H3Cインテリジェントマネジメントセンター

入門ガイド

New h3c Technologies Co.,Ltd.
http://www.h3c.com

ソフトウェアバージョン:iMC PLAT7.3(E0703)
ドキュメントバージョン:5W125-20201112

はじめに

『H3C iMC入門ガイド』には6つの章があり、iMCの主な機能と一般的な問題のトラブルシューティングについて簡単に説明しています。

ここでは、マニュアルに関する次のトピックについて説明します。

- 対象者
- 表記規則
- H3C iMCドキュメントセットについて
- ドキュメントに関するフィードバック

対象者

このマニュアルの対象読者:

- ネットワークプランナー
- フィールドテクニカルサポートおよびサービスエンジニア
- iMCで作業するネットワーク管理者

表記規則

ここでは、マニュアルで使用されている表記規則について説明します。

コマンドの規則

表記規則	説明
ボールド体	太字のテキストは、表示されているとおりに入力したコマンドとキーワードを表します。
イタリック体	斜体のテキストは、実際の値に置き換える引数を表します。
番号	ポンド(#)記号で始まる行がコメントです。

GUIの規則

表記規則	説明
ボールド体	ウィンドウ名、ボタン名、フィールド名およびメニュー項目は太字で表示されます。たとえば、New Userウィンドウが開いたら、OKをクリックします。
>	マルチレベルメニューは、山括弧で区切られます。たとえば、File > Create > Folder

記号

表記規則	説明
⚠	重要な情報への注意を喚起するアラートで、理解またはフォローしないと人身事故につながる可能性があります。
△	重要な情報への注意を喚起するアラート。理解またはフォローしていないと、データの消失、データの破損、ハードウェアまたはソフトウェアの損傷につながる可能性があります。
ⓘ	重要な情報への注意を促すアラート。

表記規則	説明
注:	追加情報または補足情報を含むアラート。
	有用な情報を提供するアラート。

本書に記載されている例

このドキュメントの例では、使用しているデバイスとハードウェアモデル、構成、またはソフトウェアバージョンが異なるデバイスが使用されている場合があります。通常、ポート番号、サンプル出力、スクリーンショット、およびその他の情報は、使用しているデバイスのものとは異なります。

H3C iMCドキュメントセットについて

H3C iMCのマニュアルセットには、次のものが含まれています。

ドキュメント	目的
ハードウェアの仕様とインストール	
H3C iMC入門ガイド	iMCの主な機能と一般的な問題のトラブルシューティングを簡単に説明します。
H3C iMC組み込みデータベースを使用したセントラルデプロイメントガイド	組み込みデータベースを使用したIMCプラットフォームおよびコンポーネントのインストールと一元展開の完全なガイドを提供します。
H3C iMCローカルデータベースを使用したセントラルデプロイメントガイド	ローカルデータベースを使用したiMCプラットフォームおよびコンポーネントのインストールと一元展開の完全なガイドを提供します。
H3C iMCリモートデータベースを使用したセントラルデプロイメントガイド	リモートデータベースを使用したiMCプラットフォームおよびコンポーネントのインストールと一元展開の完全なガイドを提供します。
H3C iMCローカルデータベースを使用した分散デプロイメントガイド	ローカルデータベースを使用したiMCプラットフォームおよびコンポーネントのインストールと分散展開の完全なガイドを提供します。
H3C iMCリモートデータベースを使用した分散デプロイメントガイド	リモートデータベースを使用しiMCプラットフォームおよびコンポーネントのインストールと分散展開の完全なガイドを提供します。
H3C iMCプローブインストレーションガイド	iMCプローブのインストールと展開の完全なガイドを提供します。
H3C iMC RSMインストールガイド	iMC RSMのインストールと展開の完全なガイドを提供します。
H3C iMC iHAToolインストレーションガイド	iMC iHAToolインストールの完全なガイドを提供します。
SQL Server2012インストールと構成ガイド	iMC用SQL Server2012のインストール手順を説明します。
SQL Server2014インストールと構成ガイド	iMC用SQL Server2014のインストール手順を説明します。
SQL Server2016インストールと構成ガイド	iMC用SQL Server2016のインストール手順を説明します。
SQL Server2017インストールと構成ガイド	iMC用SQL Server2017のインストール手順を説明します。
Oracle11gインストールおよび構成ガイド(Linux用)	Linux for iMCへのOracle11gのインストール手順を説明しています。

ドキュメント	目的
Oracle11g R2インストールおよび構成ガイド(Linux用)	Linux for iMCへのOracle11g R2のインストール手順を説明しています。
Oracle12cインストールおよび構成ガイド(Linux用)	Linux for iMCへのOracle12cのインストール手順を説明しています。
Red Hat Enterprise Linux7.0インストールガイド	Re d Hat Enterprise Linux7.0 for iIMCのインストール手順を説明します。
ソフトウェア構成	
H3C iMCエンタープライズおよび標準プラットフォーム管理者ガイド	IMCプラットフォームでの操作手順を説明します。
H3C iMC Quality of Service Manager管理者ガイド	iMC Quality of Service Managerの操作手順について説明します。
H3C IMC Resource Automation Manager管理者ガイド	リソース自動化マネージャーでの操作手順を説明します。
H3C iMC Service Health Manager管理者ガイド	Service Health Managerでの操作手順を説明します。
H3C IMCS VAN Connection Manager管理者ガイド	iMC VAN Connection Managerの操作手順について説明します。
H3C iMCS VAN Software Defined Network Manager管理者ガイド	IMC VAN Software Defined Network Managerの操作手順について説明します。
H3C iMCS VAN Fabric Manager管理者ガイド	iMC VAN Fabric Managerの動作手順について説明します。
H3C iMC Application Manager管理者ガイド	iMC Application Managerの操作手順を説明します。
H3C iMCブランチIntelligent Management System管理者ガイド	iMCブランチインテリジェントマネジメントシステムの運用手順を説明します。
H3C iMCビジネスサービスマネージャー管理者ガイド	iMCビジネスサービスパフォーマンスの操作手順を説明します。
H3C iMC IPSec VPN Manager管理者ガイド	iMC IPSec VPN Managerの動作手順について説明します。
H3C iMC MPLS VPN Manager管理者ガイド	iMC MPLS VPN Managerの動作手順について説明します。
H3C iMC Network Traffic Analyzer管理者ガイド	iMCネットワークトラフィックアナライザの操作手順について説明します。
H3C iMCサービスオペレーションマネージャー管理者ガイド	iMC Service Operation Managerの操作手順について説明します。
H3C iMC User Behavior Auditor管理者ガイド	iMC User Behavior Auditorの操作手順を説明します。
H3C iMC UC Health Manager管理者ガイド	iMC UC Health Managerの操作手順について説明します。
H3C iMC Wireless Service Manager管理者ガイド	iMC Wireless Service Managerの操作手順について説明します。
H3C iMC User Access Manager管理者ガイド	iMC User Access Managerの操作手順を説明します。
H3C iMCS TACACS+ Authentication Manager管理者ガイド	iMC TACACS+ Authentication Managerの操作手順について説明します。
H3C iMC EADセキュリティポリシーアドミニストレータ	iMC EADセキュリティの操作手順を説明します。

ドキュメント	目的
ガイド	ポリシーマネージャー。
オンラインヘルプ	iMCの適切な使用を支援します。
運用と保守	
Readmeファイル	最新のiMCリリース情報を提供します。

ドキュメントに関するフィードバック

製品ドキュメントに関するご意見は、info@h3c.comまで電子メールでお寄せください。

ご意見をいただければ幸いです。

内容

はじめに

Intelligent Management Center(iMC)は、H3Cによって提供される統合ネットワーク管理製品です。iMCは、エンドツーエンドのリソース管理、ユーザー管理、およびサービス管理のための総合ソリューションを提供します。

iMCコンポーネント

iMCにはiMCプラットフォームおよびサービスコンポーネントが含まれます。iMCプラットフォームは、iMCサービスを提供するための基本コンポーネントです。異なる要件を満たすサービスコンポーネントを選択できます。iMCは、次のサービスコンポーネントを提供します。

- アプリケーションマネージャー
- ブランチインテリジェントマネジメントシステム
- ビジネスサービスマネージャー
- EADセキュリティポリシー
- エンドポイントインテリジェントアクセス
- エンドポイントモバイルオフィス
- EoCマネージャー
- EPONマネージャー
- Intelligent Analysis Reporter
- IPSec VPNマネージャー
- ITサービスマネージャー
- MPLS VPN Manager
- ネットワークトラフィックアナライザ
- QoSマネージャー
- リソース自動化マネージャー
- セキュリティサービスマネージャー
- サービスヘルスhealth manager
- サービスオペレーションマネージャー
- Unified Communications Health Manager
- ユーザー動作の監査
- VAN接続マネージャー
- VANファブリックマネージャー
- VAN SDNマネージャー
- 音声サービスマネージャー
- ワイヤレスサービスマネージャー

iMCのインストールと展開

iMCをインストールして配備するには、次の手順に従います。

1. 次のリソースを準備します。
    - インストールCD/DVD(製品パッケージに収録)

- ライセンス証明書(製品パッケージに含まれています)

2. 配置スキームを選択します。

   iMCは、次の配置スキームをサポートしています。

   - データベースを組み込んだ一元的な導入ガイド
   - ローカルデータベースを使用した一元的な導入ガイド
   - リモートデータベースを使用した一元的な導入ガイド
   - ローカルデータベースを使用した分散配置ガイド
   - リモートデータベースを使用した分散配置ガイド

   エンタープライズまたは組織のサイズに基づいて配置スキームを選択します。適切な配置スキームの選択の詳細は、配置スキームの配置ガイドを参照してください。配置ガイドには、サーバーのハードウェア要件、インストールおよび登録手順およびアプリケーションシナリオが含まれています。これらのドキュメントは、h3cのWebサイトで入手できます。iMC配置ガイドは、URL:https://www.h3c.com/en/Support/Resource_Center/EN/Network_Management/Catalog/h3c_IMC/IMC/から参照できます。

3. 選択した配置スキームに従って、iMCのインストールに使用するサーバーを準備します。
4. iMCをインストールして展開します。
5. iMCを登録します。

   登録に必要なライセンスキーは、ライセンス証明書に記載されています。

iMCの探索

iMCは、iMCプラットフォームとさまざまなサービスコンポーネントで構成されています。iMCのインターフェイスは、インストールされているコンポーネントによって異なります。次の情報では、iMCプラットフォームがすでにインストールおよび導入されているシステムを例として使用します。

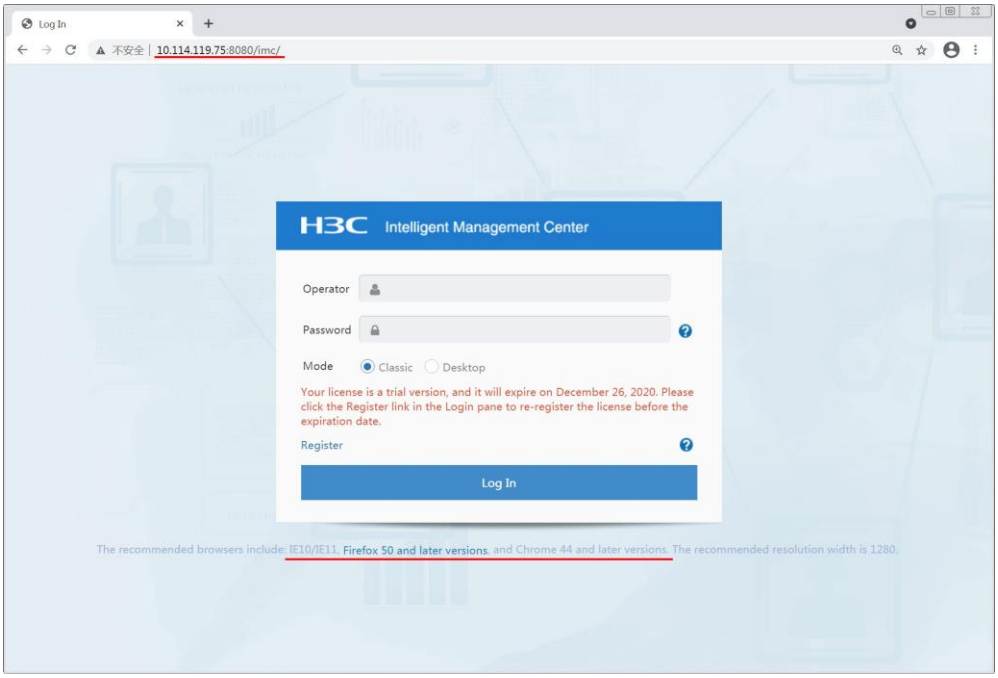
iMCへのログイン

iMCはブラウザー/サーバーモデルを採用しており、ブラウザーを介してアクセスできます。iMCを起動するには:

1. Webブラウザーを起動します。
   次のブラウザーがサポートされています。
   - IE10.0/IE11.0以降のバージョン
   - Firefox50以降のバージョン
   - Chrome44以降のバージョン

   以前のバージョンのブラウザーを使用している場合、ログインの問題が発生することがあります。詳細については、FAQを参照してください。
2. Webブラウザーを次のように設定します。
   - ポップアップブロックをオフにします。
   - Cookieを有効にします。
   - iMCを信頼済みサイトとして追加します。
   - 推奨解像度(幅1280ピクセル以上)を使用してください。
3. Webブラウザーのアドレスバーに、http://ipaddress:port number/imcまたはhttps://ipaddress:port number/imcと入力します。
   デフォルトでは、iMCはHTTPポート8080とHTTPSポート8443を使用します。
   HTTPSは、iMCログイン用のセキュアモードを提供します。HTTPSを使用してiMCにアクセスしようとすると、証明書エラーメッセージが表示される場合があります。この問題の解決方法については、FAQを参照してください。
   図1は、http://10.114.119.75:8080/imcのアドレスを持つログインページを示しています。

図1 iMCログインページ



4. 演算子名とパスワードを入力し、モードを選択してLoginをクリックします。iMC

   には次のモードがあります。

   - classic：図と表を使用してネットワーク動作ステータスを示す伝統的なユーザインターフェイスです。
   - Desktop：アプリケーションとしてiMC機能を提供するWebデスクトップ。

   最初のログインには、デフォルトのオペレーター名とパスワードadminを使用します。セキュリティ上の理由から、最初のログイン後にパスワードを変更してください。パスワードの変更手順については、FAQを参照してください。

   異なる権限を持つオペレーターをiMCに追加できます。詳細については、iMCのヘルプを参照してください。

   自動ログインを防止するには、iMCログインページのコード検証機能を有効にします。詳細については、FAQを参照してください。

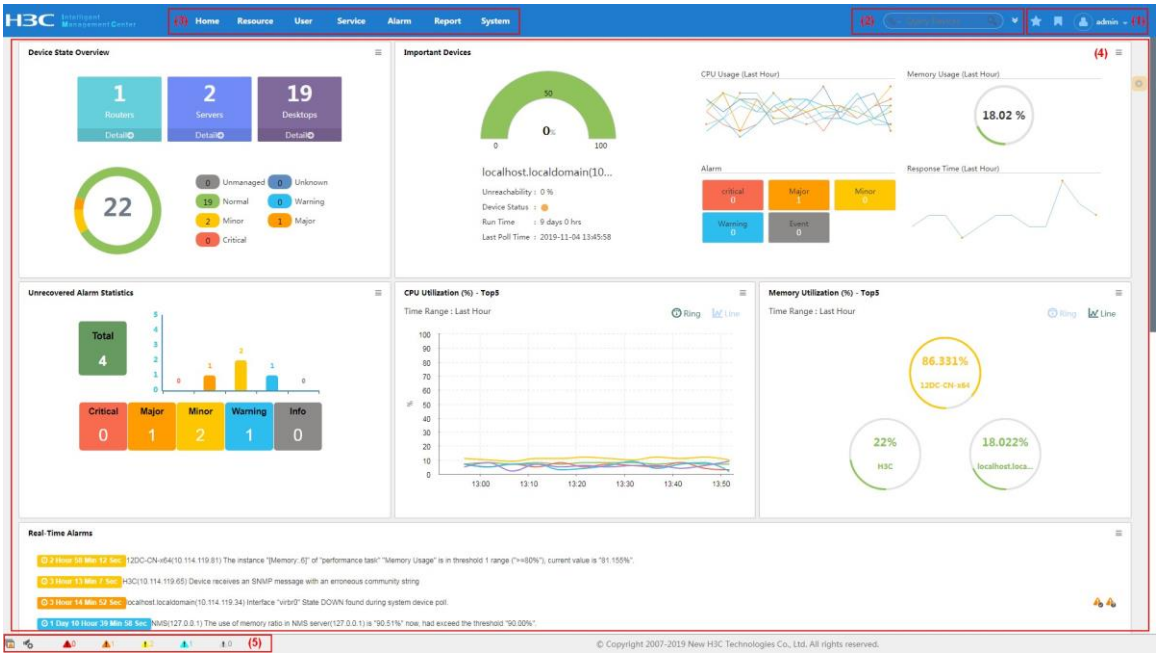
GUIの概要

ホームページには、すべてのiMC機能に簡単にアクセスできるように設計されたタブがいくつかあります。

Classic iMCのホームページ

図2に示すように、iMCのホームページでは、表示するウィジェットを指定し、ウィジェットのレイアウトを選択し、必要に応じてスペースをカスタマイズすることができます。

図2 Classic iMCのホームページ



Classic iMCページは、表1で説明されているように、次の領域で構成されています。

表1 Classic iMCホームページの説明

No.	名称	説明
1	Management links	現在のオペレーターに関する情報を表示し、Help、About、およびLogoutリンクを提供します。 現在のオペレーター名の上にポインタを置くと、オペレーターのログイン時刻とIPアドレスが表示されます。
2	Navigation bar	管理機能に構成エントリを提供します。構成エントリはタイプ別に整理されています。
3	Search bar	ユーザー、デバイスおよびインターフェイスの検索を可能にします。 複数の基準による拡張検索をサポートします。
4	Welcome page	iMCへのログイン後に開きます。iMCでは、複数の初期ページをカスタマイズしたり、デフォルトの初期ページを指定したりできます。さらに、iMCには様々なウィジェットが用意されています。必要に応じて、初期ページにウィジェットを追加できます。
5	Alarm statistics	アラーム統計情報を表示し、アラームレベルに基づいて音声プロンプトを表示します。

すべてのiMCホームページには、management links、navigation bar、search bar、およびalarm statisticsがあります。

Web desktop

Web desktopにアクセスするには、次のいずれかの方法を使用します。

- iMCにログインするときは、Desktop オプションを選択します。
- ページの右上隅にあるアイコンをクリックし、ドロップダウンリストからDesktop Viewを選択してWebデスクトップを表示します。

図3 iMC Web desktop

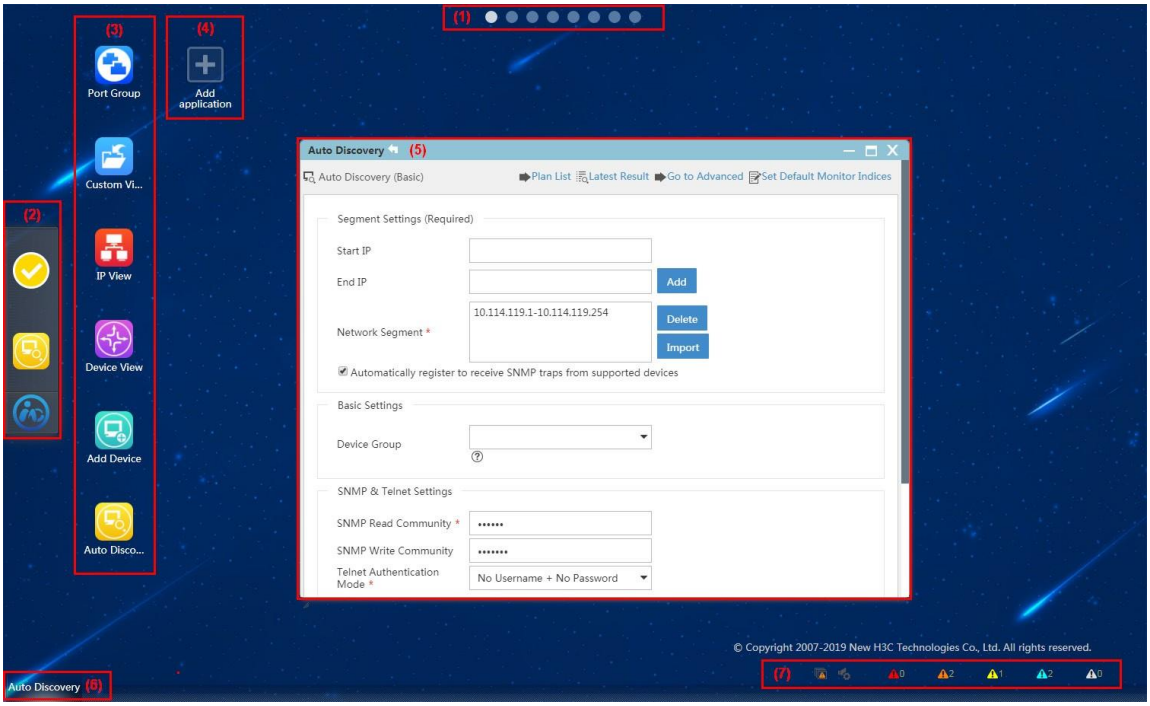


表2に示すように、Webデスクトップには次の領域があります。

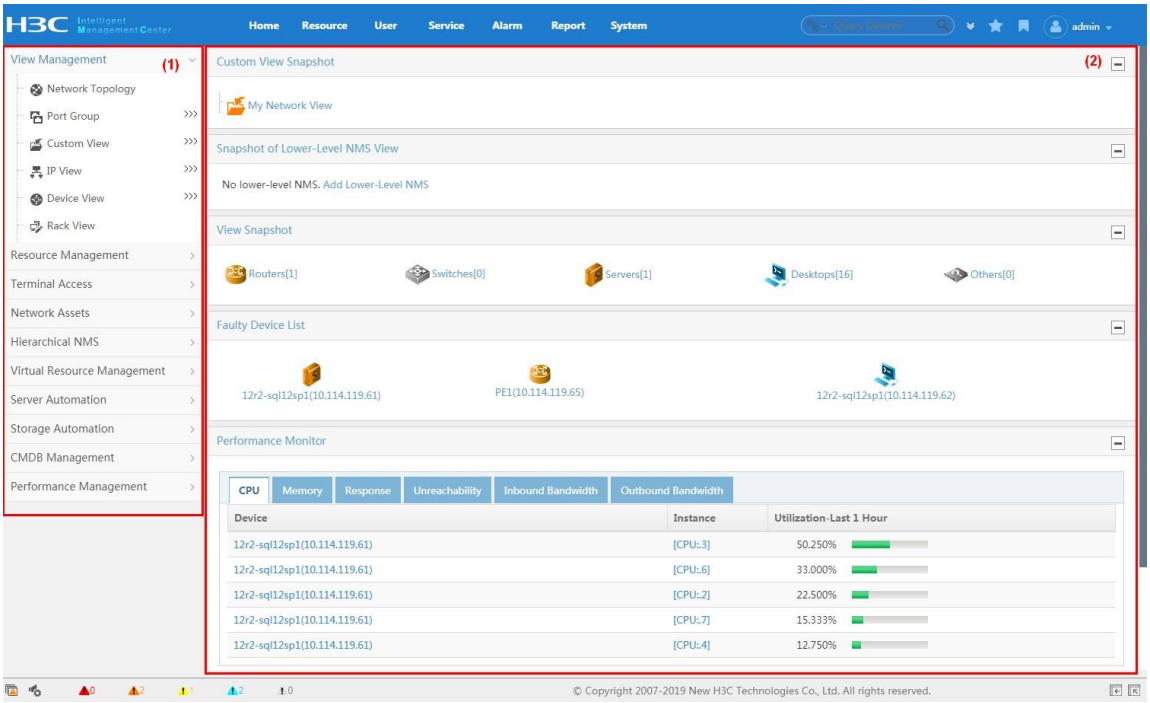
表2 Webデスクトップの説明

No.	名称	説明
1	Tool bar	さまざまなデスクトップを切り替えることができます。
2	Application launcher	さまざまなデスクトップ上のアプリケーションへのショートカットを提供します。
3	Application icons	アプリケーションを使用するには、アイコンをクリックします。
4	Add application icon	アプリケーションを現在のデスクトップに追加するには、アイコンをクリックします。
5	Application windows	アプリケーションの操作ウィンドウ。Classic iMCインターフェイスと同じ機能を提供します。
6	Task bar	実行中のアプリケーションを表示し、それらを切り替えることができます。
7	Alarm statistics	アラーム統計情報を表示し、アラームレベルに基づいて音声プロンプトを表示します。

操作インターフェイス

iMCクラシックモードとデスクトップモードでは、同様の操作インターフェイスが提供されます。図4に、リソース管理ページの例を示します。

図4 操作インターフェイス



操作インターフェイスのレイアウトは、表3に示すように、次の領域を除いて、Classic iMCホームページに似ています。

表3 操作インターフェイスの説明

No.	名称	説明
1	ナビゲーションツリー	現在のページにある機能へのリンクが表示されます。
2	操作領域	使用可能な操作機能と操作関連情報を表示します。

図4に、次の情報を示します。

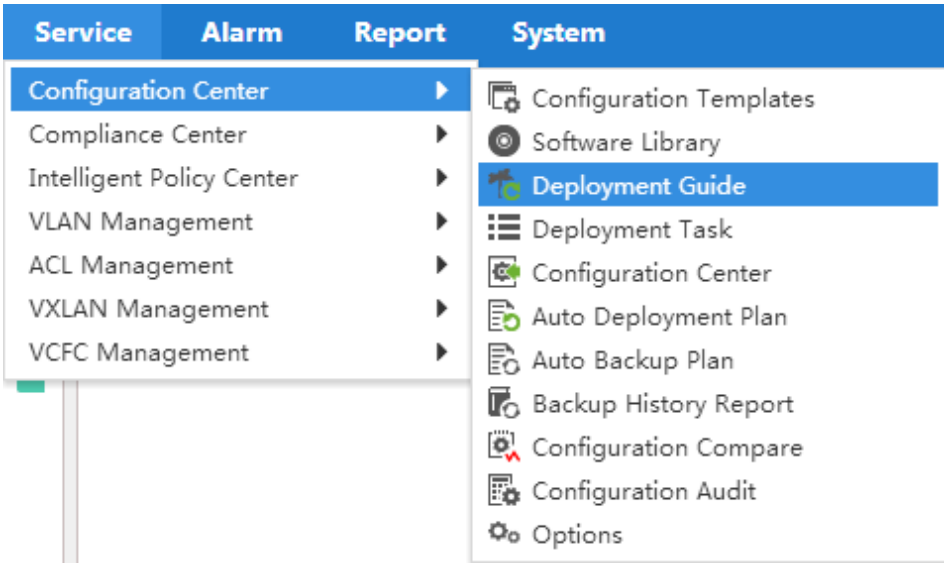
- カスタムビューまたはデバイスビューでは、カテゴリアイコンの色は、最も重大なアラームが発生しているカテゴリのデバイスのステータスによって異なります。
- デバイスビュースナップショットには、デバイスの数とアラームレベルがカテゴリ別に表示されます。
- 障害デバイスリストには、各レベルのアラームを持つ障害デバイスが表示され、アラームレベルごとにデバイスがソートされます。iMCに障害デバイスが含まれていない場合、この領域は表示されません。
- パフォーマンス監視領域には、対象となるさまざまなパフォーマンス指標が表示されます。

