



IBM Fabric Manager バージョン 4.1

BOFM 環境からの移行ガイド

2015 年 5 月 初版

発行： レノボ・エンタープライズ・ソリューションズ株式会社

担当： 部署名を入力

Microsoft、WindowsおよびWindowsロゴは、Microsoft Corporationの米国およびその他の国における商標です。

Intel、Xeonは、Intel Corporationの米国およびその他の国における商標です。

他の会社名、製品名、およびサービス名等はそれぞれ各社の商標または登録商標です。

お願い

本書に記載されている情報とそれに対応する製品をご使用になる前に、「本書をご利用になる前に」の事項を必ずご確認ください。

本書をご利用になる前に

当内容は、お客様、販売店様、その他関係者が、System x, Flex Systemなどを活用することを目的として作成しました。

詳細につきましては、URL (<http://www.lenovo.com/legal/jp/ja/>)の利用条件をご参照ください。

当技術資料に含まれるレノボ・エンタープライズ・ソリューションズ株式会社およびLenovo Enterprise Solutions (以下総称して、LES) 以外の製品に関する情報は、各提供ベンダーより提供されたものであり、LESはその正確性または完全性についてはいかなる責任も負いません。

当技術資料の個々の項目は、LESにて検証されていますが、お客様の環境において全く同一または同様な結果が得られる保証はありません。お客様の環境、その他の要因によって異なる場合があります。お客様自身の環境にこれらの技術を適用される場合は、お客様自身の責任と費用において行なってくださいますようお願いいたします。

Copyright 2015 レノボ・エンタープライズ・ソリューションズ株式会社

目次

お願い.....	3
本書をご利用になる前に	4
目次	5
要約	9
1. IBM Fabric Manager とは.....	10
1.1. サポート要件.....	10
1.2. IFM ライセンス	11
2. 移行時の注意事項	12
2.1. BOFM 3.x 使用時の注意事項	13
2.2. BOFM 4.x 使用時の注意事項	13
3. 事前準備.....	14
3.1. 移行方法の検討	14
3.2. AMM 構成情報の確認.....	14
3.2.1. TCP Command Mode 構成情報の確認	15
3.2.2. SNMP Trap 構成情報の確認.....	16
3.3. 構成ファイル (bofm.csv) のダウンロード.....	19

