

H3C iMC プラットフォーム トラブルシューティングガイド

ソフトウェアバージョン:IMC PLAT 7.3(E0701)

Copyright©2018New H3C Technologies Co., Ltd. All rights reserved.

本書のいかなる部分も、New H3C Technologies Co., Ltd.の事前の書面による同意なしには、いかなる形式または手段によっても複製または変更することはできません。

New H3C Technologies Co., Ltd.の商標を除き、本書に記載されている商標は、それぞれの所有者の所有物です。
本ドキュメントの情報は、予告なく変更されることがあります。

内容

はじめに	1
一般的なガイドライン	1
テクニカルサポートへの連絡	1
iMCプラットフォームのトラブルシューティング	2
2人のユーザーがデバイスにアクセスしている間は、iMCはデバイスに設定を割り当てるできません。	2
症状	2
ソリューション	2
VLAN対応H3Cデバイスの表示に失敗しました	2
症状	2
ソリューション	2
デバイスに到達できませんでした	3
症状	3
ソリューション	3
jserverプロセスの状態は次のとおりです。プロセスエラーのデータの監視	7
症状	7
ソリューション	8
iMCのアップグレードに失敗しました。SQL Serverデータベースが動的ポートを使用しているからです。	11
症状	11
ソリューション	12
一部のデバイスをiMCに追加できませんでした。	13
症状	13
ソリューション	13
自動構成ポーリングの実行後にシステムグループ属性の変更が反映されない	14
症状	14
ソリューション	14
SQL Server2005データベースサーバーのホスト名が変更された後、iMCをV7iにアップグレードできませんでした。	15
症状	15
ソリューション	15
iMCは、異なるデバイスに対して同一デバイスのアラームを生成します。	16
症状	16
ソリューション	16
iMCは一部のサービスファンクションの問合せ基準を自動的に記録します。	17
症状	17
ソリューション	18
データエクスポートファイルが大きすぎます	18
症状	18
ソリューション	18
管理者には、iMCリソースに対する読取り権限のみがあります。	20
症状	20
ソリューション	20
指定されたメモリーのアラームをフィルタできませんでした。	21
症状	21
ソリューション	21
アクセスデバイス上のメモリーのシャットダウンに失敗しました。	22
症状	22
iMCコンポーネントの配布に失敗した後、データベースに接続できない	24
症状	24
ソリューション	24
ファイアウォールが有効な場合、iMC LiveUpdateは使用できません。	27
症状	27
ソリューション	27

Jserver.exeを開始できない	27
症状	27
ソリューション	27
iMC NMEのトラブルシューティング	29
iMCアラームショートメッセージ転送障害	29
症状	29
ソリューション	29
アラーム分析時にiMCがルートアラームを特定できない	33
症状	33
ソリューション	33
iMCが予期されたアラームを受信しない	34
症状	34
ソリューション	34
iMCが予想されるメモリーのアップ/ダウンアラームを受信しない	35
症状	35
ソリューション	35
iMC ICCのトラブルシューティング	37
デバイスソフトウェアを導入、リストア、インポートするためのデバイスを追加できない	37
症状	37
ソリューション	37
デバイスソフトウェアの転送にTFTPを使用できませんでした。	38
症状	38
ソリューション	38
デバイス構成の手動バックアップに失敗しました	39
症状	39
ソリューション	39
FTPを使用してデバイス構成をバックアップできませんでした	41
症状	41
ソリューション	41
デバイスソフトウェアの転送にFTPを使用できませんでした。	42
症状	42
ソリューション	42
SFTPを使用してデバイスソフトウェアを転送できませんでした	43
症状	43
ソリューション	43
SCPを使用して装置構成をバックアップすることに関するエラーメッセージ	43
症状	43
ソリューション	44
iMC NetAssetのトラブルシューティング	45
iMCはネットワーク内のスタックデバイスを識別できませんでした。	45
症状	45
ソリューション	45
iMC Perfmのトラブルシューティング	46
CPU使用率を監視するためにF5デバイスインスタンスにデータが表示されない	46
症状	46
ソリューション	46
デバイスパフォーマンスモニターにデータがない	46
症状	46
ソリューション	47
非メモリーインデックスのモニターの追加に失敗しました	50
症状	50
ソリューション	51
ディレクトリ共有時にデバイス監視データが消失	52

症状.....	52
ソリューション.....	52
メモリーインデックスのモニターの追加に失敗しました.....	56
症状.....	56
ソリューション.....	57
モニターの追加直後にモニターデータを表示できませんでした。.....	59
症状.....	59
ソリューション.....	59
パフォーマンス管理の監視データはCLIの出力とは異なる.....	61
症状.....	61
ソリューション.....	61
VM移行後にVM監視インスタンスにデータがない.....	62
症状.....	62
ソリューション.....	63

はじめに

このドキュメントでは、iMCプラットフォームのトラブルシューティングについて説明します。

一般的なガイドライン

iMCの問題をトラブルシューティングする場合は、次の一般的なガイドラインに従ってください。

- 問題の原因を特定するために、次のようなシステムおよび構成情報を収集します。
 - 障害の症状および時間。
 - オペレーティングシステム、データベースおよび配布方法などのインストール環境情報。
 - ログメッセージ。
ログメッセージをダウンロードするには、System > System Configuration > Log Configurationを選択しボタンをクリックします。
 - 実行したステップとその結果。
- あなたがiMCプラットフォームが依存するWSMおよびプログラムとシステムに精通していることを確認してください。ソフトウェア依存性情報は、iMCプラットフォームの管理者ガイドに記載されています。
- プログラムファイルの置き換えまたはパッチのインストールが必要な場合は、リリースノートを使用してハードウェアおよびソフトウェアの互換性を確認してください。

テクニカルサポートへの連絡

このドキュメントのトラブルシューティング手順を使用しても問題を解決できない場合は、H3C Japanのテクニカルサポートに連絡してください。テクニカルサポート担当者に連絡するときは、次の情報を提供する準備をしてください。

- 「一般的なガイドライン」に記載されている情報。
- 製品のシリアル番号。
- テクニカルサポートの登録番号(該当する場合)。

この情報は、サポートエンジニアができる限り迅速にお客様を支援するのに役立ちます。

iMCプラットフォームのトラブルシューティング

次の情報は、iMCプラットフォームのトラブルシューティングガイダンスを提供します。

2人のユーザーがデバイスにアクセスしている間は、iMCはデバイスに設定を割り当てることができません。

症状

2人のユーザーがデバイスのシステムビュー(または機能ビュー)にアクセスしている間は、iMCはデバイスに設定を割り当てることができません。

ソリューション

考えられる原因は次のとおりです。

- iMCプラットフォームは、SNMPを介してデバイスと正しく通信できません。
- デバイスのシステムビュー(またはファンクションビュー)にアクセスしているユーザーの数が制限に達しました。一部のルータおよびハイエンドスイッチでは、ログインユーザー数に制限があり、デフォルトの制限は2です。

この問題を解決する手順は、次のとおりです。

- iMCプラットフォームがSNMPを介してデバイスと正しく通信できることを確認します。
- デバイスから1人のユーザーを切断するか、デバイスのシステムビューにアクセスできるユーザーの最大数を増やします。
デバイスのシステムビューにアクセスできるユーザーの最大数を増やすには、次のようにします。
 - a. デバイスにTelnet接続します。
 - b. システムビューを入力します。
 - c. ユーザーの最大数を変更するには、`configure-user count number`コマンドを使用します。

VLAN対応H3Cデバイスの表示に失敗しました

症状

VLAN対応H3CデバイスのVLAN情報は、SNMPツールを使用して取得できますが、iMCプラットフォームではこのデバイスをVLAN Devicesページに表示できません。デバイス上のSNMP設定は、iMCプラットフォーム上の設定と同じです。

ソリューション

デフォルトでは、H3Cデバイス上のSNMPパケットの最大サイズは1500バイトです。iMCがSNMPを介してデバイスのVLAN情報を取得するようにするには、デバイス上のSNMPパケットの最大サイズを(スイッチでサポートされるポートの最大数)/8より大きい値に設定する必要があります。

たとえば、H3Cデバイスが19200個のポートをサポートする場合、SNMPパケットがVLAN情報を格納する

には少なくとも19200ビット(2400バイト)が必要です。デバイス上のSNMPパケットの最大サイズは1500バイトであり、デバイスはVLAN情報を送信できず、iMCはデバイスのVLAN情報を取得できません。

次の式を使用して、必要なSNMPパケットの最大サイズを計算します。size=200+supported port number/8。ここで、200は、SNMPパケットの非データ部分(SNMPヘッダーなど)のサイズです。

この問題を解決するには、H3Cデバイス上のSNMPパケットの最大サイズを変更します。

1. デバイスにTelnet接続します。
2. system-viewコマンドを使用して、システムビューを入力します。
3. SNMPパケットの最大サイズを変更するには、snmp-agent packet max-size byte-countコマンドを使用します。

デバイスに到達できませんでした

症状

iMCはデバイスにpingできる場合でも、デバイスに到達できませんでした。

デバイスRDI02-S5820v2にはアクセスできません。未回復のアラームがまだ存在します。

図1 デバイスの詳細

Resource > RDSI02-S5820v2(192.168.40.101) ★ Add to My Favorites ? Help

Device Details		Action
Device Label	RDSI02-S5820v2 [Modify]	<div style="text-align: right; padding-right: 5px;">Synchronize</div> <div style="text-align: right; padding-right: 5px;">Refresh</div> <div style="text-align: right; padding-right: 5px;">Unmanage</div> <div style="text-align: right; padding-right: 5px;">Delete</div> <div style="text-align: right; padding-right: 5px;">Telnet</div> <div style="text-align: right; padding-right: 5px;">Open Web Manager</div> <div style="text-align: right; padding-right: 5px;">Ping</div> <div style="text-align: right; padding-right: 5px;">Traceroute</div> <div style="text-align: right; padding-right: 5px;">View Topology</div> <div style="text-align: right; padding-right: 5px;">MIB Management</div> <div style="text-align: right; padding-right: 5px;">IP/MAC Learning Query</div> <div style="text-align: right; padding-right: 5px;">Telnet/SSH Proxy</div> <div style="text-align: right; padding-right: 5px;">Open Device Panel</div> <div style="text-align: right; padding-right: 5px;">SSH</div>
Device Status	Unknown	
IP Address	192.168.40.101	
Mask	255.255.255.0	
sysOID	1.3.6.1.4.1.25506.1.844	
Device Model	H3C S5820V2-54QS-GE	
Device Category	Switches [Modify]	
System Description	H3C Comware Platform Software, Software Version 7.1.045, ESS 2413 H3C S5820V2-54QS-GE Copyright (c) 2004-2014 Hangzhou H3C Tech. Co., Ltd. All rights reserved.	
Maintenance Tag	No Maintenance Tag [Modify]	
System Name	RDSI02-S5820v2 [Modify]	
Contact	ZY [Modify]	
Location	DFDZ214 [Modify]	
Runtime	37 day(s) 21 hour(s) 14 minute(s) 12 second(s) 0 millisecond(s)	
Last Poll	2016-04-12 22:25:25	
Login Type	Telnet [Modify]	
Interfaces	65Interface List	

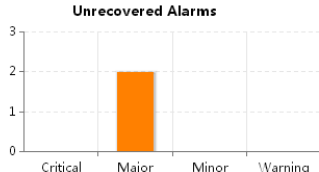
Service Monitoring | Trap Destination | Configuration Management | Network Assets

Monitoring Service Total Items: 0. [Customize](#)

Recent 10 unrecovered alarms

Level	Description	Alarm at
Major	Device "RDSI02-S5820v2" denied access.	2016-04-13 00:26:21
Major	Interface "M-GigabitEthernet0/0/0" State...	2016-02-24 02:16:25

Unrecovered Alarms



Level	Count
Critical	0
Major	2
Minor	0
Warning	0

Configure >

Performance Monitor >

Configuration Center >

VLAN Management >

ソリューション

考えられる原因は次のとおりです。

- pingパラメータが正しく設定されていません。
- Device Accessibleは、トラップフィルタリング規則に対して設定されます。
- アラーム管理コンポーネントとサーバー間の通信が異常です。

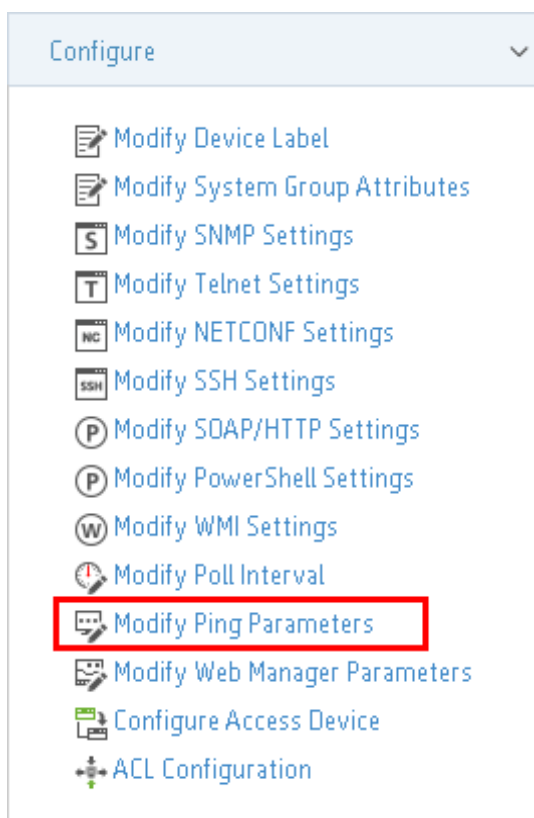
この問題を解決する手順は、次のとおりです。

- pingパラメータを変更します。
- フィルタリング規則を変更します。
- プロセスが停止状態かどうかを判別します。

pingパラメータを変更する

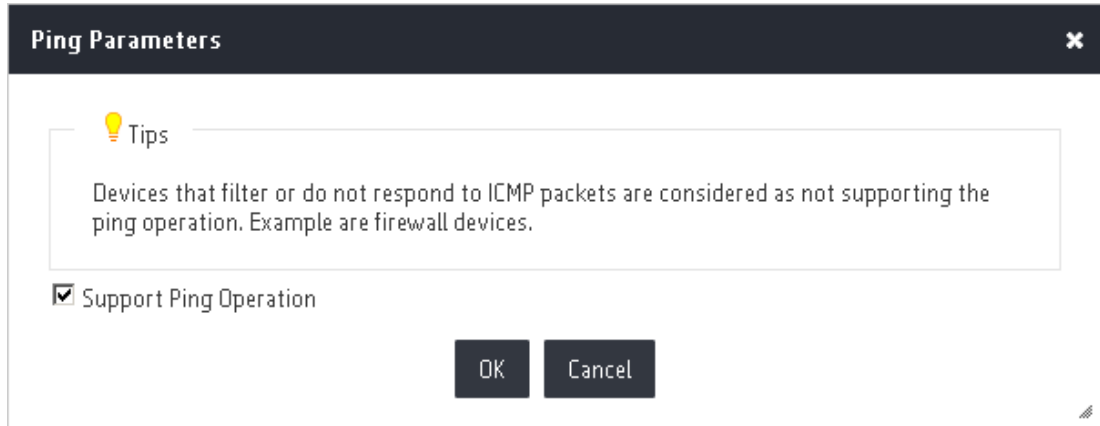
1. iMCIにAdministratorとしてログインします。
2. クエリーfield の右上隅に、デバイスのIPアドレス(たとえば、0.100)を入力します。IMCはこのフィールドに対してファジーマッチをサポートします。
3. クエリーアイコンをクリックします。
4. クエリー条件に一致するデバイスが表示されます。
5. ターゲットデバイスのデバイスラベルリンクをクリックすると、その詳細が表示されます。
6. Action領域でConfigure > Modify Ping Parametersを選択します。

図2 Pingパラメータの変更



7. pingを使用してデバイスが到達可能かどうかを識別するには、Support Ping Operationオプションを選択します。
デバイスが到達可能かどうかを識別するためにSNMPを使用する場合は、このオプションをクリアします。

図3 Pingパラメータの設定

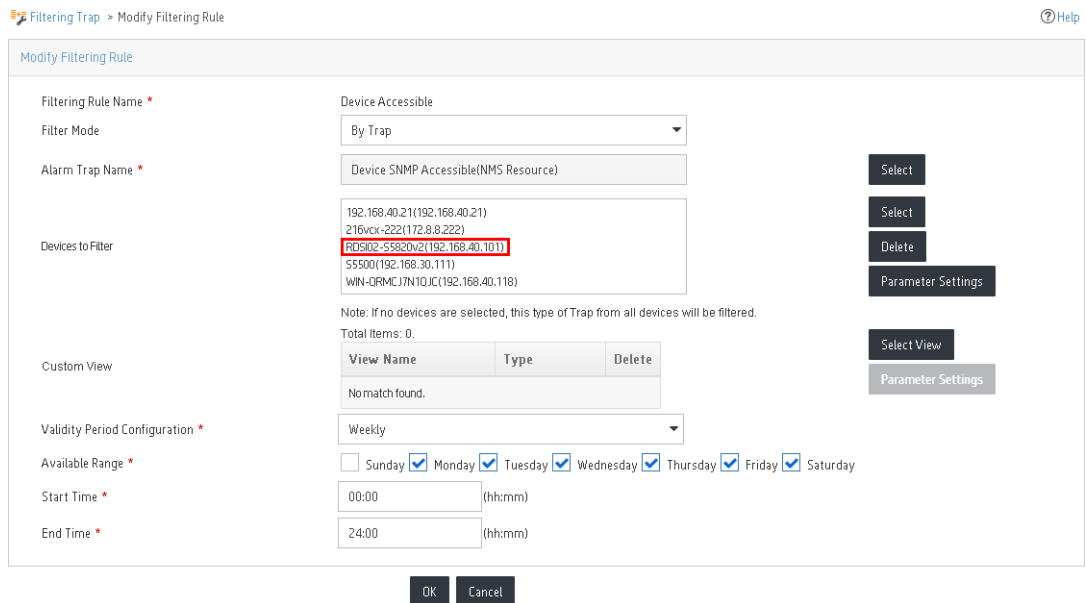


8. OKをクリックします。

フィルタリング規則を変更する

1. 管理者としてiMCIにログインします。
2. Alarmタブをクリックし、ナビゲーションツリーからTrap Management > Filtering Trapを選択します。
3. Filtering TrapページのTrap Name/Descriptionカラムで、Device AccessibleのModifyアイコンをクリックします。

図4 フィルタリング規則の変更



4. Modify Filtering RuleページでDevices to Filterから削除するデバイスを選択し、Deleteをクリックします。
5. OKをクリックします。

プロセスが停止状態かどうかを判別します。

1. マスターサーバーのIntelligent Deployment Monitoring Agentページでアラーム管理コンポーネントの展開場所を指定するためにDeployタブをクリックします。

図5 Deployタブ

Component Name	Description	Version	Status	Deployment ...
iMC Platform - Resource Management	Manages network resources such as ...	iMC PLAT 7.2 (E0403L...	Deployed	Master Server
iMC Platform - Alarm Management	Monitors and troubleshoots network ...	iMC PLAT 7.2 (E0403L...	Deployed	Master Server
iMC Platform - User Selfservice Manage...	Manages the self-service business a...	iMC PLAT 7.2 (E0403)	Undeployed	
iMC Platform - Guest Access Management	Manages guest accounts.	iMC PLAT 7.2 (E0403L...	Deployed	Master Server
iMC Platform - Intelligent Configuration...	Offers software upgrade for networ...	iMC PLAT 7.2 (E0403L...	Deployed	Master Server
iMC Platform - Report Management	Issues and displays service reports, ...	iMC PLAT 7.2 (E0403L...	Deployed	Master Server
iMC Platform - NE Management	Provides network element-level man...	iMC PLAT 7.2 (E0403L...	Deployed	Master Server
iMC Platform - Performance Management	Monitors and analyzes network perfo...	iMC PLAT 7.2 (E0403L...	Deployed	Master Server
iMC Platform - ACL Management	Configures ACLs for devices to imple...	iMC PLAT 7.2 (E0403L...	Deployed	Master Server
iMC Platform - Network Asset Manage...	Manage network assets.	iMC PLAT 7.2 (E0403L...	Deployed	Master Server
iMC Platform - Security Control Center	Monitors network events and control...	iMC PLAT 7.2 (E0403L...	Deployed	Master Server
iMC Platform - General Search Service ...	Manages the general search service ...	iMC PLAT 7.2 (E0403L...	Deployed	Master Server
iMC Platform - Syslog Management	Collects, filters, and analyzes syslog ...	iMC PLAT 7.2 (E0403L...	Deployed	Master Server
iMC Platform - VLAN Management	Manages VLAN resources.	iMC PLAT 7.2 (E0403L...	Deployed	Master Server
iMC Platform - Virtual Resource Manag...	Manages virtual resources.	iMC PLAT 7.2 (E0403L...	Deployed	Master Server
VXLAN Management	Manages VXLAN in the network.	iMC VXLAN 7.2 (E0403...	Deployed	Master Server
Resource Automation Management	Resource Automation Management	iMC RAM 7.2 (E0402)	Deployed	Master Server
QoS Manager - QoS Management	Configures and monitors QoS for the...	iMC QoS 7.2 (E0403)	Undeployed	
VAN Connection Manager	Manages virtual connections in the n...	iMC VCM 7.2 (E0402)	Deployed	Master Server
Wireless Service Manager	Manages the wireless service of the i...	iMC WSM 7.2 (E0502P...	Deployed	Master Server

Select a component, and activate the popup menu.