インターフェイス上のビューおよびデバイスアイコンはすべてリンクです。リンクをクリックすると、操作領域内の指定したデバイスに関する情報を表示できます。

タブのメニュー

iMCには、各機能タブのメニューが用意されています。

図 5 Serviceタブのメニュー

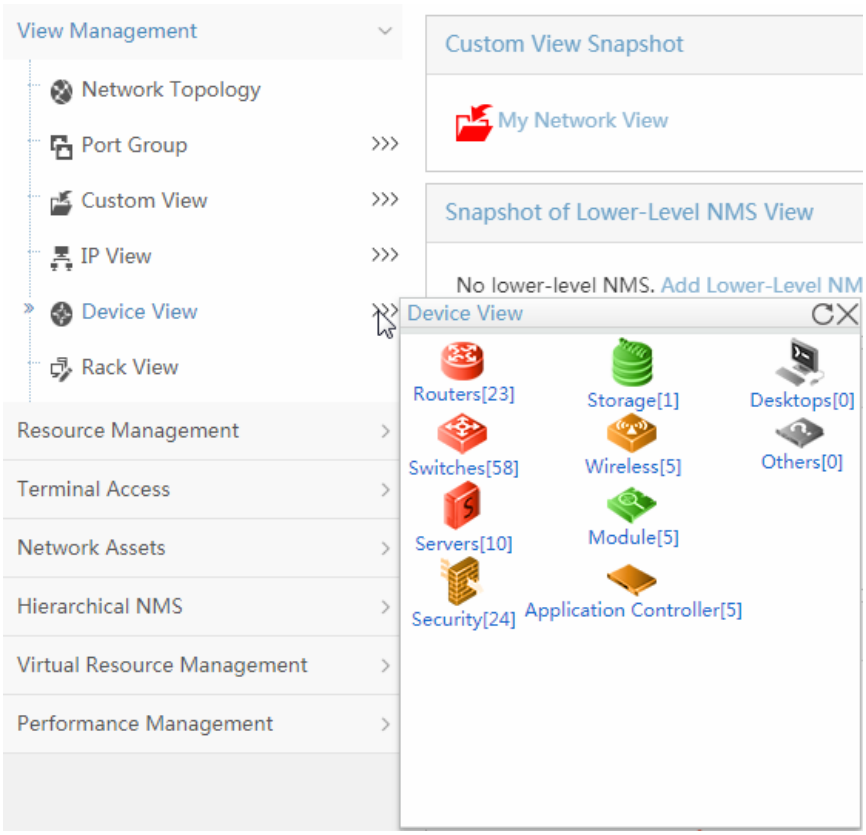


メニューを使用すると、目的の機能をすばやく見つけることができます。図5に示すように、Serviceタブ上にポインタを置くと、メニューが表示されます。目的の機能をクリックすると、対応するページに移動できます。

ナビゲーションツリーのフローティングメニュー

iMCナビゲーションに、iMCナビゲーションツリーにはフローティングメニューがあります。

図6 ナビゲーションツリーのフローティングメニュー



フローティングメニューにはエントリのセカンダリーリンクが表示され、機能リンクをすばやく検索して展開できます。

エントリの右側にあるアイコンの上にポインタを移動すると、そのエントリのフローティングメニューが表示されます。フローティングメニューのリンクをクリックすると、対応する機能ページに移動します。

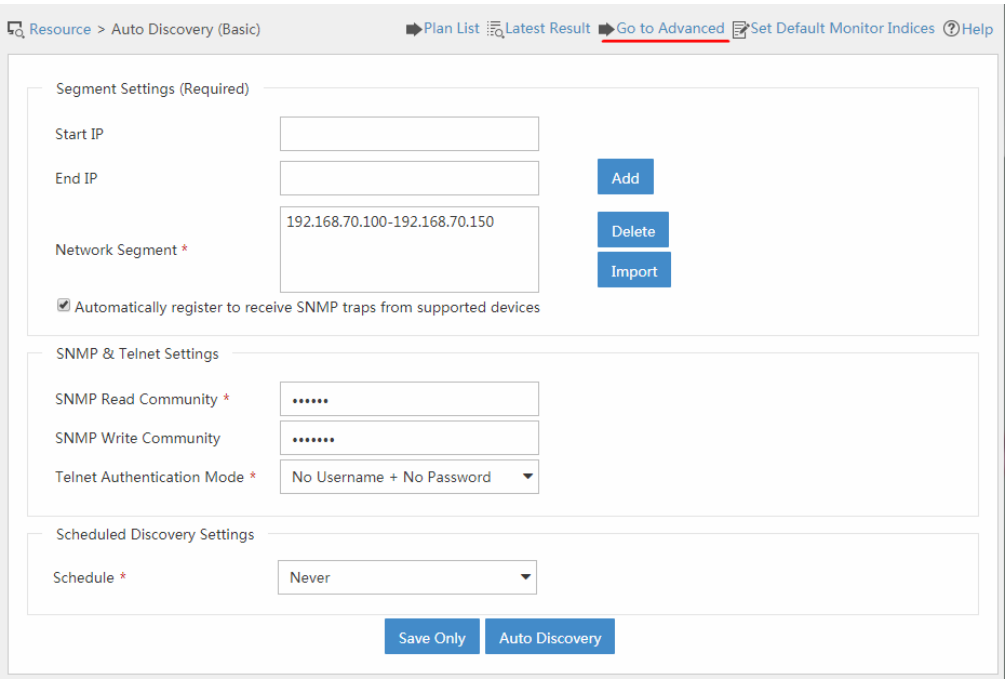
自動検出の使用

ネットワークを管理するには、まず自動検出を使用してネットワークデバイスをiMCに追加します。通常は、最初のログイン時に自動検出を使用するため、デバイスをバッチで迅速に追加できます。

自動検出を使用するには:

1. Resourceタブをクリックします。
2. Resource Management > Auto Discovery を選択して、基本的な自動検出ページを表示します(図7を参照)。

図7 基本的な自動検出

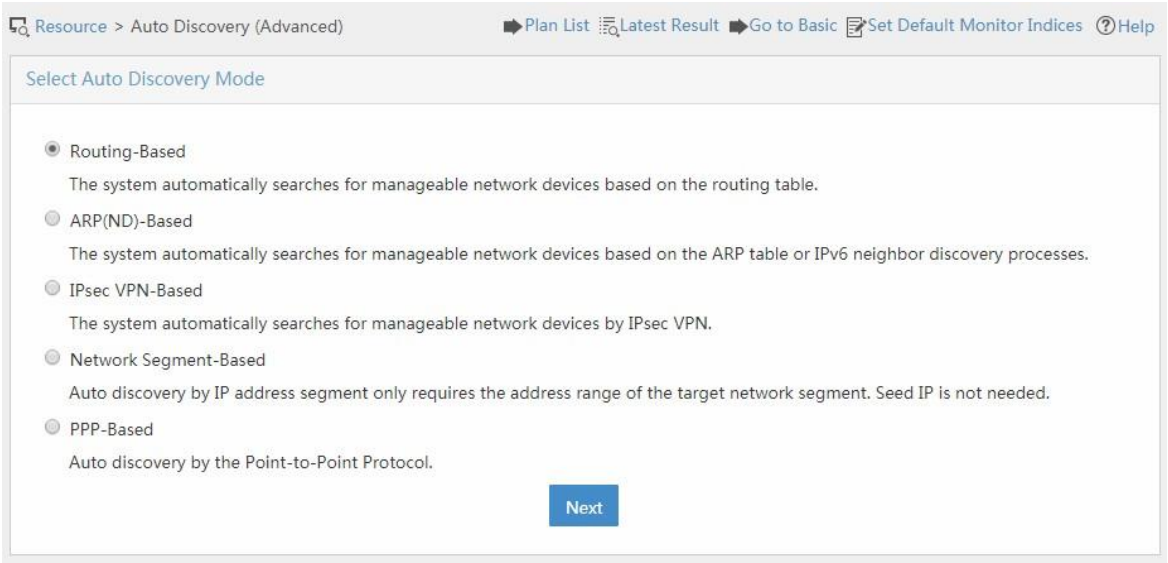


3. 開始IPアドレスと終了IPアドレスを入力します。次に、**Add**クリックしてネットワークセグメントを指定し、ネットワークセグメント上のデバイスを検出できるようにします。

   複数のネットワークセグメントを指定できます。

iMCには、デバイスを自動的に検出するための様々なモードも用意されています。これらの自動検出モードを使用するには、基本的な自動検出ページで**Go to Advanced**をクリックします。図8に示すように**Advanced Auto discovery**ページが開きます。

図8 Advanced Auto discovery



高度な自動検出モードは、さまざまなシナリオに適用されます。

- ゲートウェイまたはルータのIPアドレスだけがわかっている場合は、**Routing-Based**を選択します。
- デバイス検出を高速化するには、**ARP-Based**を選択します。
- IP Sec VPN関連デバイスのみを対象とする場合は**IPSec VPN-Based**を選択します。

- ネットワークセグメントの計画がわかっている場合は、**Network Segment-Based**を選択します。
- レイヤ3デバイスを接続するインターフェイスのIPアドレスが/30ビットサブネットマスクを使用する場合は、**PPP-Based**を選択します。

最初のログイン後のデバイスの自動検出に加えて、iMCではデバイスを手動で追加できます。手動方式は、通常、新規デバイスがネットワークに接続されている場合に使用されます。デバイスを個別に追加するには、**resource > Add device**ページにナビゲートします(詳細は表示されません)。

操作のヒント

ヘルプシステムの表示

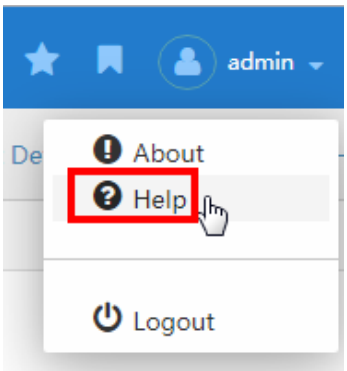
iMCは、完全で強力なオンラインヘルプシステムを提供します。iMCにログインした後、Helpをクリックしてヘルプにアクセスします。iMCヘルプには次の機能があります。

- **Full text search**：ヘルプシステム全体で関連情報を検索するには、キーワードを入力します。
- **Content-dependent help**：インストールされているコンポーネントに依存します。
- **Context-sensitive help**：特定の設定タスクに関するヘルプ情報にアクセスするためのHelpリンクが表示されます。

iMCヘルプには、次のいずれかの方法でアクセスできます。

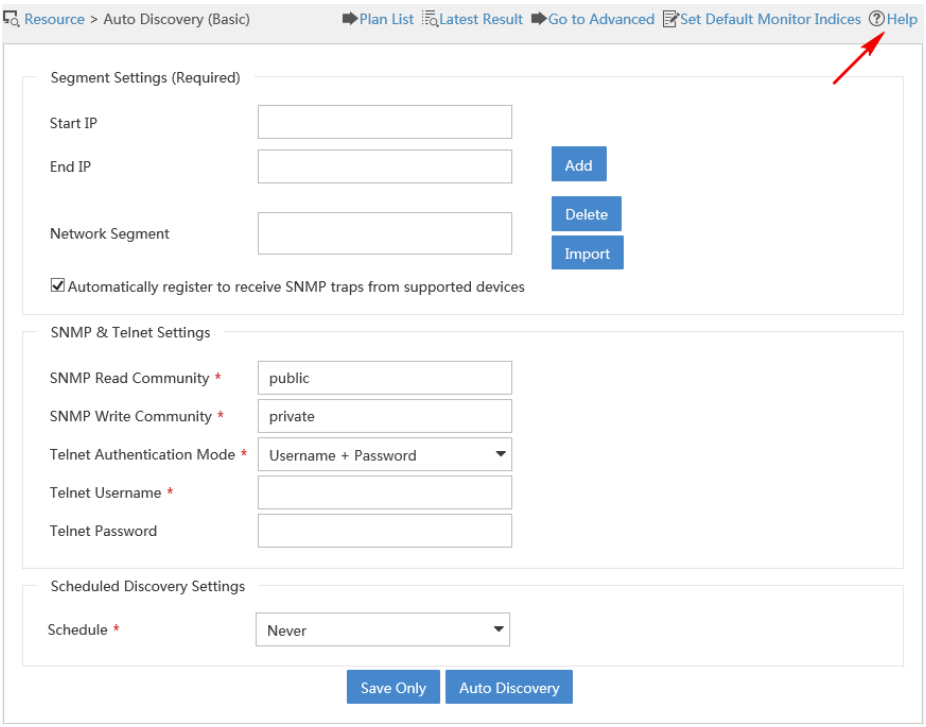
- **Access the full help**：ページの右上隅にあるアイコンをクリックし、メニューからHelpを選択します(図9を参照)。

図9 ヘルプシステムへのリンク



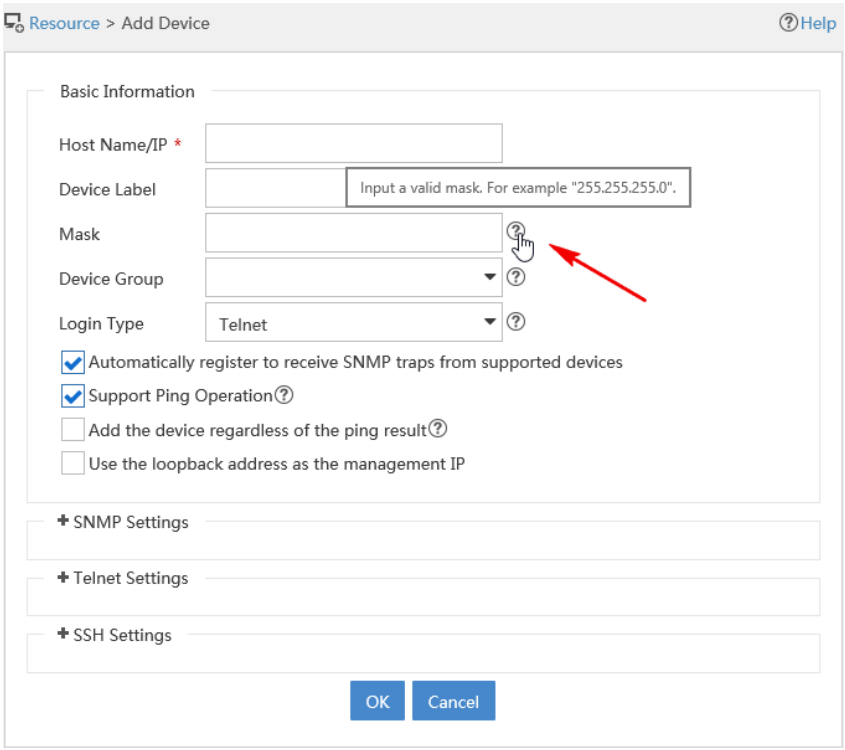
- 特定のページのヘルプ情報にアクセスする：図10に示すように、設定ページの右上隅にあるHelpをクリックします。

図10 特定の構成ページのヘルプリンク



- **View tooltips**：パラメーターの入力制限を表示するには、パラメーターのツールチップアイコン上にポインタを置きます。たとえば、図11に、**Add Device**ページの**Mask**パラメーターのヒントを示します。

図11 パラメーター入力用のツールチップ



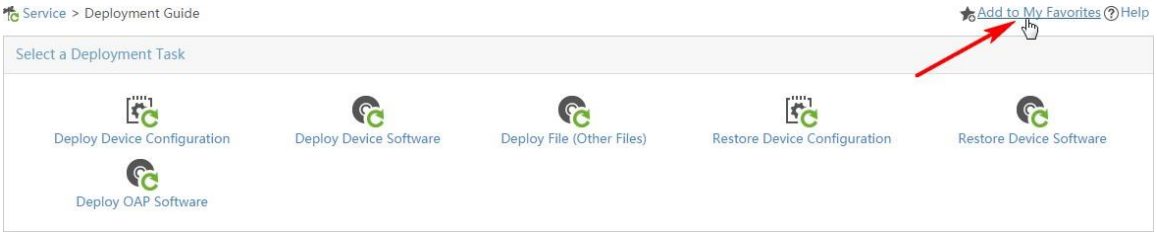
My Favoritesペインの個人用設定

頻繁にアクセスするiMC機能を**My favorite**ペインに追加して、目的のページにすばやくアクセスできるようにすることができます。

My Favoritesペインへの関数の追加

図12に示すように、ページの右上隅にある**Add to My Favorites**をクリックします。

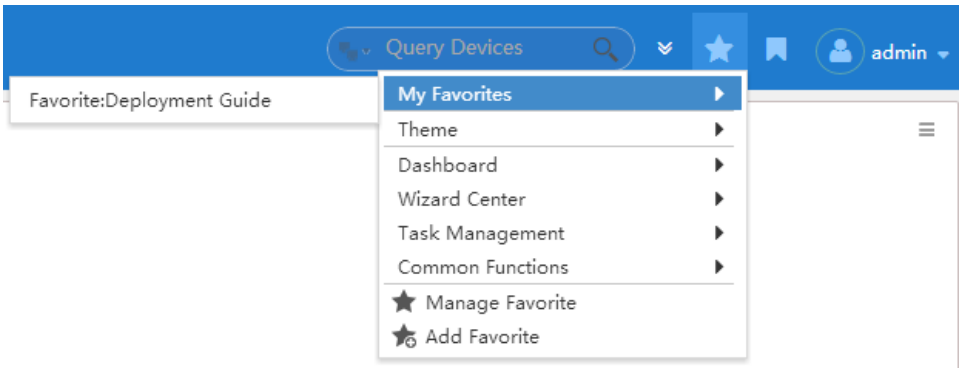
図12 My Favoritesペインへの機能の追加



My Favoritesペインへのアクセス

ページの右上隅にある星形のアイコンをクリックし、メニューからMy Favoriteを選択します(図13を参照)。

図13 My Favoritesペインへのアクセス



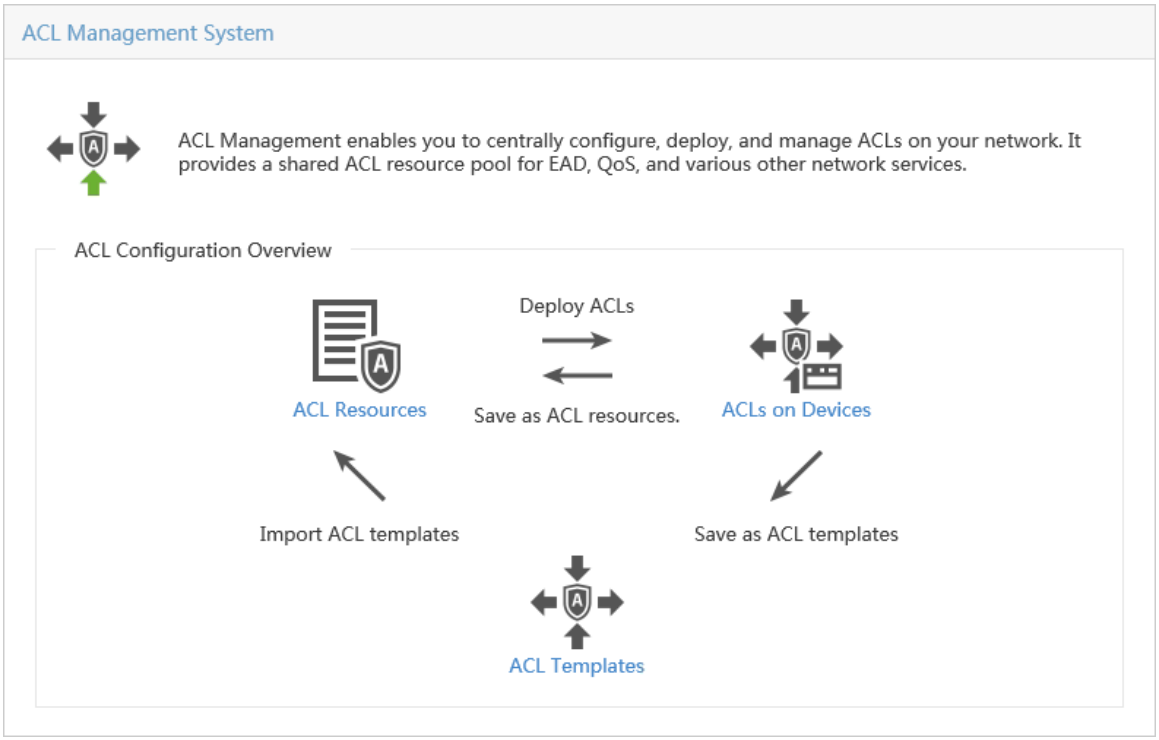
注:

図13の内容は、インストールされているサービスコンポーネントによって異なります。このドキュメントのメニューコンテンツおよびナビゲーションツリーは、実際の環境のものとは異なる場合があります。

サービスコンフィギュレーションガイドの理解

図14に示すように、一部のサービスコンポーネントには、サービス導入プロセス全体をガイドする構成ガイドが用意されています。

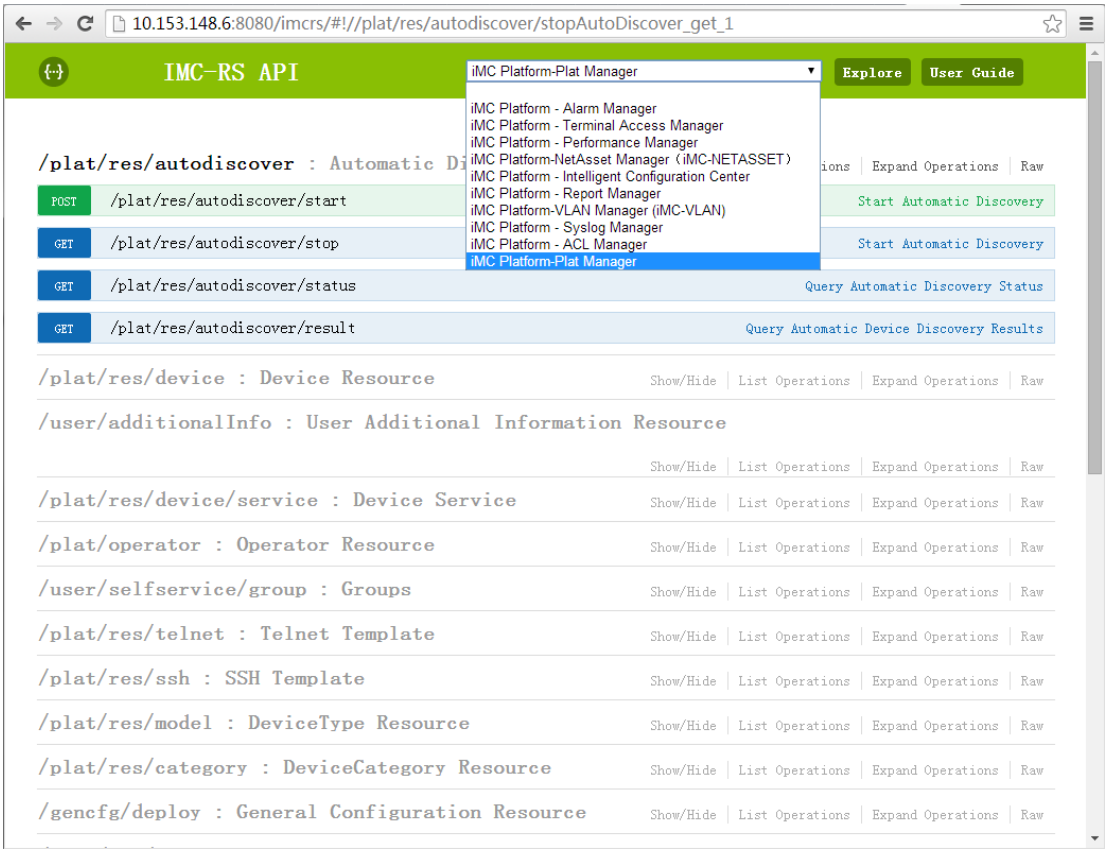
図14 ACL管理設定ガイド



iMC REST APIの使用

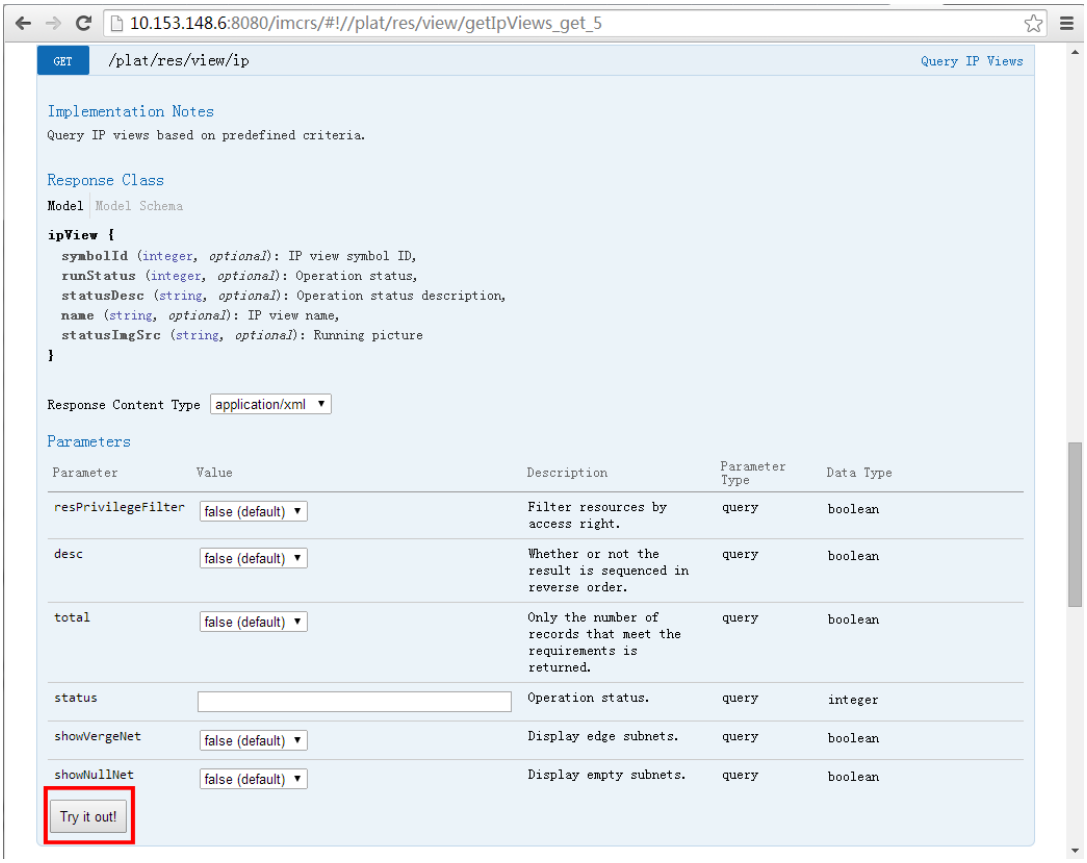
1. Webブラウザーを起動します。
2. アドレスバーにhttp://ip_address:port_number/imcrsまたはhttps://ip_address:port_number/imcrs デフォルトでは、iMCはHTTPポート8080およびHTTPSポート8443を使用します。IMC-RS API ログインページが開きます。
3. 演算子名とパスワードを入力します。演算子に**REST API**管理権限があることを確認してください。 **iMC-RS API** ページが開きます。
4. APIをフィルタする機能モジュールをリストから選択します。