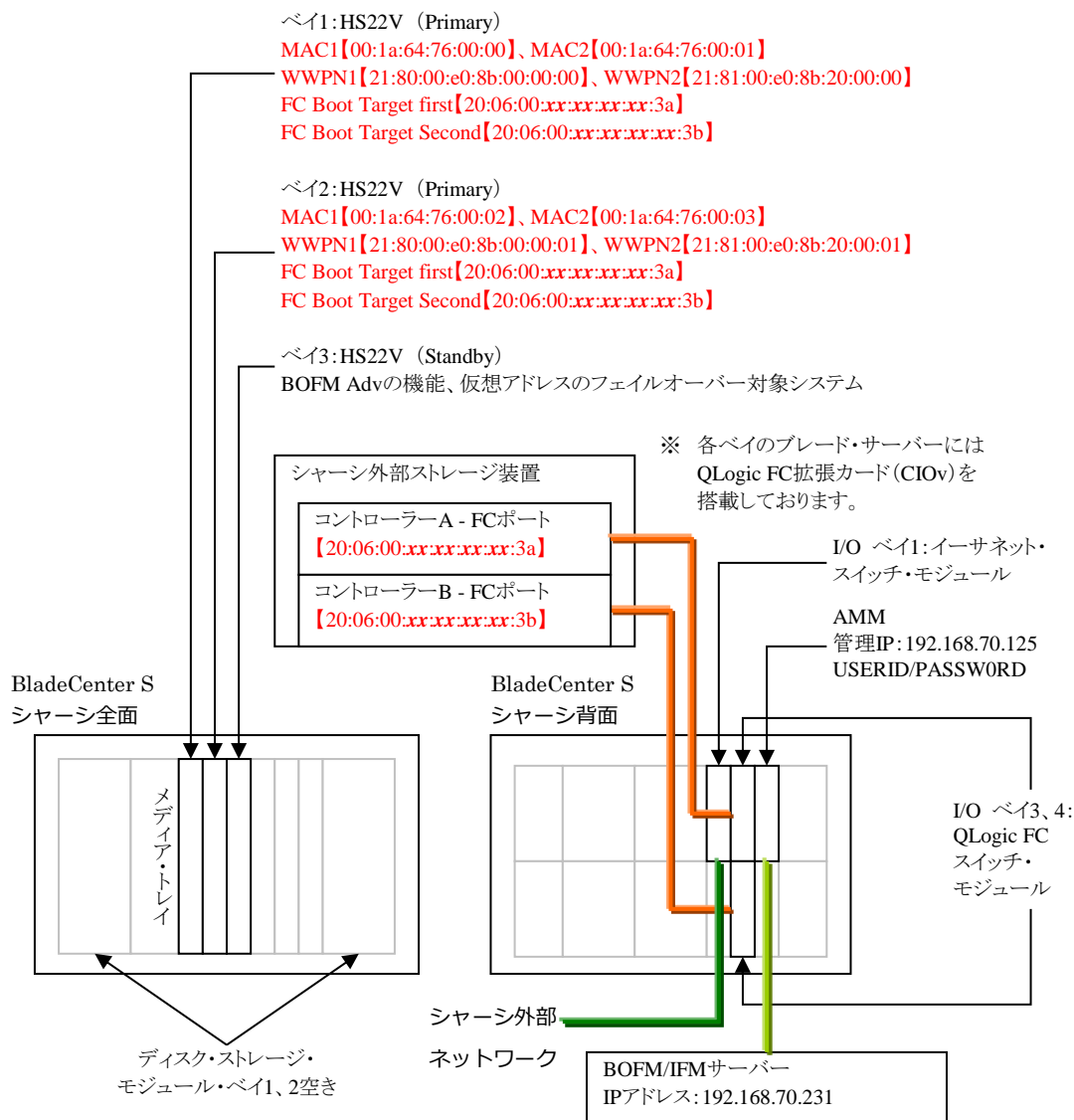
3.4.	仮想アドレスのフェイルオーバー設定確認	22
3.4.1.	BOFM 3.x を使用している場合	23
3.4.2.	BOFM 4.1 を使用している場合	24
4.	BOFM Advanced のアンインストール	27
4.1.	BOFM 3.x Advanced のアンインストール	27
4.2.	BOFM 4.1 Advanced のアンインストール	29
4.2.1.	BOFM 4.1 Advanced のアンインストール	29
4.2.2.	BOFM 4.1 Advanced 「C:\yofm」 フォルダの削除	30
5.	IFM のインストールと初期設定	31
5.1.	IFM インストール前の確認事項	31
5.1.1.	IFM ライセンスの確認	31
5.1.2.	AMM 構成情報のバックアップ	31
5.1.3.	ファームウェアの更新	31
5.1.4.	IFM をインストールするシステムの Java 確認	31
5.1.5.	IFM をインストールするシステムのファイアウォール確認	31
5.2.	IFM 4.1 のインストール	32
5.3.	IFM サービスの開始	34
5.4.	IFM SNMP trap 設定の変更	34
5.5.	IFM Web インターフェースへのログイン	35
5.6.	初回ログイン時のパスワード変更	36

5.7.	ハードウェア・デバイス（シャーシ）を追加	36
5.8.	プライマリー・ハードウェア・プール（仮想アドレスの適用範囲）を追加	38
6.	IFM にて現在の BOFM 構成を AMM から取り込む移行手順	41
6.1.	ハードウェア・プールの確認	41
6.2.	ハードウェア・プールで使用されている仮想アドレス設定をデプロイメントに取り込む	42
6.3.	デプロイメント（仮想アドレス設定）の確認	43
7.	現在の BOFM 構成を元に IFM にて構成を作成する移行手順	46
7.1.	ハードウェア・プールの確認	46
7.2.	アドレス・プールの追加	47
7.2.1.	イーサネット・プールの追加	47
7.2.2.	ファイバーチャネル・プールの追加	49
7.2.3.	SAS プールの追加	53
7.3.	テンプレートの追加	55
7.3.1.	ブート・ターゲット・テンプレートの追加	55
7.3.2.	シャーシ・テンプレートの追加	57
7.3.3.	vNIC テンプレートの追加	60
7.4.	仮想アドレスを適用するためのプロファイル作成とデプロイメント	61
7.4.1.	プロファイルの作成	61
7.4.2.	プロファイルのデプロイメント	62