- コンポーネントがマスターサーバーに配備されている場合は、次のようになります。
 - a. サーバーにログインします。
 - b. **Process**タブをクリックします。
 - c. プロセスimcfaultdm.exeのステータスを表示します。
- コンポーネントが下位サーバーにデプロイされている場合:
 - a. サーバーにログインします。
 - b. **Process**タブをクリックします。
 - c. プロセスimcfaultdm.exeのステータスを表示します。

図6 プロセス タブ

Process	Status	Location	CPU(%)	MEM(KB)	Start Time	Type	Startup M...
dbman.exe	Started	Local Host	0	6,588	2016-04-13 00:19:21	Core Process	Auto
imcaddm.exe	Started	Local Host	0	28,632	2016-04-13 00:19:10	Manageable...	Auto
imccfgbakdm.exe	Started	Local Host	0	19,072	2016-04-13 00:19:21	Manageable...	Auto
imccmdmgrdm.exe	Started	Local Host	0	18,184	2016-04-13 00:19:21	Manageable...	Auto
imcfaultdm.exe	Started	Local Host	0	27,100	2016-04-13 00:19:21	Manageable...	Auto
imccicdm.exe	Started	Local Host	0	16,340	2016-04-13 00:19:21	Manageable...	Auto
imcinventorydm.exe	Started	Local Host	0	24,452	2016-04-13 00:19:10	Manageable...	Auto
imcjobmgrdm.exe	Started	Local Host	0	17,964	2016-04-13 00:19:21	Manageable...	Auto
imcd2topodm.exe	Started	Local Host	0	33,140	2016-04-12 22:20:25	Manageable...	Auto
imcnetresdm.exe	Started	Local Host	0	47,308	2016-04-12 22:20:25	Manageable...	Auto
imcperfdm.exe	Started	Local Host	0	26,332	2016-04-13 00:19:10	Manageable...	Auto
imcramdm.exe	Started	Local Host	0	104,832	2016-04-13 00:37:37	Manageable...	Auto
imcsyslogdm.exe	Started	Local Host	0	17,104	2016-04-13 00:37:37	Manageable...	Auto
imcupgdm.exe	Started	Local Host	0	20,568	2016-04-13 00:19:21	Manageable...	Auto
imcvlandm.exe	Started	Local Host	0	26,544	2016-04-13 00:37:37	Manageable...	Auto
imcvnmdm.exe	Started	Local Host	0	44,900	2016-04-13 00:37:37	Manageable...	Auto
imcvxlandm.exe	Started	Local Host	0	35,532	2016-04-13 00:37:37	Manageable...	Auto
imcwipsdm.exe	Started	Local Host	0	26,040	2016-04-13 00:37:37	Manageable...	Auto
imcwlandm.exe	Started	Local Host	0	64,528	2016-04-13 00:37:37	Manageable...	Auto
imcwanperfdm.exe	Started	Local Host	0	43,752	2016-04-13 00:19:11	Manageable...	Auto
img.exe	Started	Local Host	0	8,124	2016-04-13 00:19:21	Core Process	Auto

2. プロセスが**Stopped**状態の場合は、次のショートカットメニューから**Start Process**を選択します。imcfaultdm.exeを実行してプロセスを開始します。

問題が解決しない場合は、H3C Japanテクニカルサポートに連絡してください。

jserverプロセスの状態は次のとおりです。プロセスエラーのデータの監視

症状

デプロイメントモニターエージェントの**Process**タブでは、jserverプロセスの状態は”プロセスエラーの監視データ”の通りです。

次のエラーメッセージまたは条件が表示される場合があります。

- Webページの応答が遅いか、応答しません。OutOfMemoryエラーがWebメモリーに表示される場合があります。
- デプロイメント監視エージェントの**Process**タブでは、jserverプロセスの状態は” jserver process is Monitoring data of process error”です。
- 次のエラーメッセージがクライアント\log\imcforeground.logに表示される場合があります。
 - java.lang.OutOfMemoryError:Java ヒープスペース。
 - java.lang.OutOfMemoryError:GC オーバーヘッドの制限を超えました。
 - java.lang.OutOfMemoryError:PermGen スペース。
- デプロイメント監視エージェントの**Process**タブでjserverプロセスを停止することはできません。

図7 プロセスタブ

Intelligent Deployment Monitoring Agent								
Monitor Process Deploy Environment								
	Process	Status	Location	CPU(%)	MEM(KB)	Start Time	Type	Startup M...
▶	dbman.exe	Started	Local Host	0	5,460	2013-09-03 16:47:03	Manageable ...	Auto
▶	imcacldm.exe	Started	Local Host	0	19,856	2013-09-03 16:47:09	Manageable ...	Auto
▶	imccfgbakdm.exe	Started	Local Host	0	15,104	2013-09-03 16:47:09	Manageable ...	Auto
▶	imccmdmgrdm.exe	Started	Local Host	0	15,444	2013-09-03 16:47:09	Manageable ...	Auto
▶	imcfaultdm.exe	Started	Local Host	0	28,308	2013-09-03 16:47:09	Manageable ...	Auto
▶	imccicdm.exe	Started	Local Host	0	12,100	2013-09-03 16:47:09	Manageable ...	Auto
▶	imcinventorydm.exe	Started	Local Host	0	15,852	2013-09-03 16:47:09	Manageable ...	Auto
▶	imcjobmgrdm.exe	Started	Local Host	0	14,580	2013-09-03 16:47:09	Manageable ...	Auto
▶	imcl2topodm.exe	Started	Local Host	0	21,536	2013-09-03 16:47:09	Manageable ...	Auto
▶	imcnetresdm.exe	Started	Local Host	0	39,864	2013-09-03 16:47:08	Manageable ...	Auto
▶	imcperfdm.exe	Started	Local Host	0	18,168	2013-09-03 16:47:09	Manageable ...	Auto
▶	imcsyslogdm.exe	Started	Local Host	0	12,248	2013-09-03 16:47:09	Manageable ...	Auto
▶	imcupgdm.exe	Started	Local Host	0	16,532	2013-09-03 16:47:09	Manageable ...	Auto
▶	imcvlandm.exe	Started	Local Host	0	16,860	2013-09-03 16:47:09	Manageable ...	Auto
▶	imcvnmdm.exe	Started	Local Host	0	24,660	2013-09-03 16:47:09	Manageable ...	Auto
▶	img.exe	Started	Local Host	0	7,856	2013-09-03 16:47:03	Core Process	Auto
▶	lftpserver.exe	Started	Local Host	0	11,404	2013-09-03 16:46:53	Manageable ...	Auto
▶	jserver	Monitoring data of process error	Local Host	0	609,192	2013-09-09 12:07:05	Manageable ...	Auto

ソリューション

次のような理由が考えられます。

- jserverプロセスに割り当てられた最大メモリーサイズは、IMCコンポーネントの要件を満たすことができません。
- Out Of MemoryEmasエラーが発生した後、jserverプロセスはアンマネージドの状態になるため、デプロイメント監視エージェントのProcessタブでは停止できません。

この問題を解決する手順は、次のとおりです。

- jserverの最大メモリーサイズを変更します。
- jserverプロセスを停止します。

jserverの最大メモリーサイズを変更します。

1. デプロイメント監視エージェントのProcessタブでiMCプロセスを停止します。
2. コマンドプロンプトウィンドウ(Windowsの場合)またはターミナルウィンドウ(Linuxの場合)を開きます。
3. setmem.bat1024 768コマンド(Windowsの場合)またはsetmem.sh1024 768コマンド(Linuxの場合)を使用して、最大メモリーサイズを変更します。次の例では、Windowsを使用します。
 - 上記の最初と2番目のエラーに対しては、Max Heap memory(setmemの最初のパラメータ)を変更します。
 - 3番目のエラーでは、max PS Perm Gen memory(setmemの2番目のパラメータ)を変更します。

図8 最大メモリーサイズの変更

```
C:\Users\Administrator>cd "c:\Program Files\iMC\client\bin"

c:\Program Files\iMC\client\bin>setmem.bat
Usage: setmem maxMemorySize [maxPermSize]
(1) maxMemorySize - Max Heap memory (mb)
    <Recommendation: 1024 in 32 bit OS or 2048 in 64 bit OS>
(2) maxPermSize   - Max PS Perm Gen memory (mb)
    <Recommendation: 512 in 32 bit OS or 1024 in 64 bit OS>
    The arguments should be integer between 256 - 32768

c:\Program Files\iMC\client\bin>setmem.bat 1024 768
Change max Heap memory from 2048m to 1024m
Change max PS Perm Gen memory from 1024m to 768m
```

jserverプロセスを停止する

次の使用例は、Windowsを使用します。

1. Windowsタスクマネージャでjserverプロセスを停止します。
2. **View > Select Columns**を選択し、表示されるSelect Process Page Columnsページで**Virtual Memory Size** (Windows Server2003の場合)または**Memory-Commit Size** (Windows Server2008以降の場合)を選択します。

図9 列の選択

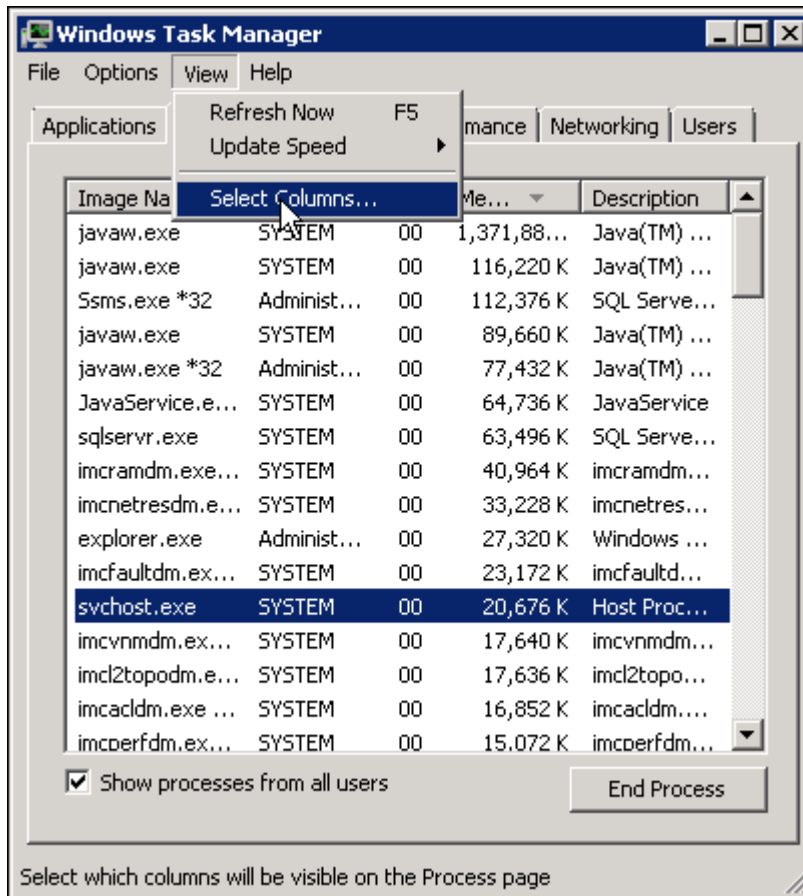
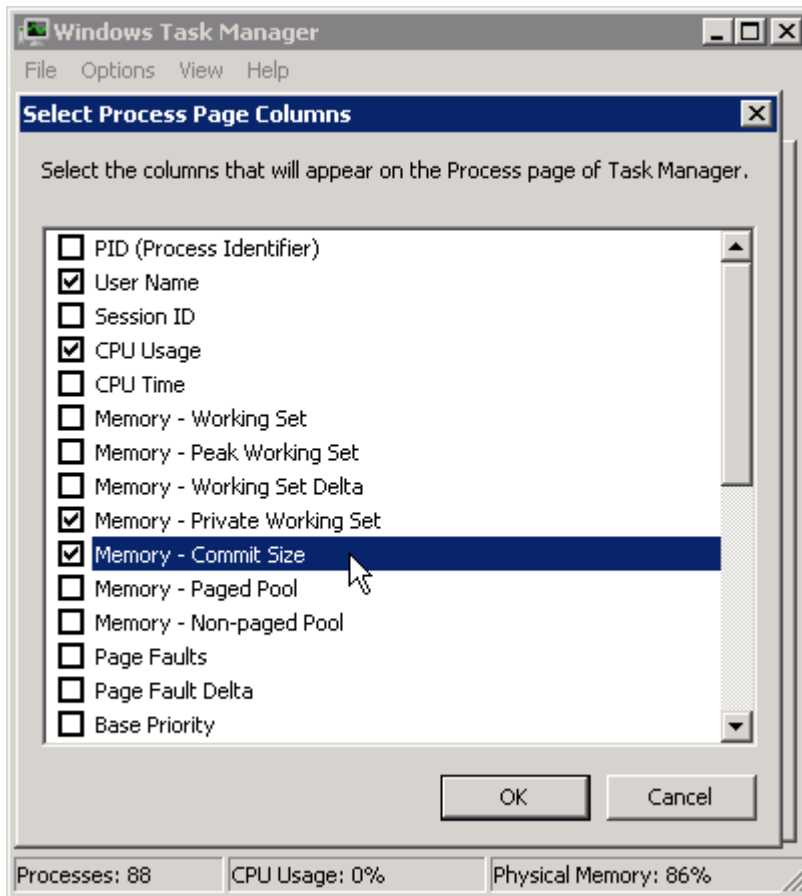


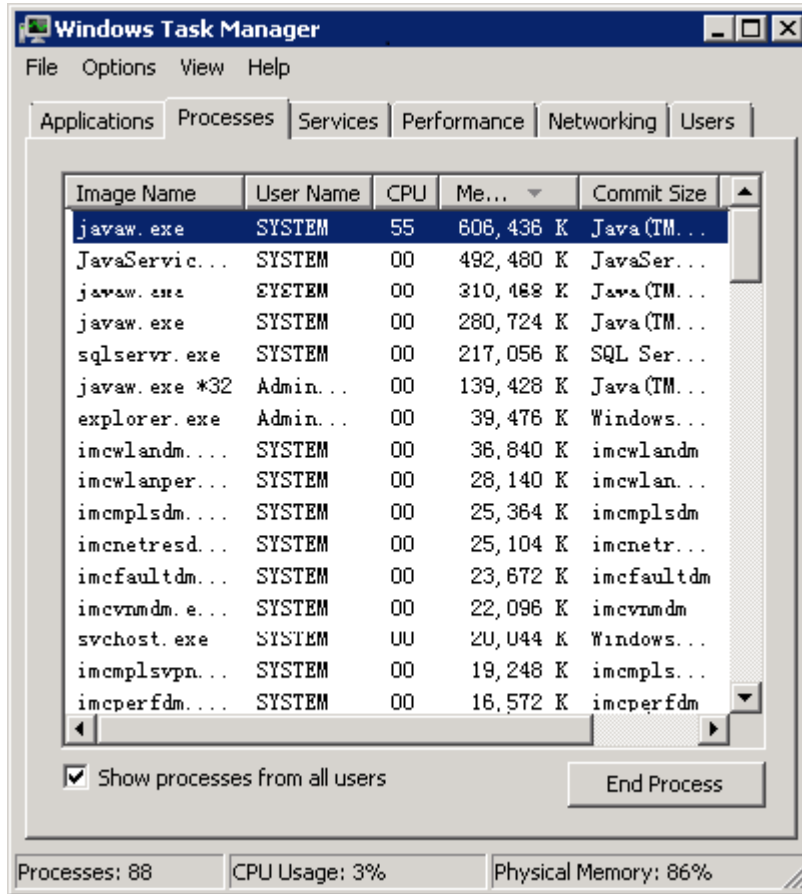
図10 メモリーの選択-コミットサイズ



3. Windowタスクマネージャで、jserverプロセスとほぼ同じ量のメモリーを使用するjavaw.exeプロセスを停止します。

Linuxの場合は、システム監視でJavaプロセスを停止します。ps -ef grep javaコマンドを使用してJavaプロセスのPIDを検索し、kill -9 pidコマンドを使用して停止することもできます。

図11 javaw.exeプロセスの停止



4. デプロイメントモニターエージェントでjserverプロセスを再始動します。

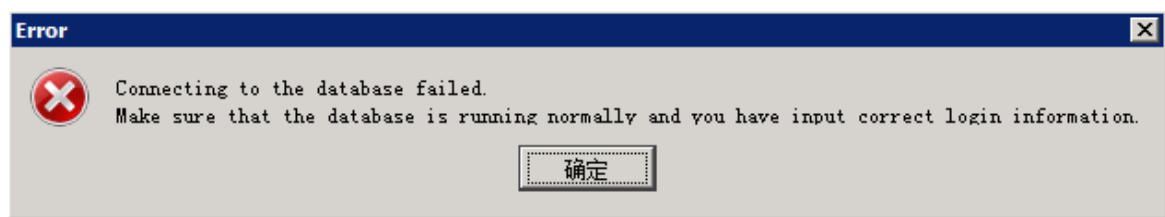
iMCのアップグレードに失敗しました。SQL Serverデータベースが動的ポートを使用しているからです。

症状

iMC V5.1は、SQL Serverデータベースが動的ポートを使用している場合、V5.2またはV7へのアップグレードに失敗することがあります。

- アップグレード中に、次のエラーメッセージが表示されます。

図12 エラーメッセージ



- デプロイメントでは
log%IMC_ROOT%\deploy\log\dmslog.txtor%IMC_ROOT%\deploy\log\dmllog.txtの場合は、

次のエラーメッセージが表示されます。

```
[ERROR] [Database Checking Thread]
[com.h3c.imc.deploy.dma.EnvPanel::retrieveSQLServerInfo(1010)] Access database error
com.microsoft.sqlserver.jdbc.SQLException: The TCP/IP connection to the host
127.0.0.1, port 50304 has failed. Error: "Connection refused: connect. Verify the
connection properties. Make sure that an instance of SQL Server is running on the host
and accepting TCP/IP connections at the port. Make sure that TCP connections to the port
are not blocked by a firewall."
```

ソリューション

考えられる理由は、SQL Serverが動的に変更される可能性のあるポートを使用するためです。

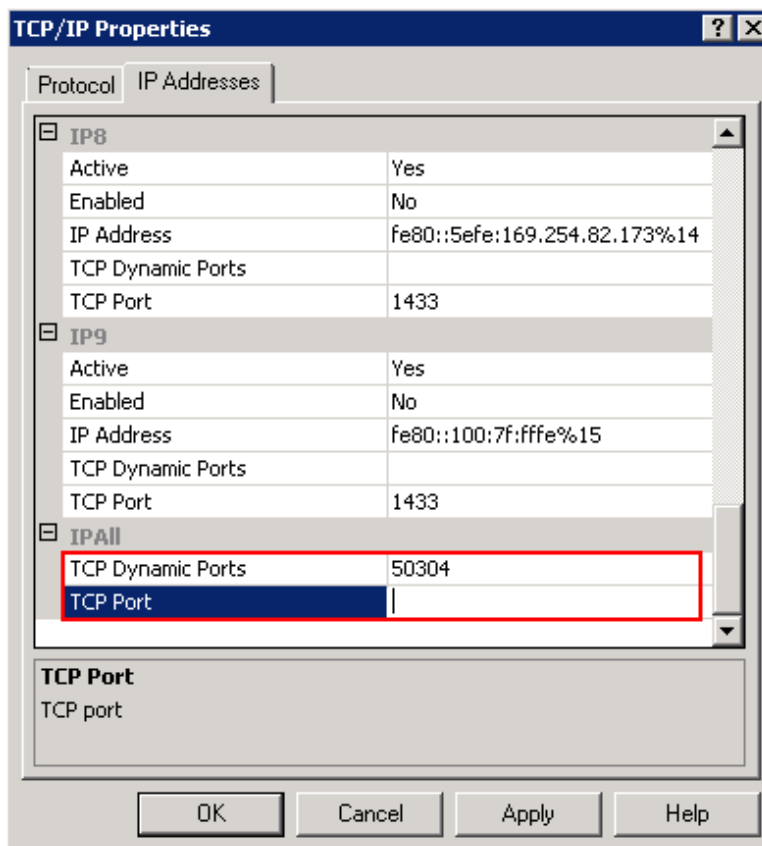
iMC V5.2以降のバージョンのSQL Serverデータベースでは、iMC V5.1以前のバージョンで使用されているJTDSドライバではなく、Microsoft JDBCドライバが使用されています。

動的ポートが使用されている場合、JDBCドライバはポートを識別できず、iMCのアップグレード中にデータベース接続が中断される可能性があります。

この問題を解決する手順は、次のとおりです。

1. SQL Server構成マネージャを開きます。
2. ナビゲーションツリーからSQL Server Network Configuration > **Protocols for MSSQLSERVER** を選択し、メインペインでTCP/IPをダブルクリックします。MSSQLSERVER文字列はデータベースインスタンスのデフォルト名です。正しいデータベースインスタンス名が選択されていることを確認してください。
3. IPAll領域で、TCP Dynamic Portsフィールドをクリアし、TCP PortにスタティックTCPポートを設定します。で変更できます。

図13 TCPポートの設定



4. SQL Serverサービスを再起動します。
5. %IMC_ROOT%\common\conf\server-addr.xmlファイルを開き、ファイル内のポート値を手順3でSQL Serverデータベース用に構成された静的ポートに変更します。

図14 ポート値の変更

```
<?xml version="1.0" encoding="UTF-8" standalone="no" ?>
-<server-addr>
- <component address="127.0.0.1" id="iMC-ACLM">
  <db-config address="127.0.0.1" dbname="aclm_db" password="-105-61-35-5-31-248-21-193-210-185-165-145-141-153-150-142-126" port="50304" type="SQLServer"
  username="imc_aclm" />
</component>
<component address="127.0.0.1" id="iMC-DM" />
- <component address="127.0.0.1" id="iMC-ETL">
  <db-config address="127.0.0.1" dbname="etl" password="-105-61-35-5-31-229-7-228-195-229-186-170-163-102-102-142-126" port="50304" type="SQLServer" username="etl" />
</component>
```

一部のデバイスをiMCに追加できませんでした。

症状

一部のデバイスをiMCに追加できませんでした。Server busy or Databaseエラーメッセージが表示されました。

図15 サーバーがビジー状態

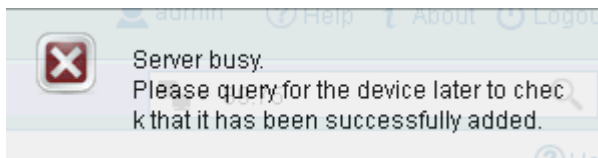
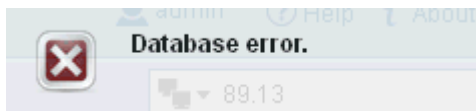