図15 フィルタリングAPI



5. APIを展開します。
6. **Try it out**をクリックして、その機能をテストします。

図16 APIのテスト



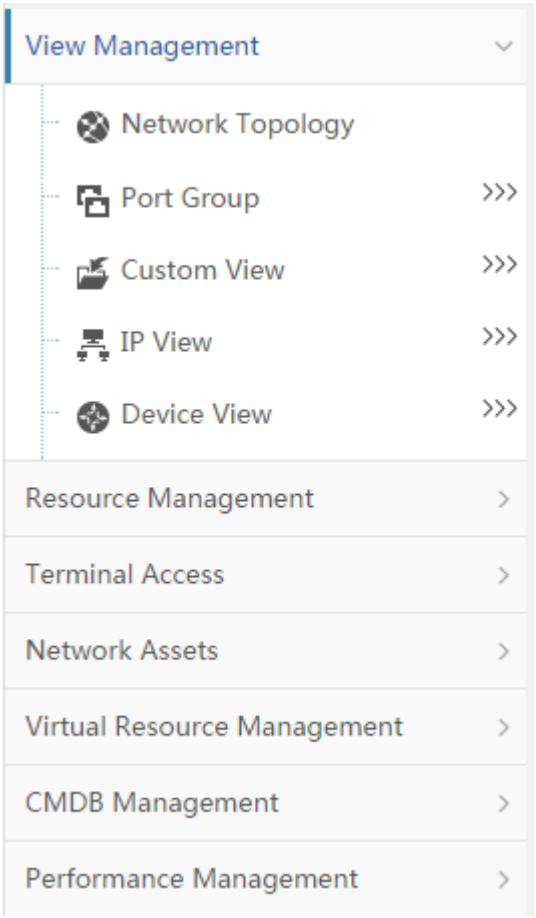
基本リソースの管理

iMCでは、基本リソースとは、デバイス、インターフェイス、リンク、仮想ネットワークなどのネットワークリソースを指します。ネットワークリソースを適切に実行することにより、ネットワーク内にサービスとアプリケーションを配置するための基礎が提供されます。

概要

ナビゲーションパスから**Resource**タブをクリックします。図17に示すように、リソースナビゲーションツリーが表示されます。

図17 リソースナビゲーションツリー



サブツリーを展開するには、サブツリーの右上隅にあるトリプル矢印アイコン(>>>)をクリックするか、サブツリー名をクリックします。

図17に示すように、ナビゲーションツリーの機能ノードは、次のカテゴリに分類されます。

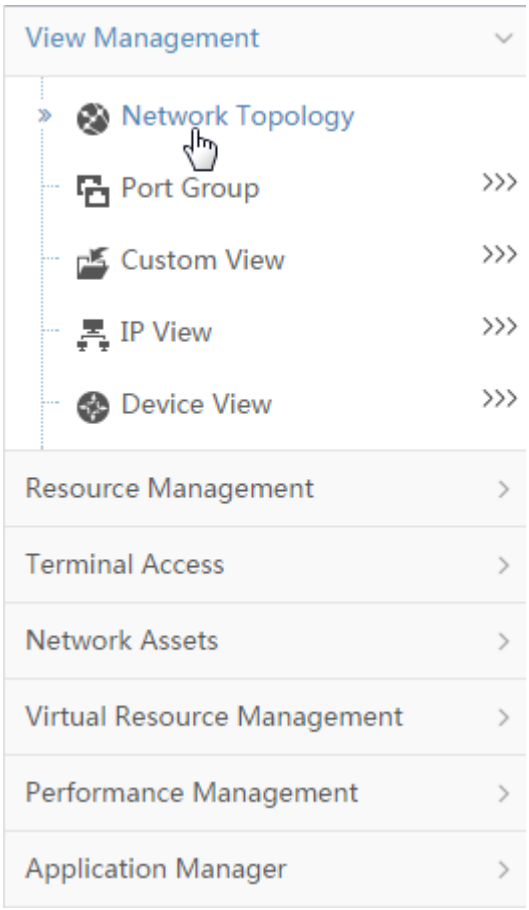
- **View Management**：トポロジービューおよびネットワークビューへのエントリを提供します。トポロジービューまたはいずれかのビューで、目的のデバイスをすばやく見つけることができます。
- **Resource Management**：デバイスを追加し、デバイスパラメーターをバッチ設定できます。
- **Terminal Access**：統一されたエンドポイント管理およびモニタリングを提供します。
- **Network Assets**：スイッチ、カード、電源モジュールなどの資産の管理に役立ちます。
- **Virtual Resource Management**：仮想ネットワーク管理用の仮想ネットワークビューおよび仮想ネットワークトポロジーへのエントリを提供します。
- **CMDB Management**:CI検索、事前定義されたCIタイプ、統計情報ビュー、システム管理など、構成アイテム(CI)の管理機能を提供します。
- **Performance Management**：一般的なデバイスパフォーマンスビューとパフォーマンス設定を提供します。

トポロジーによるネットワークの管理

ネットワークトポロジーを表示する

図18に示すように、**Network Topology**をクリックします。ネットワークトポロジーが新しいウィンドウに表示されます。

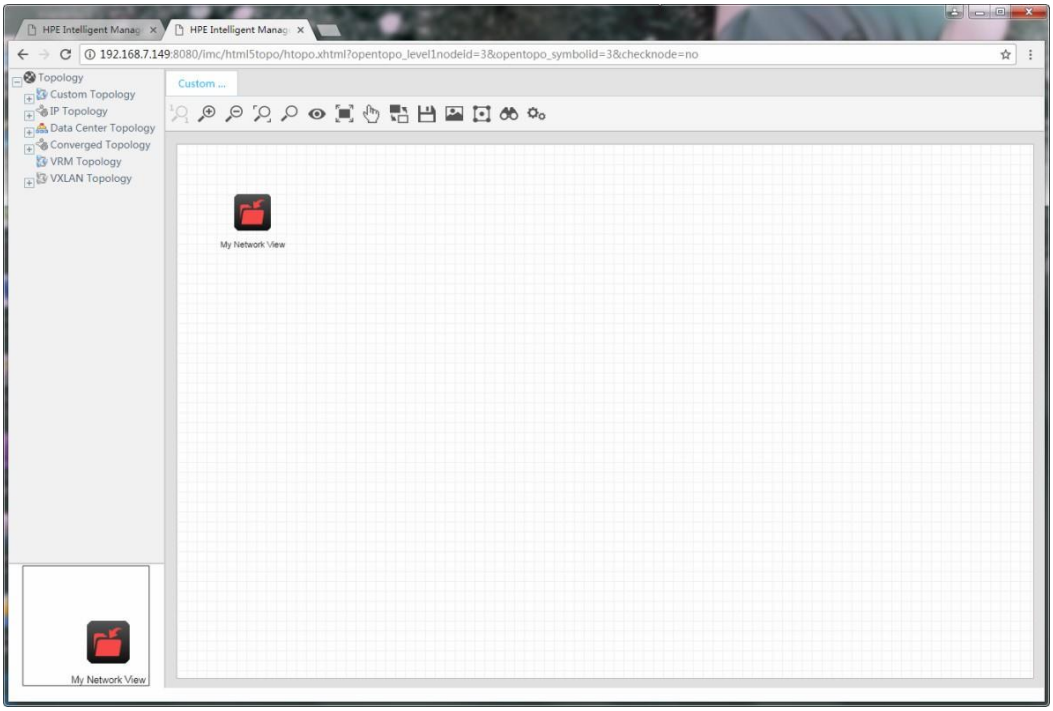
図18 ネットワークトポロジーの表示



カスタムトポロジーを表示する

図19に示すように、デフォルトでは**Network Topology**ウィンドウにカスタムトポロジーが表示されます。**My Network View**アイコンをダブルクリックして、新規タブでカスタムビューを開きます。

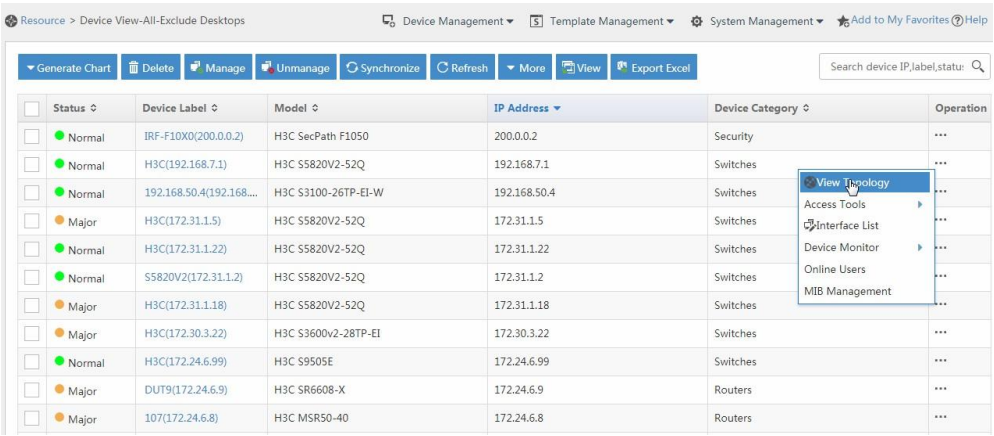
図19 カスタムトポロジーの表示



トポロジーマップ内のデバイスの検索

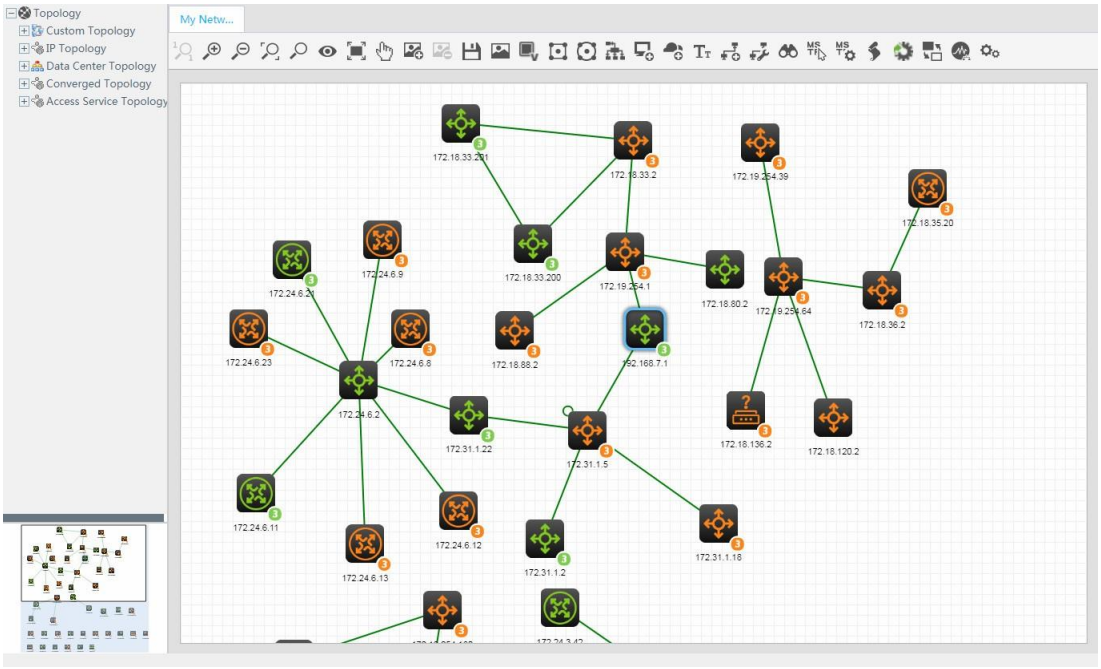
1. ナビゲーションツリーで、**Device View**をクリックします。
   デバイスビューが開きます(図20を参照)。

   図20 デバイスビュー：ルータ



2. デバイスの**Operation**リンクをクリックし、メニューから**View Topology**を選択します。図21に示すように、デバイスを自動的に配置するビューを選択します。

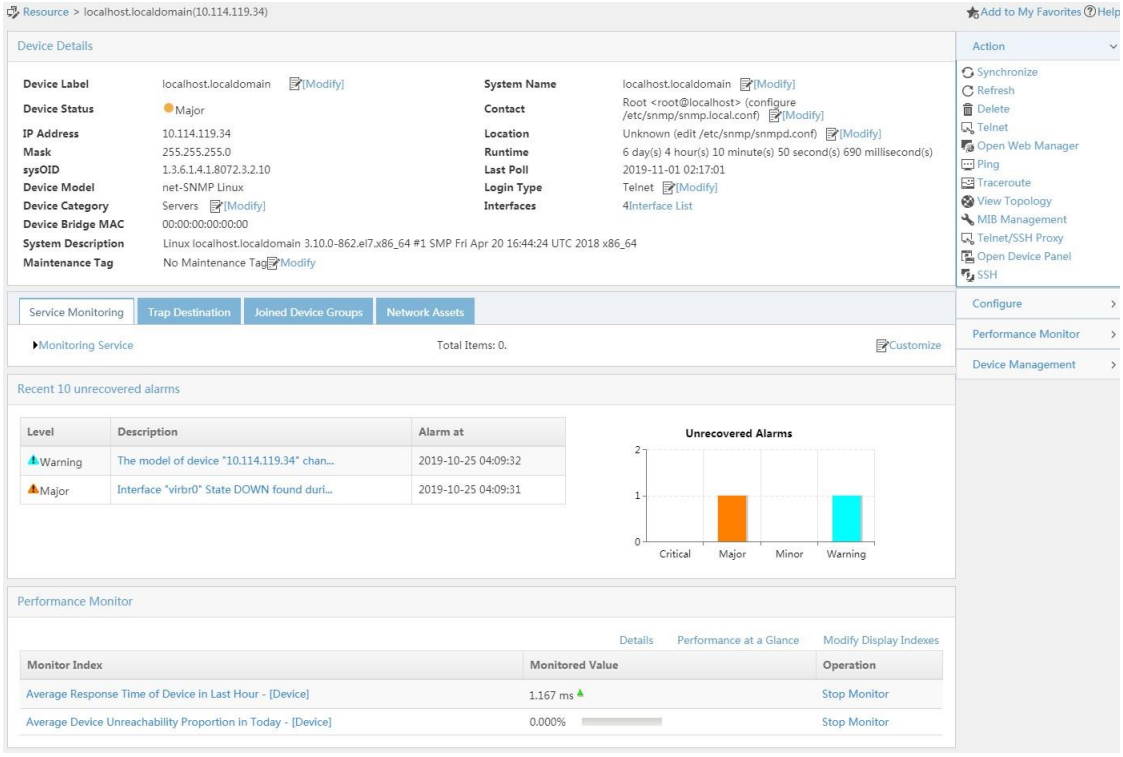
図21 トポロジーマップ内でのデバイスの検索



デバイスパフォーマンスデータおよびアラームクエリ

図20に示すように、ページ内のデバイスラベルリンクをクリックします。詳細ページが開きます。

図22 デバイスの詳細



デバイスアラーム情報の表示

アラーム情報は、リスト形式とチャート形式の両方で表示されます。

棒グラフのアラームリンクのタイプをクリックすると、**Alarm**タブに同じタイプのすべてのアラームが表示されます。

パフォーマンスモニターデータの表示

基本パフォーマンスデータがページの下部に表示されます。右上隅にある**Performance at a Glance**をクリックすると、デバイスのすべてのパフォーマンスモニターデータを表示できます。

デバイスの構成と管理

ページの右側にある操作メニューを使用して、個々のデバイスを設定および管理できます(たとえば、デバイス上でVLAN管理や構成管理を実行できます)。

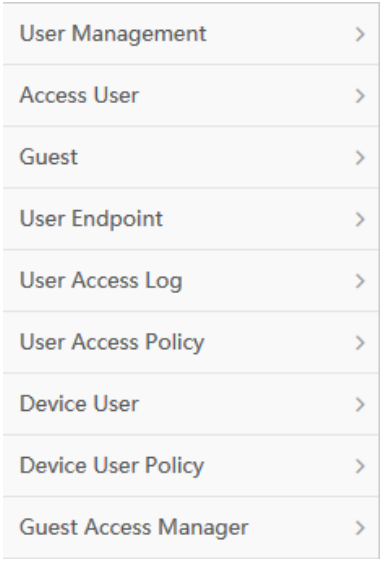
ユーザー管理

iMCでは、ユーザーはネットワークのエンドポイントユーザーおよびゲストです。

概要

ナビゲーションパスで、**user**タブをクリックします。図23に示すように、ユーザー管理ナビゲーションツリーが表示されます。**user**タブは、対応するユーザー管理サービスコンポーネント(EIAまたはEADisなど)がインストールされている場合にのみ使用できます。

図23 ユーザー管理に関連するナビゲーションツリー



ナビゲーションツリーの機能は、次のカテゴリに分類できます。

- **User account management** : ユーザー管理。
- User access management : アクセスユーザー、ユーザーアクセスポリシー、ユーザーアクセスログ、およびユーザーエンドポイント。
- **Access use security management** : ユーザーセキュリティポリシーおよびデスクトップアセットマネージャー。
- **Guest management** : GuestおよびGuest Access Manager。
- デバイスユーザー管理デバイスユーザーおよびデバイスユーザーポリシー。

User Managementおよび**Guest Access Manager**は、iMCプラットフォームがインストールされている場合に使用できます。

Access user、user access policy、user access log、user end point、guest、device user、および device user policyは、EIAがインストールされている場合に使用できます。

User security policyとdesktop asset managerは、EADがインストールされている場合に使用できます。

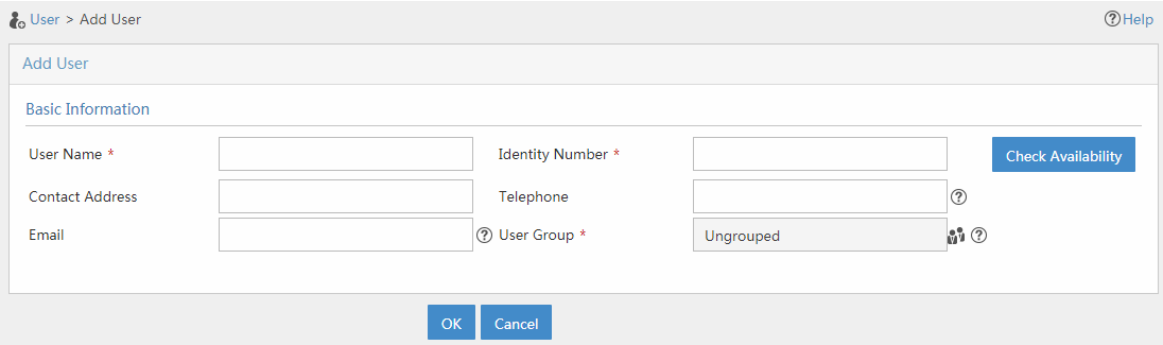
他のサービスコンポーネントがインストールされている場合は、これらのコンポーネントの機能ノードもナビゲーションツリーに表示されます。

iMCには、オペレーターとユーザーの役割があります。オペレーターとは、adminという名前のiMCオペレーターなど、iMCシステムにログインできるネットワーク管理者です。オペレーターは通常、会社のITスタッフメンバーです。ユーザーとは、ネットワークリソースにアクセスし、iMCによって管理されるユーザーです。

プラットフォームユーザー管理

iMCプラットフォームで構成されたユーザーはプラットフォームユーザーと呼ばれます。ユーザー管理を使用すると、プラットフォームユーザーの基本情報を管理できます。たとえば、ユーザーを追加する場合、図24に示すように、必須フィールドには**user name**、**identity number**および**user group**が含まれます。

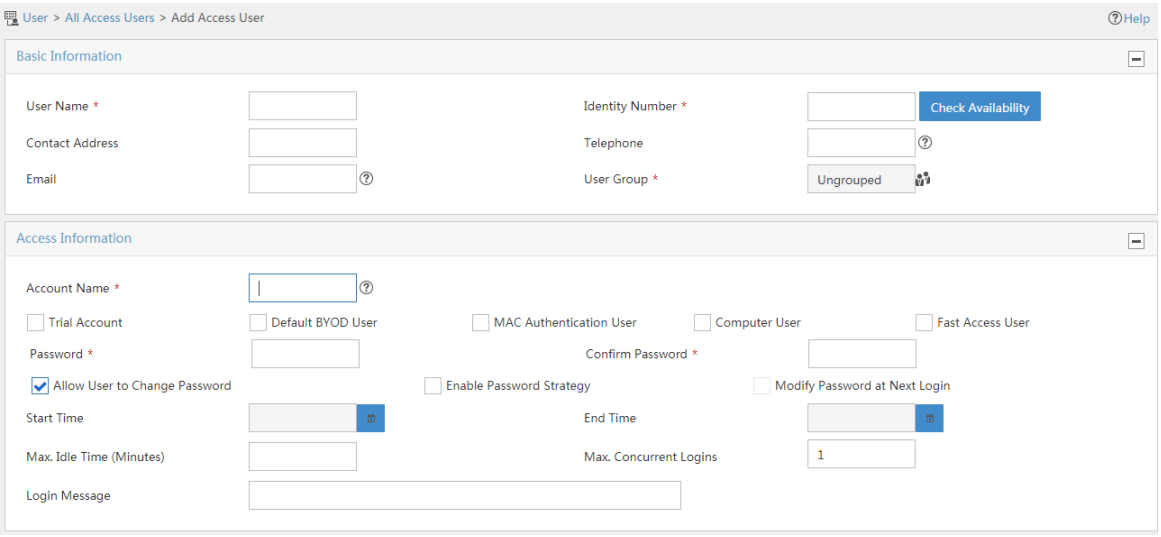
図24 ユーザーの追加



ユーザー管理へのアクセス

アクセスユーザー管理を使用すると、ユーザーアクセスを制御できます。アクセスユーザーアカウントは、認証、認可および会計用です。複数のアクセスユーザーアカウントを同じプラットフォームユーザーアカウントに関連付けることができます。たとえば、図25に示すように、アクセスユーザーを追加する場合、すべてのアクセスユーザーをプラットフォームユーザーに関連付ける必要があります。

図25 アクセスユーザーの追加



アクセスユーザーアカウントを作成した後、そのアカウントにサービスを割り当てる必要があります。サービスには、ユーザーがネットワークにアクセスするために満たす必要のある一連のアクセス要件が含まれています。

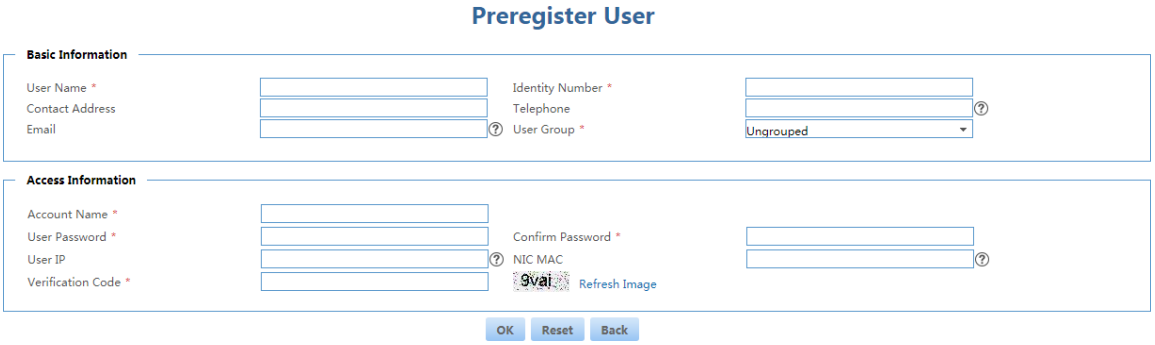
ネットワークセキュリティを強化するには、サービスにセキュリティポリシーを指定して、ユーザーがネットワークにアクセスするために満たす必要があるセキュリティ要素を定義します。

ゲスト管理

ゲストとは、ネットワークへの一時的なアクセスを必要とするエンドポイントユーザーを指し、通常は企業や組織への訪問者を指します。

ゲスト管理には、ゲストとゲストマネージャーの2つの役割があります。Self-Service Centerのログインページでは、図26に示すように、個人がゲストとして事前登録されます。その後、ゲストマネージャーがアクセス要求を監査します。

図26 ゲストの事前登録



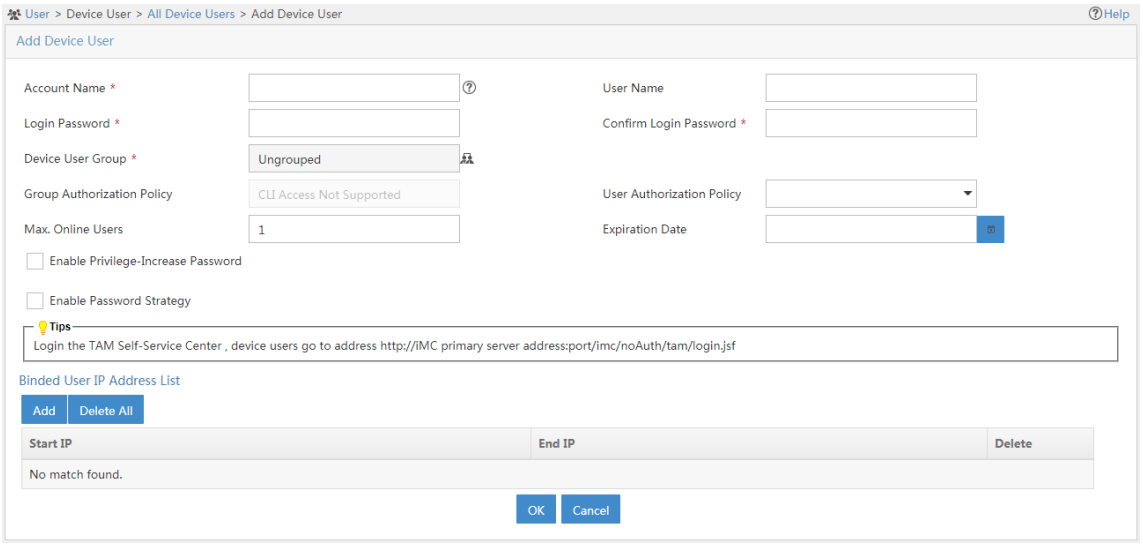
デバイスユーザー管理

オペレーターは、図27に示すように、集中管理のためにデバイスユーザーをiMCに追加できます。

iMCは、デバイスユーザーに対して次の管理機能を提供します。

- ユーザー情報のメンテナンス。
- ユーザー管理とユーザーグループ管理。
- ユーザーのオンライン監視。
- ブラックリスト管理。
- LDAPユーザー管理。
- 監査用のログ管理。

