adaptador de Automação

Sobre Esta Tarefa

Execute as etapas a seguir para ativar a segurança SSL em configurações do adaptador de automação.

1. Copie o arquivo de armazenamento confiável de chaves autorizadas para todos os nós no cluster IBM Tivoli System Automation para Multiplataformas :

scp \${0C_CONFIG_DIR}/ssl/sam.ssl.authorizedkeys.truststore.jks \
 root@<adapter-nodename>:/etc/opt/IBM/tsamp/eez/cfg/ssl/sam.ssl.authorizedkeys.truststore.jks

2. Copie o arquivo keystore do adaptador para todos os nós no cluster IBM Tivoli System Automation para Multiplataformas :

cp \${0C_CONFIG_DIR}/ssl/sam.ssl.adapter.keystore.jks \
 root@<adapter-nodename>:/etc/opt/IBM/tsamp/sam/cfg/ssl/sam.ssl.adapter.keystore.jks

3. Inicie o utilitário de configuração.

Insira o comando cfgsamadapter.

4. Especifique os parâmetros:

Na janela principal do diálogo de configuração, clique em **Configurar**. Especifique os seguintes parâmetros na guia **Segurança**, conforme descrito em <u>"Guia Segurança" na página 79</u>. Os valores abaixo são valores de amostra.

- Truststore: /etc/opt/IBM/tsamp/sam/cfg/ssl/ sam.ssl.authorizedkeys.truststore.jks
- Keystore:/etc/opt/IBM/tsamp/sam/cfg/ssl/sam.ssl.adapter.keystore.jks
- Senha do keystore: passphrase
- Alias de certificado: samadapter

Clique em **Salvar** para armazenar as mudanças na configuração.

- 5. Na janela principal do diálogo de configuração, clique em **Replicar**. Replique os arquivos de configuração para os outros nós no cluster IBM Tivoli System Automation para Multiplataformas , incluindo a configuração de SSL.
- 6. Reinicie o adaptador de automação usando o comando samadapter usado para controlar o adaptador de automação. Isso ativa a configuração de SSL.
- 7. Reinicie o Servidor System Automation Application Manager para ativar a configuração de SSL.

Use os seguintes comandos para iniciar ou parar o Servidor System Automation Application Manager manualmente:

Iniciar

/opt/IBM/WebSphere/AppServer/bin/startServer.sh server1

Parar

/opt/IBM/WebSphere/AppServer/bin/stopServer.sh server1

Nota: O ID do usuário administrativo e a senha do WebSphere Application Server são necessários para parar o Servidor System Automation Application Manager.
Usando o IBM Support Assistant

IBM Support Assistant é um aplicativo gratuito e independente que pode ser instalado em qualquer estação de trabalho. O IBM Support Assistant economiza o tempo de procura de produto, suporte e recursos educacionais, além de ajudar a reunir informações de suporte quando você precisa abrir um PMR (Problem Management Record) ou ETR (Electronic Tracking Record), que pode ser utilizado para rastrear o problema.

Você pode, então, aprimorar o aplicativo instalando módulos de plug-in específicos do produto nos produtos IBM que utilizar. O plug-in específico de produto para Tivoli System Automation for Multiplatforms fornece os seguintes recursos:

- Links de suporte
- · Links de educação
- Capacidade para enviar relatórios de gerenciamento de problemas
- Capacidade para coletar rastreios

Instalando o IBM Support Assistant e o Plug-in do Tivoli System Automation for Multiplatforms

Para instalar o IBM Support Assistant V4.1, conclua estas etapas:

• Acesse o Web site do IBM Support Assistant:

www.ibm.com/software/support/isa/

- Faça download do pacote de instalação para a sua plataforma. Observe que você precisará registrarse com um ID do usuário e senha IBM (por exemplo, um ID do usuário de MySupport ou do developerWorks). Se você ainda não tiver um ID do usuário IBM, poderá preencher o processo de registro gratuito para obtê-lo.
- Descompacte o pacote de instalação em um diretório temporário.
- Siga as instruções no *Installation and Troubleshooting Guide*, incluído no pacote de instalação, para instalar o IBM Support Assistant.