7.5. デプロイ後の仮想アドレスをブレード・サーバーに適用	63
7.5.1. デプロイメント内容の確認	63
8. 仮想アドレスをブレード・サーバーへ適用（デプロイメントのプッシュ）	71
9. フェイル・オーバー・モニター（仮想アドレスのフェイルオーバー）設定.....	74
9.1. プライマリー・ハードウェア・プールの確認	74
9.2. スタンバイ・ハードウェア・プールの追加.....	75
9.3. フェイルオーバー・モニターの追加.....	76
9.4. フェイルオーバー・モニターの開始.....	77
10. 参考資料.....	78

要約

当ガイドでは次の構成および設定を使用して、BOFMからIFM 4.0への移行手順を説明しております。



活用局面:	<input type="checkbox"/> 提案時	<input checked="" type="checkbox"/> 構築時	<input type="checkbox"/> 運用時
情報:	<input type="checkbox"/> Marketing	<input checked="" type="checkbox"/> Technical	
シリーズ:	<input checked="" type="checkbox"/> 単発	<input type="checkbox"/> 定期発行	
対象機種:	<input type="checkbox"/> 全機種	<input type="checkbox"/> 特定機種	

1. IBM Fabric Manager とは

BladeCenter 用Fabric Manager ソフトウェアは、ワールド・ワイド・ネーム(World Wide Name, WWN)およびメディア・アクセス・コントロール(Media Access Control, MAC)アドレスなどのネットワーク・パラメーターを仮想化することで、入出力およびネットワーク相互接続を簡単に管理できるように設計されています。コンピュータ・ノード、または置き換えられたコンピュータ・ノードにフェイルオーバーしても、管理下のLANおよびSAN構成は影響を受けません。当製品は、以前からご利用いただいているBladeCenter Open Fabric Manager Basic およびBladeCenter Open Fabric Manager Advanced の後継製品です。

BladeCenter 用のIBM Fabric Manager を導入することで、LAN およびSAN 接続を事前に構成することができます。コンピュータ・ノードがシャーシ内のスロットに挿入されるとI/O 接続が自動的に行われます。特別なツールやトレーニングの必要がなく、使いやすいWebベースのユーザー・インターフェースを持つ管理プログラムです。

IBM Fabric Manager ソフトウェアにより、以下の利点を得ることができます。

時間の節約	各々のブレード・サーバーに対して、1,400 を超えるLAN やSAN 接続を一括して事前に構成することができます。
管理の単純化	単一のIBM Fabric Manager のユーザー・インターフェースを用いて、機器の拡大や、それに伴う複雑さを低減するよう管理できます。
柔軟性	IBM Fabric Manager はイーサネットやファイバー・チャネル、SAS スイッチ・モジュールに対して対応できます。
操作が容易	ユーザー・インターフェースはプロファイルをベースに使用でき、簡単にセットアップや展開、管理を行うことができます。
リスクの低減	待機しているコンピュータ・ノードへのI/Oフェイルオーバーにより、ビジネス継続性を高め、リスクを低減することができます。また、IBM Fabric Manager サーバーは冗長構成とすることができます。
単一化構成	BladeCenter Open Fabric Manager Basic の機能とAdvanced 版の機能を、より簡単に使える単一の製品にまとめられており、Basic 版にもAdvanced 版にも対応しています。

IBM Fabric Manager

http://pic.dhe.ibm.com/infocenter/flexsys/information/topic/com.ibm.acc.iofm.doc/dw1li_product_page.html