図27 デバイスユーザーの追加



サービス管理

iMCのモジュラー構造は、さまざまなサービスコンポーネントとネットワーク管理ソリューションを提供する、スケーラブルなネットワーク管理プラットフォームとして機能します。

iMCには、ACLM、GAM、ICC、VLANMなどのサービスモジュールが組み込まれてお

り、サービス要件を満たすために、さまざまなオプションサービスコンポーネントが用

意されています。

内蔵サービスモジュール

ACL管理

ACL Management(ACLM)は、iMCの**Enterprise** および**Standard Edition**に含まれています。ACLMは次の機能を実装しています。

- ACL定義。
- ACLの使用。
- パケットフィルタリング。
- 個々のデバイスの設定履歴。
- バッチ展開テンプレートを柔軟に使用して、複数デバイスのACL設定をわかりやすく説明したガイドです。
- 強力な導入メカニズムとすべての側面からのタスクビューにより、管理とタスクの導入が容易になります。

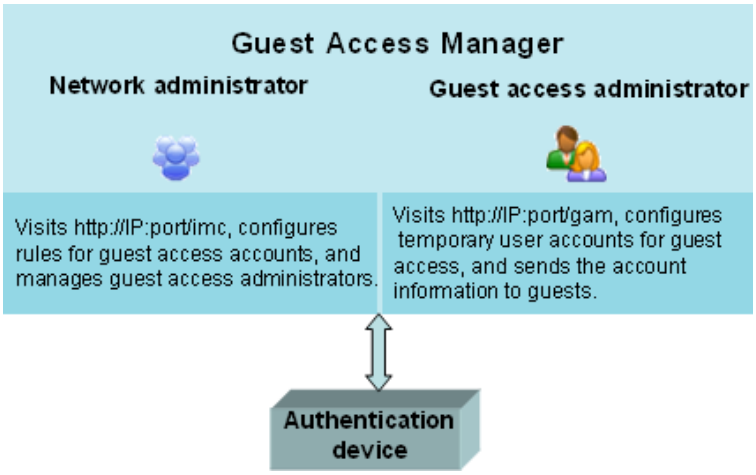
ACLMは基本的なネットワークリソースマネージャーです。このモジュールをインストールすると、ACLリソースオプションを関連するサービスコンフィギュレーションオプションに統合して、簡単なサービスコンフィギュレーションを提供できます。

ゲストアクセスマネージャー

Guest Access Manager(GAM)は、非ITスタッフが一時ユーザーアカウントを構成して、ネットワークへのゲストアクセスを提供できるようにするアプリケーションです。ネットワーク管理者による事前構成後は、非ITスタッフがゲストアカウント管理者として機能できます。

ゲストアカウント管理者は、GAMを使用して、ゲストユーザーアカウントを迅速かつ容易に作成し、アカウント情報をネットワーク内のアクセスデバイスに配布できます。ゲストアカウント管理者は、アクセデバイスの構成方法や管理方法を知っている必要はありません。図28は、GAMの概要を示しています。

図28 GAMの概要



インテリジェント構成センター

Intelligent Configuration Center(ICC)は、デバイス構成ファイルとソフトウェアバージョンを一元的に容易に管理できるように設計されています。これにより、構成ファイルのベースライン管理が可能になり、構成ファイルに加えられた変更を追跡できます。また、デバイスソフトウェアの以前のバージョンを格納して、履歴バージョンを迅速にリストアできるようになります。これらの機能により、デバイス管理が大幅に容易になり、ネットワークの保守性が向上します。

ICCには、構成テンプレートとデバイスソフトウェアライブラリも用意されており、リソースの再利用と容易なメンテナンスが可能です。

VLAN管理

VLAN Management(VLANM)は、iMCのEnterprise およびStandard Editionに含まれています。

VLAN技術は、LAN内のスイッチ間のブロードキャストを制限するために広く使用されています。ネットワークが拡大すると、多数のVLANを設定および管理することが問題になる場合があります。

VLANMを使用すると、VLANの設定の計画と展開、VLANトポロジーの表示、およびVLAN展開に関する情報の表示ができます。

サービスコンポーネント

アプリケーションマネージャー

アプリケーションマネージャー(APM)は、異機種ネットワークアプリケーションを監視します。ネットワークアプリケーションの継続的な監視を提供する一方で、APMは監視データを収集し、オペレーター用のレポートを生成してアプリケーションボトルネックを解決し、アプリケーションサービスの信頼性、可用性および継続性を確保します。表4に、監視できるアプリケーションのタイプをリストします。

表4 アプリケーションタイプ

アプリケーションクラス	アプリケーションの種類
Windowsサーバーモニター	• windows • パフォーマンスカウンタ

アプリケーションクラス	アプリケーションの種類
UNIXサーバーモニター	• AIX • FreeBSD • OpenBSD • Solaris • Mac OS • HP-UX
Linuxサーバーモニター	Linux
データベースサーバモニター	• SQL Server • MySQL • oracle • DB2 • データベースクエリー • sybase • PostgreSQL
アプリケーションサーバーモニター	• .NETサーバー • JBossサーバー • Tomcatサーバー • GlassFishサーバー • Oracle AS • WebLogicサーバー • WebSphereサーバー • Lync Server2010 • Jetty • Lotus Dominoサーバー
Webサーバーモニター	• Apacheサーバー • IISサーバー • PHP
メールサーバーモニター	• Exchange2003 • Exchange2007 • Exchange2010 • SMTP • pop3
ミドルウェア/ポータルモニター	• Office SharePoint • WebSphere MQ • ActiveMQ
Webサービスモニター	• RESTサービス • SOAPサービス
HTTPサービスモニター	URL
LDAPサービスモニター	• Active Directory • LDAP
ファイル/ディレクトリモニター	• ファイル • ディレクトリ
サービスモニター	• SNMPモニター • FTPモニター • SFTPモニター • DNSモニター • Javaランタイム • TCPポート

アプリケーションクラス	アプリケーションの種類
SAPモニター	SAP
仮想デバイスモニター	• Hyper-V • KVM • VMware ESXi

ブランチインテリジェントマネジメントシステム

Branch Intelligent Management System(BIMS)には、BIMSプラットフォームとAuto Configuration Server(ACS)が含まれています。BIMSはTR-069プロトコルを使用して、WAN内の多数のCustomer Premise Equipment(CPE)プロトコルを使用します。NATの背後にある動的IPアドレスとデバイスを管理し、ネットワークメンテナンスのコストを削減し、ネットワーク管理の効率を向上させます。BIMSは、CPEのリソース管理、サービス管理、構成管理、アラーム管理、レポート管理、およびシステム管理を提供し、サービスプロバイダーネットワーク内のCPEのさまざまな管理要件を満たすことができます。

ビジネスサービスマネージャー

Business Service Manager(BSM)は、エンタープライズネットワーク上のITサービスの長期的な監視および保守を実行できます。通常、ネットワーク、サーバーおよびミドルウェアは、サービスの実行安定性に関連しています。BMSは、ネットワーク、サーバーおよびミドルウェアのリアルタイム監視を統合し、収集されたデータを分析します。次に、BSMはサービスの実行品質を分析し、リアルタイム実行ステータスおよびしきい値アラームをサービスの可用性、健全性およびビジー性の観点で表示します。これにより、ITマネージャーは、サービスの実行ステータスを時間的に把握できます。

BSMには次の機能があります。

- **Service monitoring**：サービスを定義できます。サービスに関連付けられたネットワークデバイス、アプリケーションアプリケーションおよびホストを構成し、サービスの可用性、健全性およびビジー性のしきい値を構成できます。
- **Service Data window**：サービスカード、サービスクリスタル、タイムラインベースのサービス分析レポート、サービストポロジーなど、さまざまな形式ですべてのサービスの実行ステータスを表示します。
- **End-to-end service topology**：サービスにアクセスするエンドポイントとサービスサーバー間のネットワークトポロジーを表示できます。送信元および宛先IPアドレスを入力すると、BSMは2つのパスが通るネットワークトポロジーを描画します。
- **Maintenance plan** ：エンタープライズのホスト、サービスおよびネットワークデバイスのメンテナンスタイムプランを定義できます。メンテナンスタイムプランに含まれるサービスの一時停止は、サービスの可用性および健全性の計算に影響しません。

EADセキュリティポリシー

EADは、エンドポイントの防御機能を強化し、ネットワークアクセスを制御し、ネットワークセキュリティを確保するために、エンタープライズセキュリティポリシーをエンドポイントに適用します。EADソリューションのコアとして、EADセキュリティポリシーコンポーネントには、Endpoint Admission Defense(EAD)サービスモジュールおよびDesktop Asset Manager(DAM)サービスモジュールが含まれます。

- EADサービスモジュールは、次のことを行います。
    - アンチウイルスソフトウェア、オペレーティングシステムパッチ、Windowsレジストリエントリ、ネットワークトラフィックなどの一連のセキュリティ項目を調べて、エンドポイントのセキュリティステータスを判別します。

- ネットワークセキュリティを保護するために、セキュリティ保護されていないユーザーを隔離またはログオフします。
- 階層管理機能とレポート機能を提供します。

- DAMサービスモジュールには次の機能があります。
  - Windowsを実行するPCおよびサーバーを含むデスクトップ資産を管理および監視します。
  - iNodeクライアントを介して資産情報を収集し、この情報を監査のためにオペレーターに報告します。
  - ソフトウェアの展開およびレポート機能を提供します。

エンドポイントインテリジェントアクセス

ユーザー管理へのアクセス

ネットワークセキュリティおよびアクセスユーザーの効果的な管理のために、ユーザーアクセスマネージャー製品をイントラネットに配置する必要があります。ただし、市場に出ているこれらの製品のほとんどは、アクセス管理とネットワークリソース管理およびサービス管理を統合していません。その結果、次のような欠点があります。

- 管理の制限
- 不十分な管理
- 運用の複雑さ

これらの欠点により、サービスの展開、実装、および管理がより困難になり、展開の効率が低下します。IMCS EIAを展開することで、この問題を解決できます。次の機能があります。

- ユーザー管理へのアクセス
- ゲスト管理
- エンドポイント管理
- ユーザーアクセスログ管理
- アクセスポリシー管理

これらの機能により、EIAはさまざまなタイプのアクセスユーザーを一元管理し、有線ネットワークと無線ネットワークの両方の要件を満たすために、柔軟なユーザー認証とアクセス制御を実装します。

TACACS+ 認証管理

ネットワークデバイスメンテナーを集中管理するために、H3CではTACACS+ Authentication Manager(TAM)が提供されています。TAMはiMCプラットフォームに基づいて動作し、ネットワークデバイスメンテナーの認証、承認およびアカウンティングを提供します。TAMはiMCプラットフォームおよび他のコンポーネントとは別に導入して、システム容量を節約し、パフォーマンスを向上させることができます。

TAMは以下の機能をサポートしています。

- **Multiple device categorizing methods**：管理ドメインまたはデバイスタイプに基づいて分類できます。
- **Flexible user-defined authorization policies**：1つの認可ポリシーに対して複数のルールを定義できます。各ルールは、デバイス領域、デバイスタイプおよび認可された時間範囲などの認可シナリオに基づいて、デバイスユーザーに異なるシェルプロファイルおよびコマンドセットを割り当てることができます。
- **User group management**：オペレーターは、グループ内のユーザーを管理して、管理効率を向上させることができます。
- **LDAP user authentication**：TAMは、ユーザー認証用のLDAPサーバーと連動したり、認証用のLDAPサーバーからのユーザー情報を同期したりすることができます。

- **Integrated device user operation monitoring** : TAMはデバイスユーザーの認証、許可、およびコマンド実行操作を監視し、オペレーターによるデバイスユーザーの追跡と監査を容易にします。

エンドポイントモバイルオフィス

Endpoint Mobile Office(EMO)では、モバイルエンドポイントを使用してWindowsアプリケーションおよびデスクトップをリモートで開いたり、アプリケーションストア内のローカルリソースを使用して通信したり、エンドポイントを保護したりできます。

EMOには次のような特徴があります。

- アクセスユーザーをドメインユーザにマッピングします。
- リモートリソースへのアクセスをユーザーに許可します。
- モバイルユーザーのリモートオフィスをサポートします。
- 分散配置をサポートします。
- ユーザーアクセス許可を制御してネットワークを保護します。

EoCマネージャー

Ethernet over Coax(EoC)ネットワークは、アップリンクとCATV信号を介してデータ信号を送信し、ダウンリンクを介してデータ信号を送信します。これにより、CATV信号とデータ信号を同軸ケーブルで混在させて送信でき、双方向デジタルTVプラットフォームへのリターン伝送パスが提供されます。

EoC Manager(EoCM)は,複雑に分散した多数のCLTおよびシヌゥデバイスをEoCアクセスネットワークおよびEoCアクセスネットワーク全体で効率的に管理できます。

EoCMには次のような利点があります。

- 強力かつ柔軟なバッチ導入

  管理者がEoCデバイスに対してバッチ操作を実行できるようにします。これにより、作業負荷が軽減され、作業効率が向上します。
- 直感的なトポロジー監視

  CLTとシヌゥ間の論理関係と、CLT、CNU、およびリンクの実行ステータスを明確に表示します。同時に、管理者はトポロジー上のデバイスに対する操作を実行できます。
- グラフィカルインターフェイス

  EoCサービスを便利かつ安全に展開および監視するためのコマンドラインを必要としない、使いやすいグラフィカルな構成インターフェイスを提供します。
- 同軸ケーブルの簡単な変更

  既存の同軸ケーブルで大規模展開が可能で、使いやすさに優れています。

EPONマネージャー

EPONは、コスト効率に優れたポイントツーマルチポイント構造とパッシブファイバ伝送により、エンドユーザーを接続するための効果的な手段を提供し、最後の1マイルにおける帯域幅のボトルネックを解決します。さらに、10Gbpsイーサネットバックボーンとメトロリングを配置することにより、EPONは光ネットワークにとって最良の最後の1マイルのソリューションとなります。

EPONマネージャー(EPM)は、キャリアネットワーク内のEPONデバイスを管理するために使用されます。EPON構成をアクセスデバイスに配置するのに役立ち、手動操作はほとんど必要ありません。EPONマネージャーは、OLTとONUの接続を明示的に示す配置、アップグレードおよびトポロジー表示などの機能を提供します。これは、ネットワーク計画の参照を提供します。

IPSec VPNマネージャー

IP Sec VPN Manager(IVM)は、IPSec VPN設定の統合管理を提供します。ネットワークドメイン、IPSecデバイス設定、およびセキュリティプロポーザルテンプレートを管理するために設計されています。

IVMには、IPSec VPN、GRE over IPSecおよびDVPNのネットワークドメイン管理機能が用意されており、IPSecデバイスを同じネットワークドメインに追加して、統一された構成管理を行うことができます。ネットワークメンテナンスを容易にするために、IVMでは、バッチ導入操作、IPSecトンネルのティアダウン、およびトポロジーの表示を実行できます。さらに、NATの背後に配置され、動的IPアドレスを使用するスポークデバイスを管理するために、BIMSと連携できます。

ITサービスマネージャー

ITSM(IT Service Manager)は、ITサービスのライフサイクル全体を管理するためのITILベースのソリューションです。ITSMは、統合された、合理的で順序付けられた効率的なプロセスセットを提供し、IT部門がITサービスを体系的に実装するのを支援します。

フロー管理機能により、ITSMはすべてのIT運用およびメンテナンス活動を制御可能、測定可能、監査可能にすることができます。

ITSMはiMCプラットフォームのネットワーク構成管理機能と連携し,各種基本構成項目を組み合わせることにより,ユーザーにITネットワークの運用と保守のための構成管理環境を提供することができる。

MPLS VPN Manager

MPLS VPN Manager(MVM)は、統合されたリソース管理および再統合サービスプロセスを提供し、サービス指向アーキテクチャを使用します。MVMは、次のサービス管理機能を提供します。

- **BGP MPLS VPN**：レイヤ3VPNネットワークを管理します。これには、PEやCEなどのデバイスリソースの管理、MPLS VPNトポロジーのモニタリング、ネットワークの展開が含まれます。
- **L2VPN**：MPLSベースのVPLSネットワーク、VLLネットワーク、リンクレイヤベースのPBBネットワークなど、レイヤ2ネットワークを管理します。
- **MPLS TE**：ネットワーク内のTEデバイスの集中管理プラットフォームを提供します。これにより、TEデバイス情報、FRRポーリングタイマー、自動帯域幅調整、およびCR-LSPタイブレーク方式の集中表示および設定が可能になります。

ネットワークトラフィックアナライザ

Network Traffic Analyzer(NTA)は、帯域幅の使用者、ユーザーが帯域幅の使用を開始した時刻、ユーザーが帯域幅を使用した時間、トラフィックフローの開始者およびトラフィックルーティングに関する情報を提供することにより、エンタープライズネットワークの帯域幅使用を監視します。NTAは、トラフィック、アプリケーションおよびセッションに基づいたレポートを提供し、ネットワークトラフィックのベースラインおよびトレンドを示します。この情報は、ネットワーク障害の迅速な診断および帯域幅ボトルネックの解決に役立ちます。

NTAには、障害およびSLA分析などの詳細なルールベースおよびポリシーベースの分析が用意されており、ネットワークのステータスを直感的に把握したり、障害を迅速に特定したりするのに役立ちます。この分析は、ネットワーク最適化、ネットワークデバイス投資に関する意思決定および帯域幅最適化の参照として使用できます。また、異常なトラフィック検出、一元化されたセキュリティイベント管理、およびリソース管理プラットフォームとの相互作用により、セキュリティの脅威を正確かつ迅速に識別して対応できます。

QoSマネージャー

QoSマネージャー(QoSM)は、ネットワークデバイス上のQoS設定を管理して、ネットワーク全体のサービス品質を制御および管理します。

QoSMを使用すると、さまざまな分類子、動作、およびポリシーを設定し、デバイスインターフェイスまたはVLANにポリシーをバインドして、QoS展開計画を作成できます。

QoS導入プランは、QoSMとデバイス間の相互作用の基本単位です。QoSMは、QoS導入プランをデバイスに導入して、デバイスのQoS構成を変更できます。また、既存のデバイスのQoS設定をQoS展開計画として保存して、将来の設定、アップグレード、およびメンテナンスを管理します。

ステップバイステップの手順に従って、複雑なQoSM設定を行います。同時に、QoSMは、統一された構成管理インターフェイスを使用することにより、異なるデバイス上のコマンドラインと設定ロジックの不整合を無視します。これにより、オペレーターの作業負荷が軽減され、ネットワークリソースの計画が簡素化されます。

リソース自動化マネージャー

リソース自動化マネージャー(RAM)は、ユーザーのネットワークサービスをカスタマイズしたり、ネットワークサービスを自動的に導入したりするために使用されます。

基本的なネットワーク機能には、MSTP、VLAN、OSPF、RIP、VRRP、ACL、およびQoSがあります。

セキュリティサービスマネージャー

Security Service Manager(SSM)は、集中型ネットワークセキュリティ管理用のiMCコンポーネントです。任意のネットワークで使用でき、さまざまなベンダーのデバイスをサポートしています。

SSMは、ネットワーク上のファイアウォールデバイスをリアルタイムで監視し、セキュリティイベントとログを収集して分析し、リアルタイムのネットワークセキュリティ情報とグラフおよびリストの傾向を提供します。また、SSMを使用すると、ファイアウォールデバイスにセキュリティポリシーを展開できます。

SSMには次の機能があります。

- セキュリティトポロジー
- セキュリティイベント管理
- グローバルリソース管理
- ファイアウォールサービスの設定

SSMには、Load Balancing Manager(LBM)と呼ばれるサブコンポーネントがあります。これにより、LBデバイス上のロードバランシングサービスを管理および設定したり、ロードバランシングパフォーマンス統計情報を表示したりできます。

LBMは、仮想サービスを介して実サーバーおよびサーバーファームのロードバランシングを実装します。LBMは、すべての設定をLBデバイスに展開します。

アプリケーションテンプレートにより、LBサービス構成の再利用性が向上します。LBデバイス、仮想サービス、実サーバーおよびサーバーファームのパフォーマンス統計は、LBサービスのステータスおよびパフォーマンスを示しています。

LBMには次の機能があります。

- クイックスタート
- リソース管理
- パフォーマンス管理

- サービス管理
- 構成テンプレート
- グローバルパラメーター

サービスヘルスマネージャー

Service Health Manager(SHM)は、視覚的なサービス品質管理機能を提供します。SHMは、アラーム、パフォーマンス、NTAおよびNQAデータを統合し、KQIおよびSLAを使用してサービスヘルスを監視、測定および視覚的に管理します。SHMには、SLA統計および評価結果をダイアグラムおよび表に視覚的に表示するレポートが用意されているため、全体的なサービスレベルを理解し、潜在的な問題を迅速に検出できます。

サービスオペレーションマネージャー

Service Operation Manager(SOM)は、企業のITネットワークの運用と保守を支援するもので、ITILライフサイクルにおける主要なサービス切り替えと運用部分、およびITネットワーク運用と保守に関連するフローのサポートに焦点を当てています。

フロー管理機能により、SOMはすべてのIT運用とメンテナンス活動(例えば、構成変更とトラブルシューティング)を制御可能、測定可能、監査可能にします。

SOMは、統合されたCMDB、カスタムフローフレームワークおよびセルフサービスフレームワークによって提供される自動化された操作および保守機能に基づいて、資産、構成、変更、要求/イベント/障害、トラブルシューティング、およびITILサービス操作および保守のナレッジベースを管理します。また、ITネットワークサービスの統合管理ポータルとしてService Deskも提供します。

Unified Communications Health Manager

Unified Communications Health Manager(UCSM)は、Microsoft Lync Serverとともに導入されたネットワークの稼働状態を監視するためのソリューションです。Lyncサーバー、公衆網ゲートウェイ、Lyncクライアントエンドポイントなどのネットワークリソースを管理できます。

UCSMは自動検出機能をサポートしています。この機能では、Topology Builderの設定ファイルを使用してネットワークを検索し、検出されたすべてのLyncサーバーと一公衆網ゲートウェイをUCSMに追加します。この機能により、デバイスを手動でインポートする必要がなくなり、インポートエラーが発生しなくなります。

ユーザー動作の監査

User Behavior Auditor(UBA)は、オペレーターがネットワークアクセス情報(送信者johndoe@hpe.comに対応する受信者など)を表示して問題を特定できるようにする、シンプルで効率的なログ監査ツールです。

UBAは、高度なNetStreamおよびプローブテクノロジーを使用しているため、導入に必要な時間と帯域幅がほとんどないため、ハイパフォーマンスソリューションとなります。

UBAでは、膨大な量の複雑なログデータをフィルタリングし、その情報を簡略化した形式で表示することで、ネットワーク全体の状態を監視し、ネットワークの問題を迅速に発見して特定し、ネットワークリソースを計画することができます。これにより、ネットワークの品質と安定性が向上します。

VAN接続マネージャー

VAN Connection Manager(VCM)は、VM移行のために物理ネットワークと仮想ネットワーク間の通信を保証します。

VCMは、VMの開始、停止、および移行プロセスをトレースすることによって、VMがアクセスする新しい物理ネットワークを決定します。VMが新しい物理ネットワークに移行する前に、物理ネットワーク構成の移行を完了します。これにより、物理ネットワーク構成がVMとともに移行されます。

VANファブリックマネージャー

VAN Fabric Manager(VFM)は、iMCプラットフォームに基づくデータセンター管理ソフトウェアです。VANは、仮想化、自動化、およびソフトウェア定義のネットワークテクノロジを使用します。ファブリックは、FCoEスイッチ、サーバー、およびストレージデバイスで構成されるネットワークです。

VFMは、HPEおよびH3Cデバイスを使用して、データセンターのLANとSANの両方を管理するための統合ソリューションを提供することを目的としています。VFMは、仮想マシンの移行情報を取得するためにVNMに依存しています。

VFMには次の機能があります。

- 概要(At a Glance)。
- VANファブリックトポロジー。
- DC管理。
- SAN構成。
- LAN構成。
- 統計情報。

VAN SDNマネージャー

VAN SDN Manager(SDNM)は、OpenFlowベースのSDNを管理するためのiMCサービスコンポーネントです。

SDNMでは、RESTful APIを使用してOpenFlowネットワークを管理できます。iMCベースプラットフォームのデバイス管理、レポート、およびホームページウィジェットと組み合わせると、SDNMではOpenFlowネットワーク上で視覚的な管理と監視を行うことができます。

音声サービスマネージャー

Voice Service Manager(VSM)は、企業レベルの音声ネットワーク用に設計されています。VSMはiMCプラットフォームと連携することにより、音声ネットワークのメンテナンスコストを削減し、メンテナンス効率を向上させます。VSMには次の機能があります。

- 音声デバイスの動作を監視します。
- デバイスタイプ別に音声デバイスを管理します。デバイスタイプには、VCX、NBX、ゲートウェイ、およびIP電話があります。
- IP電話のエンドツーエンドのトラブルシューティングを提供します。
- IP Phoneのコール履歴を表示し、電話番号グループを管理します。
- 音声サービスデータレポートを生成します。

ワイヤレスサービスマネージャー

Wireless Service Manager(WSM)は、統一された有線および無線ネットワーク管理を実装するためのWLAN管理機能を提供します。これにより、H3C、HPE(MSMシリーズ)、Aruba、Ciscoなどのさまざまなベンダーの AC、Fat AP、およびFit APを一元管理できます。また、クライアント検出、構成、監視などのクライアント管理機能も提供します。

WSMでは、次の操作を実行できます。

- WLANを設定および展開します。
- ワイヤレスデバイスの動作と使用を監視します。
- ローミングドメイン、フロア、またはカテゴリ別にデバイスを管理します。
- デバイスのステータス、位置、およびAPの接続を表示します。

よくある質問

Webブラウザーを使用してiMCおよびソリューションにアクセスすると、どのような問題が発生する可能性がありますか?