図16 データベースエラー



ソリューション

サーバービジーエラーは、次の状況で発生する可能性があります。

- iMCのimcnetresdm.exeプロセスで例外が発生しました。
- デバイスを追加する時間がデフォルトのタイムアウト時間を超えました。

データベースエラーは、SQL実行の失敗が原因で発生する場合があります。これは通常、デバイス情報に認識できない文字が含まれている場合に発生します。

この問題を解決する手順は、次のとおりです。

- imcnetresdm.exeプロセスを再起動します。
 - a. Intelligent Deployment Monitoring Agentで、Processタブをクリックします。実行中のすべてのプロセスが表示されます。
 - b. imcnetresdm.exeのショートカットメニューからStop Processを選択してプロセスを停止します。

- c. imcnetresdm.exeのショートカットメニューからStart Processを選択して、プロセスを再開します。
 - タイムアウト時間を変更します。
- iMCサーバーにログインします。
- a. iMCインストールパスの/client/confディレクトリにあるmsgcomm.Propertiesファイルを開きます。
 - b. java.cpp.adddev.timeout=100の100を180~300の範囲の値に変更します。
 - c. jserver.exeプロセスを再起動します(imcnetresdm.exeの再起動手順を参照してください)。プロセス)。
- 次の手順を実行します。
 - a. iMCサーバーにログインします。
 - b. iMCインストールパスの/server/conf/logディレクトリにあるログファイルimcnetresdm.txtを開きます。
 - c. 重大度レベルがエラーのログのうち、tbl_devまたはtbl_if_infoへの挿入を含むログを問い合わせます。
 2013-10-14 10:35:21.785 [ERROR (3092)] [THREAD(4408)] [CQvDBConnADP::executeSQL]
 Execute "insert into
 tbl_if_info(dev_id,ifindex,ifdesc,iftype,ifspeed,ifphyaddress,ifadminstatus,if
 optstatus,ifmtu,iflastchange,ifalias,ifStatus, ifAlarmStatus, userifspeed,
 ifPhyAttribute,ifTrapFilterType, ifSendAlarmFlag,
 iflastchangetime,ifduplexstatus)
 values(263,289407002,'Ethernet5/0/1',6,'0','00:0f:e2:3d:ab:27',1,2,9216,'5708'
 ,'**?,8,4,-1,1,0,0,convert(datetime,'2013-10-10 11:05:15:000',120),1)" failed,
 errorMsg:Incorrect syntax near '2013'.
 出力には、デバイス情報に認識されない文字が含まれているため、SQLの実行に失敗したことが示されています。たとえば、Ethernet5/0/1の説明には漢字が含まれています。
 - d. descriptiontextコマンドを実行して、メモリーEthernet5/0/1の説明を変更します。
メモリーの説明を変更するコマンドのサポートは、デバイスモデルによって異なります。

自動構成ポーリングの実行後にシステムグループ属性の変更が反映されない

症状

自動構成ポーリングは実行されますが、システムグループ属性の変更は反映されません。たとえば、contactおよびlocation属性の値は古い値のままです。

ソリューション

属性は構成ポーリング中にポーリングされません。デフォルトでは、システムは2時間ごとに部分構成ポーリングを実行し、6回の部分構成ポーリング間隔ごとに完全構成ポーリングを実行します。部分構成ポーリング中は、デバイスステータスやメモリーステータス情報などの共通情報のみが同期化されます。完全構成ポーリング中は、すべてのデバイス情報が同期化されます。

この問題を解決する手順は、次のとおりです。

設定ポーリングが完了するまで待つか、デバイス情報を手動で同期します。

SQL Server2005データベースサーバーのホスト名が変更された後、iMCをV7にアップグレードできませんでした。

症状

iMCではSQL Server2005が使用され、データベースのインストール後にデータベースサーバーのホスト名が変更されます。

ユーザーがiMCをV5.1またはV5.2からV7.0(E0102)にアップグレードしようとする、エラーが発生し、アップグレード操作が失敗します。

次のエラーメッセージがdmslog.txt又はファイル

```
%IMC_ROOT%\deploy\log\dmslog.txt(%IMC_ROOT%はiMCのインストールパスです)に見つかります。  
Could not find server 'CURR-HOSTNAME' in syssservers. Execute sp_addlinkedserver to add  
the server to syssservers.
```

出力では、文字列CURR-HOSTNAMEはデータベースサーバーの現在のホスト名を表します。

ソリューション

SQL Server2005のインストール時に、SQL Serverは実行するデータベースサーバーのホスト名を自動的に記録します。サーバーのホスト名が変更されるたびに、レコードを手動で更新する必要があります。更新しないと、SQL Server2005の一部の機能に障害が発生したり、使用できなくなったりする可能性があります。

iMCをアップグレードするときにSQL Server2005のホスト名レコードを更新しないと、SQL Server2005の機能障害によりアップグレード操作が失敗します。

この問題を解決するには、SQL Server2005のホスト名レコードを更新し、iMCアップグレード環境を修復します。

CLIでSQL Server2005をホストするサーバー上で次のコマンドを実行します。

1. データベースサーバーの現在のホスト名を確認して記録します。

```
hostname
```

2. saアカウント(または同じ権限を持つ別のアカウント)を使用してデータベースにログインします。

```
Osql -Usa -Ppassword
```

文字列passwordはsaユーザーのパスワードを表します。

3. SQL Serverによって記録されたサーバーホスト名を表示します。

```
Select @@servername
```

```
go
```

```
exit
```

4. saアカウントを使用してデータベースに再ログインし、SQL Serverによって記録されたホスト名エントリを変更します。

```
Osql -Usa -Ppassword
```

```
exec sp_dropserver 'OLD-HOSTNAME'
```

```
go
```

```
exec sp_addserver 'NEW-HOSTNAME', 'LOCAL'  
go  
exit
```

OLD-HOSTNAMEを古いホスト名に、NEW-HOSTNAMEを現在のホスト名に置き換えます。

5. SQL Serverサービスを再起動して、変更を検証します。

以前の障害後にiMCを再アップグレードする前に、まず次のいずれかの方法を使用してiMCプラットフォームを修復します。

- DBMANを使用してデータベースをバックアップした場合は、DBMANを使用してバックアップデータベースをリストアしてから、iMCを再アップグレードします。
- データベースをバックアップしていない場合は、最初にdeploy.xmlファイルを次の場所にバックアップします。
%IMC_ROOT%\deploy\components\iMC-PLAT\700R001B01D005\ディレクトリで、元のファイルを添付ファイルに置き換えてから、iMCを再アップグレードします。



Deploy.zip

iMCは、異なるデバイスに対して同一デバイスのアラームを生成します。

症状

iMCは、実際には異なるデバイスであるのに、同一デバイスのアラームを生成します。

ソリューション

iMCはMIBノード情報を読み取り、2つのデバイスまたは2つのデバイスメモリーのMACアドレスが同じであることを検出します。

この問題を解決する手順は、次のとおりです。

1. iMCにログインし、Alarmタブをクリックします。
2. ナビゲーションツリーから、Trap Management > Filtering Trapを選択します。サービスの導入ページが開きます。
3. Addをクリックします。Add Filtering Ruleページが開きます。図17に示すように、Filtering Rule Name、Filter ModeおよびAlarm Trap Nameフィールドを構成し、他のすべてのフィールドはデフォルトのままにします。
4. OKをクリックします。

図17 フィルタリング規則の追加

Filtering Trap > Add Filtering Rule Help

Add Filtering Rule

Filtering Rule Name *

Filter Mode

Alarm Trap Name *

Devices to Filter

Note: If no devices are selected, this type of Trap from all devices will be filtered.
Total Items: 0.

View Name	Type	Delete
No match found.		

Custom View

Validity Period Configuration *

Available Range * Sunday Monday Tuesday Wednesday Thursday Friday Saturday

Start Time * (hh:mm)

End Time * (hh:mm)

iMCは一部のサービスファンクションの問合せ基準を自動的に記録します。

症状

iMCプラットフォーム7.0以前のバージョンでは、問合せ操作を使用すると、一部のサービス機能(レポートなど)の問合せ基準が自動的に記録されます。

次の例では、レポートテンプレートを使用します:

1. Report Template Listページで、問合せ基準を入力します。Queryをクリックします。
2. その他のページにアクセスします。
3. Report Template Listページに再度アクセスします。以前に入力した問合せ基準は存在します。

図18 Report Template List

Report > Report Template List Help

Query Template

Template Name Type

+ Add Refresh Access Rights Download Data Source File

Template Name	Type	Definition Type	Details	Modify	Delete
Topology Report	Resource Statistics ...	Pre-defined			

1-1 of 1. Page 1 of 1.

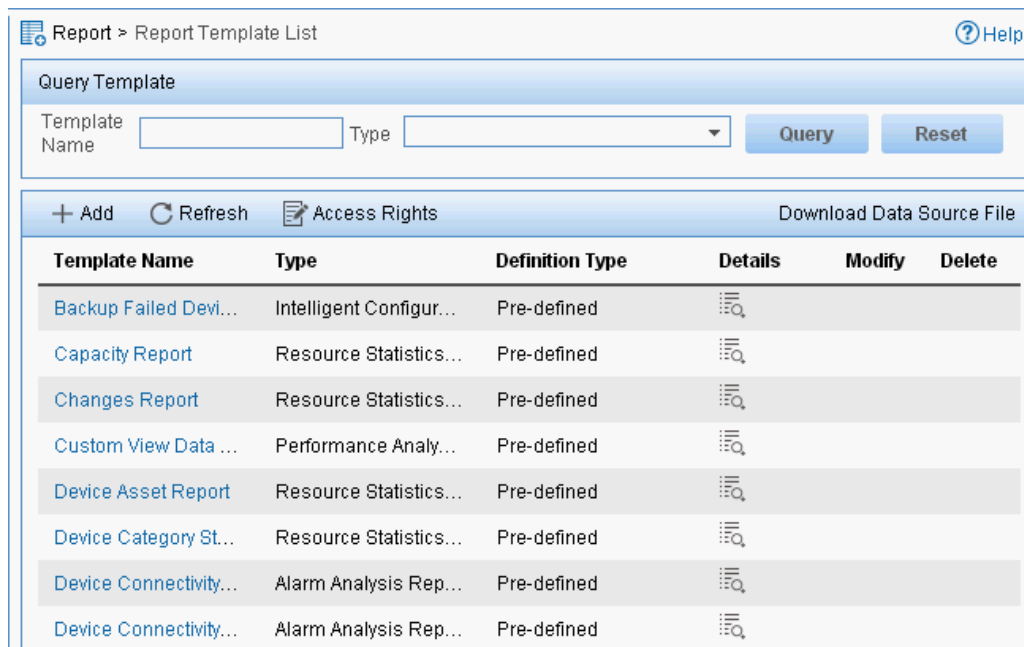
ソリューション

iMCでは、同じログイン中に問合せ操作を使用すると、一部の共通サービス機能の問合せ基準が自動的に記録されます。次に同じページにアクセスするときに、問合せ基準を再度入力せずに既存の問合せ結果を使用できます。

この問題を解決するには、次のいずれかの方法を使用します。

- ログアウトしてから再度ログインします。
- **Query Template**領域でResetをクリックします。

図19 問合せ基準のリセット



データエクスポートファイルが大きすぎます

症状

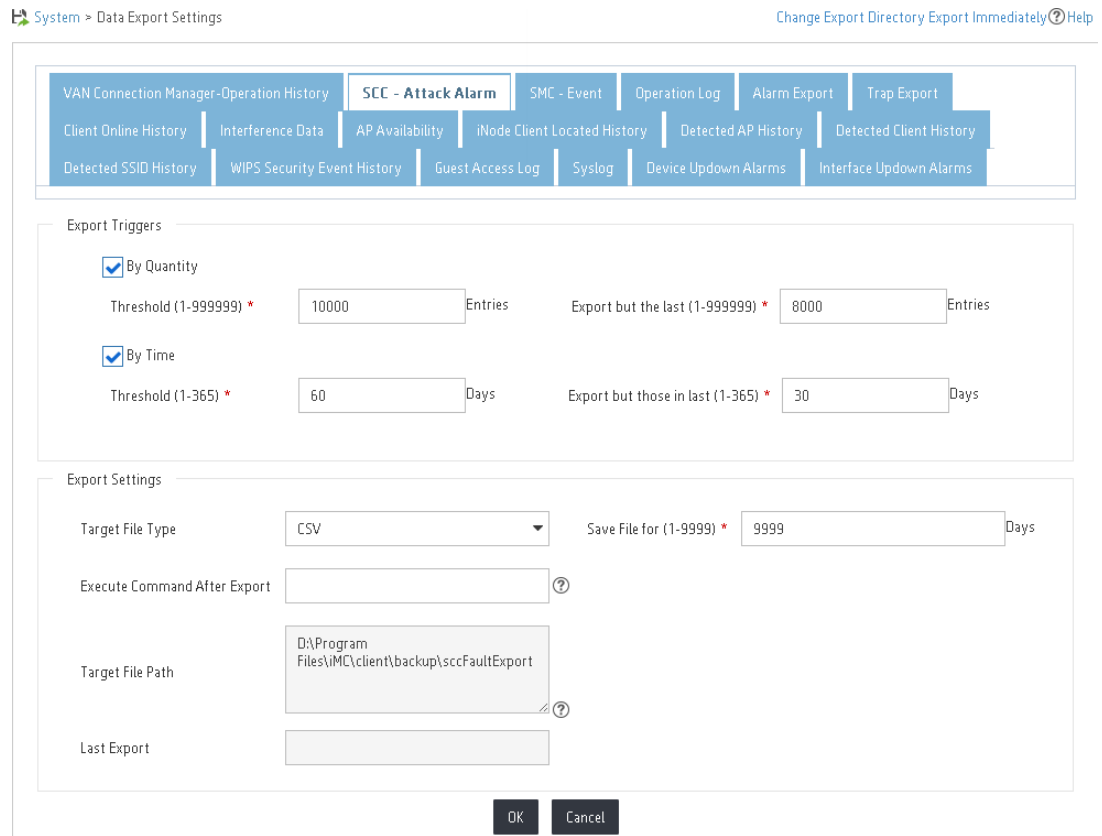
データエクスポートファイルが大きすぎて、大きすぎるディスクスペースが必要です。

ソリューション

データエクスポートファイルには大量のデータが含まれており、使用可能なディスク領域を大量に消費します。この問題を解決するには、次の手順を実行します。

- Save File for(1-9999)N Daysの値を変更します。期限切れのデータエクスポートファイルは自動的に削除されます。
 - a. iMCにログインし、Systemタブをクリックします。
 - b. ナビゲーションツリーから、System Configuration > Data Exportを選択します。
 - c. Data Export Settingsページで、Save File for(1-9999)N Daysフィールドを変更します。
 - d. OKをクリックします。

図20 データエクスポート設定の変更



- エクスポートディレクトリを変更します。新しいデータエクスポートファイルは、新しいストレージスペースに保存されます。
 - a. iMCにログインし、Systemタブをクリックします。
 - b. ナビゲーションツリーから、System Configuration > Data Exportを選択します。
 - c. Data Export Settingsの右上隅にあるChange Export Directoryリンクをクリックします。となります。
 - d. 開いたChange Export Directoryページで、新しいエクスポートディレクトリパスを入力します。
 - e. OKをクリックします。

図21 エクスポートディレクトリの変更

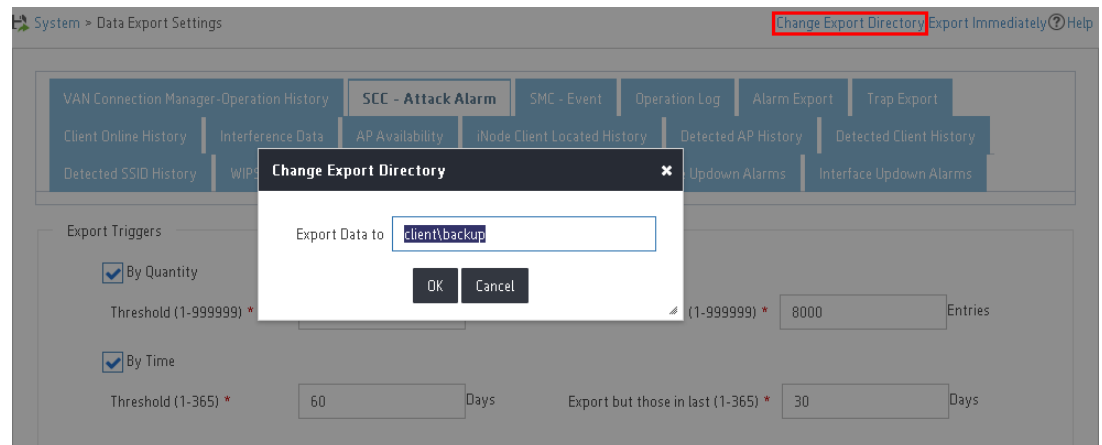
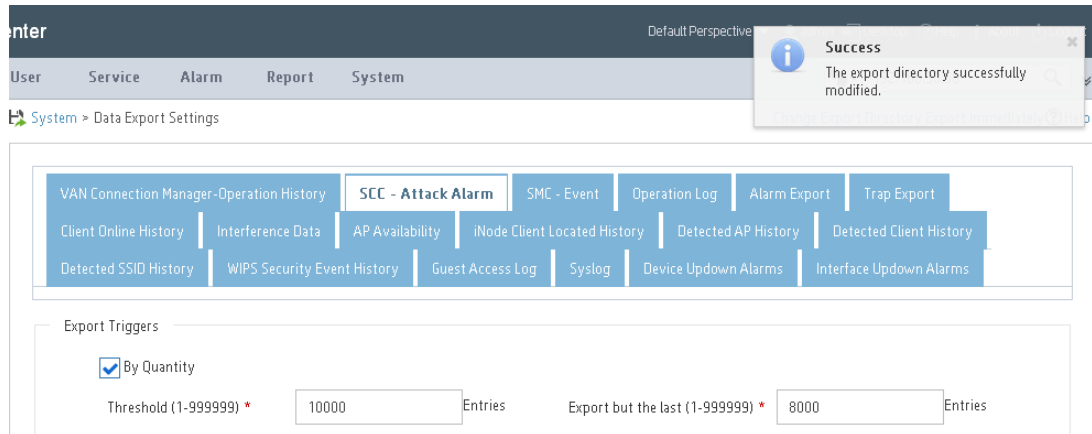


図22 エクスポートディレクトリの変更



- 不要なデータエクスポートファイルを手動で削除します。
 - a. iMCにログインし、Systemタブをクリックします。
 - b. ナビゲーションツリーから、System Configuration > Data Exportを選択します。
 - c. Data Export SettingsページのExport Settings領域で、ターゲットファイルパスを表示します。
 - d. このターゲットファイルディレクトリに移動し、不要なデータエクスポートファイルを削除します。

管理者には、iMCリソースに対する読取り権限のみがあります。

症状

オペレータは、別のiMCホストで生成されたライセンスを使用して、iMCをバックアップサーバーとして登録します。再起動してiMCにログインした後は、管理者はiMCリソースに対する読取り権限のみを持ちます。

ソリューション

ライセンスは別のiMCホストによって生成され、バックアップiMC管理者にiMCリソースを変更する権限は付与されません。

この問題を解決する手順は、次のとおりです。

1. 正しいiMCシリアル番号を持つ新しいライセンスを生成します。
2. Register Your Productページにアクセスし、アクティベーションキーファイルの横にあるChoose Fileをクリックして指定したホストによって生成されたライセンスを選択します。
3. OKをクリックします。
4. ライセンスの種類としてPrimaryを選択します。
5. OKをクリックします。

図23 iMCの登録

指定されたメモリのアラームをフィルタできませんでした。

症状

Interface Up/Down Alarm FilterパラメータがFilterとして設定された後でも、指定されたメモリのアップまたはダウンアラームを受信できません。

図24 メモリのダウン

<input type="checkbox"/>	Level	Alarm Source	Type	Description	Recovery	Ack Status
<input type="checkbox"/>	Major	WIN-VQQ8T6E4F2U(192.168.40.130)	iMC	The instance "[Device]" of "performance task" "Device Unreachability Proportion" is in threshold range (">=50%"), current value is "100%".	Unrecovered	Unacknowledged
<input type="checkbox"/>	Major	S5500(192.168.30.11)	Trap	The interface GigabitEthernet2/0/20 is DOWN.	\$SYSTEM	Unacknowledged
<input type="checkbox"/>	Major	S5500(192.168.30.11)	Trap	The interface GigabitEthernet2/0/23 is DOWN.	\$SYSTEM	Unacknowledged
<input type="checkbox"/>	Major	S5500(192.168.30.11)	Trap	The interface GigabitEthernet2/0/6 is DOWN.	\$SYSTEM	Unacknowledged
<input type="checkbox"/>	Major	WIN-VQQ8T6E4F2U(192.168.40.130)	iMC	The instance "[Device]" of "performance task" "Device Unreachability Proportion" is in threshold range (">=50%"), current value is "100%".	\$SYSTEM	Unacknowledged
<input type="checkbox"/>	Major	h04143z.h3c.huawei-3com.com(192.168.5.40)	iMC	The instance "[Memory:1]" of "performance task" "Memory Usage" is in threshold range (">=90%"), current value is "92.349%".	\$SYSTEM	Unacknowledged