本ガイドでは、IBM Fabric Manager (以降、IFM) の導入と基本的な設定手順を前提でご説明します。

1.1. サポート要件

IFM の導入サポートOS、IFM の動作要件、IFM サポート・ハードウェアは以下のガイド、および、Readme ファイルを参照ください。

BladeCenter Interoperability Guide (BIG) - IBM BladeCenter

<http://www.ibm.com/support/entry/portal/docdisplay?brand=5000020&Indocid=MIGR-5073016>

IBM Fabric Manager (インフォメーション・センター)

http://pic.dhe.ibm.com/infocenter/flexsys/information/topic/com.ibm.acc.iofm.doc/dw1li_product_page.html

1.2. IFM ライセンス

既にBOFM のライセンスを購入済みの場合でも、IBM Fabric Manager のライセンスを購入する必要があります。購入可能なライセンスに関しては以下の発表レターを参照ください。

IBM Fabric Manager Standalone Application for BladeCenter の発表

http://www.ibm.com/common/ssi/ShowDoc.wss?docURL=/common/ssi/rep_ca/1/760/PCS12381/index.html&lang=ja&request_locale=ja

入手したライセンス証書をご用意いただき、Features on Demand サイトにてアクティベーション・キーを入手します。

Features on Demand

<http://www.ibm.com/systems/x/fod/>

FoDサイトでのアクティベーション・キーの入手手順に関しましては下記のサイトを参照ください。

IBM Feature on Demand (FOD) ライセンス・アクティベーション・ガイド

<http://www.ibm.com/jp/domino04/pc/support/Sylphd07.nsf/jtechinfo/SYJ0-03B4811>

2. 移行時の注意事項

IFM 4.1では、AMMのファームウェア・バージョンBPET64G以降をサポートします。(最新のIFMでサポートするAMMのファームウェア・バージョンに関しましてはダウンロード・パッケージに含まれる `ibm_ifm_vXX_chg_hist.chg` (XXはバージョンにより異なります)を確認してください)
そのため、AMM のファームウェアがIFMの要件を満たしていない場合、Fix Centralサイトより、AMMのファームウェアをダウンロードし、適用してください。(Fix Central からのダウンロードにはIBM IDでのログインが必要です)

Fix Central

<http://www.ibm.com/support/fixcentral/>

※ ファームウェアにつきましては、ダウンロード時点での最新バージョンを適用することを推奨いたします。

IFM コンソールを起動するには、Web ブラウザーからSSL 接続を行います。

[https://\(IFM サーバーのIPアドレス\):8044/](https://(IFMサーバーのIPアドレス):8044/)

または、[https://\(IFMサーバーのホスト名\):8044/](https://(IFMサーバーのホスト名):8044/)

IFM サーバーへの初回ログインには、以下のデフォルト・ユーザー名とパスワードを使用します。

ユーザー名:USERID

パスワード:PASSWORD (0は数字のゼロ) (初回ログイン後、変更する必要あり)

BOFM Basic にて使用していた設定情報(CSV ファイル)を直接IFM にインポートすることができませんので、事前にAMM よりCSV ファイルをダウンロードしておきます。

IFM の設定を行う際には、事前にダウンロードしたCSVファイルの内容を元に仮想アドレスの設定を行います。

AMM ではSNMP trap の通知先ポート番号を一つしか設定できないため、IFM を使用する環境におきまして、他のアプリケーションでもAMM をSNMP 監視する場合にはご注意ください。

BOFM Basic のみ使用されている場合でも、IFM のライセンスを購入する必要があります。

BOFM Basic のみ使用されている環境から、IFM 環境へ移行する場合には、IFM サーバーをインストールするサーバーが別途必要となります。

BOFM で使用していたライセンス・キーはそのまま使用することができますが、IFM のライセンスは別途購入する必要があります。

2.1. BOFM 3.x 使用時の注意事項

IBM Systems Director サーバーにて設定していたBOFM 関連のイベント自動化プランは削除します。

BOFM 3.x Advanced アンインストールの際は、IBM Systems Director サーバーが停止します。アンインストール終了後、システムの再起動が自動的に行われる場合があります（再起動が自動的に行われない場合は、手動でシステムを再起動してください）。システム再起動後、IBM Systems Director サーバーが起動するまで、IBM Systems Director サーバーを使用した管理・監視を行うことはできません。