表5に、発生する可能性のある問題の解決策を示します。

表5 問題と解決策

課題	解決策
操作によっては、Webページまたはシステムデータのエラーが発生する場合があります。	次のことは避けてください。 1. ブラウザーの進むまたは戻るボタンを使用してページを切り替える。 2. IE、Firefox、またはChromeで File > New windowを選択して新しいウィンドウを開く。 3. 2つのFirefoxまたはChromeウィンドウを同時に開いて、iMCとともにインストールされている同じサーバーにアクセスします。 4. テキストボックスに入力した文字数が多すぎます。 5. ブラウザーの**Stop**アイコンをクリックすると、ページに進行状況バーが表示されます。その後は、ブラウザーのRefreshアイコンをクリックしてシステムのホームページに戻るまで、操作を続行できません。 6. 短期間に、ブラウザー内のオブジェクト(ボタン、リンク、メニューなど)を頻繁にクリックする。
iMCのアップグレード後、ブラウザーiMCページが正しく表示されない。	ブラウザーが古いバージョンのiMCページをキャッシュした場合、次のエラーが発生する可能性があります。 • ブラウザーにスクリプトエラーメッセージが表示される。 • ページ上のリンクが無効になります。 • ページ上の要素を正しく表示できません。 この問題を解決するには、ブラウザーのキャッシュをクリアしてブラウザーを再起動します。
新しくインストールされたWindowsオペレーティングシステム(2003、2008、2008R2、2012、または2012R2)のIEからiMCにログインできない。	これは、新しくインストールされたWindowsオペレーティングシステムのIEがデフォルトで高いセキュリティレベルに設定されているためです。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: 1. セキュリティレベルを**Medium**に設定します。 ○ IEを起動し、**Tools > Internet Options**を選択します。 ○ **Security**タブを選択し、**Internet**をクリックします。 ○ セキュリティレベルを**Medium**に設定します。 2. iMCシステムのWebサイトを信頼済みサイトに追加します。 ○ IEを起動し、**Tools > Internet Options**を選択します。 ○ securityタブ、**Trusted site**の順に選択し、**Sites**をクリックします。 ○ iMCシステムのWebサイトを追加します。

Firefox経由でiMCにログインした後、iMCにはセキュリティ上の問題があります。オペレーターがブラウザーで次の操作を実行すると、ユーザー情報を入力せずにiMCにログインできます。**Go back one page**をクリックしてログインページに戻り、**Go forward one page**をクリックします。	セキュリティ上の理由から、右上隅にあるLogoutをクリックするか、Webブラウザーを閉じてiMCシステムを終了してください。
Firefoxでサイズが数バイトしかない小さなファイルをアップロードすると、アップロードが失敗する。	このような障害が発生した場合は、IEを介してファイルをアップロードするか、別のクライアントを使用してファイルをアップロードできます。
単一デバイス用にACLを設定する場合Firefoxでは、タブは2行で表示されます。	これは、Firefox固有の制限と関数の使用には影響しません。これを回避する場合は、代わりにIEを使用できます。
Firefoxを介してオペレーターを追加すると、ログインユーザ名とパスワードがページに表示されます。	iMCログインパスワードがFirefoxによって保存されています。この問題を回避するには、iMCにログインするときに**Never for This site**または**Not now**をクリックするか、保存されているパスワードをクリアします
iMCシステムにログインした後、ブラウザーの履歴にあるiMCのWebページにアクセスしようとすると、アクセスが拒否されたり、アラームボードが消えたり、トポロジーが開かないなどの問題が発生します。	これらの問題を回避するには、次の操作を実行します。 **1.** ブラウザーのアドレスバーにページのURLを入力するのではなく、iMCナビゲーションツリーからiMCページにアクセスします。 ブラウザーで履歴レコードを保持できないようにすることをお勧めします。これを行うには、**Tools > Internet options**を選択し、History領域の**the Days to keep pages in history**テキストボックスに**0**と入力します。
私がIEで印刷したウェブページには、背景色も画像もありません。	IEで次の操作を実行します。 **1.** **Tools > Internet Options**を選択します。 **2.** **Advanced**タブを選択します。 **3.** **Printing**の下の**Print background colors and images**チェックボックスをオンにします。
ネットワーク管理にIEを使用する場合、Waitingメッセージボックスに進行状況が表示されません。	これはIE固有の制限が原因であり、関数の使用には影響しません。FirefoxやChromeではプログレスバーが正しく表示されます。
ポップアップウィンドウをブロックすると、スクリプトエラーメッセージが表示されます。	一部のiMC構成インターフェイスは、ポップアップウィンドウに表示されます。ポップアップウィンドウを許可するようにブラウザーを構成することをお薦めします。
IMCヒントは、IEでは数秒間だけ表示されます。	これは、IE固有の制限が原因です。iMCヒントがトリガーされた後もオンのままであるFirefoxまたはChromeを使用できます。

注:

上記の状況を除き、ブラウザーのプラグイン設定をチェックして、iMCが正常に動作することを確認してください。

iMCインターフェイスは応答せず、ログインページまたはその他のスクリプトエラーを表示します。どうすればいいですか?

次のように問題をトラブルシューティングします。

- IEブラウザーを再起動し、同じページにアクセスします。
- IEブラウザーの最新のパッチをインストールします。

  iMCサイトをIEブラウザーの信頼済みサイトに追加します。
- 別のPCから同じページにアクセスします。

上記のいずれでも問題が解決しない場合は、テクニカルサポートに連絡してください。

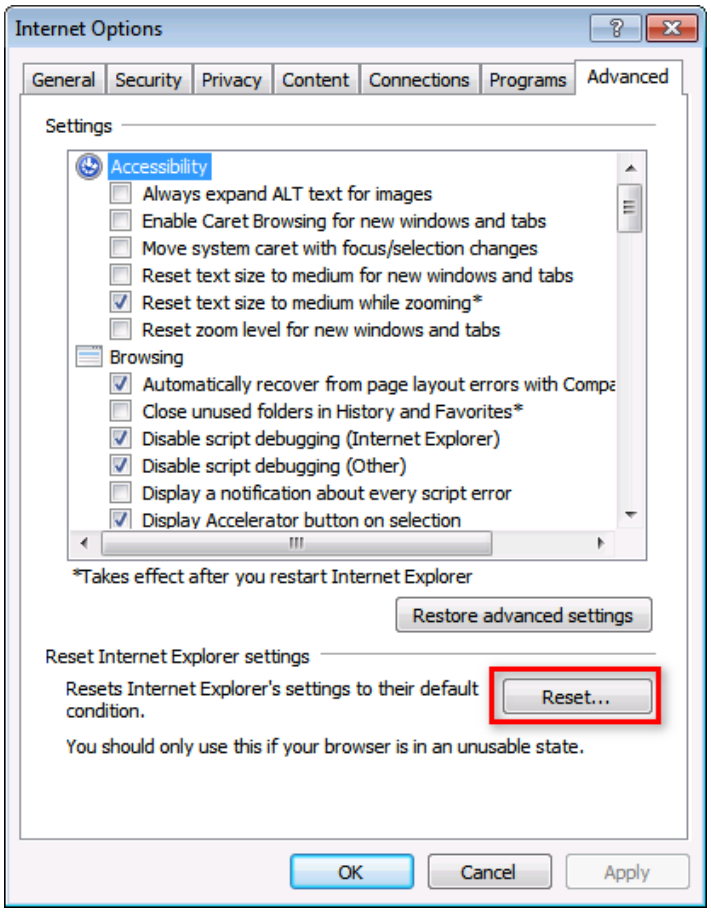
OSにログインする際の注意点は何ですか?

iMCを正常にインストールして実行するには、管理者アカウントを使用してオペレーティングシステムにログインすることをお勧めします。

IEからiMCにアクセスすると、iMCホームページが表示されないのですが、どうしたらいいですか?

1. IEを開き、**Tools > Internet Options**を選択してinternet propertiesウィンドウを開きます。
2. 図29に示すように、**Advanced**タブをクリックし、**reset**をクリックします。

図29 Advancedタブ



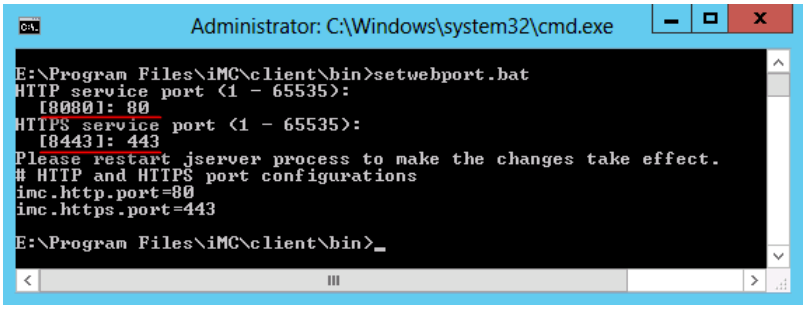
iMCのインストールが完了した後で、iMCとともにインストールされたサーバーのWebサービスポート番号を変更する方法は?

setwebportツールを使用して、iMC Webサービスポート番号を変更します。

iMCサービスポート番号を変更するには、次のようにします。

1. Windowsの場合は、iMCインストールパスで\client\bin\setwebport.batを実行します。
   Linuxでは、iMCインストールパスで/client/bin/setwebport.shを実行しま
   す。この例では、Windowsを使用しています。
2. 図30に示すように、HTTPポート番号を8080から80に、HTTPSポート番号を8443から443に変更します。

図30 setwebport.batツールの実行結果



3. **jserver**プロセスを再起動します。
4. iMCが分散モードで配置されている場合は、iMCとともにインストールされているすべてのサーバー上で上記の手順を繰り返します。
5. EIAモジュールがインストールされている場合は、iMCサービスポート番号を新しいHTTPポート番号に変更します。そうしないと、ゲストマネージャーは事前登録されたゲストを正式に登録できません。

   iMCサービスポート番号を変更するには、次の手順を実行します。

   a. トップナビゲーションバーの**User**タブをクリックし、**User Access Policy Manager > service parameters** を選択します。
      Service parametersページが開きます。
   b. **System config**リンクをクリックします。System configページが表示されます。
   c. **System Parameters**の**Configure**アイコンをクリックし、図31に示すように、iMCサービスポート番号として**80**を入力します。
   d. **OK**をクリックします。

図31 iMCサービスポート番号の変更

デバイスにTelnet接続すると、ポップアップダイアログボックスが自動的に閉じます。どうすればいいですか?

Telnetコマンドはローカルで実行されるため、ローカルOSのセキュリティ設定の影響を受ける可能性があります。IEまたはFirefoxのデフォルト設定を復元する必要があります。デフォルト設定を復元する手順の

詳細は、iMCプラットフォームのヘルプを参照してください。

スーパー管理者adminのログインパスワードを変更するにはどうすればよいですか?

スーパー管理者adminとしてiMCシステムにログインし、次の操作を実行します。

1. **System**タブをクリックします。
2. **Operator management**ナビゲーションツリーで、**Modify password**を選択します。
3. 古いパスワードと新しいパスワードを入力し、新しいパスワードを確認します。
4. **OK**をクリックします。

パフォーマンスビューを追加すると、パフォーマンス管理権限のない一部のユーザーグループにアクセス権が付与されます。なぜですか?

これはiMCの適切な管理設計に準拠しており、通常の運用には影響しません。オペレーター権限には次のものがあります。

- 機能権限(ナビゲーションメニューの操作など)。
- リソース権限(オペレーティングデバイスやユーザーなど)。
- データ権限(オペレーティングカスタムビュー、パフォーマンビュー、レポートなど)。

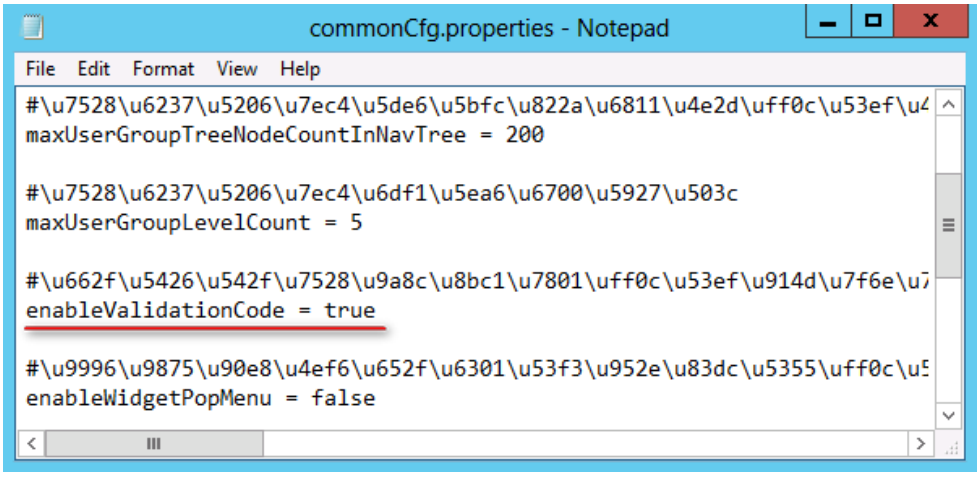
関数権限の優先順位が最も高くなります。iMCは、同じ関数権限を持つ演算子をリソース権限およびデータ権限でフィルタします。

iMCログインの検証コード機能を有効にするにはどうすればよいですか。

デフォルトでは、iMCログインの検証コード機能は無効になっています。この機能を有効にするには、次のタスクを実行します。

1. テキストエディタを使用して、iMC設定ファイル**commonCfg.properties**を開きます。
   - Windowsでは、このファイルはiMCインストールパスの\client\confディレクトリにあります。
   - Linuxの場合、ファイルはiMCインストールパスの/client/confディレクトリにあります。この例では、Windowsを使用しています。
2. **enableValidationCode**フィールドの値を**true**に変更して、ファイルを保存します。

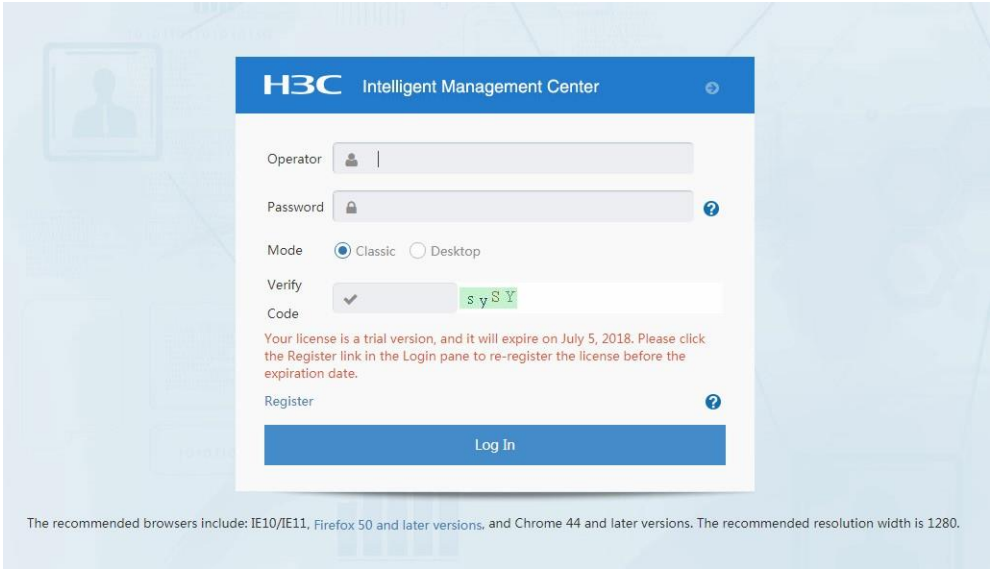
   図32 commonCfg.properties構成ファイルの変更



3. iMCを再起動し、iMC Loginページを開きます。

   図33に示すように、**Verify Code**機能が有効になっています。

図33 検証コード機能の有効化



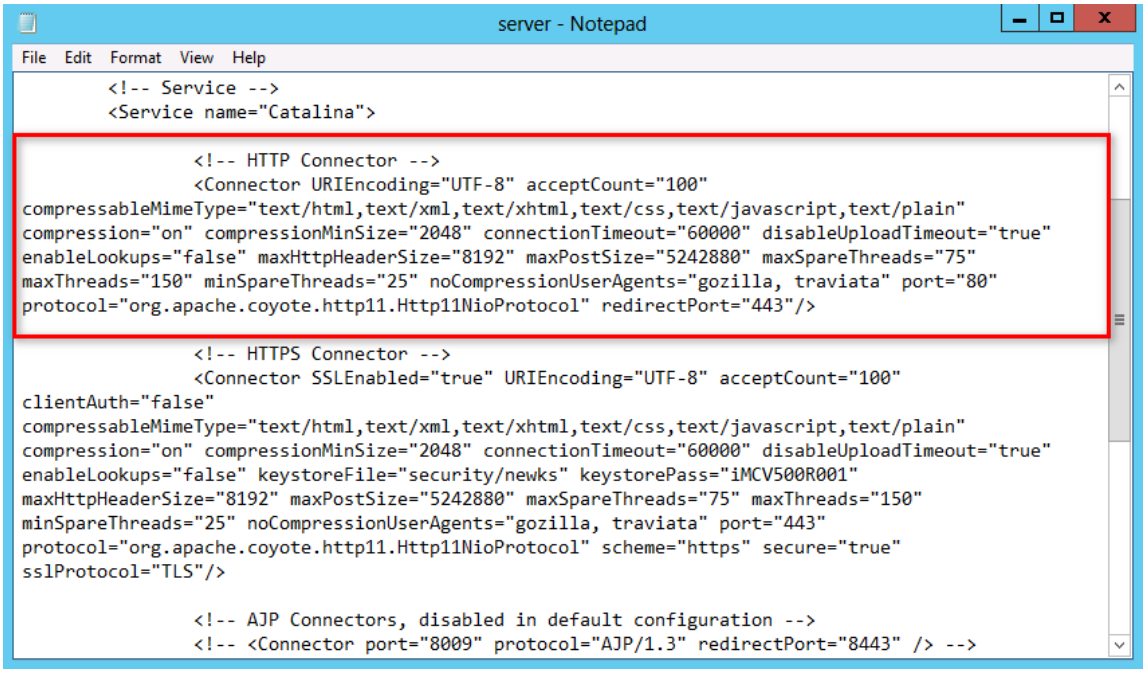
HTTPSだけを介してアクセスするようにiMCを設定するにはどうすればよいですか。

デフォルトでは、iMCはHTTPおよびHTTPSを介してアクセスできます。

HTTPSだけを介してアクセスされるようにiMCを設定するには、次の作業を実行します。

1. テキストエディタを使用して、IMC設定ファイル**server.xml**を開きます。
   - Windowsでは、このファイルはiMCインストールパスの\client\confディレクトリにあります。
   - Linuxの場合、ファイルはiMCインストールパスの/client/confディレクトリにあります。この例では、Windowsを使用しています。
2. 図34に示す赤いボックス内のテキストを削除またはコメントアウトします。
3. iMCを再起動します。

図34 HTTPおよびHTTPSの設定



iMC用にHTTPからHTTPSへの自動リダイレクションを設定する方法を教えてください。

デフォルトでは、iMCはHTTPおよびHTTPSを介してアクセスできます。

HTTPアクセスをHTTPSアクセスに自動的にリダイレクトするには、次の作業を実行します。

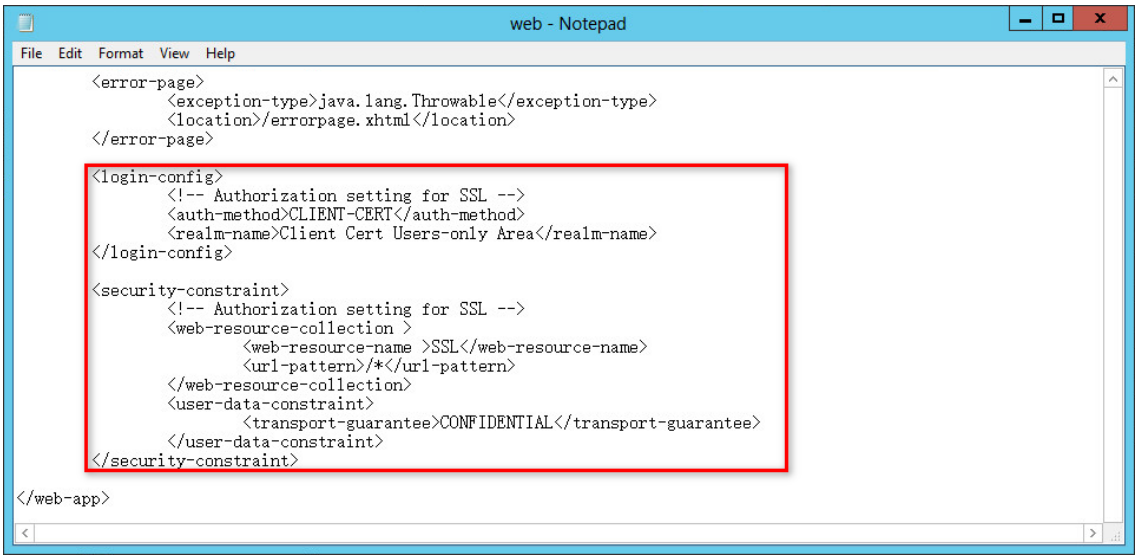
1. テキストエディタを使用して、iMC設定ファイルweb.xmlを開きます。
   - Windowsでは、このファイルはiMCインストールパスの\client\web\apps\imc\WEB-INF\assemblyディレクトリにあります。
   - Linuxでは、このファイルはiMCインストールパスの/client/web/apps/imc/WEB-INF/assemblyディレクトリにあります。

   この例では、Windowsを使用しています。
2. 図35に示すように、行</error-page>と行</web-app>の間に次の構成を追加します。

```
<login-config>
<!-- Authorization setting for SSL -->
<auth-method>CLIENT-CERT</auth-method>
<realm-name>Client Cert Users-only Area</realm-name>
</login-config>
<security-constraint>
<!-- Authorization setting for SSL -->
<web-resource-collection >
<web-resource-name >SSL</web-resource-name>
<url-pattern>/*</url-pattern>
</web-resource-collection>
<user-data-constraint>
<transport-guarantee>CONFIDENTIAL</transport-guarantee>
</user-data-constraint>
</security-constraint>
```

3. iMCを再起動します。

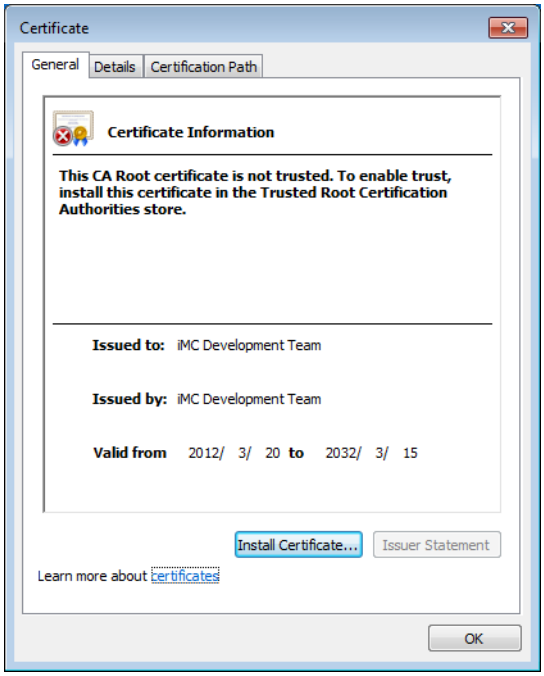
図35 構成ファイルweb.xml



iMC用の証明書をインストールする方法は?

デフォルトでは、に示すように、iMC開発チームによって作成された証明書がiMCに提供されます。

図36 証明書



Windowsで実行されているiMC用の別の証明書をインストールするには、以下の手順に従ってください。

1. iMCを停止します。
2. cmdウィンドウで、iMCインストールパスのclient\securityディレクトリに移動します。
3. ファイルnewksの名前をnews.bakに変更します。

   rename newks newks.bak
4. 新しい証明書を作成します。

   <installation directory>\common\jre\bin\keytool.exe -genkey -v -alias iMC -validity 3650 -keyalg RSA -dname "CN=192.168.1.100, OU=R&D, O=Company, L=Beijing, S=China, C=CN" -keypass iMCV500R001 -storepass iMCV500R001 -keystore newks

   -dnameパラメーターの説明:

   - **CN**：iMCサーバホストのドメイン名またはIPアドレス。
   - **OU**：組織単位。
   - **O**：会社名または組織名。
   - **L**：市名。
   - **S**：国/地域名。
   - **C**：2桁の国/地域コード。

   CNの値がiMCサーバホストのドメイン名またはIPアドレスでない場合、管理者がブラウザーからiMCにログインすると、システムは証明書アドレスエラーメッセージを表示します。
5. 作成された証明書を表示します。

   <installation directory>\common\jre\bin\keytool.exe -list -v -alias iMC -keystore <installation directory>\client\security\newks -storepass iMCV500R001
6. iMC構成ファイルを変更します。

   証明書を作成するコマンドの**-keypass**および**-storepass**パラメーターは、証明書および証明書ストアのパスワードを指定するために使用されます。証明書ストアにiMCV500R001の代わりに別のパスワードを使用する場合は、次のように設定ファイルを変更する必要があります。

   a. テキストエディタを使用して、iMCインストールディレクトリにある\client\conf\server.xmlファイル

を開きます(図37を参照)。

b. ファイル内のiMCV500R001を証明書ストアの新しいパスワードで置き換えます。

図37 Windows上のserver.xmlファイル

```
<!--  HTTPS Connector  -->
<Connector port="8443" protocol="org.apache.coyote.http11.Http11NioProtocol" maxPostSize="5242880"
  URIEncoding="UTF-8" maxHttpHeaderSize="8192" maxThreads="150" minSpareThreads="25"
  maxSpareThreads="75" enableLookups="false" acceptCount="100" connectionTimeout="60000"
  compression="on" compressionMinSize="2048" noCompressionUserAgents="gozilla, traviata"
  compressableMimeType="text/html,text/xml,text/xhtml,text/css,text/javascript,text/plain"
  disableUploadTimeout="true" SSLEnabled="true" scheme="https" secure="true" clientAuth="false"
  sslProtocol="TLS" keystoreFile="security/newks" keystorePass="iMCV500R001" />
```

7. iMCを再起動します。

   Webブラウザーからimcにログインするには、管理者が新しく作成した証明書の信頼を有効にする必要があります。この手順の詳細については、次のFAQトピックを参照してください。

Linuxで動作するiMC用の証明書をインストールするには、上記の設定のバックスラッシュ(\)をスラッシュ(/)に置き換え、keytool.exeをkeytoolに置き換えます。

図38は、Linux上のserver.xmlファイルを示しています。

図38 Linux上のserver.xmlファイル

```
                <!-- HTTPS Connector -->
                <Connector SSLEnabled="true" URIEncoding="UTF-8" acceptCount="100"
clientAuth="false" compressableMimeType="text/html,text/xml,text/xhtml,text/css,text/
javascript,text/plain" compression="on" compressionMinSize="2048" connectionTimeout="60000"
disableUploadTimeout="true" enableLookups="false" keystoreFile="security/newks"
keystorePass="iMCV500R001" maxHttpHeaderSize="8192" maxPostSize="5242880"
maxSpareThreads="75" maxThreads="150" minSpareThreads="25" noCompressionUserAgents="gozilla,
traviata" port="443" protocol="org.apache.coyote.http11.Http11NioProtocol" scheme="https"
secure="true" sslProtocol="TLS"/>
```

IE7.0以降を使用してHTTPS経由でログインすると、証明書エラーメッセージが表示されます。どのように対処すればいいですか?