Para instalar o plug-in do Tivoli System Automation for Multiplatforms, execute estas etapas:

- 1. Inicie o aplicativo IBM Support Assistant. IBM Support Assistant é um aplicativo da Web que é exibido no navegador da Web padrão configurado pelo sistema.
- 2. Clique na guia Atualizador no IBM Support Assistant.
- 3. Clique na guia **Novos Produtos e Ferramentas**. Os módulos de plug-in são listados pela família de produtos.
- 4. Selecione Tivoli > Tivoli Tivoli System Automation for Multiplatforms.
- 5. Selecione os recursos que você deseja instalar e clique em **Instalar** . Certifique-se de ler as informações sobre licença e as instruções de uso.
- 6. Reinicie o IBM Support Assistant.

Tivoli System Automation for Multiplatforms : Tivoli System Automation for Multiplatforms V4.1: Guia de Instalação e Configuração

Estas informações foram desenvolvidas para produtos e serviços oferecidos nos Estados Unidos.

É possível que a IBM não ofereça os produtos, serviços ou recursos discutidos nesta publicação em outros países. Consulte um representante IBM local para obter informações sobre produtos e serviços disponíveis atualmente em sua área. Qualquer referência a produtos, programas ou serviços IBM não significa que apenas produtos, programas ou serviços IBM possam ser utilizados. Qualquer produto, programa ou serviço funcionalmente equivalente, que não infrinja nenhum direito de propriedade intelectual da IBM poderá ser utilizado em substituição a este produto, programa ou serviço. Entretanto, a avaliação e verificação da operação de qualquer produto, programa ou serviço não IBM são de responsabilidade do Cliente.

A IBM pode ter patentes ou solicitações de patentes pendentes relativas a assuntos tratados nesta publicação. O fornecimento desta publicação não lhe garante direito algum sobre tais patentes. Pedidos de licença devem ser enviados, por escrito, para:

Gerência de Relações Comerciais e Industriais da IBM Brasil Av. Pasteur, 138-146, Botafogo Botafogo Rio de Janeiro, RJ CEP 22290-240

Os licenciados deste programa que desejarem obter informações sobre este assunto com o propósito de permitir: (i) a troca de informações entre programas criados independentemente e outros programas (incluindo este) e (ii) o uso mútuo das informações trocadas, deverão entrar em contato com:

Av. Pasteur, 138-146, Botafogo Av. Pasteur, 138-146 Botafogo Rio de Janeiro, RJ CEP 22290-240

Tais informações podem estar disponíveis, sujeitas a termos e condições apropriadas, incluindo em alguns casos o pagamento de uma taxa.

O programa licenciado descrito nesta publicação e todo o material licenciado disponível são fornecidos pela IBM sob os termos do Contrato com o Cliente IBM, do Contrato Internacional de Licença do Programa IBM ou de qualquer outro contrato equivalente.

Para pedidos de licença relacionados a informações de DBCS (Conjunto de Caracteres de Byte Duplo), entre em contato com o Departamento de Propriedade Intelectual da IBM em seu país ou envie pedidos de licença, por escrito, para:

Intellectual Property Licensing Legal and Intellectual Property Law IBM Japan, Ltd. 1623-14, Shimotsuruma, Yamato-shi Kanagawa 242-8502 Japan

O parágrafo a seguir não se aplica a nenhum país em que tais disposições não estejam de acordo com a legislação local: A INTERNATIONAL BUSINESS MACHINES CORPORATION FORNECE ESTA PUBLICAÇÃO "NO ESTADO EM QUE SE ENCONTRA", SEM GARANTIA DE NENHUM TIPO, SEJA EXPRESSA OU IMPLÍCITA, INCLUINDO, MAS A ELAS NÃO SE LIMITANDO, AS GARANTIAS IMPLÍCITAS DE NÃO INFRAÇÃO, COMERCIALIZAÇÃO OU ADEQUAÇÃO A UM DETERMINADO PROPÓSITO. Alguns países não permitem a exclusão de garantias expressas ou implícitas em certas transações; portanto, essa disposição pode não se aplicar ao Cliente. Essas informações podem conter imprecisões técnicas ou erros tipográficos. São feitas alterações periódicas nas informações aqui contidas; tais alterações serão incorporadas em futuras edições desta publicação. A IBM pode, a qualquer momento, aperfeiçoar e/ou alterar os produtos e/ou programas descritos nesta publicação, sem aviso prévio.