IFM はIBM Systems Director と連携せずにAMM からSNMP trap で受け取ったHWイベントをトリガーにフェイルオーバーを行います。SNMP trap を受け取るためにIFM で使用しているポート番号は50990（デフォルト値）となります。ファイアーウォールが設置されている環境では50990ポートを開ける必要があります。

フェイルオーバー設定にて指定可能なトリガー・イベントは以下の項目となります。

トリガー・イベント(Triggering events)

Power off	サーバーの電源がオフになっているときに検出したとき
CPU failure	CPUハードウェア障害を検出したとき
Memory failure	メモリハードウェア障害を検出したとき
No power	電源障害時に検出します。
PFA	事前障害分析は、差し迫った障害を検出し、それ以上の損傷を防ぐために、サーバーをシャットダウンするとき
Removal	サーバーがシャーシから物理的に除かれたとき
Hard drive failure	ハードディスクドライブの障害を検出したとき
Communication error	AMMとブレードサーバー上のシステム管理プロセッサの通信障害のとき
Voltage warning	異常な電圧のとき

2.2. BOFM 4.x 使用時の注意事項

BOFM 4.xで使用中のAddress Manager Template、Standby Pool Template、Failover Monitorsの各構成内容は、自動的にIFMへ引き継がれません。

BOFM 4.xで作成したバックアップはIFMに使用できません。

3. 事前準備

3.1. 移行方法の検討

BOFM環境をIFMに移行するには次の2通りの手順があります。それぞれのメリット、デメリットをご確認の上で移行方法を確定してください。

- IFM にて現在の BOFM 構成を AMM から取り込む。
現在の構成を継続して使用するので移行作業時の設定ミスによるトラブルを軽減できます。また、短時間で移行作業を完了できます。
IFM で仮想アドレスの構成に必要な各テンプレートを作成しないので、将来の構成変更が必要となった時には IFM から行えません。
仮想アドレスの構成は従来の BOFM Basic と同じ手順で行い、仮想アドレスのフェイルオーバー・モニターを IFM で行います。
- 現在の BOFM 構成を元に IFM にて構成を作成する。
IFM の構成に必要な各テンプレートから作成するため、将来の構成変更時に対応が容易です。
手作業で現在の構成を IFM に移行するため、作業時の設定ミスによるトラブルが発生する場合があります。また、移行作業に時間がかかります。
仮想アドレスの構成やフェイルオーバー・モニターは IFM で行います。

3.2. AMM 構成情報の確認

IFMで仮想アドレスの管理を行うために必要となるAMMの構成情報を確認します。

BOFM Basicの機能(仮想アドレスの管理)のみ移行する場合に設定または確認する項目と、当ガイドにて使用している値は次の通りです。

管理IPアドレス	192.168.70.125
管理ユーザー名	USERID
管理ユーザー・パスワード	PASSWORD (0は数字のゼロ)
TCP Command Mode ポート	6090
TCP Command Mode Protocol	Command modeを20に設定

※ これらの項目はIFMヘッシャーを登録するために必須の項目です。

BOFM Advancedの仮想アドレス・フェイルオーバー機能を使用する場合に設定または確認が必要な項目と、当ガイドにて使用している値は次の通りです。

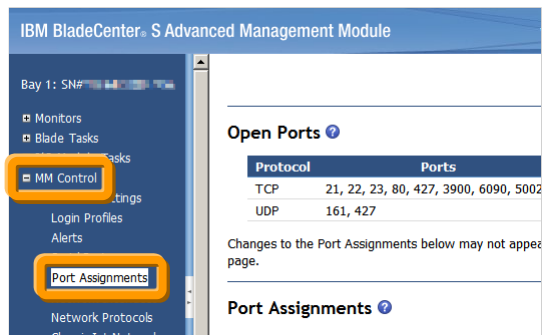
SNMP Trap ポート	50990
SNMP Trap 設定	有効
SNMP v1 agent	有効
Community name	trap
Access Type	Get
Fully Qualified Hostnames or IP Addresses	IFMサーバーのホスト名またはIPアドレス
Remote Alert Recipients	SNMP over LANを設定
Monitored Alerts	<input checked="" type="checkbox"/> Critical Alerts <input checked="" type="checkbox"/> Warning Alerts <input checked="" type="checkbox"/> Informational Alerts