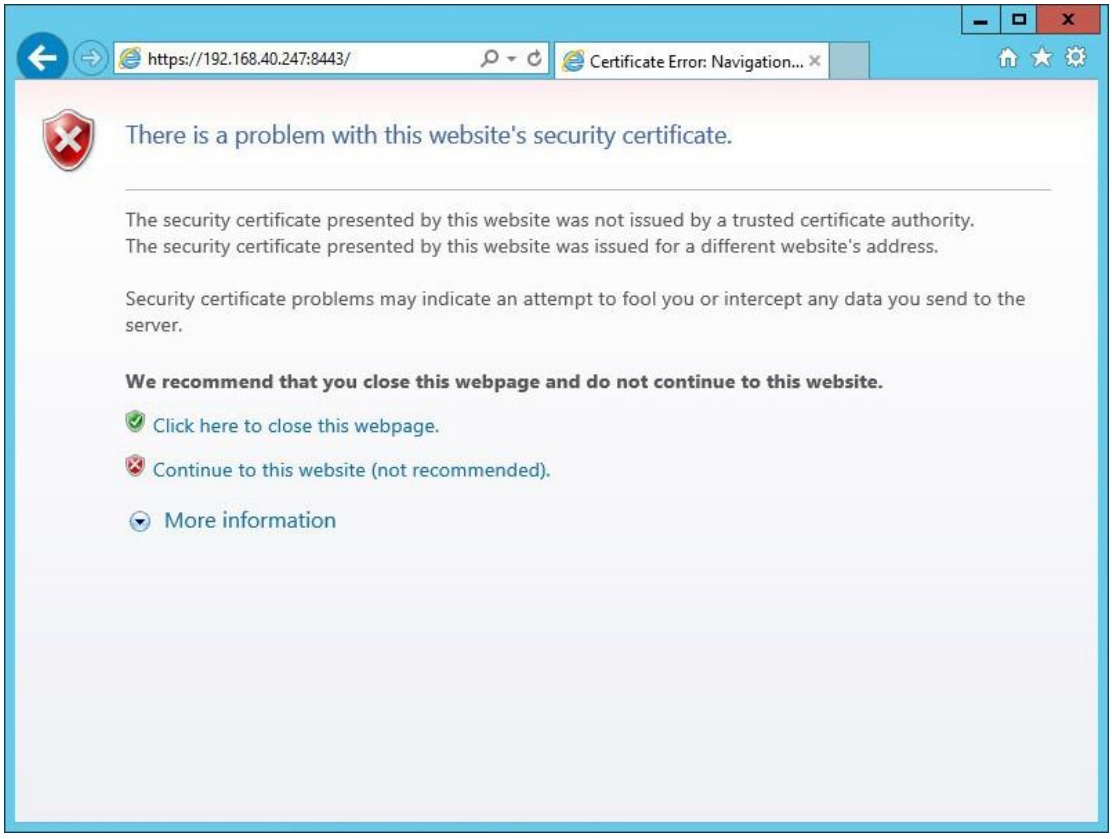
これは、iMCで使用される証明書が信頼されていないために発生します。管理者は証明書の信頼を有効にする必要があります。

例えば、IE10.0で証明書の信頼を有効にするには:

1. HTTPSを使用してiMCにログインします。

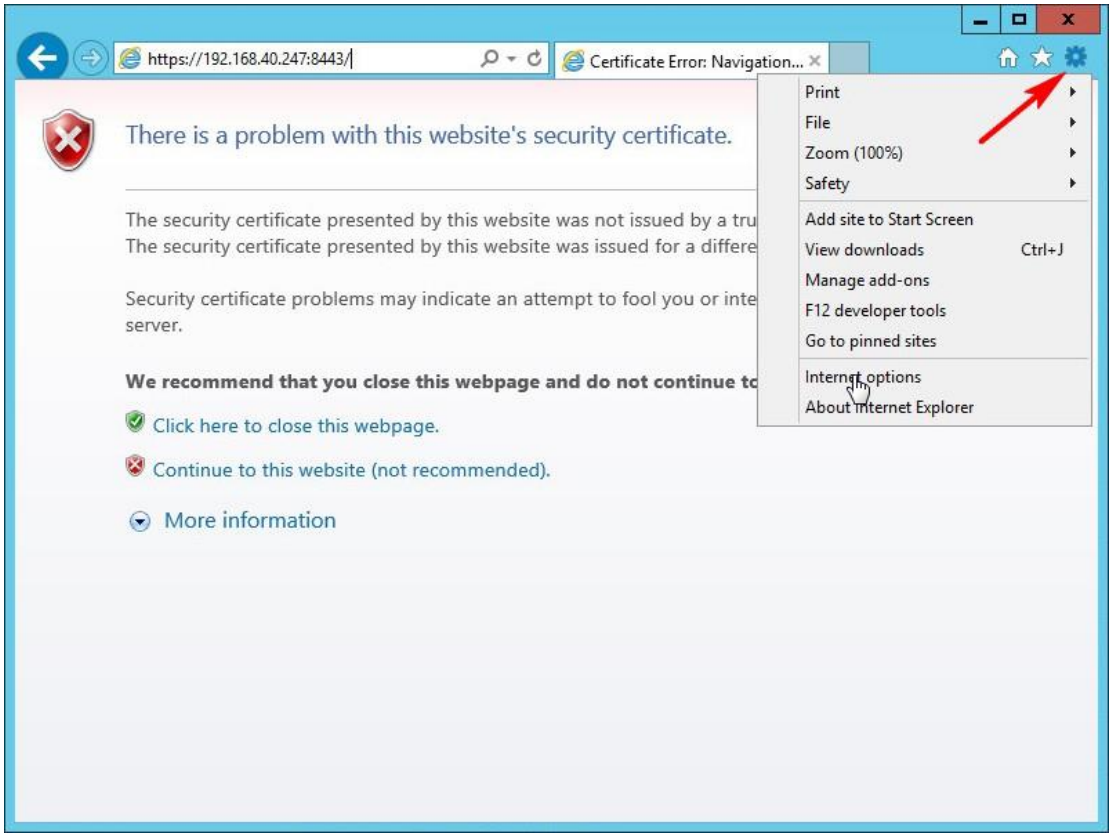
   図39に示すように、エラーメッセージが表示されます。

図39 HTTPSログイン時のエラーメッセージ



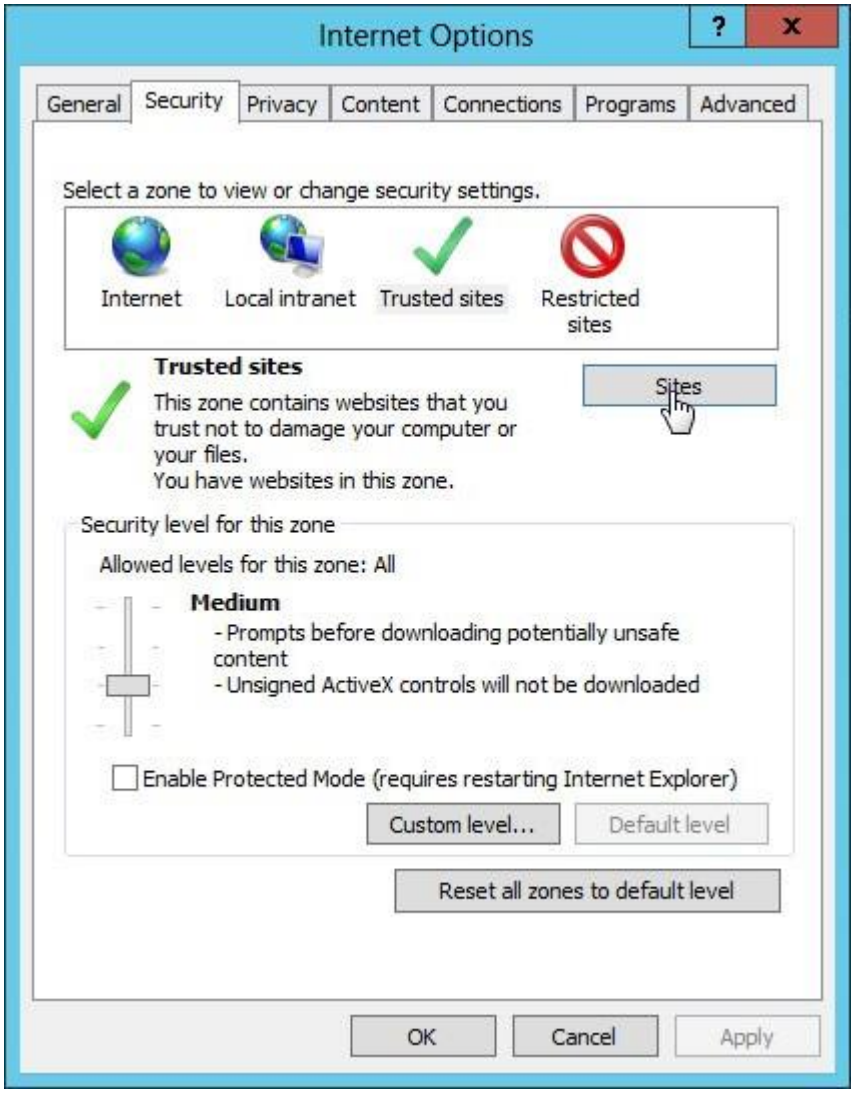
2. アドレスバーの右側にあるToolsアイコンをクリックし、メニューから**Internet Options**を選択します(図40を参照)。

図40 IE Toolsメニュー



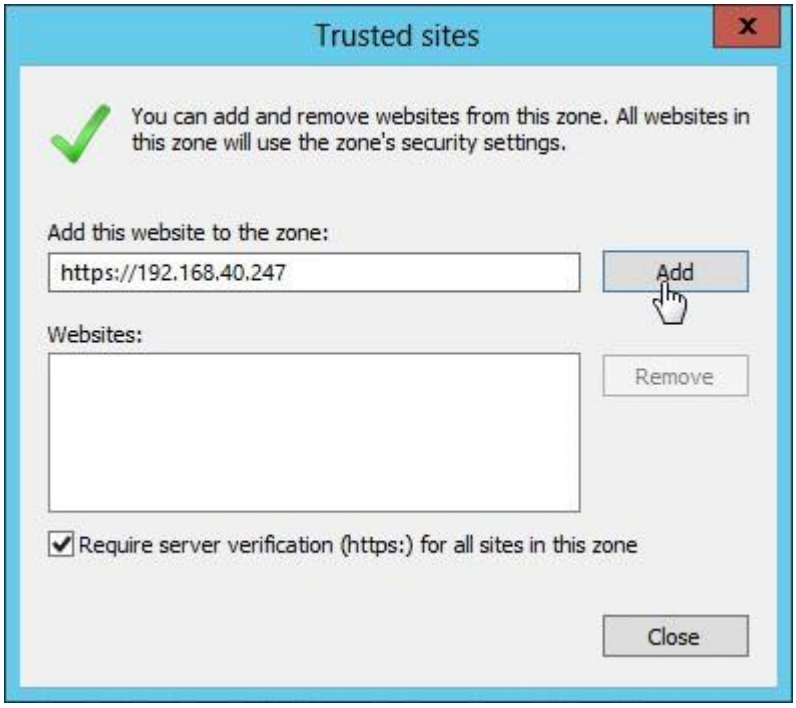
3. **Internet Options**ダイアログボックスで、**security**タブをクリックし、**Trusted site**をクリックしてサイト(図41を参照)。

図41 IE Securityタブ



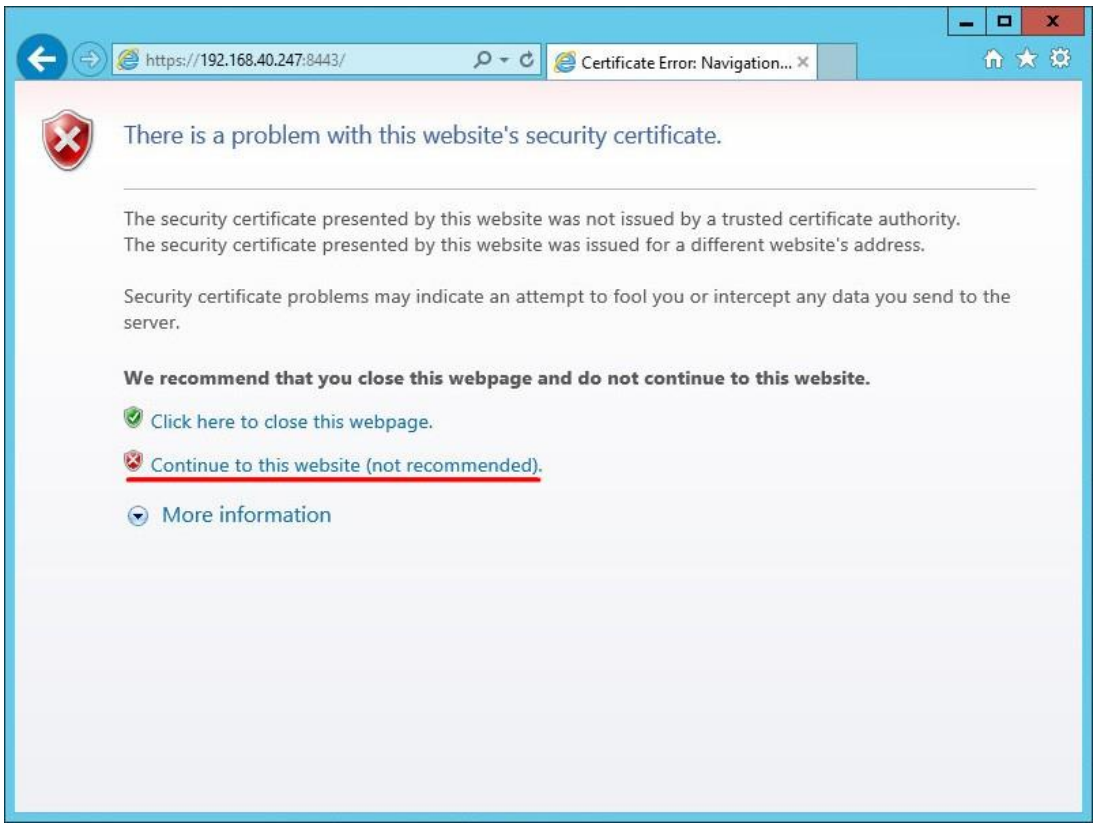
4. **Add this website to the zone**フィールドにiMCサーバーのIPアドレスを入力し、**Add**をクリックしてWebサイトを信頼済みサイトに追加してから**Close**をクリックします(図42を参照)。

図42 信頼済みサイト



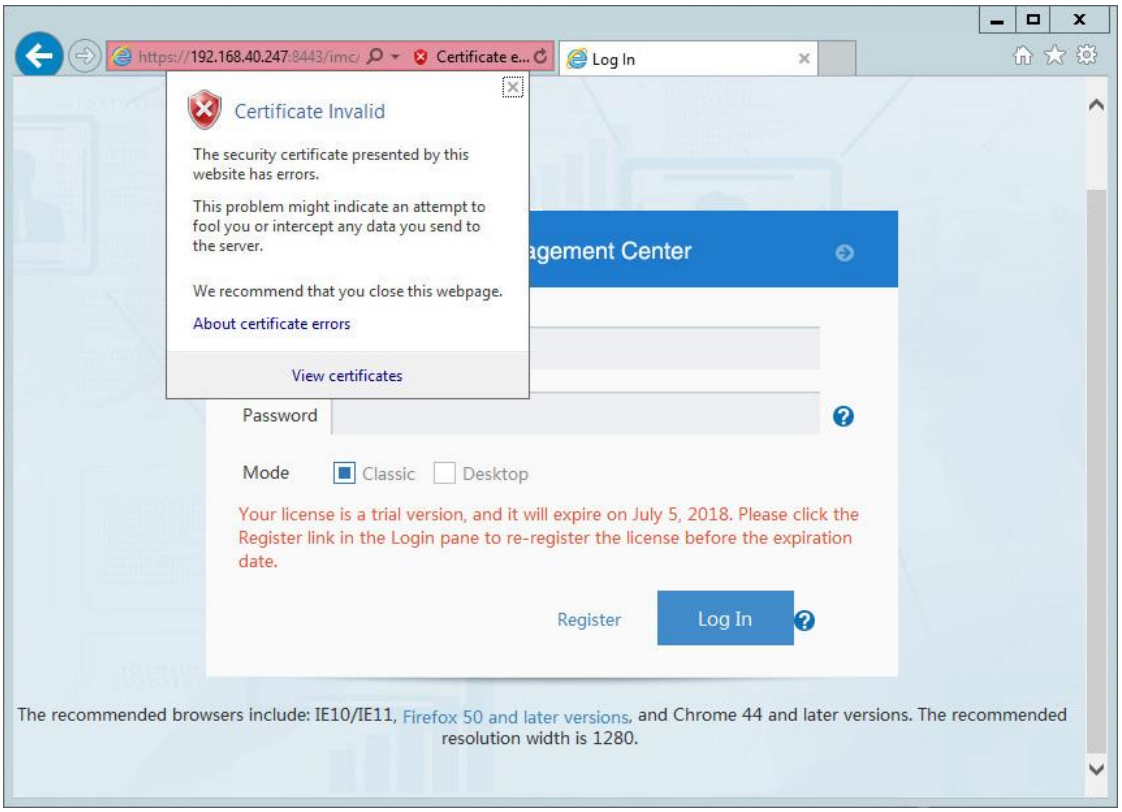
5. **Internet Options**ウィンドウで、**OK**をクリックします。
6. 図43に示すように、エラーメッセージページを更新し、**Continue to this website**(推奨しません)をクリックします。

図43 HTTPSログイン



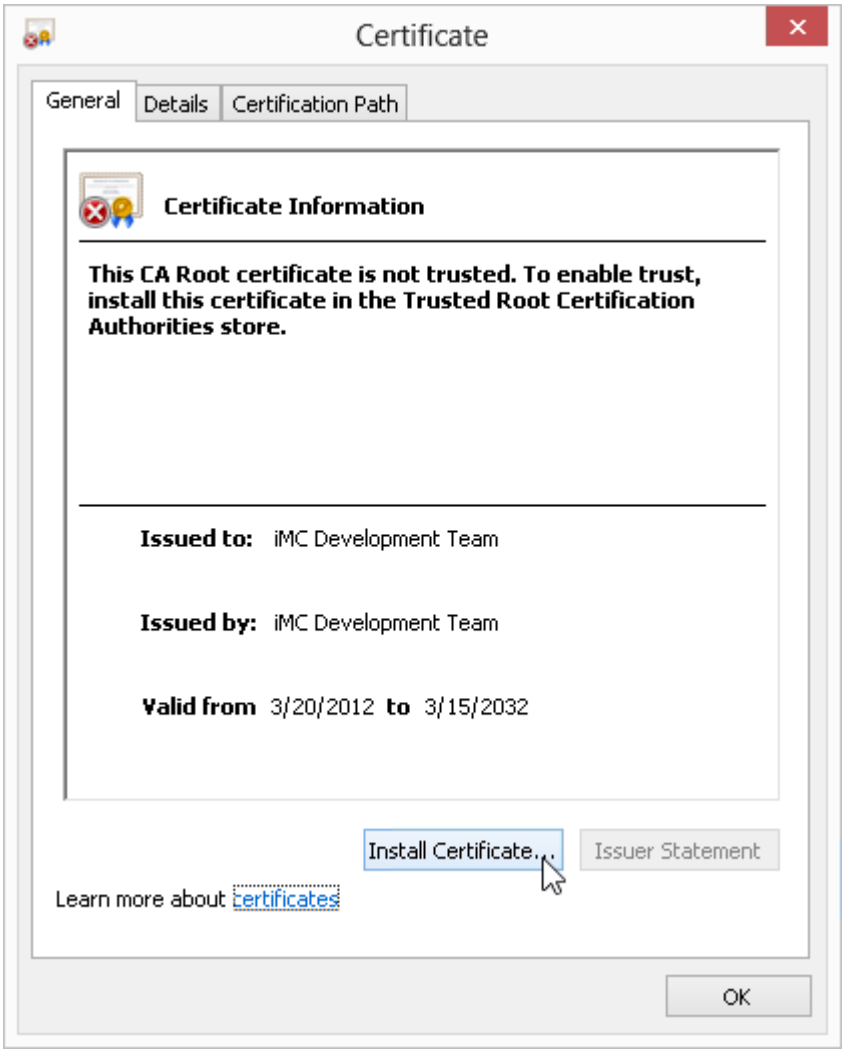
7. **Certificate error**をクリックします。図44に示すように、表示された**Certificate invalid**ダイアログボックスで、**view certificate**リンクをクリックします。

図44 無効な証明書



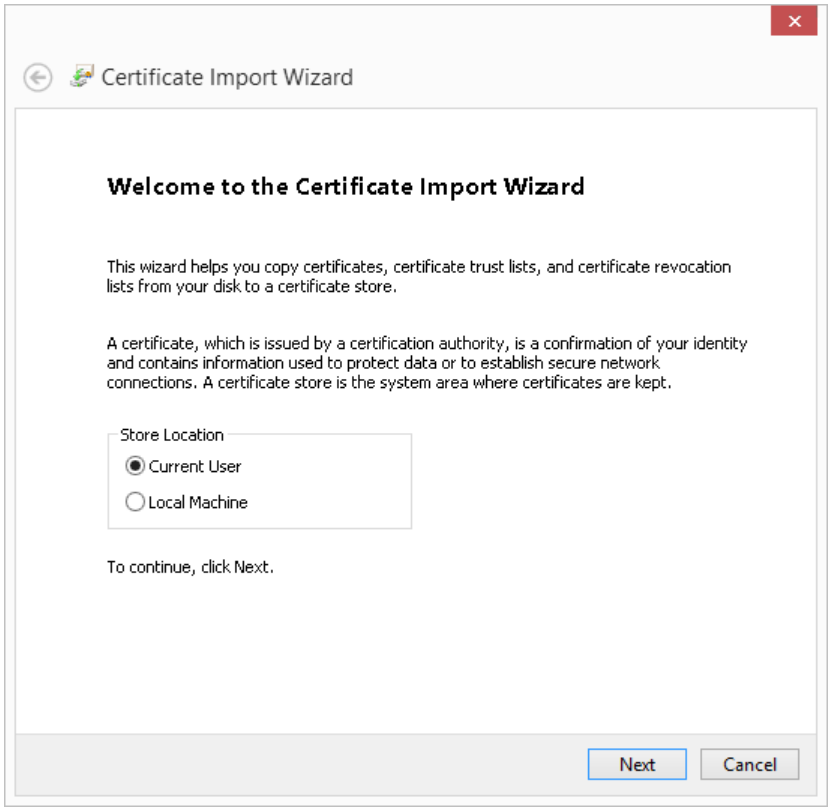
8. **Certificate**ウィンドウで、Install Certificateをクリックします(図45を参照)。

図45 証明書



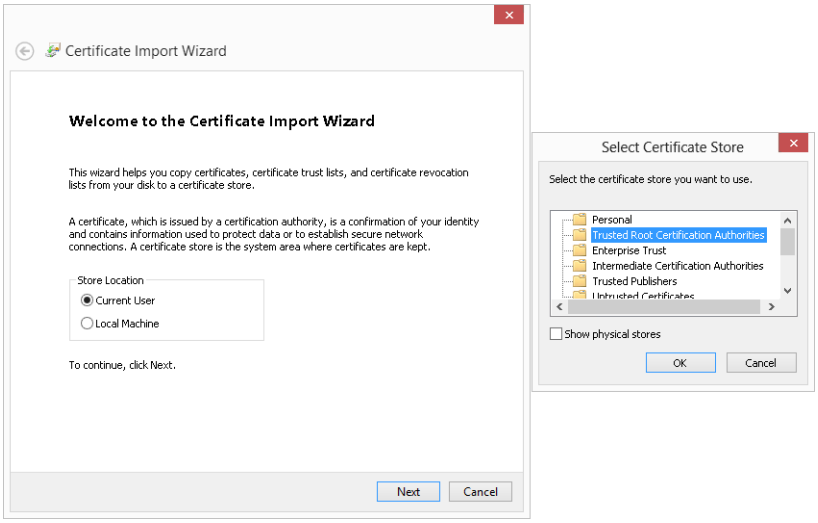
9. **Certificate Import Wizard**ウィンドウで、Current Userを選択し、**Next**をクリックします(図46を参照)。

図46 証明書のインポートウィザード



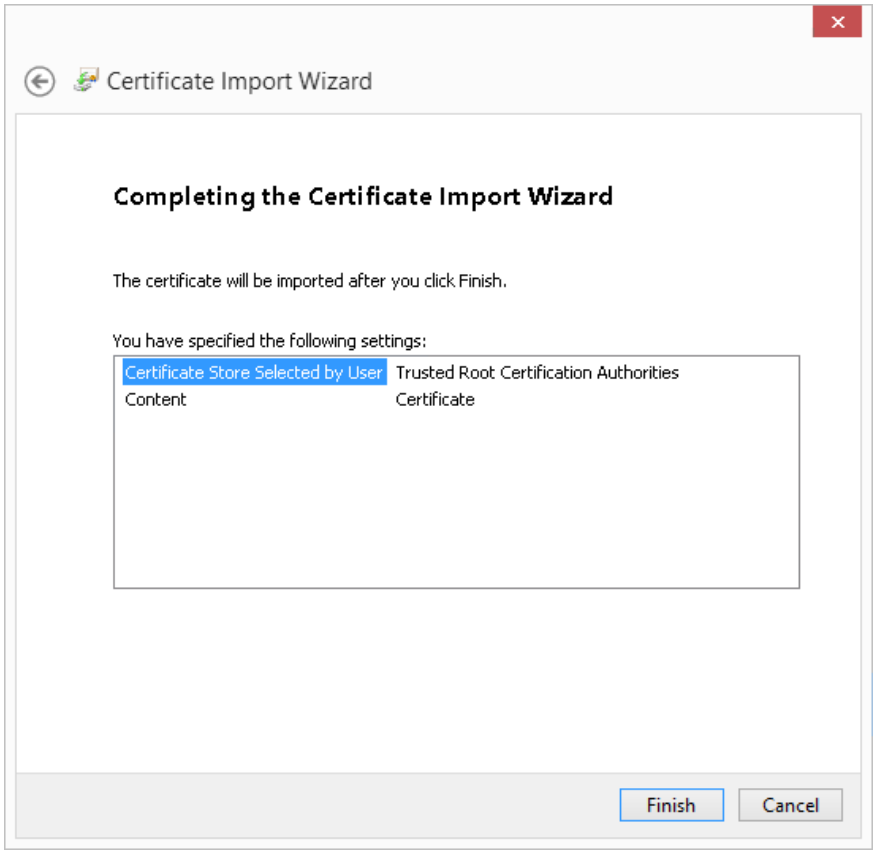
10. Place all certificates in the following storeを選択し、Browseをクリックします。Select Certificate StoreウィンドウでTrusted Root Certificate Authoritiesを選択し、OKをクリックします。図47に示すように、Certificate Import WizardウィンドウでNextをクリックします。