ソリューション

次のような理由が考えられます。

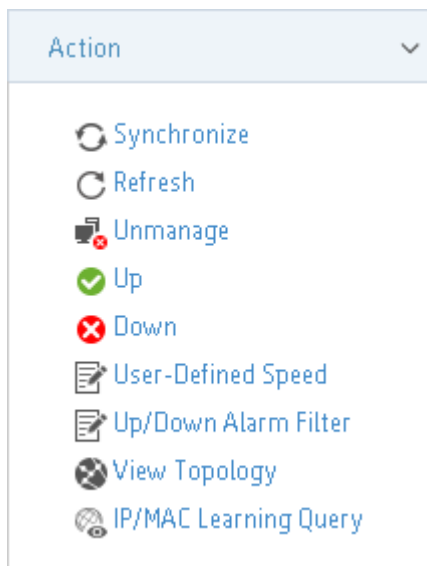
- メモリーに接続するPCまたはホストは、iMCに追加されません。
- Interface Up/Down Alarm FilterパラメータはFilterとして設定されません。

この問題を解決するには、次の手順を実行します。

- メモリーに接続するPCまたはホストをiMCに追加します。
 - a. 管理者としてiMCにログインします。
 - b. Resourceタブをクリックし、ナビゲーションツリーからResource Management > Add Deviceを選択します。
 - c. Add Deviceページで、Host Name/IPIにPCまたはホストのIPアドレスを入力します。

- d. OKをクリックします。
- e. 指定したメモリーのInterface Up/Down Alarm Filter設定を変更します。
- a. 管理者としてiMCにログインします。
- b. Resourceタブをクリックし、ナビゲーションツリーから View Management > Port Groupを選択します。
- c. Port Groupページで、グループ名のリンクをクリックして、メモリーの詳細を表示します。
- d. Interface Description列で、ターゲットメモリーの名前リンクをクリックします。
- e. ページ右側のActionエリアでUP/Down Alarm Filterを選択します。

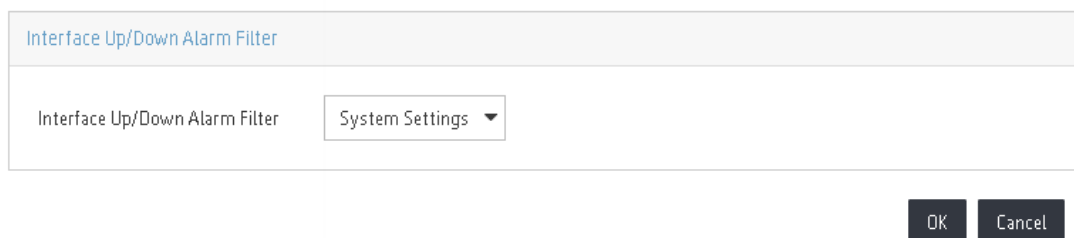
図25 Up/Downアラームフィルタ



- f. Interface Up/Down Alarm FilterリストからSystem Settingsを選択します。
- g. OKをクリックします。

図26 Configure interface Up/Downフィルタ

Resource > 55500(192.168.30.111) > Interface List > GigabitEthernet2/0/20 > Interface Up/Down Alarm Filter



アクセスデバイス上のメモリーのシャットダウンに失敗しました。

症状

不明なデバイスがメモリーを介してネットワークにアクセスしようとする、iMCはセキュリティポリシーに従

ってアクセスデバイス上のメモリーをシャットダウンできません。

ソリューション

アクセスデバイス上の読取りおよび書き込みコミュニティ名は、iMC上の名前と同じではありません。この問題を解決する手順は、次のとおりです。

1. 管理者としてiMCにログインします。
2. Resourceタブをクリックし、ナビゲーションツリーからView Management > Device Viewを選択します。
3. Device Labelカラムで、読取りおよび書き込みコミュニティ名を変更するデバイスの名前リンクをクリックします。
4. Device Detailsページで、ページの右端にあるConfigure領域で、Modify SNMP Settingsを選択します。
5. Read-Write Community Stringには、アクセスデバイス(この例ではprivate)に設定されているRead-Writeコミュニティ名を入力します。

図27 SNMPパラメータの変更

The screenshot shows a web browser window with the URL `192.168.1.135/imc/res/paratemplate/snmp/select.jsf?beanName=...`. The main content area contains a form with the following elements:

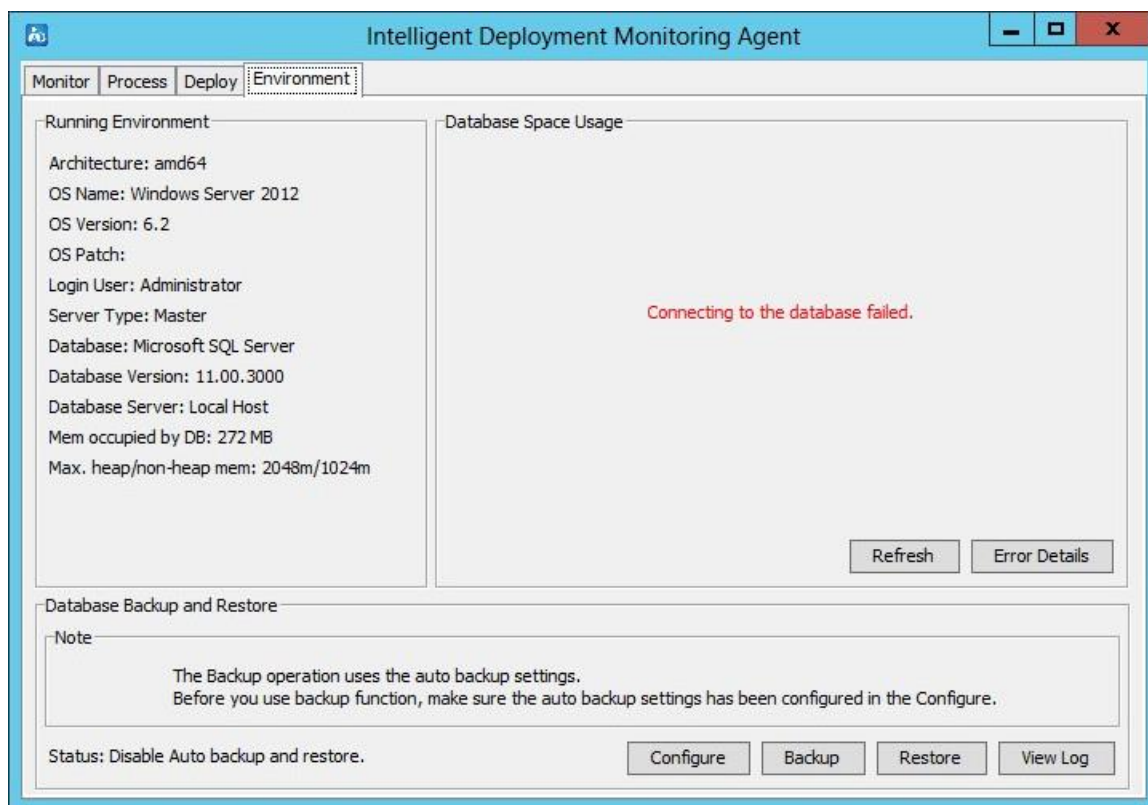
- Two radio buttons: Edit SNMP Parameters and Select an Existing Template.
- A dropdown menu for "Parameter Type" with the value "SNMPv2c".
- A text input field for "Read-Only Community String" containing six dots.
- A text input field for "Read-Write Community String" containing six dots.
- A text input field for "Timeout (1-60 seconds)" with the value "4".
- A text input field for "Retries (1-20)" with the value "3".
- Three buttons at the bottom: "Test", "OK", and "Cancel".

iMCコンポーネントの配布に失敗した後、データベースに接続できない

症状

iMCの展開が完了した後にユーザーがiMCを起動しようとすると、Intelligent Deployment Monitoring Agentによって、データベースに接続できないというプロンプトが表示されます。

図28 データベースへの接続に失敗した場合



ソリューション

考えられる原因は、iMCコンポーネントの配備に失敗したものの、その設定情報がserver-addr.xmlファイルに残っているために、iMCがコンポーネントのデータベースへの接続に失敗したことです。

この問題を解決する手順は、次のとおりです。

1. 接続できないデータベースを識別するには、次のいずれかの方法を使用します。
 - Intelligent Deployment Monitoring AgentのEnvironmentタブにあるError Detailsをクリックして、エラーの詳細を表示します。
 - iMCインストールパスの/deploy/logディレクトリにあるデプロイメントログファイルdmalog.txtを表示します。

この例では、qosm_dbという名前のデータベースは接続できません。

図29 エラーの詳細

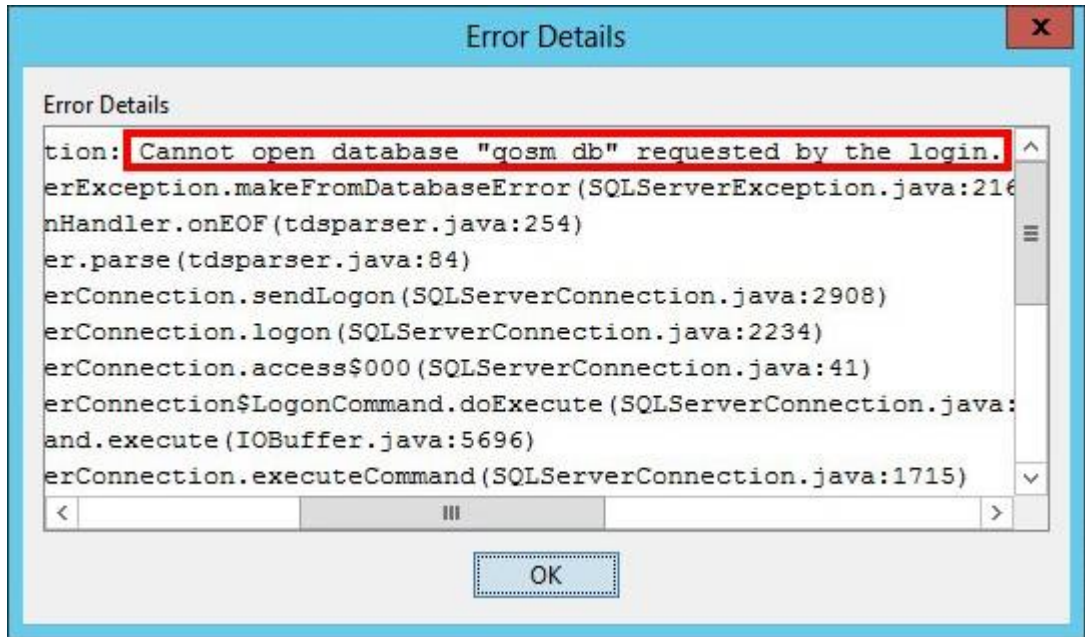
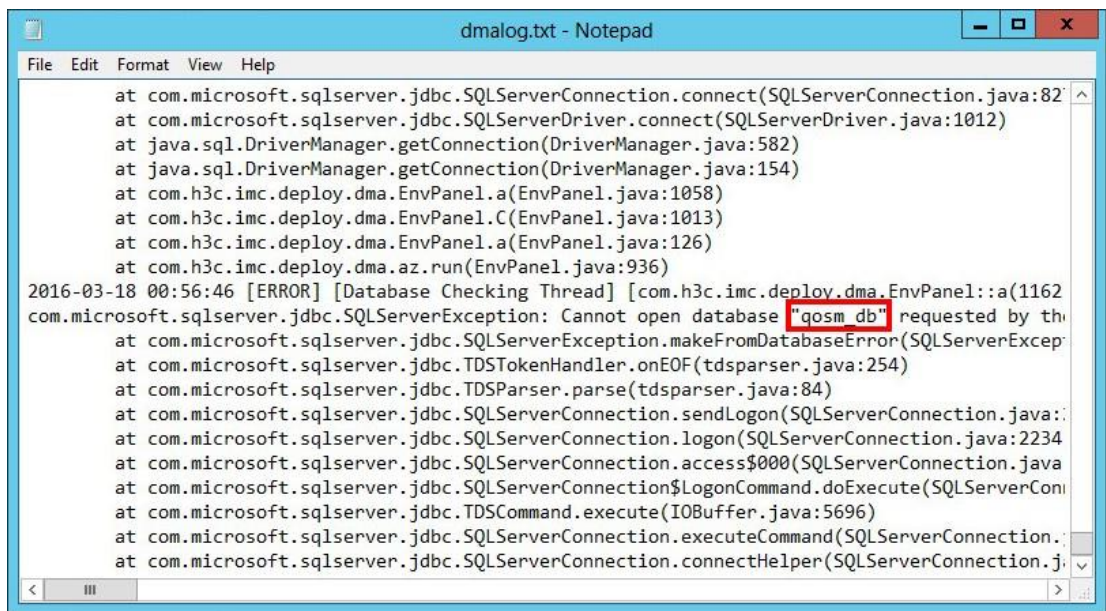


図30 エラーログ



2. iMCインストールパスの\common\confディレクトリにあるserver-addr.xmlファイルを開き、データベースが関連付けられているコンポーネントを検索します。コンポーネントがデータベースに正しく関連付けられていることを確認します。

ファイルにあるように、qosm_dbという名前のデータベースは、iMC QoS Managerコンポーネントに関連付けられています。

図31 QoS構成の検索

```

server-addr.xml - Notepad
File Edit Format View Help
<db-config address="127.0.0.1" dbname="perf_db" instance="IMCDB" password="-105-61-35-7-31-31" />
</component>
<component address="127.0.0.1" id="iMC-PLAT">
  <db-config address="127.0.0.1" dbname="config_db" instance="IMCDB" password="-105-61-35-7-31-31" />
</component>
<component address="127.0.0.1" id="iMC-PORTAL-KERNEL">
  <custom-addr name="PORTAL_IP" value="200.2.2.100"/>
  <custom-addr name="PORTALSERVER_IPv6_ADDR" value="" />
  <custom-addr name="PORTAL_SERVER_ID" value="20160303181956692"/>
</component>
<component address="127.0.0.1" id="iMC-QOSM">
  <db-config address="127.0.0.1" dbname="qosm_db" instance="IMCDB" password="-105-61-35-5-31-31" />
</component>
<component address="127.0.0.1" id="iMC-REPORT">
  <db-config address="127.0.0.1" dbname="reportplat_db" instance="IMCDB" password="-105-61-35-38-31-31" />
  <db-config address="127.0.0.1" dbname="report_db" instance="IMCDB" password="-105-61-35-38-31-31" />
</component>
<component address="127.0.0.1" id="iMC-SCC"/>
<component address="127.0.0.1" id="iMC-SEPLAT"/>
<component address="127.0.0.1" id="iMC-SSA">

```

- Intelligent Deployment Monitoring Agent のDeploy タブで、QoS Managerコンポーネントを右クリックし、ショートカットメニューからDeployを選択してコンポーネントを再デプロイします。

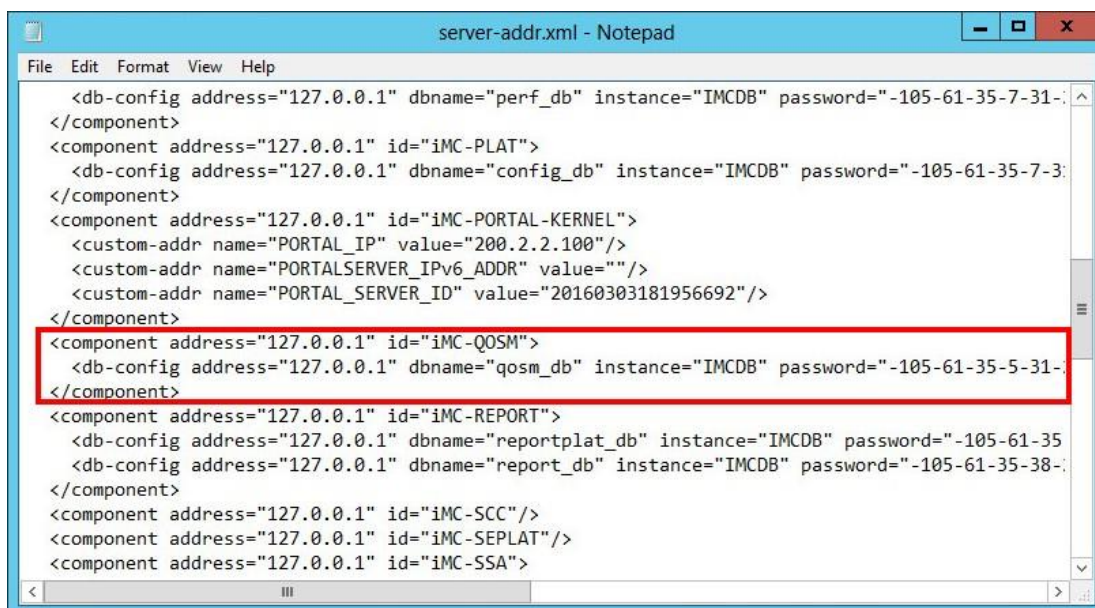
図32 Deployタブ

Component Name	Description	Version	Status	Deployment...
iMC Platform - Network Asset Manage...	Manage network assets.	iMC PLAT 7.2 (E0403)	Deployed	Master Server
iMC Platform - Security Control Center	Monitors network events and control...	iMC PLAT 7.2 (E0403)	Deployed	Master Server
iMC Platform - General Search Service ...	Manages the general search service ...	iMC PLAT 7.2 (E0403)	Deployed	Master Server
iMC Platform - Syslog Management	Collects, filters, and analyzes syslog...	iMC PLAT 7.2 (E0403)	Deployed	Master Server
iMC Platform - Virtual Resource Manag...	Manages virtual resources.	iMC PLAT 7.2 (E0403)	Deployed	Master Server
iMC Platform - Server & Storage Auto...	Manages network resources such as...	iMC SSA 7.2 (E0403)	Deployed	Master Server
VXLAN Management	Manages VXLAN in the network.	iMC VXLAN 7.2 (E0403)	Deployed	Master Server
Intelligent Strategy Proxy	iMC Intelligent Strategy Proxy	iMC ISP 7.2 (E0403)	Deployed	Master Server
User Access Manager - User Access M...	Configures users and access service...	iMC UAM 7.2 (E0403)	Deployed	Master Server
User Access Manager - Portal Server	Delivers Portal authentication.	iMC UAM 7.2 (E0403)	Deployed	Master Server
User Access Manager - EIP Server	Delivers End User Intelligent Profiling...	iMC EIP 7.2 (E0403)	Deployed	Master Server
User Access Manager - EIP Sub Server	Delivers End User Intelligent Profiling...	iMC EIP 7.2 (E0403)	Undeployed	
User Access Manager - Policy Server	Delivers security authentication.	iMC UAM 7.2 (E0403)	Deployed	Master Server
User Access Manager - User SelfService	Offers self-query and maintenance ...	iMC UAM 7.2 (E0403)	Deployed	Master Server
Third-Party Page Publish Server	Provides a special Web container to ...	iMC UAM 7.2 (E0403)	Deployed	Master Server
User Access Manager - Portal Server	Delivers Portal authentication.	iMC UAM 7.2 (E0403)	Undeployed	
User Access Manager - WeChat Authe...	Users can access the Internet by foll...	iMC UAM 7.2 (E0403)	Undeployed	
Third-Party Page Publish Server	Provides a special Web container to ...	iMC UAM 7.2 (E0403)	Undeployed	
QoS Manager - QoS Management	Configures and monitors QoS for the...	iMC QoSM 7.2 (E0403)	Undeployed	

Select a component, and activate the popup menu.