※ 仮想アドレスのフェイルオーバー機能を使用する場合に必要となります。

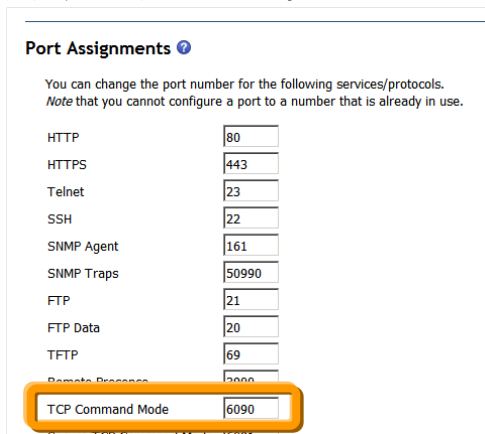
各項目は次からの手順を参考に確認し、必要な場合には設定を行ってください。

3.2.1. TCP Command Mode 構成情報の確認

1. AMM Web インターフェイスにログイン後、画面左側にある「MM Control」の「Port Assignments」を選択します。

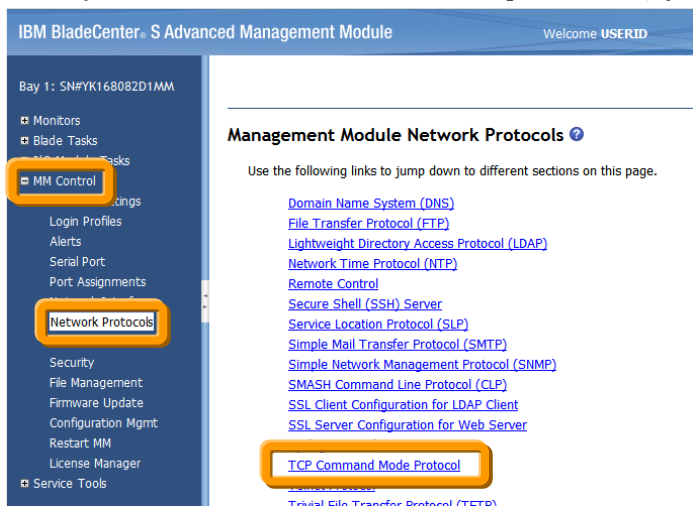


2. 画面右側に表示された一覧から「TCP Command Mode」の値(ポート番号)を確認します。

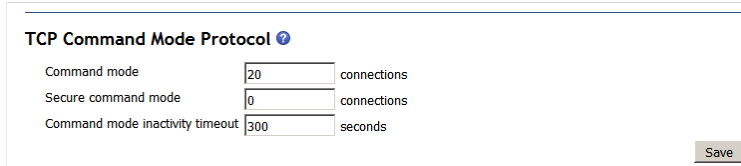


当ガイドでは AMM のデフォルト値:6090 を使用します。異なる値を設定している場合には IFM 登録時に指定可能です。

3. AMM Web インターフェイス画面左側にある「MM Control」の「Network Protocols」を選択後、画面右側の一覧から「TCP Command Mode Protocol」を選択します。



4. 「TCP Command Mode Protocol」の「Command mode」の値(セッション数)を確認します。



TCP Command Mode Protocol

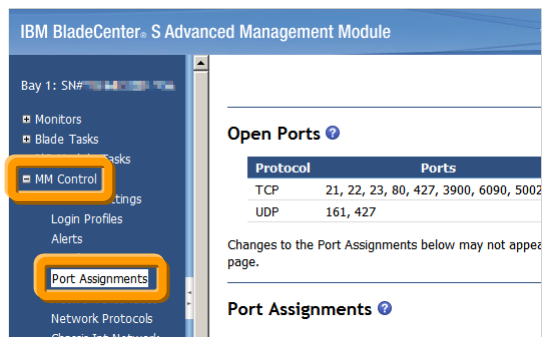
Command mode	20	connections
Secure command mode	0	connections
Command mode inactivity timeout	300	seconds