図47 証明書のインポートウィザード



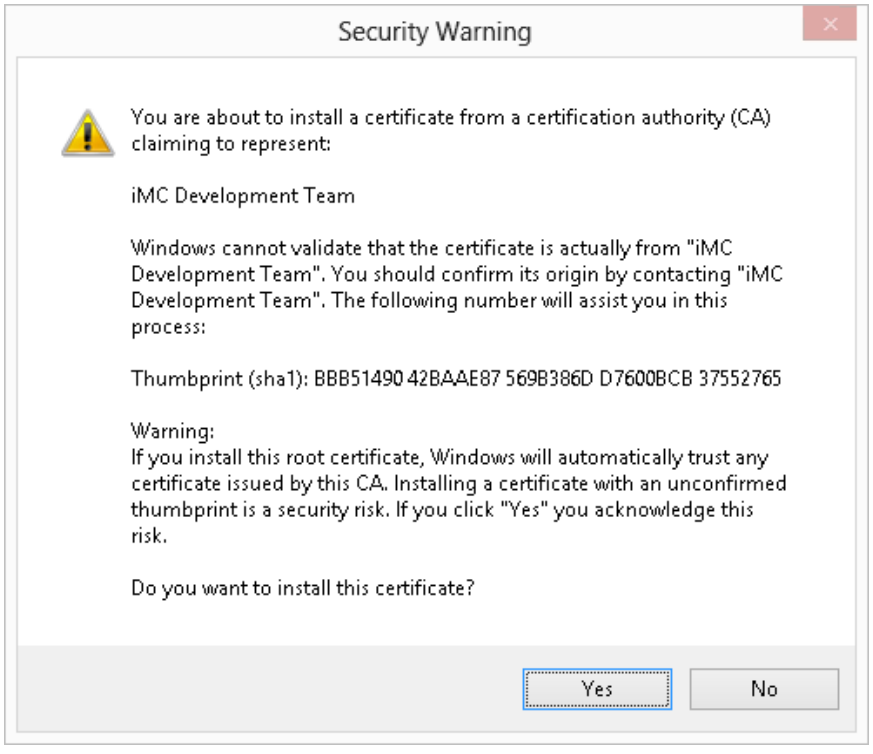
11. **Finish**をクリックします(図48)。

図48 証明書のインポートウィザードの完了



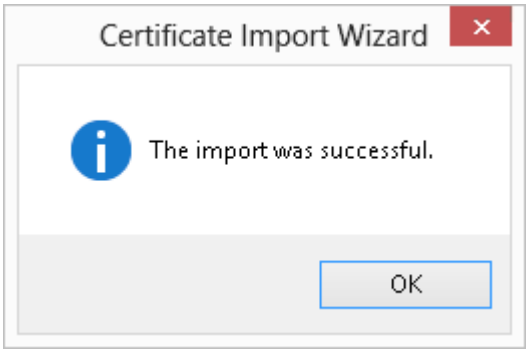
12. 図49に示すように、警告メッセージで**Yes**をクリックします。

図49 セキュリティ警告



13. インポート成功通知が表示されたら、図50に示すように**OK**をクリックします。

図50インポート成功の通知



14. **Warn about certificate address mismatch*Internet**オプションの選択を解除します。

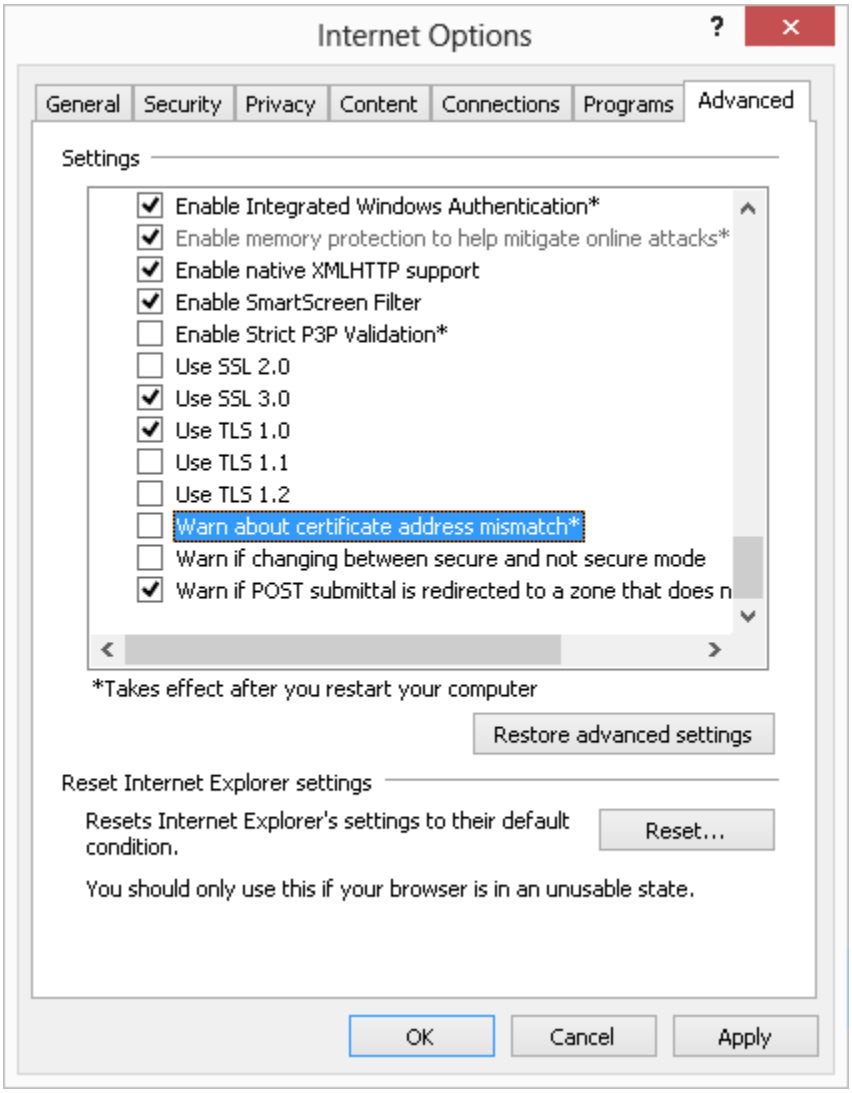
管理者がすでにiMC用の証明書をインストールしており、その証明書のCN値がiMCサーバホストのドメイン名またはIPアドレスに設定されている場合は、この手順をスキップしてください。

a. アドレスバーの右側にある**Tools**メニューの**Internet Options**をクリックします。**Internet Options**ダイアログボックスが表示されます。

b. **Advanced**タブをクリックします。

c. **Warn about certificate address mismatch***チェックボックスをオフにし、**OK**をクリックします(図51を参照)。

図51インターネットオプション



64ビットWindows Server2008R2オペレーティングシステムのIE8.0では、デバイスの詳細ページからデバイスにTelnet接続できません。どうすればいいですか?

この問題の原因は次のとおりです。

- Windowsオペレーティングシステムの一部のバージョンでは、デフォルトでTelnetクライアントが提供されません。
- IEの一部のバージョンでは、デフォルトでTelnetクライアントを使用できません。

詳細については、iMCヘルプのFAQを参照してください。

デバイスによっては、WebベースのNMSインターフェイスを開くことができない場合があります。これはなぜですか。

WebベースのNMS機能は、デバイス構成の影響を受けます。この機能は、選択したデバイスでWebベースのネットワーク管理がサポートされ、有効になっている場合にのみ使用できます。

iMCがしばらく実行された後、トポロジーを表示できません。これはなぜ発生するのですか。

これは、システムのTempフォルダに一時ファイルが多すぎる場合に発生します。フォルダから不要なファイルを削除して領域を解放してください。Tempフォルダのデフォルトパスは、オペレーティングシステムによって異なります。

- Windows XPでは、このフォルダはC:\Documents and Settings\ADM\Local Settings\Tempディレクトリにあります。

- Windows7および8では、このフォルダはC:\Users\ADM\AppData\Local\Tempにあります。
  で行ないます。

ADMをオペレーティングシステムの現在のユーザー名に置き換えます。

デバイスを別のIPアドレスを使用する別のデバイスと交換すると、ネットワークトポロジーが正しくなくなります。どうすればいいですか?

iMCがデバイスの変更を認識していないため、ネットワークトポロジー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ます。

- 古いデバイスをiMCから削除し、新しいデバイスを手動でIMCに同期させます。
- 新しいデバイスのIPアドレスと古いデバイスのIPアドレスを設定し、新しいデバイスをiMCに手動で同期します。

データエクスポート機能のExecute Command After Exportフィールドで設定したコマンドを実行すると、CPU使用率が長時間にわたって高くなります。どうすればいいですか?

コマンドにGUIが含まれておらず、バックグラウンドで実行され、実行後に自動的に終了できることを確認します。

既存のビューと同じ名前で大文字と小文字が異なるビューを追加した場合、そのビューがすでに存在することが表示されるのはなぜですか?

SQL Serverデータベースでは大文字と小文字が区別されません。新しいビューを作成するには、一意の名前を選択する必要があります。

iMCがSQL Serverデータベースを使用して一定期間実行されると、メモリ使用率が非常に高くなり、回復できなくなります。どうすればいいですか?

この問題を解決するには、次の手順を実行してSQL Serverの最大バッファサイズを変更します。

1. setsqlservermaxmem.bat-server server-sAPwd password-maxMemを実行します。
   iMCインストールパスの\client\bin\ディレクトリにあるmaxmemコマンド。

   パラメーターの説明:

   - **-server** server : SQL Serverデータベースサーバーの名前またはIPアドレス。このパラメーターは
     は
     オプション。デフォルト設定はlocalhostです。
   - **-sAPwd** password : saユーザーのパスワード。このパラメーターは必須です。
   - **-maxMem** maxmem : 最大バッファサイズ(MB)。このパラメーターはオプションです。
2. SQL Serverデータベースを再起動して構成を検証します。

たとえば、iMCが集中モードで配置され、192.168.100.199のリモートSQL Serverデータベースを使用しているとします。**sa**ユーザーのパスワードはiMC123です。データベースのバッファサイズを1024MBに設定するには、iMCインストールパスの\client\binディレクトリで次のコマンドを実行します:

setsqlservermaxmem.bat -server 192.168.100.199 -sAPwd iMC123 -maxMem 1024

注:

- データベース自体がある程度のバッファスペースを使用するため、実際に使用されているバッファサイズは、設定した値よりも大きい場合があります。
- 上記の設定は、データベースをリブートすると有効になります。

iMCリソースを表示しようとすると、デバイスが表示されません。なぜこのようなことが起こるのでしょうか?

この問題が発生する主な理由は、ハードウェアリソースが不足していることです。その他にも、次のような理由が考えられます。

- iMCプロセスは自動的に再起動します。
- システムの応答が遅く、常に不十分なリソースを要求します。
- 定期レポートを生成できません。

この問題を解決するには、iMCがインストールされているサーバーのメモリおよび関連するハードウェアリソースをアップグレードします。

iMCの実行中にシステム時刻を変更できますか?

iMCの実行中は、システム時刻を手動で変更しないでください。システム時刻を変更すると、データの混乱やプロセスエラーが発生する可能性があります。

システム時刻の変更が原因でiMCプロセスエラーが発生した場合は、iMC関連プロセス(Intelligent Deployment Monitoring AgentおよびIntelligent Management Serverサービスを含む)を再起動します。

長いファイル名のファイルをiMCにインポートすると、システムが応答しません。どうすればいいですか?

ファイル名の長さの制限は、オペレーティングシステムまたはブラウザーによって異なります。ファイル名を短くして、ファイルを再度インポートしてください。

iMCに長い文字列を入力すると、インターフェイスが正しく表示されません。どうすればいいですか?

これはブラウザー固有の問題であり、通常の操作には影響しません。このような問題を回避するには、必要に応じてテキストにスペースを追加します。ブラウザーはインターフェイスのレイアウトを自動的に調整します。

リストの最後のページに移動すると、ページの下部に表示される合計ページ数が、リストの上に表示されるページ数よりも多くなります。なぜだ?

問合せを高速化するために、最後の問合せで取得された合計ページ数が自動的にキャッシュされます。キャッシュされた数は、最後のページへのナビゲートに使用されます。最後のページが表示されると、合計ページ数が再計算され、ページの下部に表示されます。

2つの問合せ間にエントリが追加されると、ページ全体が一貫して表示されない場合があります。新しいページを参照するには、ページ下部のナビゲーションリンクを使用します。

管理用PCからiMCにログインしようとすると、システムリソース不足エラーが表示されます。どうすればいいですか?

この問題は、システムのJavaヒープサイズを変更することで解決できます。次の操作を行います。

- Windowsでは、iMCインストールパスの\client\binディレクトリにあるsetmem.bat Maxsizeコマンドを実行します。
- Linuxでは、iMCインストールパスの/client/binディレクトリにあるsetmem.sh Maxsizeコマンドを実行します。

コマンドのMaxsize文字列を必要なJavaヒープサイズに置き換えます。推奨されるJavaヒープサイズについては、表6および表7を参照してください。

表6 32ビットオペレーティングシステムで推奨されるJavaヒープサイズ

ノード	コレクションユニット	オンライン事業者	Javaヒープサイズ
0から200	0～5K	20	512MB(Windows) 512MB(Linux)
	5Kから50K	10	

200から500	0～10K	30	1GB(Windows) 1GB(Linux)
	10Kから100K	10	

表7 64ビットオペレーティングシステムで推奨されるJavaヒープサイズ

ノード	コレクションユニット	オンライン事業者	Javaヒープサイズ
0から200	0～5K	20	2GB(Windows)
	5Kから50K	10	2GB(Linux)
200～1K	0～10K	30	2GB(Windows) 4GB(Linux)
	10Kから100K	10	
1Kから2K	0～20K	30	4GB(Windows) 6GB(Linux)
	20K～200K	10	
2Kから5K	0～30K	40	8GB(Windows) 8GB(Linux)
	30K～300K	20	
5Kから10K	0～40K	50	12GB(Windows) 12GB(Linux)
	40～400K	20	
10Kから15K	0～40K	50	16GB(Windows) 16GB(Linux)
	40～400K	20	

収集単位数は、5分間隔で収集されたパフォーマンスインスタンスの合計数と等しくなります。収集間隔が5分より大きい場合、収集単位数は減少します。収集間隔が5分より小さい場合、収集単位数は増加します。

たとえば、表8にリストされているパフォーマンスインスタンスが5分ごとに収集される場合、収集単位の合計はパフォーマンスインスタンスの数(24)と同じです。収集単位が5分間隔(10分)の2倍である場合、収集単位の数はパフォーマンスインスタンスの合計数(12)の半分になります。

表8 パフォーマンスインスタンス

監視対象項目	番号	パフォーマンス指標	パフォーマンスインスタンス
中央処理装置	1	CPU使用率	1
メモリ	1	メモリ使用量	1
インターフェイス	10	受信レート	10
		送信レート	10
デバイス	1	到達不能率	1
		応答時間	1
		合計	24

注:

- Javaヒープサイズを変更する前に、iMCを停止していることを確認してください。
- 32ビットオペレーティングシステムの場合、Javaヒープサイズは1GBを超えることはできません。が必要です。64ビットオペレーティングシステムを使用してください。

テクニカルサポートのためにiMCログを収集する方法は?

IMCが提供するログ収集ツールを使用します。

- Windowsでは、このツールはIMCインストールパスの\deploy\logfiles.batディレクトリにあります。
- Linuxの場合、このツールはIMCインストールパスの/deploy/logfiles.shディレクトリにあります。この例ではLinuxを使用しています。

iMCインストールパスに/deployディレクトリを入力し、次のいずれかのタスクを実行します。

- 過去7日間のログを収集するには、logfiles.shコマンドを実行します。
- 7日間を超えるログを収集するには、関連するパラメーターを入力する必要があります。たとえば、過去30日間のログを収集するには、logfiles.sh30コマンドを実行します。

ログは、log_YYYYMMDDhhmmss.zipという名前の.zipファイルとして)にlog_YYYYMMDDhhmmss.zipという名前の.zipファイルとして保存されます。YYYYMMDDhhmmss文字列は、ファイルが作成された時刻(年、月、日、時、分、秒を含む)を示します。

iMCサーバーに複数のNICがある場合、IPアドレスの1つを使用してHTTP/HTTPSサービスを受信するにはどうすればよいですか。

以下のタスクを実行してください。

1. テキストエディタを使用して、iMC設定ファイル**server.xml**を開きます。
   - Windowsでは、このファイルはiMCインストールパスの\client\confディレクトリにあります。
   - Linuxの場合、ファイルはiMCインストールパスの/client/confディレクトリにあります。この例では、Windowsを使用しています。
2. 図52に示すように、address="IP address"をファイルに追加します。
3. ファイルを保存してiMCを再起動します。
   iMCには、server.xmlファイルで指定されたIPアドレスからのみアクセスできるようになりました。

図52server.xmlファイルの変更

```
- <Service name="Catalina">
    <!--  HTTP Connector  -->
    <Connector URIEncoding="UTF-8" acceptCount="100"
      compressableMimeType="text/html,text/xml,text/xhtml,text/css,text/javascript,text/plain"
      compression="on" compressionMinSize="2048" connectionTimeout="60000"
      disableUploadTimeout="true" enableLookups="false" maxHttpHeaderSize="8192"
      maxPostSize="5242880" maxSpareThreads="75" maxThreads="150" minSpareThreads="25"
      noCompressionUserAgents="gozilla, traviata" port="80"
      protocol="org.apache.coyote.http11.Http11NioProtocol" redirectPort="443"
      address="192.168.1.163" />
    <!--  HTTPS Connector  -->
    <Connector SSLEnabled="true" URIEncoding="UTF-8" acceptCount="100" clientAuth="false"
      compressableMimeType="text/html,text/xml,text/xhtml,text/css,text/javascript,text/plain"
      compression="on" compressionMinSize="2048" connectionTimeout="60000"
      disableUploadTimeout="true" enableLookups="false" keystoreFile="security/newks"
      keystorePass="iMCV500R001" maxHttpHeaderSize="8192" maxPostSize="5242880"
      maxSpareThreads="75" maxThreads="150" minSpareThreads="25"
      noCompressionUserAgents="gozilla, traviata" port="443"
      protocol="org.apache.coyote.http11.Http11NioProtocol" scheme="https" secure="true"
      sslProtocol="TLS" address="192.168.1.163" />
    <!--  AJP Connectors, disabled in default configuration  -->
```

分散iMC展開環境では、すべてのプライマリーサーバーとセカンダリーサーバーが再起動された場合、データベースをセカンダリーサーバー上のコンポーネントにアップロードできません。この問題を解決するにはどうすればいいですか。

これは、セカンダリーサーバーの再起動前にプライマリーサーバーが再起動されたために発生します。プ

ライマリーサーバー上のjserverプロセスをセカンダリーサーバー上のデータベースに接続できません。したがって、データベースをセカンダリーサーバー上のコンポーネントにアップロードできません。

この問題を解決するには、セカンダリーサーバーの再起動後に、プライマリーサーバーでjserverプロセスを手動で再起動します。

iMCに仮想デバイスを追加する方法を教えてください。

デバイスタイプPCを選択して、自動検出によってデバイスを追加します。システムが仮想デバイスを認識するようにするには、次の場合にSOAPパラメーターを設定します。

1. 仮想マシン(VM)の場合、SOAPパラメーター設定は必要ありません。
2. vCenter+ESX/ESXi環境では、vCenter専用のSOAPパラメーターを設定します。
3. 独立したESX/ESXi環境では、各ESX/ESXiのSOAPパラメーターを設定します。

デバイスの詳細ページで、構成メニューからModify SOAP Settingsを選択し、SOAPパラメーターを構成します。構成が同期化されると、仮想デバイスを認識できます。

図53に示すように、iMCのインストール時にデータベースチェックエラーが発生します。この問題を解決するにはどうすればよいですか。

図53データベースチェックエラー

```
2010-10-25 16:24:27 [WARN ] [AWT-EventQueue-0] [com.h3c.imc.deploy.Util::getInstallInfo(614)] Can not find
instInfoFile - C:\WINDOWS\iMC-Reserved\instinfo.txt
2010-10-25 16:24:27 [WARN ] [AWT-EventQueue-0] [com.h3c.imc.deploy.Util::getInstallInfo(614)] Can not find
instInfoFile - C:\WINDOWS\iMC-Reserved\instinfo.txt
2010-10-25 16:24:34 [WARN ] [AWT-EventQueue-0] [com.h3c.imc.deploy.Util::getInstallInfo(614)] Can not find
instInfoFile - C:\WINDOWS\iMC-Reserved\instinfo.txt
2010-10-25 16:24:34 [WARN ] [AWT-EventQueue-0] [com.h3c.imc.deploy.Util::getInstallInfo(614)] Can not find
instInfoFile - C:\WINDOWS\iMC-Reserved\instinfo.txt
2010-10-25 16:24:35 [INFO ] [Thread-3]
[com.h3c.imc.deploy.dma.wizard.DatabaseSelectPanelDescriptor::isSQLServer2000Installed(347)] SQL Server 2000 is
Installed
2010-10-25 16:24:35 [INFO ] [Thread-3]
[com.h3c.imc.deploy.dma.wizard.DatabaseSelectPanelDescriptor::isSQLServer2000Installed(347)] SQL Server 2000 is
Installed
2010-10-25 16:24:50 [ERROR] [SwingWorker-pool-1-thread-1]
[com.h3c.imc.deploy.dma.wizard.DatabaseSelectPanelDescriptor$DbConnectCheckingWorkingDialog::doWork(1173)] Connect
to database error
java.sql.SQLException: Unable to get information from SQL Server: 127.0.0.1.
        at net.sourceforge.jtds.jdbc.MSSqlServerInfo.<init>(MSSqlServerInfo.java:97)
        at net.sourceforge.jtds.jdbc.ConnectionJDBC2.<init>(ConnectionJDBC2.java:276)
        at net.sourceforge.jtds.jdbc.ConnectionJDBC3.<init>(ConnectionJDBC3.java:50)
        at net.sourceforge.jtds.jdbc.Driver.connect(Driver.java:184)
        at java.sql.DriverManager.getConnection(DriverManager.java:582)
        at java.sql.DriverManager.getConnection(DriverManager.java:154)
```

SQL Server2005以降のバージョンをインストールし、デフォルト以外のインスタンスを使用する場合は、SQLブラウザーサービスを有効にする必要があります。有効にしないと、Javaがデータベースへの接続に失敗する可能性があります。

SOMモジュールが削除されると、アラーム、ICCM、ACLm、またはVLANMモジュールによって作成され、サブミットされたSOMプロセスは実行できなくなります。どうしたらいいですか?

SOMモジュールが削除されると、残りのSOMプロセスは無効になります。SOMプロセスを削除してください。

OracleデータベースまたはMySQLデータベースを使用すると、一部のiMCモジュールでデータベースエラーが発生します。どうすればいいですか?

通常、このような問題は、Oracleプロセスの最大数またはOracle接続制限が不十分であることが原因です。デフォルトでは、Oracleデータベースは最大150の接続を許可します。iMCモジュールが集中モードで配置されている場合、Oracleデータベースプロセスの最大数およびOracle接続制限を適切に設定する必要があります。

表9に、iMCモジュールに必要なOracle接続制限を示します。

表9 iMCモジュールでのOracle接続制限

iMCモジュール	Oracle接続の制限
iMCプラットフォーム	14
アラーム管理	24
Syslog管理	9
パフォーマンス管理	11
レポート管理	10
ゲストアクセスマネージャー	5
ユーザーセルフサービス管理	5
ネットワークアセットマネージャー	5
仮想リソース管理	9
構成センター	9
ACL管理	7

iMCモジュール	Oracle接続の制限
VLAN管理	11
セキュリティコントロールセンター	5
VXLAN管理	4
サーバーとストレージの自動化	6
VANファブリックマネージャー	27
リソース自動化マネージャー	16
QoSマネージャー	5
サービスヘルスマネージャー	60
ユーザーアクセス管理/CAMs会計マネージャー	100
EADセキュリティポリシー設定	25
デスクトップアクセスマネージャー	40
MPLS VPNマネージャー	9
L2VPNマネージャー	17
アプリケーションマネージャー	10
ブランチインテリジェントマネジメントシステム	10
IPSec VPNマネージャー	8
VAN接続マネージャー	5
ワイヤレスサービスマネージャー	50
セキュリティサービスマネージャー	10
ロードバランシングマネージャー	5

Oracleプロセスの最大数とOracle接続制限を表示および変更するには、次の手順に従います。

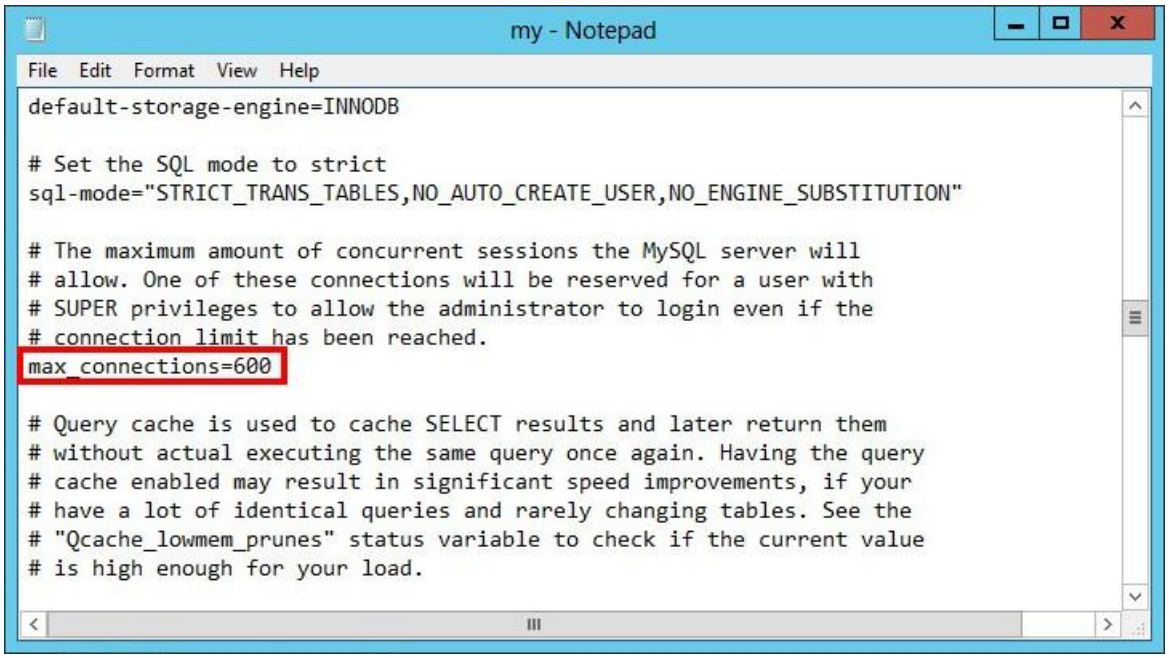
1. oracleユーザーに切り替えます。
   Su - oracle
2. Oracleデータベースにsysdbaとしてログインします。
3. <password>をsysユーザーのパスワードに置き換えます。
   sqlplus sys/<password> as sysdba
4. Oracleプロセスの数とOracle接続制限を表示します。
   - Oracleプロセスの数を表示します。
     Show parameter processes
   - Oracle接続制限を表示します。
     Show parameter sessions
5. インストールされているiMCモジュールに応じて、Oracleプロセスの最大数とOracle接続制限を変更します。
   - Oracleプロセスの最大数を変更します。必要に応じて<600>を別の値に置き換えます。
     alter system set processes=<600> scope=spfile
   - Oracle接続制限を変更します。必要に応じて<600>を別の値に置き換えます。
     alter system set sessions=<600> scope=spfile
6. 変更を有効にするには、Oracleデータベースを再起動します。

WindowsでMySQL接続制限を表示および変更するには、次の手順に

従います。

1. my.iniファイルを開きます。my.iniファイルのデフォルトのデータパスは C:\Program Files\MySQL\MySQL Server5.6です。
2. MySQLの接続制限を変更します。図54に示すように、必要に応じてmax_connections値を置き換えます。

図54 My.ini

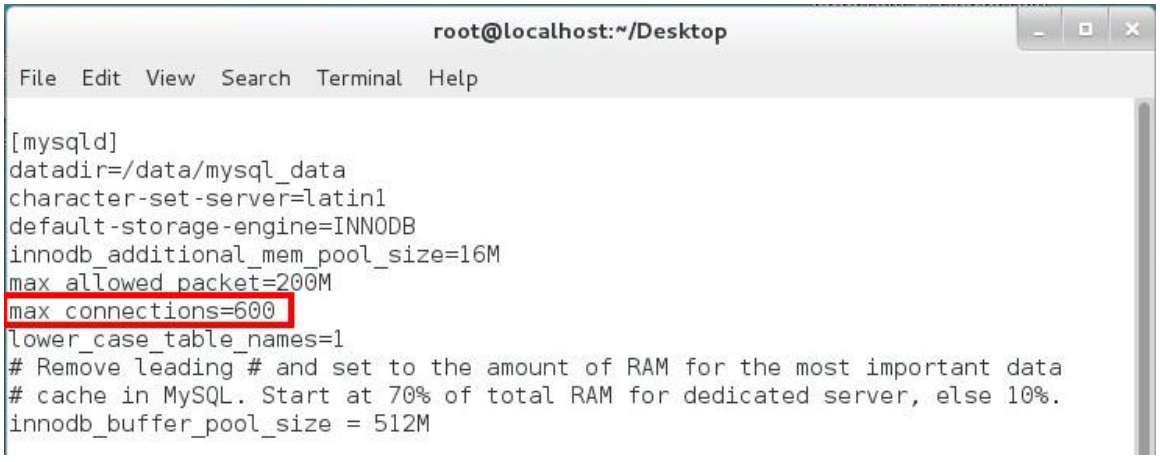


MySQL接続制限の最大数を表示および変更するには、次の手順に従います。

1. my.cnfファイルを開きます。

   Vi /etc/my.cnf
2. iと入力して編集モードに入ります。
3. MySQLの接続制限を変更します。図55に示すように、必要に応じてmax_connections値を置き換えます。

図55 my.cnf



Windows Server2012でIE10.0を使用してiMCにログインすると、Flashプラグインをインストールするように求められますが、新しいバージョンのFlashプラグインをインストールできません。どうすればいいですか?