- それでも展開に失敗する場合は、server-addr.xmlファイル内のコンポーネント情報を削除します。

図33 QoS構成の削除



```
server-addr.xml - Notepad
File Edit Format View Help
<db-config address="127.0.0.1" dbname="perf_db" instance="IMCDB" password="-105-61-35-7-31-31" />
</component>
<component address="127.0.0.1" id="iMC-PLAT">
  <db-config address="127.0.0.1" dbname="config_db" instance="IMCDB" password="-105-61-35-7-31-31" />
</component>
<component address="127.0.0.1" id="iMC-PORTAL-KERNEL">
  <custom-addr name="PORTAL_IP" value="200.2.2.100"/>
  <custom-addr name="PORTALSERVER_IPv6_ADDR" value="" />
  <custom-addr name="PORTAL_SERVER_ID" value="20160303181956692" />
</component>
<component address="127.0.0.1" id="iMC-QOSM">
  <db-config address="127.0.0.1" dbname="qosm_db" instance="IMCDB" password="-105-61-35-5-31-31" />
</component>
<component address="127.0.0.1" id="iMC-REPORT">
  <db-config address="127.0.0.1" dbname="reportplat_db" instance="IMCDB" password="-105-61-35-38-31-31" />
  <db-config address="127.0.0.1" dbname="report_db" instance="IMCDB" password="-105-61-35-38-31-31" />
</component>
<component address="127.0.0.1" id="iMC-SCC" />
<component address="127.0.0.1" id="iMC-SEPLAT" />
<component address="127.0.0.1" id="iMC-SSA" />
```

5. Intelligent Deployment Monitoring Agentを再起動します。

ファイアウォールが有効な場合、iMC LiveUpdateは使用できません。

症状

iMC LiveUpdate機能は、iMCが配置されているサーバーでファイアウォールが有効になっている場合は使用できません。

ソリューション

iMCがインストールされているサーバーでファイアウォールを有効にすると、データベースサーバーはiMC LiveUpdate要求などのiMC通信要求を受信できなくなります。

この問題を解決するには、iMCが存在するサーバーでファイアウォールをディセーブルにします。

Jserver.exeを開始できない

症状

iMCのデプロイメントが完了すると、iMCメインプロセスjserver.exeを開始できなくなり、iMCが正常に動作しなくなります。

ソリューション

次の理由により、jserver.exeプロセスを開始できません。

- iMCメインプロセスjserver.exeによって使用されるポートは、サーバー上で実行されている別のプロセスによって占有されます。
- iMCはデータベースサーバーに接続できません。
- iMCはWindows Server2003 64ビット版に導入されておりWindowsServer2003-KB942288-v4-x64.exeは、iMCの導入前にはインストールされていません。
- iMCがデプロイされているサーバーに十分なメモリーがありません。
- Java仮想マシンのメモリーが不足しています。
- iMC内部リスナーを開始できません。
- その他不明な理由。

この問題を解決するには、次の手順に従います。

- ポートが別のプロセスによって占有されている場合は、次のいずれかの方法を使用します。
 - iMCを停止します。iMCのインストールパスにある\client\conf\http.propertiesファイルにアクセスします。ファイル内のimc.http.portまたはimc.https.portの値を、サーバーで使用可能なポート番号に変更します。
 - jserverが使用するポートを占有しているプロセスを停止します。
- iMCサーバーがデータベースサーバーに正しく接続されているかどうか、およびiMCデータベースがデータベースサーバー上で正しく起動されているかどうかを確認します。
- iMCを停止し、WindowsServer2003-KB942288-v4-x64.exeパッチをサーバーにインストールしてから、iMCインストールパスで\deploy\components\server\vcredist.exeを手動で実行します。
- readme_platに記載されているサーバー要件に従って、サーバー設定を調整します。
- iMCが32ビットオペレーティングシステムにインストールされている場合は、Webプロセス用割当て可能なJava実行メモリーを手動で変更します。
 - a. iMCインストールパスで\client\bin\setmem.batスクリプトまたはsetmem.shスクリプトを実行します。
 - b. setmem 1024 512コマンドを実行します。
 - 値1024は最大ヒープメモリーサイズです。値512は最大PermGenメモリーサイズです。
 - 32ビットオペレーティングシステムでは、ヒープメモリーサイズは1024を超えることはできません。また、PermGenメモリーサイズは768を超えることはできません。
 - c. jserverプロセスを再起動します。jserver.exeプロセスがまだ起動できない場合は、メモリーサイズを小さくして、起動できるようになるまでjserverを再起動します。
- 内部リスナーが失敗した場合、または原因が見つからない場合は、/client/logにあるすべてのログを収集します。
iMCインストールパスのディレクトリを指定し、H3C Japanテクニカルサポートに送信して分析を依頼します。

iMC NMEのトラブルシューティング

次の情報は、iMC NMEのトラブルシューティングガイドを提供します。

iMCアラームショートメッセージ転送障害

症状

iMCアラームショートメッセージ通知機能が有効になり、iMCはアラームを受信できますが、携帯電話はアラームショートメッセージを受信できません。

ソリューション

GSMモデムの性能を考慮して、メッセージ通知機能を設定するときには、アラームレベルをあまり多く選択しないでください。

考えられる原因は次のとおりです。

- GSMモデムで問題が発生。
- アラーム通知の設定が正しくありません。

この問題を解決するには、次の手順に従います。

- GSMモデムが正しく動作していることを確認します。
- qvdm.confファイルのLogLevelを変更します。
- アラーム通知設定が正しいことを確認してください。

GSMモデムが正しく動作していることを確認します。

1. iMCアラームプロセスを停止します(このプロセスでは、GSMモデム用のポートが使用される場合があります)。
 - a. iMCにログインし、Intelligent Deployment Monitoring Agentに移動します。
 - b. Processタブをクリックします。
 - c. imcfaultdm.exeプロセスを右クリックし、ショートカットメニューからStop Processを選択します。
2. GSMモデムをiMCサーバーシステムに接続します。分散iMCシステムの場合は、GSMモデムをアラームプロセスを実行しているホストに接続する必要があります。
3. GSMモデムの電源を入れ直します。数秒待つて、モデムが正常に動作しているかどうかを確認します。通信LEDが約3秒間隔で点滅する場合は、モデムは正常に動作しています。モデムが正常に動作していない場合は、モデムのトラブルシューティングを行います。詳細については、モデムのマニュアルを参照してください。
4. ターミナルエミュレーションプログラム(HyperTerminalなど)を実行してモデムに接続し、正しい通信設定を構成します。速度設定が正しくない場合は、文字化けして表示されます。
5. atコマンドを入力して、モデムが正しく接続されているかどうかを確認します。OKが返された場合は、モデムは正しく接続されています。ERRORが返された場合は、手順4に進んで設定を変更します。
6. at+cscsaコマンドを入力して、正しいSMSC番号が設定されているかどうかを確認します。SMSC番号がまだ設定されていない場合は、at+cscsa="+8613800100500"コマンドを入力してSMSC番号を設定します。この例では、SMSC番号は8613800100500です。

7. モデムが短いメッセージを送信できることを確認します。

短いメッセージをテキスト形式で送信するようにモデムを設定するには、次の手順を実行します。

- a. `at+cmgf=1`と入力して、メッセージフォームをテキストに設定しま

`at+cmgs=18310042216`と入力します。この例では、ショートメッセージを受信する電話番号は18310042216です。

- b. 大なり記号(>)に続けて短いメッセージを入力し、携帯電話がメッセージを受信するかどうかを確認します。携帯電話がメッセージを受信しない場合は、モデムを交換します。

図34 ショートメッセージの設定

```
at
OK
at+cscs?
+CSCA: "+8613800100500",145

OK
at+cmgf=1
OK
at+cmgs=18310042216
> hello→
+CMGS: 88

OK
-
```

PDU形式で短いメッセージを送信するようにモデムを設定するには、次の手順を実行します。

- a. `at+cmgf=0`と入力して、メッセージフォームをPDUに設定します。

- b. `at+cmgs=20`と入力して、PDUパケット長を設定します。

- c. `>0891683108100005f011ff0b818113002412f60008a806c8329bfd0e01`と入力し、Ctrl+Zを押します。携帯電話にHello!というメッセージが表示されるかどうかを確認します。メッセージが表示されない場合は、モデムを交換してください。

図35 PDUの構成

```
at
OK
at+cmgf=0
OK
at+cmgs=20
> 0891683108100005f011ff0b818113002412f60008a806c8329bfd0e01→
+CMGS: 95

OK
-
```

PDU形式文字列は次の部分から構成されます。

- **0891**
- SMSC番号文字列:この文字列は、次の手順で取得されます。
 - 数値文字列の末尾にFを追加します。
 - 2文字ごとにスワップします。
- **11ff0b**
- 宛先番号タイプ81は国内番号で、91は国際番号です。

- Destination phone number string:この文字列は次の手順で取得されます。
 - 数値文字列の末尾にFを追加します。
 - 2文字ごとにスワップします。
- **00**
- 言語コード08は中国語で、00は英語です。
- **a8**
- メッセージ長(バイト単位)この例では、メッセージHello!は6バイトを使用します。
- この例では、Messageは4f60597d0021(Hello!のコード)。

qvdm.confファイルのLogLevelを変更します。

モデムが正常に動作している場合は、\server\conf内のqvdm.confファイルのLogLevelを変更します。
iMCインストールパスのディレクトリ:LogLevel=DEBUG。

アラーム通知設定が正しいことを確認します。

1. 端末エミュレーションプログラムをクローズし、アラーム処理を開始または再起動します。iMCアラーム処理を開始または再起動する手順は、次のとおりです。
 - a. iMCにログインし、Intelligent Deployment Monitoring Agentに移動します。
 - b. Processタブをクリックします。
 - c. imcfaultdm.exeプロセスを右クリックし、ショートカットメニューからStart Processを選択します。
2. Systemタブをクリックし、ナビゲーションツリーからSystem Configuration > SMSC Settingsの順に選択して、SMSC Configurationページにアクセスします。
3. SMSC項目のAddまたはModifyアイコンをクリックします。✎

図36 SMSCの変更

4. モデムの設定と同じになるように設定します。
5. Alarmタブをクリックし、ナビゲーションツリーからAlarm Settings > Alarm Notificationを選択して、アラーム通知および転送管理ページを表示します。

図37 アラーム通知

Alarm Notification ★ Add to My Favorites ? Help

[Configure Mail Server](#)

Add Refresh

Mail Notification Total Items: 0.

Rule Name	Destination Mail Address	Status	Modif	Copy	Delete
No match found.					

[Configure SMSC](#)

Add Refresh Export

Message Notification Total Items: 0.

Rule Name	Mobile Phone Number	Status	Modif	Copy	Delete
No match found.					

Add Refresh

Alarm Forwarding Total Items: 0.

Rule Name	Destination Address/Port	Status	Modif	Copy	Delete
No match found.					

6. ショートメッセージ通知の設定を正しく構成します。

ショートメッセージ通知設定がすでに構成されている場合は、ルール Modify アイコンをクリックして、ルール名以外の設定を変更します(既存のルールのルール名は変更できません)。

ショートメッセージ通知設定が設定されていない場合は、次のように設定を追加します。

- a. Add をクリックします。
- b. 次の設定を行います。
 - Rule name - ルール名を入力します。
 - Telephone Number - ショートメッセージを受信した電話機の番号を電話番号リストに追加します。
 - Concerned Alarm Levels - 関連するアラームレベルを選択します。モデムのパフォーマンスを考慮して、選択するレベルが多すぎないようにしてください。
 - Concerned Devices - 関連するデバイスを選択します。All Devices を選択するか、iMC プラットフォームからデバイスを選択できます。
 - Connected Alarms - 関連するアラームを選択します。すべてのアラームを得るには All Alarms を選択します。
 - Time Ranges - システムがショートメッセージ通知を送信する時間範囲を選択します。
- c. OK をクリックします。

アラーム分析時にiMCがルートアラームを特定できない

症状

iMCでは、デバイスから生成されたすべてのアラームからルートアラームを正しく分析および検出できません。

ソリューション

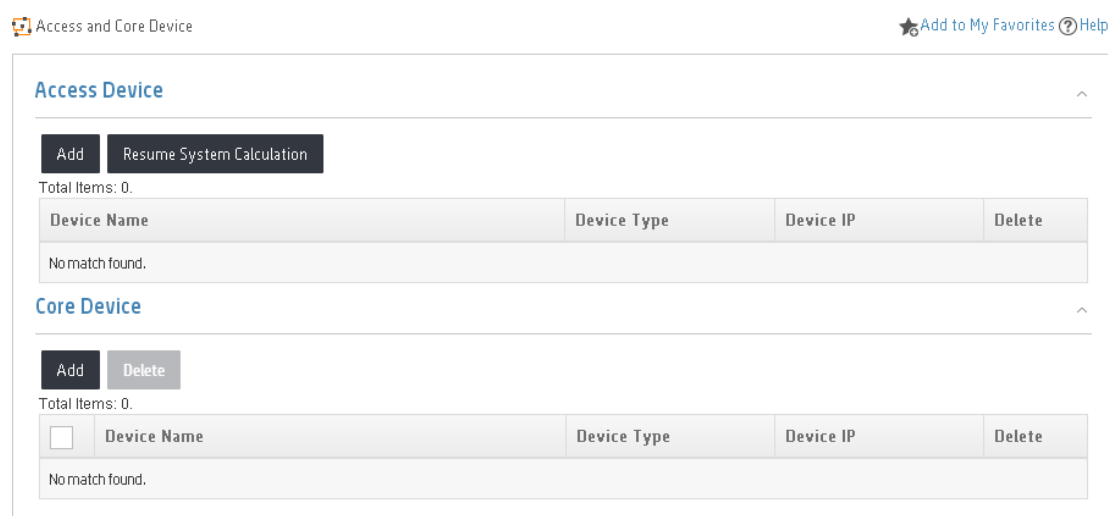
次のような理由が考えられます。

- 現在のアラームが存在するデバイスと、アラームソースが存在するデバイスは直接接続されていません。
- アクセスデバイスまたはコアデバイスが設定されていないか、正しく設定されていません。

この問題を解決するには、次の手順を実行します。

1. アラームを生成する2つのデバイス間にリンクが存在するかどうかを確認します。
 - a. Resourceタブをクリックします。
 - b. ナビゲーションツリーから、View Management > Network Topologyを選択します。
 - c. 2つのデバイスを見つけ、それらの間にリンクが存在するかどうかを確認します。
2. アクセスデバイスおよびコアデバイスを設定します。
 - a. Alarmタブをクリックします。
 - b. ナビゲーションツリーで、Alarm Settings > Access and Core Deviceを選択します。
 - c. Access Device領域とCore Device領域でAddをクリックして、アクセスデバイスとコアデバイスをそれぞれ追加します。

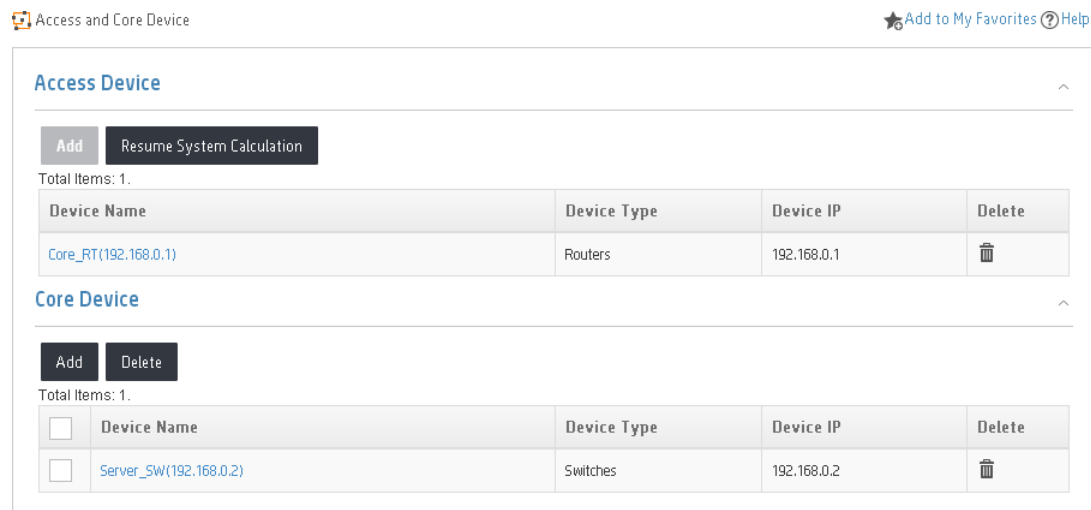
図38 アクセスおよびコアデバイス



3. アクセスデバイスおよびコアデバイスを変更します。
 - a. ネットワークトポロジを分析して、適切なアクセスデバイスとコアデバイスを特定します。
 - b. Alarmタブをクリックします。

- c. ナビゲーションツリーで、Alarm Settings > Access and Core Deviceを選択します。
- d. Access Device and Core Deviceで既存のデバイスのDeleteアイコンをクリックします。🗑領域で指定します。
- e. Access Device領域とCore Device領域でAddをクリックして、それぞれ正しいアクセスデバイスとコアデバイスを追加します。

図39 アクセスおよびコアデバイスの追加



iMCが予期されたアラームを受信しない

症状

デバイスがトラップを送信した後、予期されたアラームはiMCに表示されません。

ソリューション

次のような理由が考えられます。

- iMCが予想されるメモリーのアップ/ダウンアラームを受信しない場合は、“iMCが予想されるメモリーのアップ/ダウンアラームを受信しない”を参照してください。
- ユーザー定義のトラップフィルタ規則によって、トラップが除外されます。
- トラップはiMCで定義されていません。不明なトラップフィルタ規則によってトラップが除外されます。
- トラップは、特定の間隔で複数回送信されます。重複トラップフィルタルールにより、トラップが除外されます。
- トラップは、リンクステータス変更トラップなどの短い間隔で変更および復元されます。断続的なトラップ分析ルールにより、トラップが除外されます。
- トラップを送信するデバイスはiMCに追加されません。iMCルールにないデバイスのトラップフィルタによって、トラップが除外されます。または、デバイスがiMCで管理外の状態にあるため、トラップがアラームにエスカレーションされません。
- iMCはトラップを受信しますが、対応するTrap-to-Alarmルールが存在しないか、無効になっています。

この問題を解決するには、管理者としてiMCにログインし、次のタスクを実行します。

1. “iMCが予想されるメモリーのアップ/ダウンアラームを受信しない”のソリューションを参照してください。
2. ユーザー定義のトラップフィルタ規則を確認します。

- a. Alarmをクリックします。
- b. ナビゲーションツリーで、Trap Management > Filtering Trapを選択します。ユーザー定義のトラップフィルタルールによってトラップが除外されるかどうかを確認します。除外される場合は、設定を削除または変更します。
3. トラップ定義をチェックします。
 - a. Alarmタブをクリックします。
 - b. ナビゲーションツリーで、Trap Management > Trap Definitionを選択します。
 - c. トラップが定義されているかどうかを確認します。定義されていない場合は、Addをクリックしてトラップを定義します。
4. 重複トラップフィルタ規則を確認します。
 - a. Alarmタブをクリックします。
 - b. ナビゲーションツリーで、Trap Management > Filtering Trapを選択します。
 - c. 重複トラップフィルタルールのLength of Time Windowの値をチェックします。時間範囲内でトラップが複数回送信されるかどうかをチェックします。複数回送信される場合は、Unfiltered Duplicated Trapsフィールドにトラップを追加します。
5. 断続トラップ分析規則を確認します。
 - a. Alarmタブをクリックします。
 - b. ナビゲーションツリーで、Trap Management > Filtering Trapを選択します。
 - c. Length of Time Window値およびトラップリストを確認します。たとえば、リンクステータス変更トラップがあるとして、トラップがリストにあり、リンクの状態が構成された時間範囲内で変更および復元される場合は、設定を変更または削除します。
6. iMCでデバイスを問い合わせます。デバイスが管理用にiMCに追加されていることを確認します。
7. トラップからアラームへの規則を確認します。
 - a. Alarmタブをクリックします。
 - b. ナビゲーションツリーで、Trap Management > Trap to Alarmを選択します。
 - c. トラップOIDによってトラップからアラームへの規則を問い合わせます。トラップのトラップからアラームへの規則が存在し、イネーブルになっているかどうかを確認します。
 - d. Trap-to-Alarm規則が存在しない場合は、Addをクリックして、トラップのTrap-to-Alarm規則を追加します。
 - e. Trap-to-Alarmルールがディセーブルの場合は、そのルールをイネーブルにします。

iMCが予想されるメモリーのアップ/ダウンアラームを受信しない

症状

メモリーの状態が変化しても、iMCはメモリーのアップ/ダウンアラームを受信しません。

ソリューション

次のような理由が考えられます。

- iMCは、メモリーのアップ/ダウンアラームをフィルタリングします。
- ユーザー定義のトラップフィルタ規則は、メモリーのトラップを除外します。

- トラップは、特定の間隔で複数回送信されます。重複トラップフィルタルールにより、トラップが除外されます。
- メモリーの状態は短い間隔で変化し、リストアされます。断続的なトラップ分析ルールにより、メモリーのアップ/ダウントラップが除外されます。
- トラップを送信するデバイスはiMCに追加されません。iMCルールに含まれないデバイスのトラップフィルタによって、トラップが除外されます。または、デバイスがiMCでアンマネージド状態であるため、トラップがアラームにエスカレーションされません。iMCはトラップを受信しますが、対応するTrap-to-Alarmルールはディセーブルです。

この問題を解決するには、管理者としてiMCにログインし、次のタスクを実行します。

1. iMCシステム設定を確認します。
 - a. Systemタブをクリックします。
 - b. ナビゲーションツリーから、System Configuration > System Settingsを選択します。
 - c. メモリーのアップ/ダウンアラームフィルタの設定がメモリーに影響するかどうかを確認します。影響する場合は、設定を変更します。
2. ユーザー定義のトラップフィルタ規則を確認します。
 - a. Alarmタブをクリックします。
 - b. ナビゲーションツリーで、Trap Management > Filtering Trapを選択します。
 - c. アップ/ダウントラップグループによって実行されるユーザー定義のトラップフィルタルールのメモリーリストにメモリーがあるかどうかを確認します。ある場合は、設定を削除または変更します。
3. 重複トラップフィルタ規則を確認します。
 - a. Alarmタブをクリックします。
 - b. ナビゲーションツリーで、Trap Management > Filtering Trapを選択します。
 - c. 重複トラップフィルタルールのLength of Time Windowの値をチェックします。時間範囲内でトラップが複数回送信されるかどうかをチェックします。複数回送信される場合は、Duplicate Trap Filterフィールドにトラップを追加します。
4. 断続トラップ解析規則を確認します。
 - a. Alarmタブをクリックします。
 - b. ナビゲーションツリーで、Trap Management > Filtering Trapを選択します。
 - c. Intermittent Trap Analyze規則のLength of Time Windowの値とトラップリストを確認します。メモリーのアップ/ダウントラップがリストにあり、メモリーの状態が時間範囲内で変更および復元される場合は、設定を変更または削除します。
5. iMCでデバイスを問い合せます。デバイスが管理用にiMCに追加されていることを確認します。
6. トラップからアラームへの規則を確認します。
 - a. Alarmタブをクリックします。
 - b. ナビゲーションツリーで、Trap Management > Trap to Alarmを選択します。
 - c. NMSリソースおよびSNMPルールが有効になっていることを確認します。メモリーのアップ/ダウントラップは、このルールが有効な場合にのみアラームにエスカレートされます。

iMC ICCのトラブルシューティング

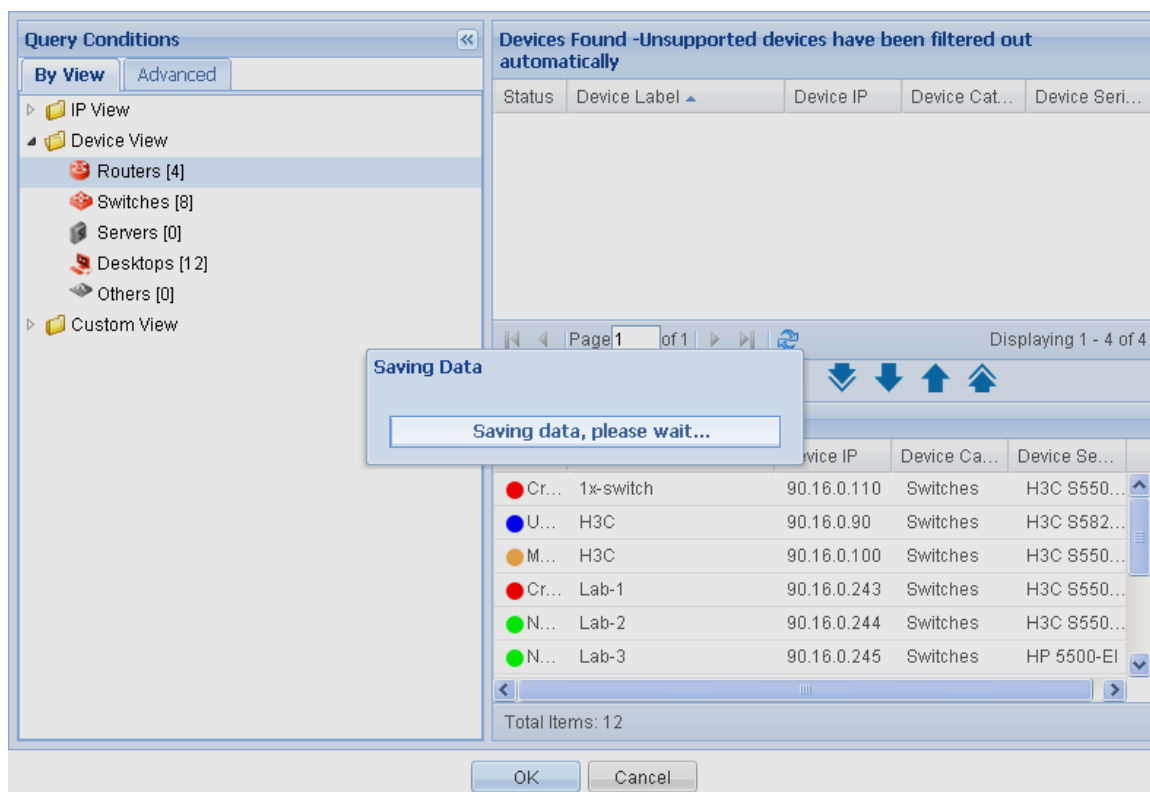
次の情報は、iMC ICCのトラブルシューティングガイダンスを提供します。

デバイスソフトウェアを導入、リストア、インポートするためのデバイスを追加できない

症状

デバイスソフトウェアを配布、リストアまたはインポートするためにデバイスを追加できません。ソフトウェアの配布、リストアまたはインポート用にデバイスを選択すると、次のページでシステムが停止します。