Referências nestas informações a websites não IBM são fornecidas apenas por conveniência e não representam de forma alguma um endosso a esses websites. Os materiais contidos nesses websites não fazem parte dos materiais desse produto IBM e a utilização desses websites é de inteira responsabilidade do Cliente.

Se estas informações estiverem sendo exibidas em cópia eletrônica, as fotografias e ilustrações coloridas podem não aparecer.

Marcas comerciais

- IBM, o logotipo IBM, ibm.com, AIX, DB2, developerWorks, HACMP, NetView, Tivoli, Tivoli Enterprise, Tivoli Enterprise Console, WebSphere e z/OS são marcas comerciais da International Business Machines Corporation nos Estados Unidos e/ou em outros países. IBM Redbooks e o logotipo IBM Redbooks são marcas registradas da IBM.
- Adobe, Acrobat, Portable Document Format (PDF) e PostScript são marcas registradas ou marcas comerciais da Adobe Systems Incorporated nos Estados Unidos e/ou em outros países.
- Microsoft, Windows e o logotipo Windows são marcas comerciais da Microsoft Corporation nos Estados Unidos e/ou em outros países.
- Java e todas as marcas comerciais baseadas em Java são marcas comerciais da Sun Microsystems, Inc. nos Estados Unidos e/ou em outros países.
- Linux é uma marca registrada de Linus Torvalds nos Estados Unidos e/ou em outros países.
- Red Hat e todas as marcas comerciais baseadas em Red Hat são marcas comerciais ou marcas registradas da Red Hat, Inc., nos Estados Unidos e em outros países.
- UNIX é uma marca registrada do The Open Group nos Estados Unidos e em outros países.
- Outros nomes de empresas, produtos e serviços podem ser marcas comerciais ou marcas de serviço de terceiros.

Índice Remissivo

Caracteres Especiais

árvore de serviços do TBSM incluindo colunas <u>117</u>

A

Adaptador de Automação automatizando 81 diálogo de configuração 73 usuário não raiz 90 adaptador de automação de ponta a ponta clusters UNIX e Linux 73 guia criador de logs 79 guia do adaptador 74 guia relatório 76 guia segurança 79 adaptadores de automação protegendo a conexão 126 arquivos de propriedades de entrada editando 84 modo silencioso 83 autorização como gerenciar 121 AVN 29

С

capacidade simultânea 34 chaves SSL públicas e privadas keystore e truststore 126 comportamento do sistema exemplo 48 comutador de segurança 88 configuração salvar 81 configuração do adaptador ativar segurança SSL 128 configuração silenciosa chamando 83 gerenciador de automação de ponta a ponta 83 configurando Adaptador de Automação 74 adaptador de automação de ponta a ponta 72 desempatador 48 system automation 45 Configurando Adaptador de Automação guia publicação de eventos 78 adaptador de automação de ponta a ponta configuração silenciosa 82 adaptador HACMP Guia Host que Usa o Adaptador 75 conhecimento obrigatório para este guia xi consoles de eventos Tivoli Enterprise Console

consoles de eventos *(continuação)* Tivoli Enterprise Console *(continuação)* Tivoli Netcool/OMNIbus <u>99</u>

D

desempatador AIX DISK 53 configurando 48 desempatador do NFS 63 disco compartilhado 50 ECKD z/VM 59 rede 61 SCSI 52 SCSIPR 56, 57 desempatador de disco SCSI 55 desempatador de rede comportamento de reserva 62 configurar 62 logs do sistema 63 recurso RSCT 63 desempatador do NFS configurando 66 proteção de tempo limite 68 desinstalando fix pack de serviço 41 recurso xDR 43 dispositivo de armazenamento caminho único 11 dispositivos de armazenamento caminhos múltiplos 12 distribuição eletrônica 1 DVD conteúdo 1

E

ECKD configuração do desempatador <u>50</u> ECKD DASD z/VM <u>60</u> empacotando recurso xDR <u>41</u> endereço de e-mail <u>xii</u> Ethernet on POWER systems <u>85</u> extensão IBM TEC instalando 108