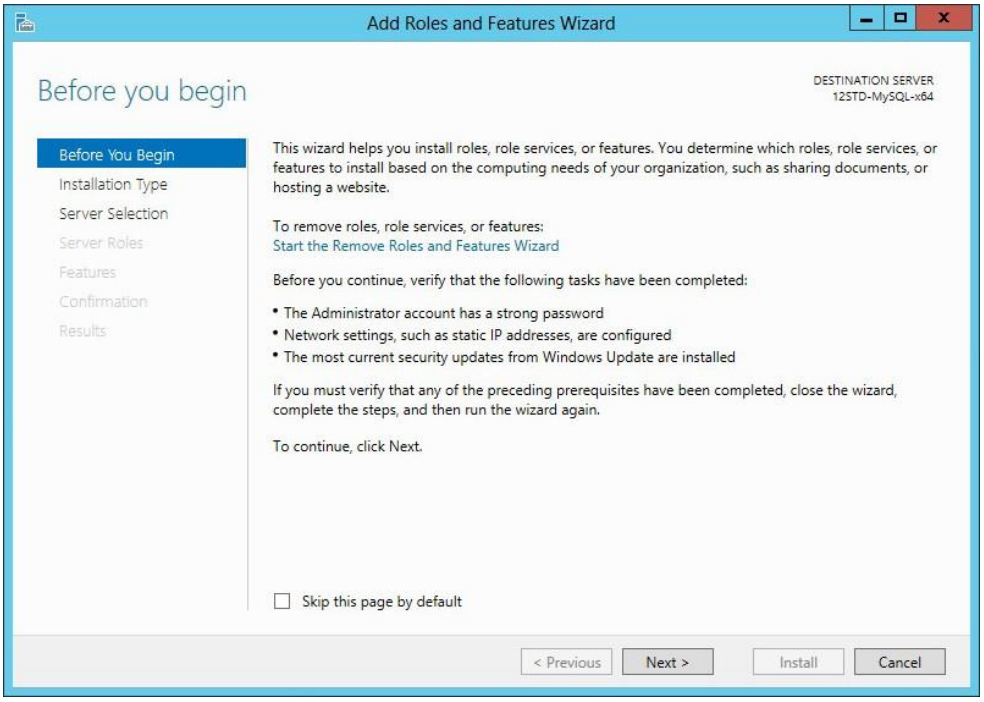
これは、Windows Server2012ではフラッシュプラグインがIE10.0に統合されていますが、デフォルトでは有効になっていないためです。新しいバージョンのフラッシュプラグインをインストールすると、統合されたフラッシュプラグインが検出されます。その結果、インストールが失敗します。

この問題は、Windows Server2012に統合されているフラッシュプラグインを有効にすることで解決できます。

この例では、Windows Server2012ビルド6.2.9200.16384およびIE10.0ビルド10.0.9200.16599を使用しています。Flashプラグインを有効にするには:

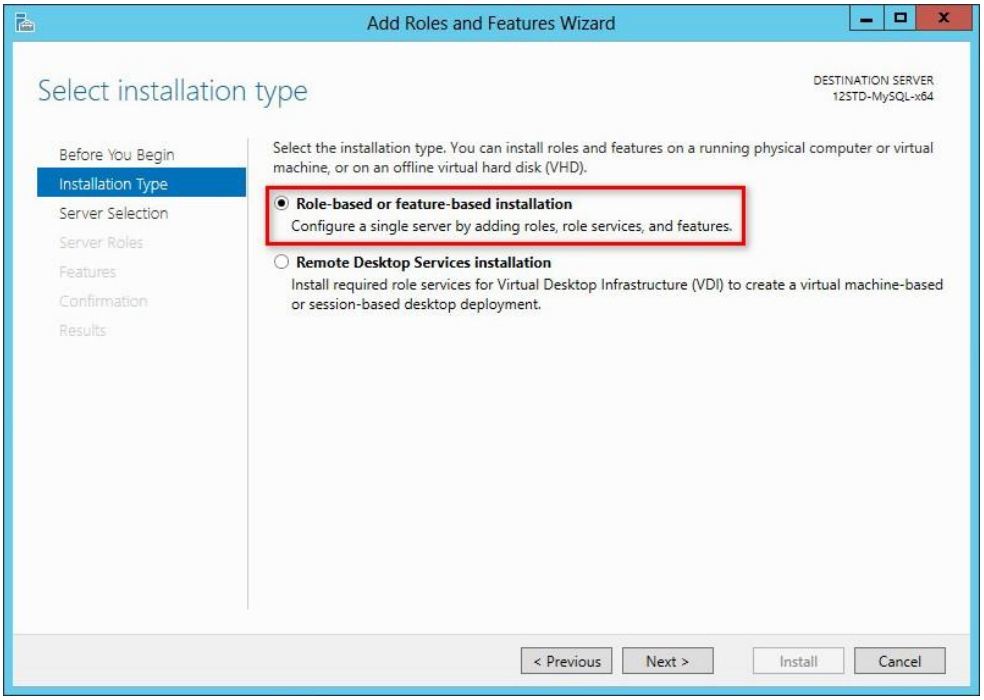
1. **Add Roles and Features Wizard**を起動し、**Next**をクリックします(図56を参照)。

   図56 Before you begin



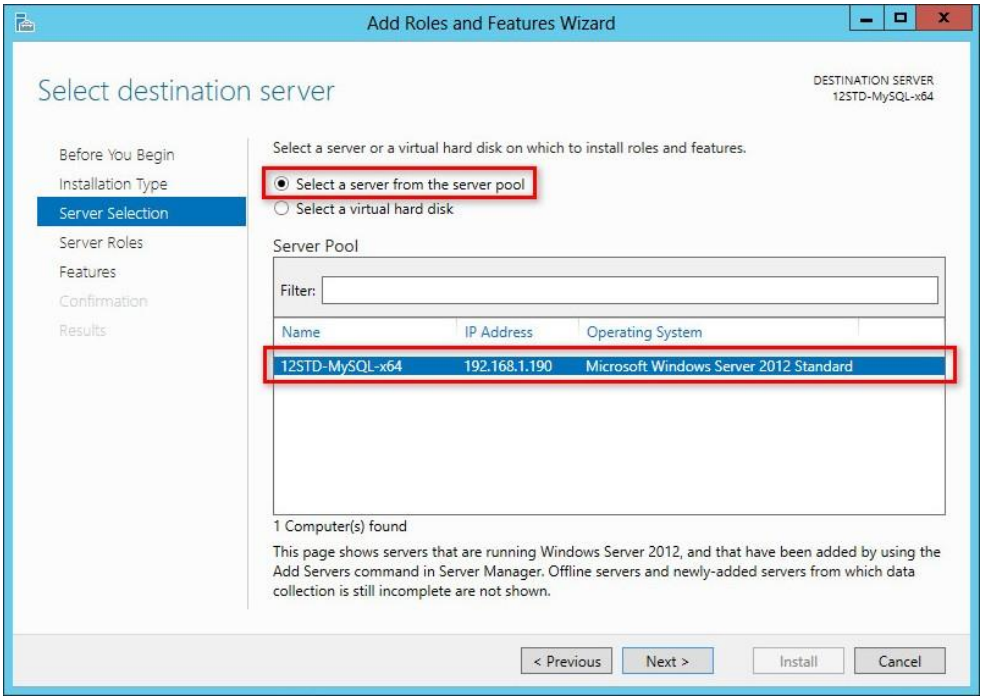
2. 図57に示すように、役割ベースまたは機能ベースのインストールを選択し、Nextをクリックします。

図57 Select installation type



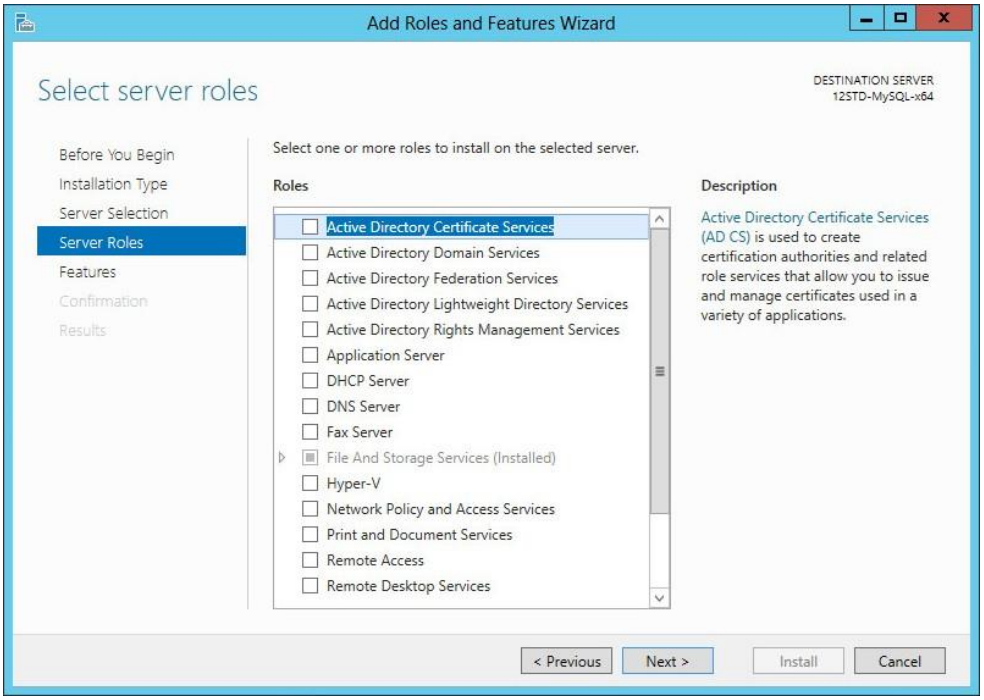
3. 図58に示すように、Select a server from the server poolオプションを選択し、サーバプールから現在のサーバーを選択して、Nextをクリックします。

図58 Select destination server



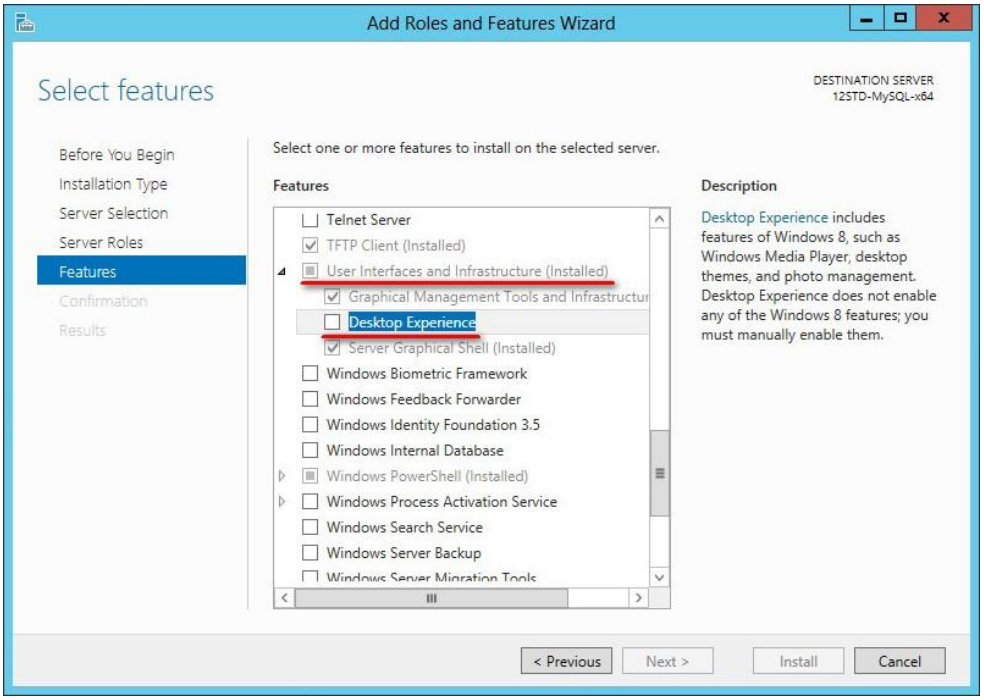
4. Roles領域のすべてのオプションをクリアし、Nextをクリックします(図59を参照)。

図59 Select server roles



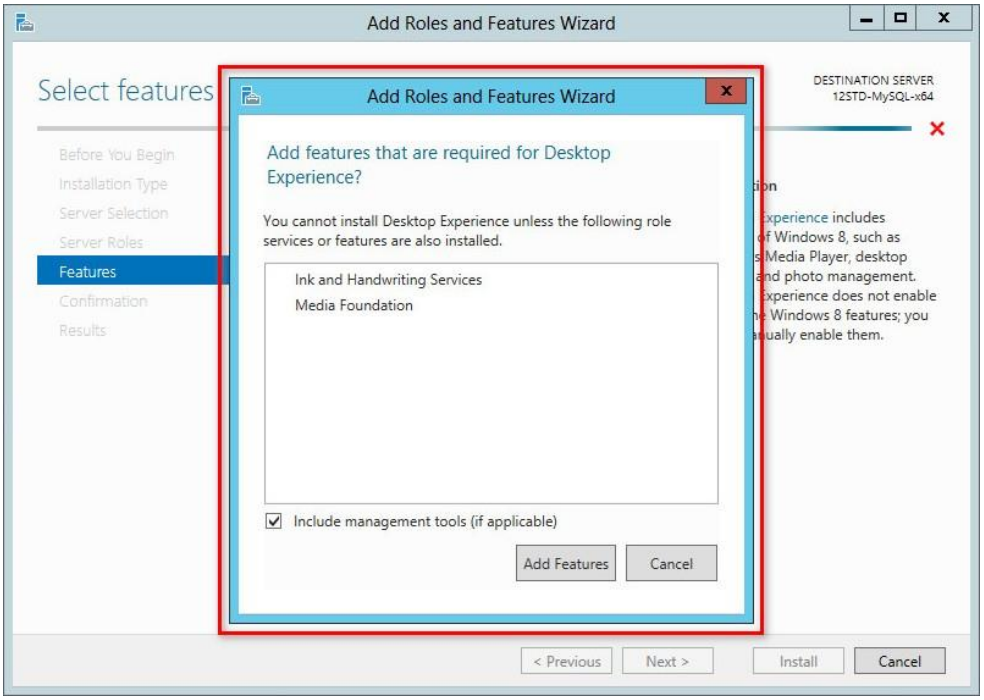
5. 図60に示すように、User InterfaceとInfrastructureおよびDesktop Experienceを選択し、Nextをクリックします。

図60 Select features



6. 図61に示すように、表示されたダイアログボックスでAdd Featuresをクリックします。ダイアログボックスが閉じます。

図61 Add Roles and Features Wizard

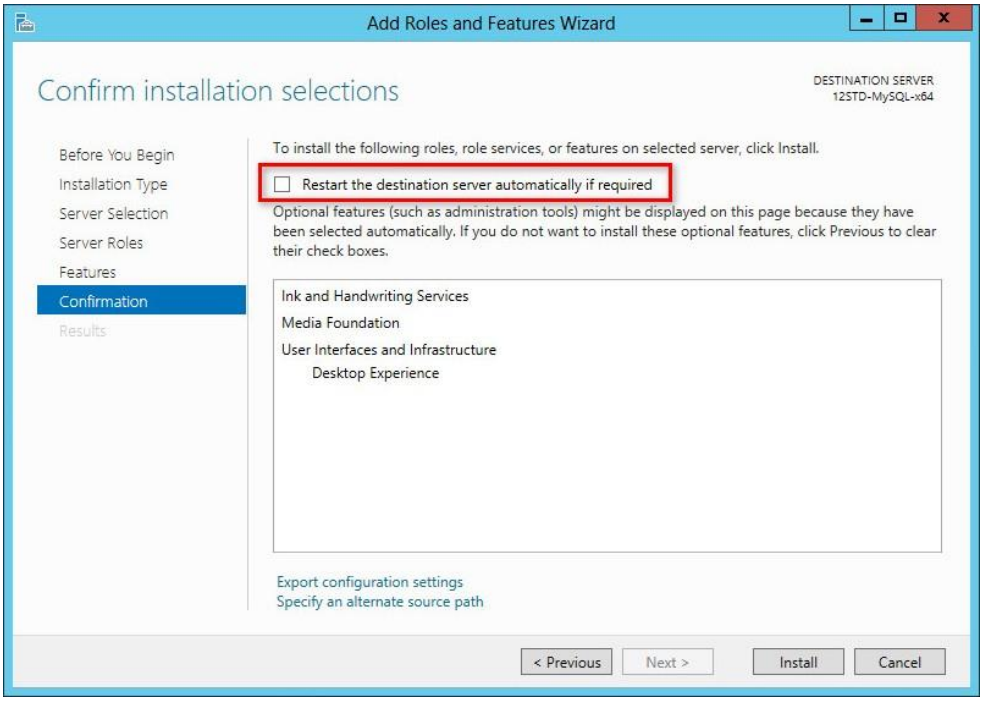


7. Nextをクリックします。

必要に応じて、Restart the destination server automatically if requiredを選択し、図62に示すように、installをクリックします。

このページにはインストールプロセスが表示されます。

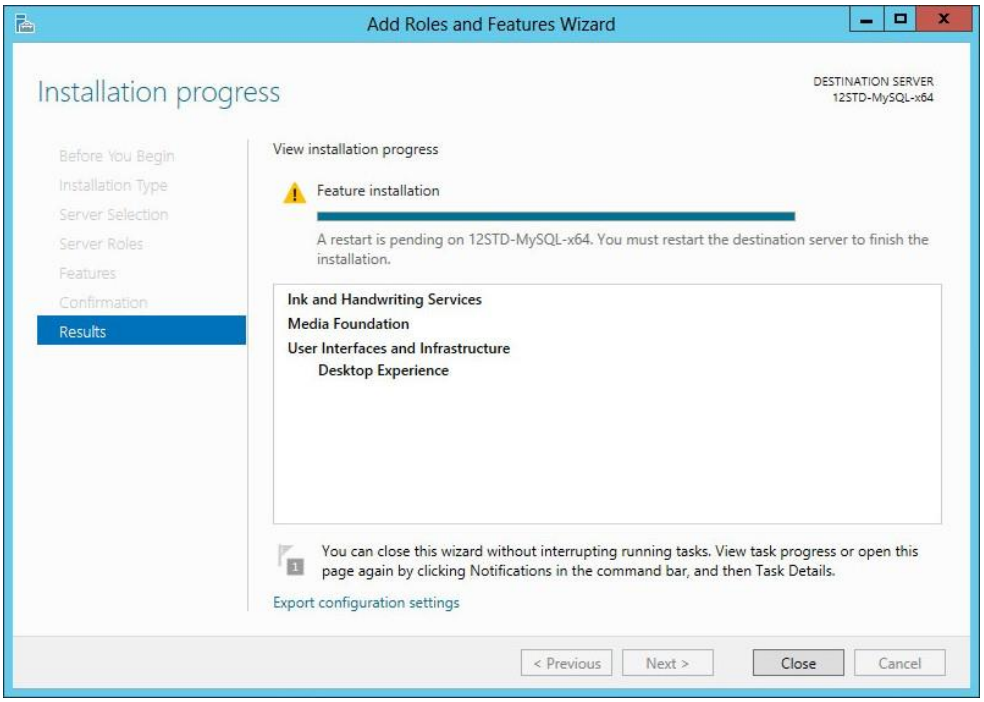
図62 Confirm installation selections



8. インストールが完了したら、図63に示すようにCloseをクリックします。

デスクトップエクスペリエンス機能は、サーバーが自動的に再起動した後、またはサーバーを手動で再起動したときに有効になります。

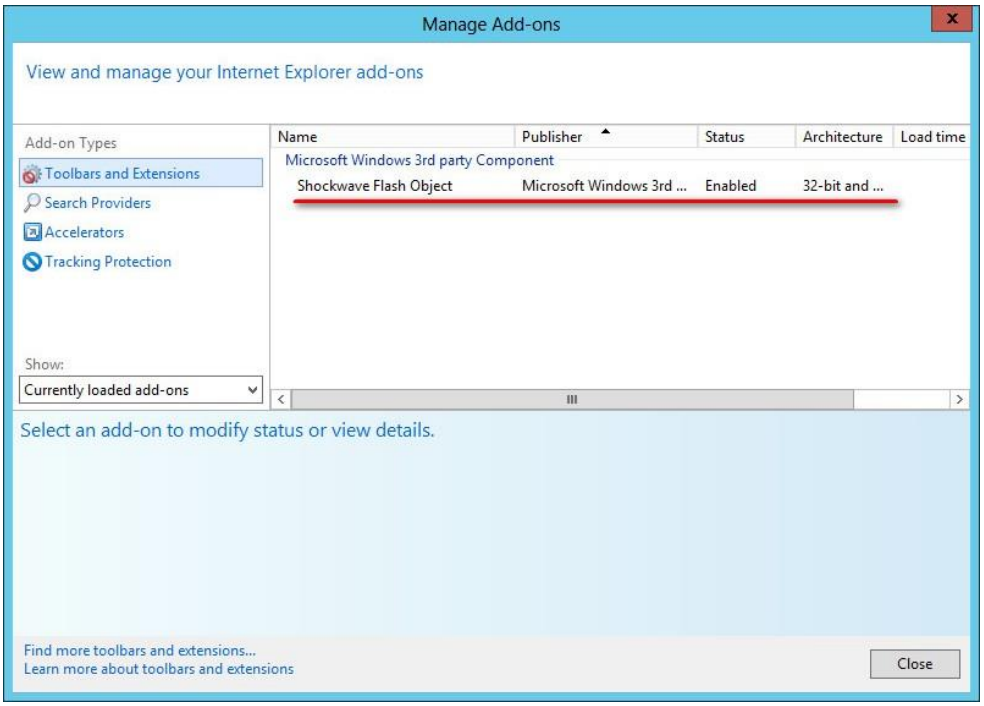
図63 Installation progress



9. サーバーの再起動後、IE10.0を使用して、Flashプラグインを必要とするiMCページにアクセスし、IE10.0アドオンを表示します。

図64に示すように、されており、有効になっています(図64を参照)。

図64 IE10.0 Add-ons



adminアカウントのパスワードを忘れてしまいました。どうすればリセットできますか?

1. Windowsでは、iMCのインストールパスで**\client\bin\resetpwd.bat**を実行します。Linuxでは、iMCのインストールパスで**/client/bin/resetpwd.sh**を実行します。この操作により、adminアカウントのパスワードがadminにリセットされます。
2. adminアカウントとパスワードadminでIMCにログインします。
3. adminアカウントの新しいパスワードを設定します。

HTTPS経由でiMCにアクセスする場合、TLSプロトコルだけをイネーブルにし、SSLv3プロトコルをシールドするにはどうすればよいですか。

そのためには、次の手順を実行します。

1. iMCインストールパス\client\conf\server.xmlファイルを開きます。
2. "<!-- HTTPS connector -->"の下の"<Connector…"を見つけ、属性"sslProtocol="TLS""の後ろに新しい属性"sslEnabledProtocols="TLSv1,TLSv1.1,TLSv1.2""を追加します。
3. ファイルを保存します。
4. jserverプロセスを再起動します。

ドメイン名を使用してiMCにアクセスするにはどうすればよいですか。

1. iMCインストールパスのファイル\client\conf\http.propertiesをバックアップします。
2. テキストエディタを使用してiMCインストールパスのファイルclient\conf\http.propertiesを開き、図65に示すようにHTTPポートを8080から80に変更します。
3. ファイルを保存し、jserverプロセスを再起動します。
4. DNSサーバー上のiMCサーバーのドメイン名とIPアドレスのマッピングを設定します。

図65 HTTPポート構成ファイル