図40 データの保存



ソリューション

考えられる理由は、iMCがデバイスとは異なる読み取り専用コミュニティストリングを使用しているためです。この問題を解決するには、次の手順を実行します。

1. 管理者としてiMCにログインし、Resourceタブをクリックします。
2. ナビゲーションツリーからView Management > Device Viewを選択して、デバイスビューを入力します。となります。
3. Device Listでデバイスのラベルをクリックして、Device Detailsページを表示します。
4. 右側のペインで、Configure > Modify SNMP Settingsをクリックします。

5. 読み取り専用コミュニティストリングを、デバイスによって使用される読み取り専用コミュニティストリングと同じになるように変更します。
6. OKをクリックします。

図41 SNMPパラメータの変更

Edit SNMP Parameters Select an Existing Template

Parameter Type *

Read-Only Community String

Read-Write Community String

Timeout (1-60 seconds) *

Retries (1-20) *

デバイスソフトウェアの転送にTFTPを使用できませんでした。

症状

ソフトウェアの展開、復元、またはインポート操作中に、TFTPを使用してデバイスソフトウェアを転送できませんでした。

ソリューション

考えられる理由は、iMCがデバイスとは異なる読み取り専用コミュニティストリングを使用しているためです。

この問題を解決するには、次の手順を実行します。

1. Resourceタブをクリックします。
2. ナビゲーションツリーからView Management > Device viewを選択して、デバイスビューを入力します。となります。
3. Device Listでデバイスのラベルをクリックして、Device Detailsページを表示します。
4. 右側のペインで、Configure > Modify SNMP Settingsをクリックします。
5. read-onlyコミュニティストリングを、デバイスによって使用されるread-onlyコミュニティストリングと同じになるように変更します。
6. OKをクリックします。

図42 SNMPパラメータの変更

Edit SNMP Parameters Select an Existing Template

Parameter Type *

Read-Only Community String

Read-Write Community String

Timeout (1-60 seconds) *

Retries (1-20) *

デバイス構成の手動バックアップに失敗しました

症状

デバイス構成の手動バックアップが失敗し、デバイスログイン失敗のエラーメッセージが表示された

ソリューション

デバイス構成の手動バックアップでは、ICCは最初にSNMPを使用しようとします。SNMP方式が使用できない場合、ICCはバックアップのためにデバイスのCLIにログインしようとします。次のいずれかのエラーが発生した場合、ICCはデバイスのCLIにログインできません。

- ファイル転送プロトコルは、CLIログイン方式をサポートしていません。
- 一部のログイン設定が正しくありません。

この問題を解決するには、次の手順に従います。

正しいログイン方法を選択し、正しいログイン設定を構成します。

- ファイル転送プロトコルがTFTPまたはFTPの場合は、Telnetを選択します。
- ファイル転送プロトコルがSFTPまたはSCPの場合は、SSHを選択します。

次の例では、TFTPが使用されています。Telnetを選択し、Telnet設定を構成する必要があります。

1. 管理者としてIMCIにログインします。
2. ナビゲーションツリーでService > Configuration Center > Optionsをクリックします。
3. デフォルトの転送モードとしてTFTPを選択し、OKをクリックします。

図43 ファイル転送モードの設定

Service > Options

Help

Device Capability Set | **File Transfer Mode** | Backup Policy | VPN Instance

Default Transfer Mode

⚠ iMC will forcibly enable SFTP/TFTP server if it is not enabled on HP E-series devices. Please revert the changes back manually if required.

TFTP

FTP

SFTP (Make sure the SFTP server is enabled on the device, and correct SSH parameters are configured for the device in iMC.)

SCP (Make sure the SCP server is enabled on the device, and correct SSH parameters are configured for the device in iMC.)

Enable FTP Transfer Mode

⚠ Please install third-party FTP server software at iMC, and set server\tmp under the iMC installation directory as the root directory of the FTP service.

FTP User Name

FTP Password

Single Device Transfer Mode

⚠ All the devices that are not configured separately with the file transfer mode adopt the default transfer mode.

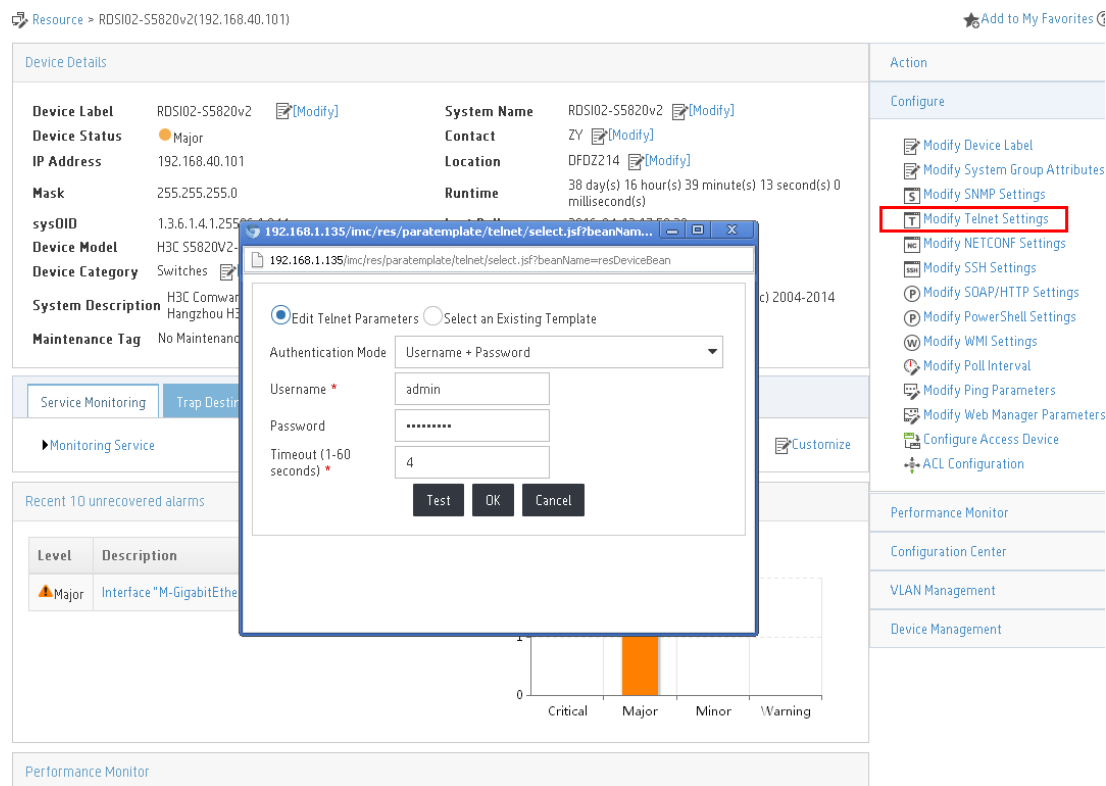
Select Device Set Mode Cancel Mode

<input type="checkbox"/>	Device Name	Device Model	IP Address	Transfer Mode
No match found.				
Total Items: 0.				

OK

4. Service > Configuration Center > Configuration Centerをクリックします。Device Detailsページを表示するためにデバイスのラベルをクリックします。
5. ログイン方法をTelnetに変更します。右側のペインで、Configure > Modify Telnet Settingsをクリックして、正しいTelnet設定を行います。

図44 Telnetパラメータの設定



6. ICC上のデバイス構成を手動で再度バックアップします。操作は正常に行われます。

FTPを使用してデバイス構成をバックアップできませんでした

症状

FTPを使用してデバイス構成をバックアップできませんでした。FTPサービスが使用不可であることを示すエラーメッセージが表示されます。

FTPサーバーが開始されていません。

ソリューション

次のような理由が考えられます。

- FTPサーバーはインストールされていません。
- FTPサーバーはイネーブルになっていません。
- FTPサーバーは、ループバックアドレス127.0.0.1をサポートするように設定されていません。

この問題を解決するには、必要に応じて次の方法を使用します。

- FTPサーバーをインストールします。
- FTPサーバーをイネーブルにします。
- ループバックアドレス127.0.0.1をサポートするようにFTPサーバーを設定します。

デバイスソフトウェアの転送にFTPを使用できませんでした。

症状

デバイスソフトウェアをiMCに転送するためにFTPを使用できませんでした。

ソリューション

次のような理由が考えられます。

- ICCに保存されているFTPユーザー名またはパスワードが正しくありません。
- FTPディレクトリ内に同じファイル名を使用する読み取り専用ファイルがあります。
- FTPユーザーには、FTPディレクトリで操作を実行する権限がありません。
- iMCサーバーにはファイアウォールがインストールされています。

この問題を解決するには、必要に応じて次の方法を使用します。

- ICCで、FTPユーザー名とパスワードを変更します。
 - a. 管理者としてiMCにログインし、Serviceタブをクリックします。
 - b. ナビゲーションツリーからConfiguration Center > Optionsを選択します。
 - c. FTPのユーザー名とパスワードを変更します。

図45 ファイル転送モードの設定

Service > Options

Device Capability Set | **File Transfer Mode** | Backup Policy | VPN Instance

Default Transfer Mode

⚠ iMC will forcibly enable SFTP/TFTP server if it is not enabled on HP E-series devices. Please revert the changes back manually if required.

TFTP

FTP

SFTP (Make sure the SFTP server is enabled on the device, and correct SSH parameters are configured for the device in iMC.)

SCP (Make sure the SCP server is enabled on the device, and correct SSH parameters are configured for the device in iMC.)

Enable FTP Transfer Mode

⚠ Please install third-party FTP server software at iMC, and set server/tmp under the iMC installation directory as the root directory of the FTP service.

FTP User Name *

FTP Password *

Single Device Transfer Mode

⚠ All the devices that are not configured separately with the file transfer mode adopt the default transfer mode.

Select Device | Set Mode | Cancel Mode

Device Name	Device Model	IP Address	Transfer Mode
No match found.			
Total Items: 0.			

OK

- デバイス上で、同じファイル名を使用するread-onlyファイルを削除します。
- デバイス上で、FTPユーザーに操作の実行を許可するか、操作を実行する権限を持つFTPユーザーアカウントを使用します。

- IMCサーバーで、FTPアクセスを許可するようにファイアウォールを設定します。

SFTPを使用してデバイスソフトウェアを転送できませんでした

症状

ソフトウェアの展開、復元、またはインポート操作中にデバイスソフトウェアを転送するためにSFTPを使用できませんでした。

ソリューション

次のような理由が考えられます。

- デバイスでSSHサービスがイネーブルになっていません。
- デバイス上のSSHサービス設定が正しくありません。

この問題を解決するには、次のいずれかの方法を使用してください。

- デバイスにログインし、デバイスでSSHサービスをイネーブルにします。
- デバイスにログインして、SSHサービス設定を変更します。

SCPを使用して装置構成をバックアップすることに関するエラーメッセージ

症状

SCPを使用したデバイスコンフィギュレーションバックアップ操作は成功しましたが、結果の詳細ページに、伝送プロトコルがサポートされていないことが示されました。

図46 伝送プロトコルはサポートされていない

Service > Configuration Center > Configuration File Backup Result

Configuration File Backup Result

✓ Device configuration files manually backed up. Total: 1, backed up: 1, failures: 0.

Device Name	Device Model	File Type	Time	Result	Configuration File Name	Details
			2013-11-01 17:27:07	✓ Back up configuration files. Total: 2, running files: 1, startup files: 1.		
Lab-1(192.168.12.200)	H3C S5500-28C-PWR-EI	Startup	2013-11-01 17:27:06	✓ Configuration backup succeeded.	192.168.12.200_startup_20131101172700.cfg	
Lab-1(192.168.12.200)	H3C S5500-28C-PWR-EI	Running	2013-11-01 17:27:06	✓ Configuration backup succeeded.	192.168.12.200_running_20131101172653.cfg	
			2013-11-01 17:26:42	✓ Starting to backup configuration files.		

http://192.168.1.17/imc/fcc/taskmng/viewTaskResultDetailFactjsf?queryType=2&jobId=42&devId=115 - Windows Internet Explorer

http://192.168.1.17/imc/fcc/taskmng/viewTaskResultDetailFactjsf?queryType=2&jobId=42&devId=115&fileType=1&decodeIso=true

Device Name: Lab-1(192.168.12.200)

Index	Description	Result	Suggestion	Begin Time	Finish Time
1	Initialize task parameters.	Succeeded.		2013-11-01 17:26:43	2013-11-01 17:26:44
2	Back up device startup configuratio...	Transmission protocol not supported.	Please correct the file transmission protocol of the device.	2013-11-01 17:26:45	2013-11-01 17:26:50
3	Initialize redo task parameters.	Succeeded.		2013-11-01 17:26:50	2013-11-01 17:26:51
4	Back up device startup configuratio...	Succeeded.		2013-11-01 17:26:52	2013-11-01 17:27:07

ソリューション

iMCがSCPをサポートするコードを提供しない場合は、自動的にサードパーティスクリプトが使用されます。結果詳細ページのエラーメッセージには、iMCがサードパーティスクリプトを使用したことが示されます。

この問題は通常の使用には影響しません。問題を解決するための操作は必要ありません。

iMC NetAssetのトラブルシューティング

次の情報は、iMCネットワーク資産管理のトラブルシューティング情報を提供します。

iMCはネットワーク内のスタックデバイスを識別できませんでした。

症状

スタックデバイスがiMCに追加された後、iMCはそれらをデバイス詳細ページでスタックデバイスとして識別できなくなり、それらのアイコンはネットワークポロジページのスタックデバイスアイコンではなくなります。アイコンをダブルクリックしてもスタックデバイスのトポロジを開くことはできません。

ソリューション

考えられる原因は次のとおりです。

- network asset moduleがiMCプラットフォームにインストールされていないため、デバイスの資産情報をiMCに追加できません。
- スタックデバイスのエンティティ情報が多すぎるため、iMCがエンティティ情報を読み取ってiMCに追加するには時間がかかります。
- network asset moduleのOptionsページで、iMCプラットフォームにデバイスを追加するときにデバイスをネットワークアセットに追加するAdd devices to Network Assets when adding them to the iMC platformオプションはNoになります。
- デバイスにはエンティティMIB実装エラーがあります。たとえば、エンティティMIBの一部のフィールドに認識されない文字が含まれているなどです。

この問題を解決する手順は、次のとおりです。

- iMCプラットフォームにnetwork assetモジュールをインストールし、新しいデバイスのasset情報をiMCに読み込みます。
- しばらく待って最新のデバイス情報を表示した後、デバイスの詳細ページおよびネットワークポロジページを更新します。
- Add devices to Network Assets when adding them to the iMc platformオプションをYesにし、デバイス詳細ページのデバイス情報と同期させます。そして、しばらく待って最新のデバイス情報を表示した後、デバイスの詳細ページとネットワークポロジページを更新します。
- デバイスの正規のソフトウェアバージョンを使用します。

iMC Perfmのトラブルシューティング

次の情報は、iMCパフォーマンス管理のトラブルシューティングガイダンスを示します。

CPU使用率を監視するためにF5デバイスインスタンスにデータが表示されない

症状

iMCプラットフォーム7.0(E0102)以前のバージョンでは、パフォーマンス管理モジュールは、F5デバイスの既存のCPUモニタリングインスタンスからデータを収集できません。

ソリューション

iMCプラットフォーム7.0(E0102L01)以降のバージョンでは計算式が変更されるため、Performance Managementモジュールは、F5デバイスの既存のCPU監視インスタンスからデータを収集できません。

この問題を解決する手順は、次のとおりです。

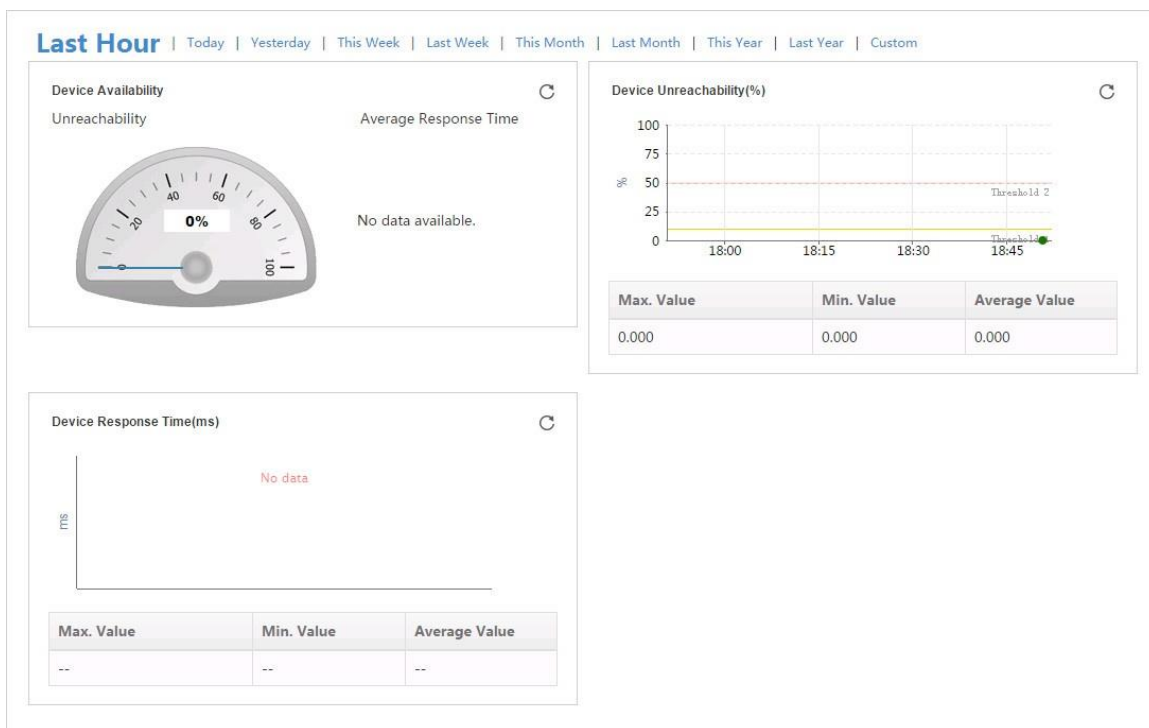
1. F5デバイスの既存のCPU監視インスタンスを削除します。
2. CPU使用率を監視するために、F5デバイスの新しいインスタンスを追加します。

デバイスパフォーマンスモニターにデータがない

症状

特定のデバイスのリアルタイム監視ページにはデータがありません。

図47 監視情報なし



ソリューション

考えられる原因は、デバイス上でハードウェアが変更されたことです。次に例を示します。

- カードが取り外されたか、新しいカードが挿入されました。
- スタックデバイスのメンバが変更されました。

この問題を解決するには、監視するデバイス上のインスタンスを更新します。

1. Resourceタブをクリックします。
2. ナビゲーションツリーから、Performance Management > Monitoring Settingsを選択します。

図48 監視の設定

Resource > Monitoring Settings Last Statistical Time: 2016-04-20 17:30:00 Re-collect Overall Monitoring Statistics ReportV2
Add to My Favorites Help

Total number of index instances monitored: 14 Total collecting frequency (times/hour): 168 Total number of collecting units: 14
 Total number of instances managed by performance management: 14 Total collecting frequency of the instance managed by performance management (times/hour): 168 Total number of collecting units of the instance managed by performance management: 14

Add Monitor **Cancel Monitor** **Modify Index** **Refresh** **Save** Query

Only Display Monitored Devices [Switch to Instance List](#)

<input type="checkbox"/>	Device Name	Device Model	Instances	Operation	Data
<input type="checkbox"/>	▶ 12DC-CN-X64(192.168.7.159)	ICMP	2	Add Cancel Modify Index	🗑️
<input type="checkbox"/>	▶ 172.19.254.242(172.19.254.242)	ICMP	2	Add Cancel Modify Index	🗑️
<input type="checkbox"/>	▶ 172.31.1.5(172.31.1.5)	ICMP	2	Add Cancel Modify Index	🗑️
<input type="checkbox"/>	▶ 192.168.7.1(192.168.7.1)	H3C S5820V2-52Q	4	Add Cancel Modify Index	🗑️
<input type="checkbox"/>	▶ 192.168.8.23(192.168.8.23)	ICMP	2	Add Cancel Modify Index	🗑️
<input type="checkbox"/>	▶ 192.168.8.25(192.168.8.25)	ICMP	2	Add Cancel Modify Index	🗑️

- IPアドレスが192.168.7.1のデバイスの横にあるAddをクリックします。Monitoring Settings-Add Monitorページが開きます。

図49 監視設定モニターの追加

Monitoring Settings-Add Monitor Refresh Instance

Monitoring Device Monitoring Instance

Select Index

Add **Delete All**

Total Items: 0.