F

fazendo upgrade recurso xdr <u>43</u> fix pack fix pack (continuação) desinstalando <u>41</u> nomenclatura de archive <u>39</u> obtendo 38

G

gerenciador de automação de ponta a ponta configuração silenciosa <u>83</u> grupos de volumes compartilhados <u>34</u>

I

IBM.TieBreaker 48 idiomas 25 iniciar operações 46 instalação executar 24 extensão IBM TEC 108 licença do produto 25 planejamento 1 pré-requisitos 2, 4 preparando 9 tarefas de pós-instalação 34 instalando 4.1.0.1 37 fix pack de serviço 40 fix packs do serviço 38 novas plataformas 37 política do SAP 43 xDR 41 instruções de uso arquivos específicos da plataforma 39 integração **Tivoli Business Service Manager 111** integrando 99 interface de rede falhas 85 Linux on System z 86 interface Ethernet 19 interfaces de rede redes separadas 14 Suportado 6 IP de serviço mover 15 ISO 9000 xii IVN 29

Κ

keystore e truststore chaves SSL públicas e privadas <u>126</u>

L

licença instalando 25 Try & Buy, atualizando 23 licença do recurso xDR instalando 42 ligação de interface 18 live partition mobility requisitos 7

Μ

marcas comerciais 134 mecanização ativar 47 desativar 47 mensagens de eventos do TEC ou do OMNIbus código do idioma 109 migrando Adaptador de Automação 30 concluindo 29 domínio 27 domínio de automação do sistema 27 nó 28 modelo de serviço definição 113 Tivoli Business Service Manager 112 modo silencioso arquivos de propriedades de entrada 83 saída 84 trabalhando 82

Ν

Netcool/OMNIbus definindo o acionador <u>114</u> network file system <u>7</u> número da versão <u>29</u>

0

o que há de novo? 4.1 xiii

Ρ

parâmetro ExcludedNodes 47 parâmetros ExcludedNodes 47 planejamento infraestrutura da rede 10 plataformas suportadas 5 Planejamento instalação 1 System Automation for Multiplatforms 1 pontos de montagem do NFS padrão 68 pós-instalação 34 pré-requisitos instalando 4 verificação 3 xDR 42 procedimento de retrocesso AIX e Linux 36 protegendo 121 publicações xi público deste guia xi pulsação de disco ativar 86

Q

quorum operacional

136 Tivoli System Automation for Multiplatforms : Tivoli System Automation for Multiplatforms V4.1: Guia de Instalação e Configuração

quorum operacional *(continuação)* substituindo <u>72</u>

R

realce <u>xi</u> recursos críticos protegendo <u>88</u> redes fisicamente separadas <u>17</u> redes físicas <u>15</u> redes lógicas <u>15</u> replicando arquivos de configuração <u>81</u> reserva persistente da SCSI**AIX** <u>55</u> ResoruceRestartTimeout <u>47</u> RetryCount <u>45</u> RSCT informações relacionadas xii

S

SCSI reserva persistente 55 SCSIPR desempatador 56 Linux for System z 57 segurança SSL ativar 128 servidor NFS AIX 66 llinux 65 sobre este guia xi SSL protegendo a conexão 126 suporte a códigos de idiomas 25 Suporte IPv6 ativando 89

T

TimeOut 45 Tivoli Business Service Manager configurando 112 integração com o System Automation for Multiplatforms 111 integrando recursos 114 modelo de serviço designação manual 114 pré-requisitos 112 Tivoli Enterprise Console configurando 108 consoles de eventos 99 Tivoli Netcool/OMNIbus ativar o arquivo de regras 106 atualizar banco de dados 105 campos de eventos 101 configurando 105 consoles de eventos 99 mapeamento de gravidade 104 pré-requisitos 100 **Tivoli System Automation** preparando a instalação 9

V

verificando <u>29</u> visualizações do TBSM customizando <u>116</u> VMware vMotion 7

Ζ

z/VM imagem de sistema único <u>8</u> realocação de convidado em tempo real 8

Tivoli System Automation for Multiplatforms : Tivoli System Automation for Multiplatforms V4.1: Guia de Instalação e Configuração



Número do Programa: 5724-M00

S517-1566-04