Name	Index Group	Configure	Delete
No match found.			

Select Device

Add **Delete All**

Total Items: 1.

Device	Device Type	Device IP	Delete
192.168.7.1	H3C S5820V2-52Q	192.168.7.1	🗑️

Monitoring Settings

All interfaces
 Up interfaces
 Monitor Physical Interfaces only
 Up physical interfaces

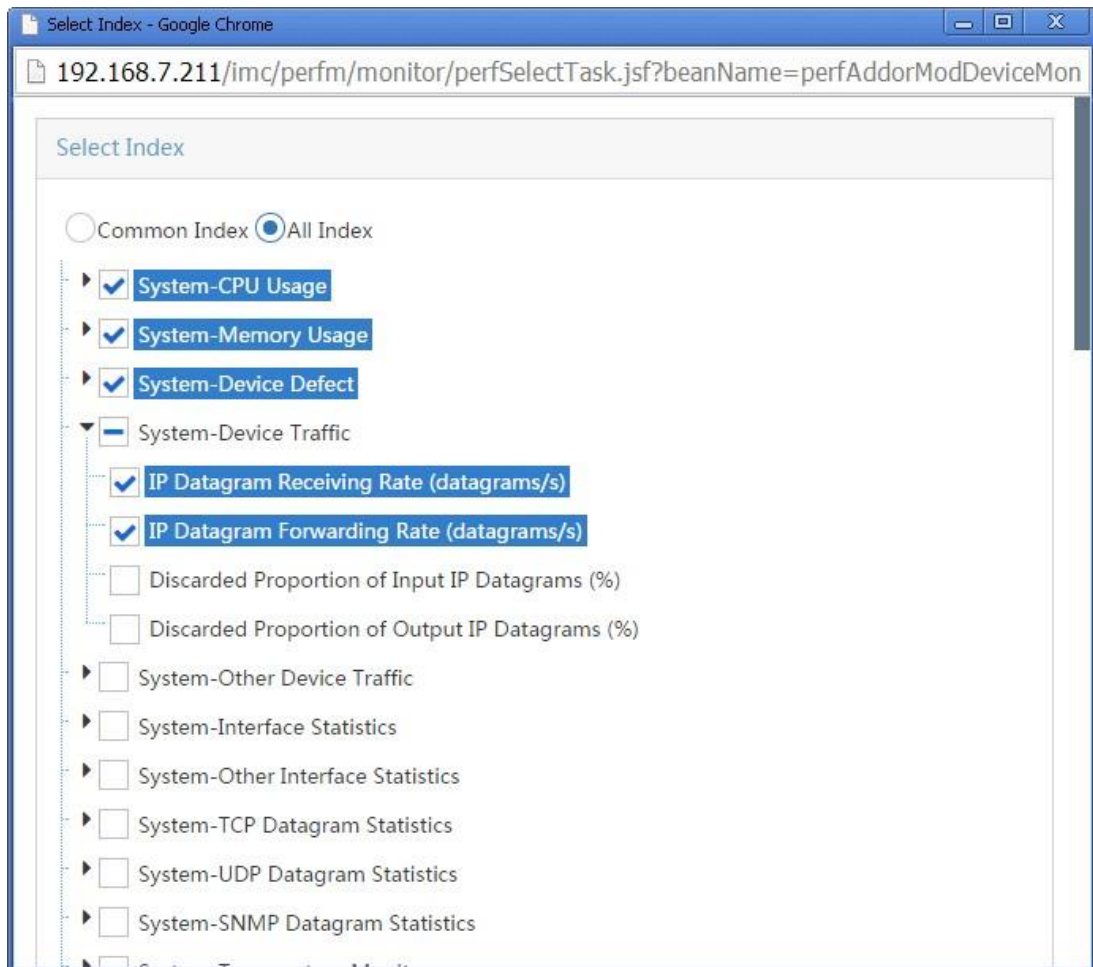
Meet these requirements

Interfaces Connected to SNMP Devices
 Interfaces Connected to Servers
 Interfaces Connected to PCs

OK **Cancel**

4. Select Index領域でAddをクリックし、監視するインデックスを選択します。

図50 インデックスの選択



5. OKをクリックします。
Select Indexページが閉じます。
6. Refresh Instanceボックスを選択します。

図51 リフレッシュインスタンスの選択

Monitoring Settings-Add Monitor Refresh Instance

Monitoring Device Monitoring Instance

Select Index

Add Delete All

Total Items: 6.

Name	Index Group	Configure	Delete
CPU Usage	System-CPU Usage		
Memory Usage	System-Memory Usage		
IP Datagram Receiving Rate	System-Device Traffic		
IP Datagram Forwarding Rate	System-Device Traffic		
Response Time of Device	System-Device Defect		
Device Unreachability Proportion	System-Device Defect		

Select Device

Add Delete All

Total Items: 1.

Device	Device Type	Device IP	Delete
192.168.7.1	H3C S5820V2-52Q	192.168.7.1	

Monitoring Settings

All interfaces
 Up interfaces
 Monitor Physical Interfaces only
 Up physical interfaces

Meet these requirements

Interfaces Connected to SNMP Devices Interfaces Connected to Servers Interfaces Connected to PCs

OK Cancel

7. OKをクリックします。
8. 監視情報をリフレッシュします。

非メモリーインデックスのモニターの追加に失敗しました

症状

CPU使用率やメモリー使用率などの非メモリーインデックスのモニターを追加できませんでした。

IPアドレスが192.168.1.111のデバイスのモニターを追加できませんでした。IPアドレスが172.10.0.100のデバイスのモニターを追加すると、デバイスアクセス タイムアウト エラーメッセージが表示されました。

図52 デバイスアクセス タイムアウト

Device Name	Result
12DC-CN-X64(192.168.7.159)	0 Failed
CPU Usage	0 Failed
Memory Usage	0 Failed

ソリューション

次のような理由が考えられます。

- iMCプラットフォームでは、デバイスと同じSNMP設定を使用しません。
- デバイスの負荷が大きすぎるため、デバイスはiMCからの要求メッセージにすぐに応答しません。
- デバイスは、特定のインデックスの監視をサポートしていません。

この問題を解決するには、次の手順に従います。

- SNMPパラメータを次のように変更します。
 - a. iMCにログインし、デバイスの詳細ページにアクセスします。
 - b. Actionメニューで、Configureをクリックし、Modify SNMP settingsを選択します。
 - c. 表示されるページでSNMPパラメータを変更します。

図53 SNMPパラメータの編集

Edit SNMP Parameters Select an Existing Template

Parameter Type *

Read-Only Community String ?

Read-Write Community String ?

Timeout (1-60 seconds) *

Retries (1-20) *

- 後でデバイスの負荷が低下したときに再実行してください。
- 監視するインデックスの監視がデバイスでサポートされているかどうかを確認します。

ディレクトリ共有時にデバイス監視データが消失

症状

管理者がiMCデータベースサーバー上のディレクトリを共有すると、デバイス監視データが消失します。

パフォーマンス管理モジュールには、次のログコンテンツがあります；

オペレーティングシステムエラーコード5(アクセス拒否)。

ソリューション

iMCディレクトリが共有されると、SQL Serverサービス起動アカウントのアクセス権が変更されます。この問題は通常、アカウントがNT AUTHORITY\NetworkServiceであり、共有ディレクトリが\$(iMc)\server\data\perfdmまたはその親パス\$(iMc)\server\data、\$(iMc)\server、または\$(iMc)です。\$(iMc)はiMCのインストーパスです。

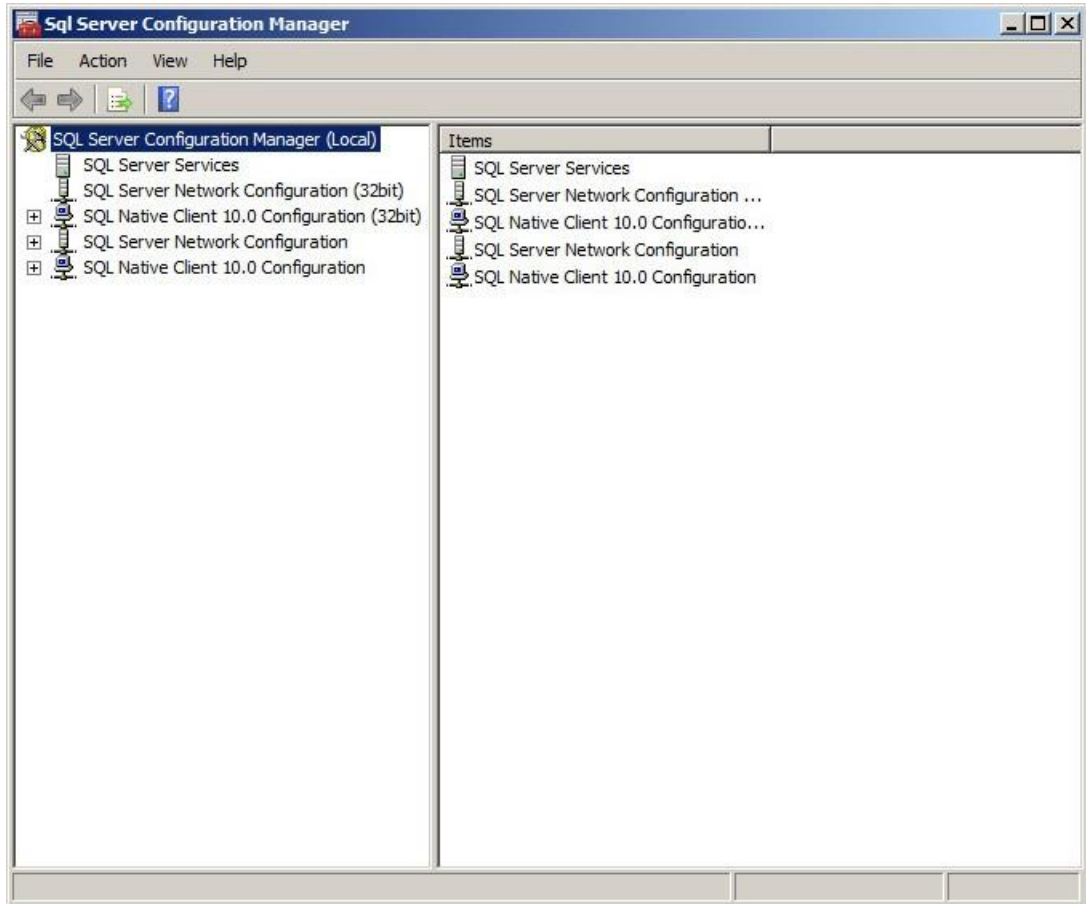
この問題を解決するには、次の手順に従います。

- SQL Serverサービスの起動アカウントとしてローカルアカウントを設定します。
- 共有フォルダの読み取り/書き込み権限をSQL Serverサービスの起動アカウントに付与します。

ローカルアカウントをSQL Serverサービスの起動アカウントとして構成する

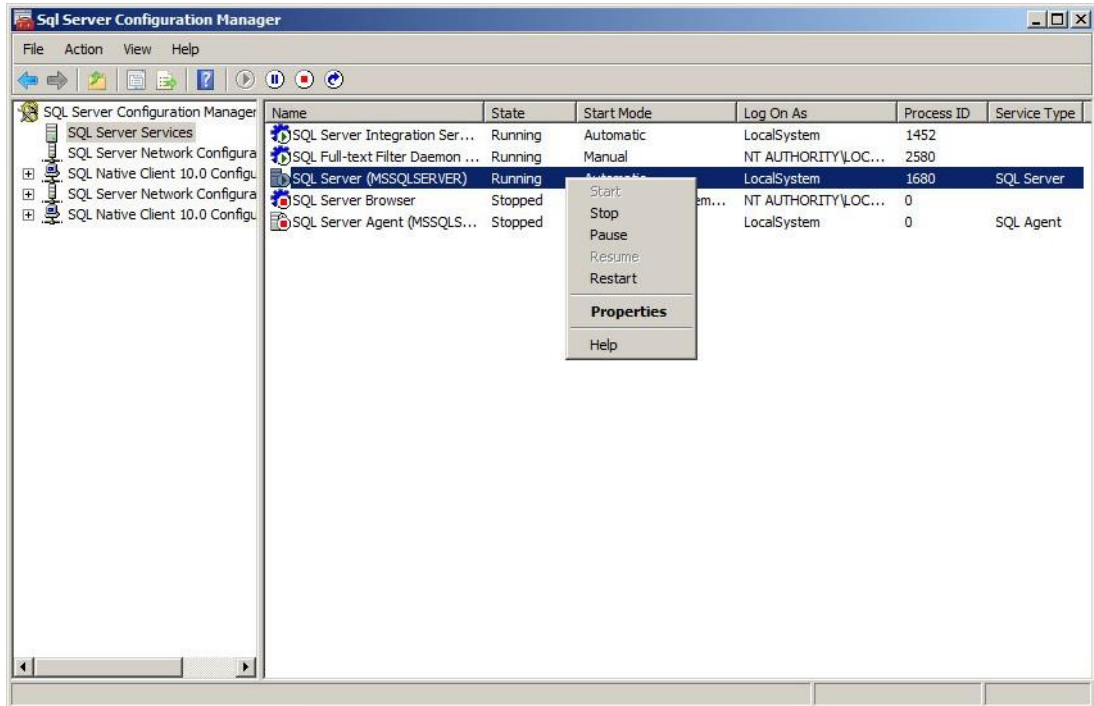
1. iMCデータベースが存在するサーバーにログインします。
2. **Start**ボタンをクリックし、**All programs > Microsoft SQL Server2008R2 > Configuration Tools > SQL Server Configuration Manager**を選択します。

図54 SQL Server構成マネージャ



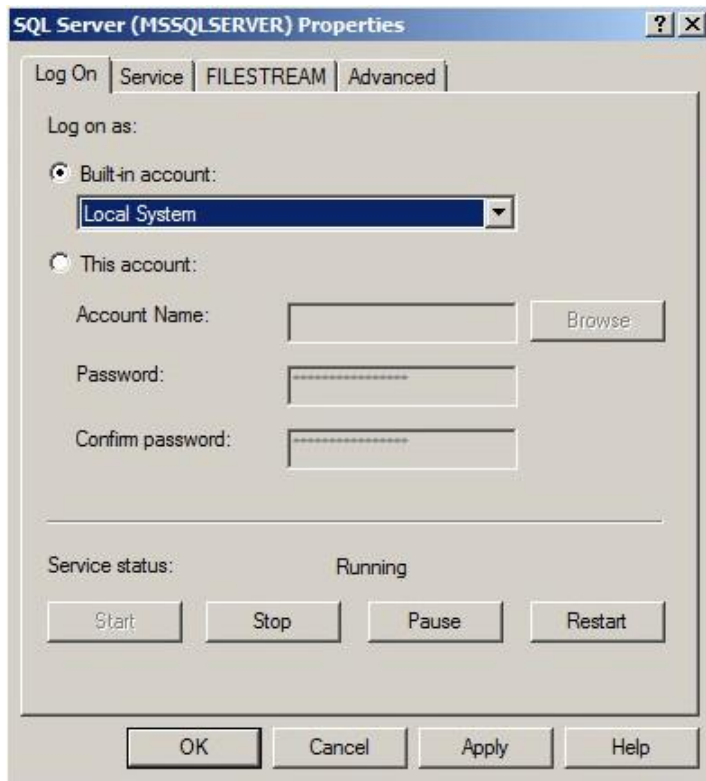
3. ナビゲーションツリーで、SQL Server Servicesをクリックします。
4. 作業領域でSQL Server(MSSQLSERVER)を右クリックし、ショートカットメニューからPropertiesを選択します。

図55 プロパティの構成



5. Log onタブで、Built-in AccountリストからLocal Systemを選択します。
6. OKをクリックします。

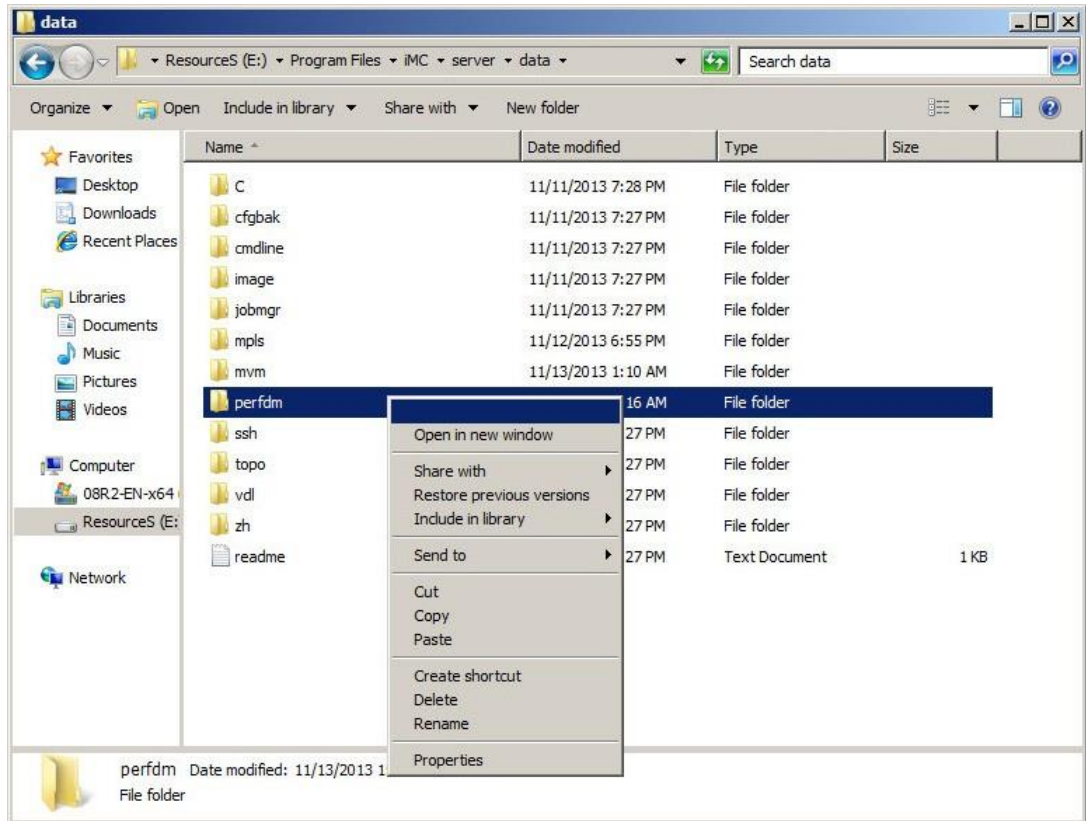
図56 Select Local System



SQL Serverサービスの起動アカウントに共有フォルダの読み取り/書き込み権限を付与する

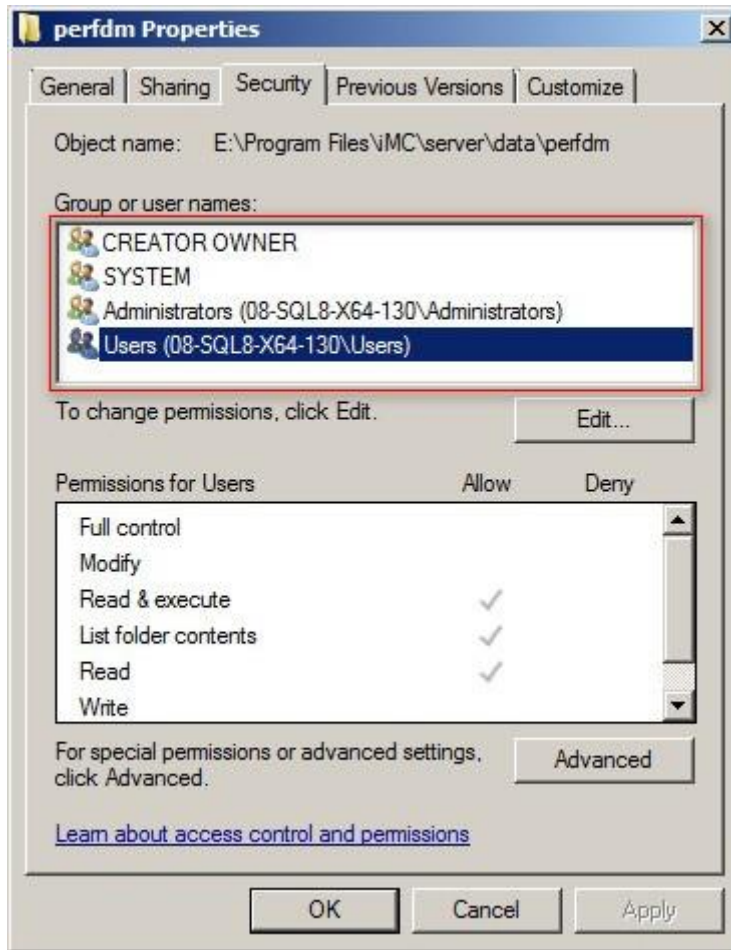
1. iMCが実行されているサーバーにログインし、iMCインストールパスのディレクトリ\Server\dataを開きます。
2. perfdmフォルダを右クリックし、ショートカットメニューのPropertiesを選択します。

図57 プロパティの構成



3. Securityタブで、CREATOR OWNER、UsersおよびAdministratorsがGroup or user namesにあることを確認しなさい。一覧に表示されていない場合は、Editをクリックして追加します。

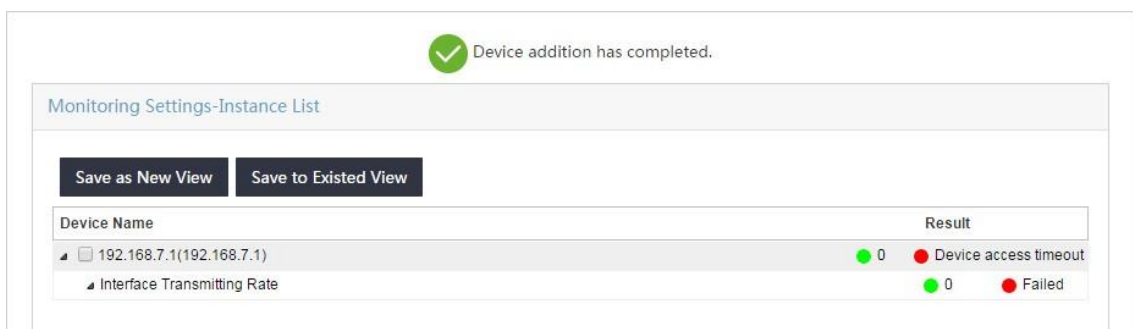
図58 グループ名またはユーザー名の構成



メモリーインデックスのモニターの追加に失敗しました 症状

メモリー受信レートやメモリー送信レートなどのメモリーインデックスのモニターを追加できませんでした。
IPアドレスが90.16.0.5であるデバイスSR11-11上のメモリー転送レートのモニターを追加できませんでした。

図59 メモリー転送レートのモニターの追加に失敗しました



ソリューション

次のような理由が考えられます。

- iMCプラットフォームでは、デバイスと同じSNMP設定を使用しません。
- デバイスの負荷が大きすぎるため、デバイスはiMCからの要求メッセージにすぐに応答しません。
- メモリーがモニターリング設定の要件を満たしていません。
- デバイスは、特定のインデックスの監視をサポートしていません。

この問題を解決するには、次の手順に従います。

- SNMPパラメータを次のように変更します。
 - a. iMCにログインし、デバイスの詳細ページにアクセスします。
 - b. Actionメニューで、Configureをクリックし、Modify SNMP Settingsを選択します。
 - c. 表示されるページでSNMPパラメータを変更します。

図60 SNMPパラメータの編集

Edit SNMP Parameters Select an Existing Template

Parameter Type *

Read-Only Community String ?

Read-Write Community String ?

Timeout (1-60 seconds) *

Retries (1-20) *

- 後でデバイスの負荷が低下したときに再試行してください。
- 次のいずれかの操作を行います。
 - デバイスメモリーがモニターリング設定の要件を満たしているかどうかを確認します。デフォルトでは、iMCはメモリーを監視し、メモリーが接続されるデバイスはSNMPデバイス(スイッチおよびルータ)またはサーバーである必要があります。

図61 監視の設定

Monitoring Settings-Add Monitor Refresh Instance

Monitoring Device Monitoring Instance

Select Index

Add **Delete All**

Total Items: 1.

Name	Index Group	Configure	Delete
Interface Transmitting Rate	System-Interface Statistics		

Select Device

Add **Delete All**

Total Items: 1.

Device	Device Type	Device IP	Delete
192.168.7.1	H3C S5820V2-52Q	192.168.7.1	

Monitoring Settings

All interfaces
 Up interfaces
 Monitor Physical Interfaces only
 Up physical interfaces

Meet these requirements

Interfaces Connected to SNMP Devices
 Interfaces Connected to Servers
 Interfaces Connected to PCs

OK **Cancel**

- Monitoring Instanceを選択します。iMCでは、監視インスタンスの作成時に監視設定(メモリーおよびメモリーが接続されているデバイス)が無視されます。

図62 インスタンスの監視

Monitoring Settings-Add Monitor Refresh Instance

Monitoring Device Monitoring Instance

Select Index

Add **Delete All**

Total Items: 1.

Name	Index Group	Configure	Delete
Interface Transmitting Rate	System-Interface Statistics		

Select Instances

Select **Delete All**

192.168.7.1(192.168.7.1)
 Interface Transmitting Rate

OK **Cancel**

- 監視するインデックスの監視がデバイスでサポートされているかどうかを確認します。

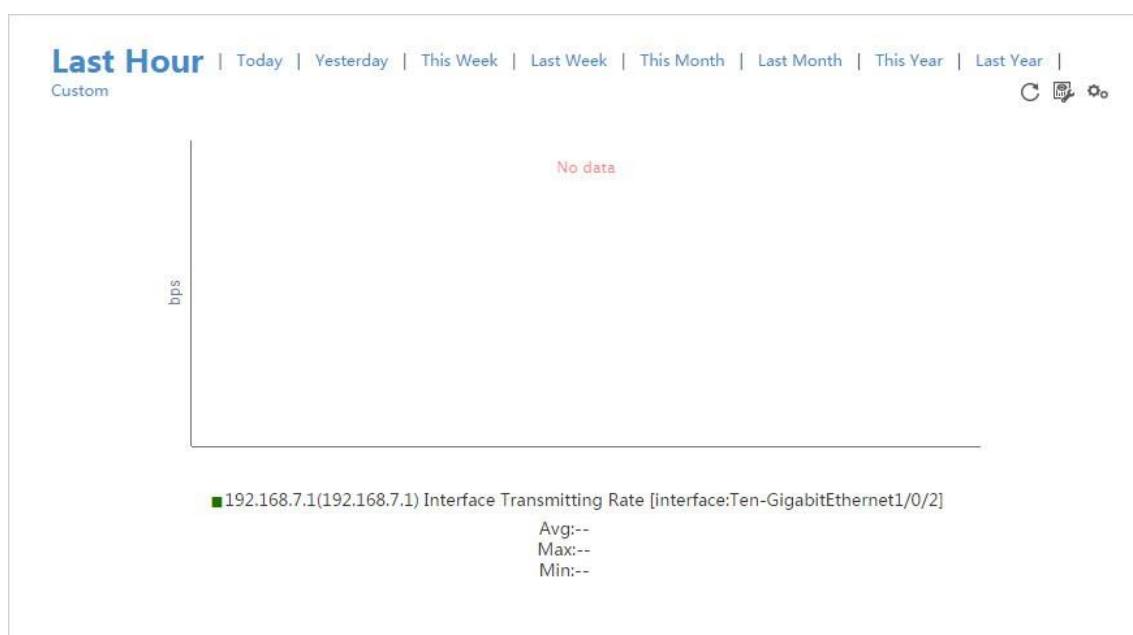
モニターの追加直後にモニターデータを表示できませんでした。

症状

モニターを追加すると、iMCプラットフォームはモニターリングデータをすぐに表示できず、しばらくしてからモニターリングデータを表示します。

たとえば、IPアドレスが192.168.7.1のデバイスに対してInterface Transmitting Rateのモニターを追加した場合、iMCプラットフォームでは、Interface Transmitting Rateのモニターリングデータページにそのモニターのデータは表示されません。

図63 データなし



ソリューション

iMCでは、少なくとも2つの収集間隔で収集された2つのデータ間の差を計算することによって監視データが生成されるため、iMCでは、モニターの追加後に少なくとも2つのデータ収集間隔で監視データが表示されます。

この問題を解決する手順は、次のとおりです。

- 少なくとも2回のデータ収集間隔が経過したら再試行してください。
- データ収集間隔を変更することもできます。

データ収集間隔を変更する手順は、次のとおりです。


1. Access Monitorページにアクセスします。Interface Transmitting RateのConfigureアイコンをクリックします。 Interface Transmitting Rateの設定ページが開きます。



図64 インデックスの構成

Monitoring Settings-Add Monitor Refresh Instance

Monitoring Device Monitoring Instance


Select Index

Total Items: 1.

Name	Index Group	Configure	Delete
Interface Transmitting Rate	System-Interface Statistics		

Select Device

Total Items: 1.

Device	Device Type	Device IP	Delete
192.168.7.1	H3C S5820V2-52Q	192.168.7.1	

Monitoring Settings

All interfaces
 Up interfaces
 Monitor Physical Interfaces only
 Up physical interfaces

Meet these requirements

Interfaces Connected to SNMP Devices Interfaces Connected to Servers Interfaces Connected to PCs

2. Global Index Settingを消去し、必要に応じてIntervalおよびその他のパラメータを変更します。OKをクリックします。

図65 間隔の構成

Tip:
Click OK to save the current threshold information.

Interface Transmitting Rate

Global Index Settings

Threshold 1 Enable Threshold 2 Enable

Match Mode \geq

Value 1 * 10.000 Value 1 * 50.000

Measurement Mbps Measurement Mbps

Repeat Times * 3 Repeat Times * 3

Alarm Level Minor Alarm Level Major

Interval (Sec.) * 300

OK Close

3. Interface Transmitting Rateのモニタリングデータページを更新し、モニタリングデータを表示します。

パフォーマンス管理の監視データはCLIの出力とは異なる

症状

Performance Managementの監視データは、CLIの出力とは異なります。

ソリューション

次のような理由が考えられます。

- パフォーマンス管理のデータ収集間隔(デフォルトでは5分)は、デバイスのデータ収集間隔とは異なります。
- モニタリングインデックスの場合、MIBには計算用の複数のアルゴリズムがあります。MIBで1つのアルゴリズムを選択することによって取得されるデバイスデータiMCは、CLI出力とは異なります。

この問題を解決するには、パフォーマンスパラメータを計算するための正しいアルゴリズムを見つけ、次の手順を実行してカスタムインデックスを追加します。

1. Resourceタブをクリックします。
2. ナビゲーションツリーからPerformance Management > Global Index Settingsを選択します。
3. Add Custom Indexをクリックします。
デバイス設定に従ってパラメータを設定します。

図66 カスタムインデックスの追加

Resource > Global Index Settings > Add Custom Index ? Help

Add Custom Index

Tip:

1. Enter the type of the index in the Index type field in the format of [index1[0|2];NAME:TYPE:LENGTH].[index2[0|2];NAME:TYPE:LENGTH], where 0 indicates a MIB leaf node while 2 indicates a non-leaf node; in the TYPE field, 1 indicates integer, 2 indicates OID string, 3 indicates IP address, 4 indicates printable string, and 5 indicates MAC address; Value in the LENGTH field indicates the index length, which is 0 for integer index and non-hierarchical index; a dot "." is used to separate length values of hierarchical indices; For example, [index1[2];Interface:1:0] and [index1[2];Frame:1:0],[index2[2];Slot:1:0],[index3[2];Memory:1:0]
2. Enter the object identifier (OID) of the index definition in the Index Instance Label (Definition OID) field, use a colon ":" to separate the OIDs for hierarchical indices, and enter 0 if no OID is provided. For example, 1.3.6.1.2.1.2.2.1.2 and 1.3.6.1.4.1.2011.10.2.75.2.1.2.1.6:0
3. Enter the MIB node to be monitored and the calculation algorithm in the Index Formula field, containing MIB OID, + - * / t ' (), where "t" must be lowercase, indicating the query interval; The quotation mark (') must be placed right after the OID, indicating the value of the previous polling and being used for offset calculation; For example, 1.3.6.1.2.1.11.1 means to use the value of the MIB node as the index value; 1.3.6.1.2.1.11.1-1.3.6.1.2.1.11.1' means to use the difference between two pollings as the index value; (1.3.6.1.2.1.11.1-1.3.6.1.2.1.11.1)/t means to use the value obtained by dividing the difference between two pollings by the polling interval as the index value.

Please test the custom index before adding it.

Name * ?

Measurement Predefined Custom ?

Type * ?

Instance Label (Definition OID) * ?

?

Formula * ?

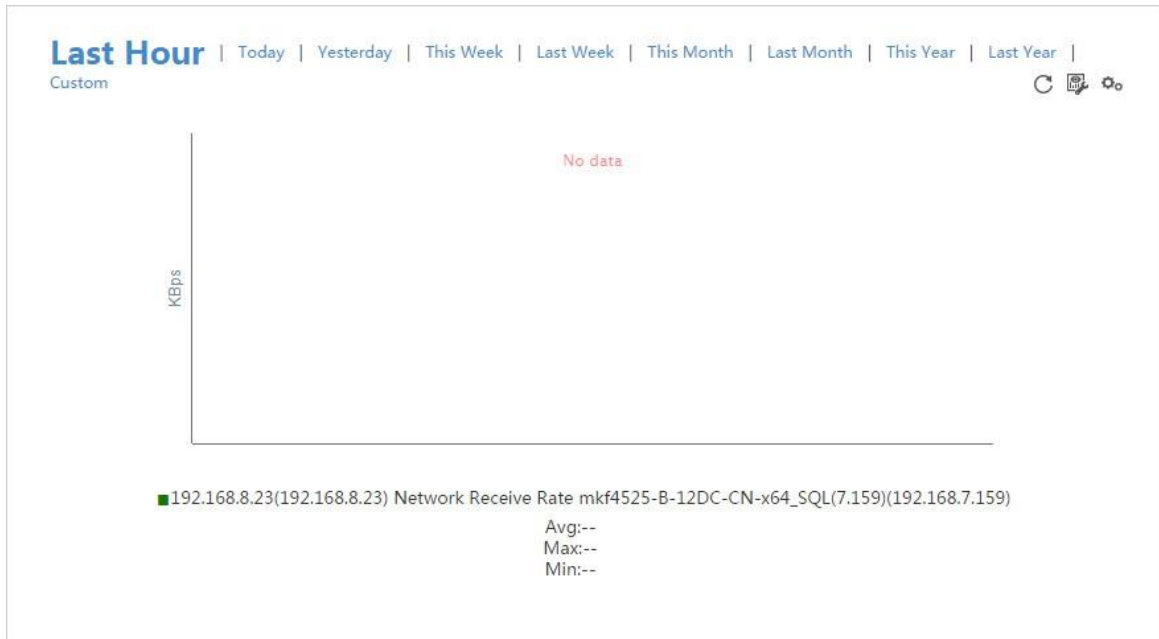
4. Testをクリックして、インデックスを確認します。
5. Applyをクリックします。
6. 新しいカスタムインデックスを使用して、監視インスタンスを追加します。

VM移行後にVM監視インスタンスにデータがない 症状

iMCからの仮想マシンの移行により、監視インデックスが変更され、VM-CPUモニター、VM-メモリーモニター、VM-ディスク/I/Oモニター、およびVM-ネットワークモニターはデータを収集できません。

物理サーバーのIPアドレスは192.168.8.23で、仮想マシンのIPアドレスは192.168.7.159です。仮想マシンの移行後、VMネットワーク受信率インスタンスにデータは表示されません。

図67 データなし



ソリューション

仮想マシンが移行されると、VM監視インスタンスとそのインデックスが変更されます。仮想マシンの新しい監視インスタンスを追加する必要があります。

この問題を解決する手順は、次のとおりです。

1. Resourceタブをクリックします。
2. ナビゲーションツリーからPerformance Management > Monitoring Settingsを選択します。

図68 監視インデックスの追加

Resource > Monitoring Settings Last Statistical Time: 2016-04-20 05:30:00 Re-collect Overall Monitoring Statistics ReportV2 Add to My Favorites Help

Total number of index instances monitored: 12	Total collecting frequency (times/hour): 144	Total number of collecting units: 12
Total number of instances managed by performance management: 12	Total collecting frequency of the instance managed by performance management (times/hour): 144	Total number of collecting units of the instance managed by performance management: 12

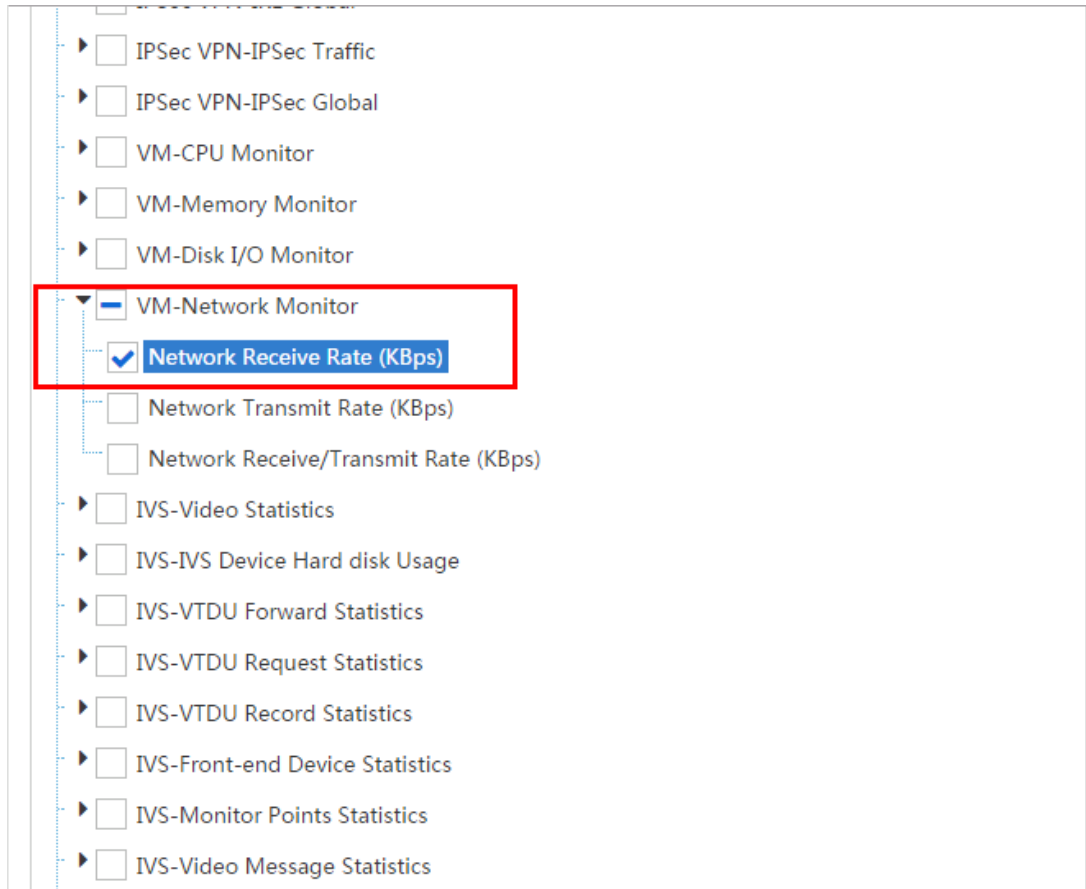
Only Display Monitored Devices [Switch to Instance List](#)

<input type="checkbox"/>	Device Name	Device Model	Instances	Operation	Data
<input type="checkbox"/>	▶ 172.19.254.242(172.19.254.242)	ICMP	2	Add Cancel Modify Index	
<input type="checkbox"/>	▶ 172.31.1.5(172.31.1.5)	ICMP	2	Add Cancel Modify Index	
<input type="checkbox"/>	▶ 192.168.7.1(192.168.7.1)	H3C S5820V2-52Q	4	Add Cancel Modify Index	
<input type="checkbox"/>	▶ 192.168.8.23(192.168.8.23)	ICMP	2	Add Cancel Modify Index	
<input type="checkbox"/>	▶ 192.168.8.25(192.168.8.25)	ICMP	2	Add Cancel Modify Index	

1-5 of 5, Page 1 of 1. << < 1 > >> 15

3. 物理サーバー192.168.8.23の横にあるAddをクリックします。
4. 図69に示すように、Select Indexページで索引を確認します。

図69 インデックスの選択



5. OKをクリックします。
6. Monitoring Settings-Add Monitorページで、Monitoring Instance and Refresh Instanceをオンにして、Select Instances領域でインスタンスを選択します。

図70 インスタンスの選択

Monitoring Settings-Add Monitor Refresh Instance

Monitoring Device Monitoring Instance

Select Index

Total Items: 1.

Name	Index Group	Configure	Delete
Network Receive Rate	VM-Network Monitor		

Select Instances

Device Name

- 192.168.8.23(192.168.8.23)
- Network Receive Rate
 - z10069C.vmnic2
 - z10069C.vmnic3
 - z10069C.vmnic0
 - z10069C.vmnic1
 - z10069C
 - mkf4525-B-12DC-CN-x64_SQL(7.159)(192.168.7.159).4000
 - mkf4525-B-12DC-CN-x64_SQL(7.159)(192.168.7.159).4001
 - mkf4525-B-12DC-CN-x64_SQL(7.159)(192.168.7.159).vmnic2
 - mkf4525-B-12DC-CN-x64_SQL(7.159)(192.168.7.159).vmnic3
 - mkf4525-B-12DC-CN-x64_SQL(7.159)(192.168.7.159).vmnic0
 - mkf4525-B-12DC-CN-x64_SQL(7.159)(192.168.7.159).vmnic1
 - mkf4525-B-12DC-CN-x64_SQL(7.159)(192.168.7.159)
 - mkf4525-D-12DC-CN-x64_SQL(7.174)(192.168.40.195).vmnic2
 - mkf4525-D-12DC-CN-x64_SQL(7.174)(192.168.40.195).vmnic3
 - mkf4525-D-12DC-CN-x64_SQL(7.174)(192.168.40.195).vmnic0
 - mkf4525-D-12DC-CN-x64_SQL(7.174)(192.168.40.195).vmnic1
 - mkf4525-D-12DC-CN-x64_SQL(7.174)(192.168.40.195).4000
 - mkf4525-D-12DC-CN-x64_SQL(7.174)(192.168.40.195)

7. OKをクリックします。
新しいインスタンスがMonitoring Settings-Instanceリストに表示されます。

図71 追加された監視索引

Device addition has completed.

Monitoring Settings-Instance List

Device Name	Result
<input type="checkbox"/> 192.168.8.23(192.168.8.23)	1
<input type="checkbox"/> Network Receive Rate	1
mkf4525-B-12DC-CN-x64_SQL(7.159)(192.168.7.159)	Succeeded

8. Closeをクリックします。
9. インスタンスの監視データを表示します。