Save

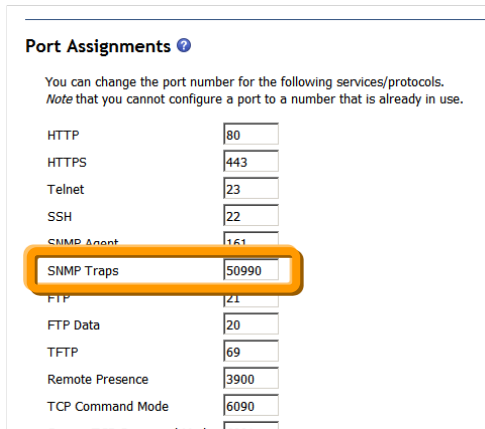
当ガイドでは BOFM Advanced 4.1 で設定される 20 を使用します。AMM のデフォルト値は 1 です。必要に応じて 5～20 の範囲で設定してください。

3.2.2. SNMP Trap 構成情報の確認

1. AMM Web インターフェースにログイン後、画面左側にある「MM Control」の「Port Assignments」を選択します。



2. 画面右側に表示された一覧から「SNMP Traps」の値(ポート番号)を確認します。



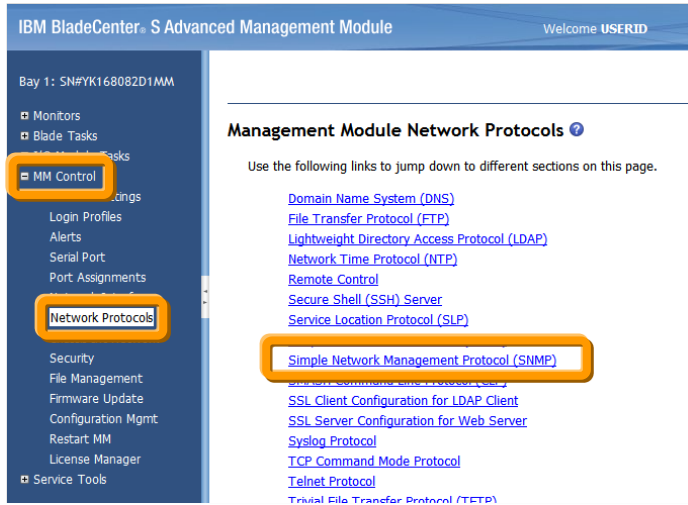
Port Assignments

You can change the port number for the following services/protocols.
Note that you cannot configure a port to a number that is already in use.

HTTP	80
HTTPS	443
Telnet	23
SSH	22
SNMP Agent	161
SNMP Traps	50990
FTP	21
FTP Data	20
TFTP	69
Remote Presence	3900
TCP Command Mode	6090
Secure TCP Command Mode	6001

当ガイドでは BOFM Advanced 4.1 で設定される 50990 (IFM デフォルト値) を使用します。AMM のデフォルト値は 162 です。異なる値を設定している場合には IFM 起動前に変更可能です。

3. AMM Web インターフェース画面左側にある「MM Control」の「Network Protocols」を選択後、画面右側の一覧から「Simple Network Management Protocol (SNMP)」を選択します。



4. 「Simple Network Management Protocol (SNMP)」の「SNMP traps」が「Enabled」、「SNMPv1 agent」が「Enable」、IFM サーバー宛の SNMPv1 trap 設定が行われていることを確認します。

Simple Network Management Protocol (SNMP)

SNMP traps* Enabled

* If you enabled SNMP traps, you must also define an alert recipient from the Alerts page, and one of the SNMP agents, below, must be enabled and configured.

SNMPv1 agent† Enabled

† If you enabled the SNMPv1 agent, you must also define at least one community below.

Community Name	Access Type	Fully Qualified Hostnames or IP Addresses
1. public	Get	1. 0.0.0.0
2.	Get	1.
3. trap	Get	1. 192.168.70.231
4.	Get	1.
5.	Get	1.

‡ The value 0.0.0.0 is not a valid trap destination IP address, so it is ignored for sending traps. One of the remaining IP addresses of that community may be configured with an explicit trap destination IP address.

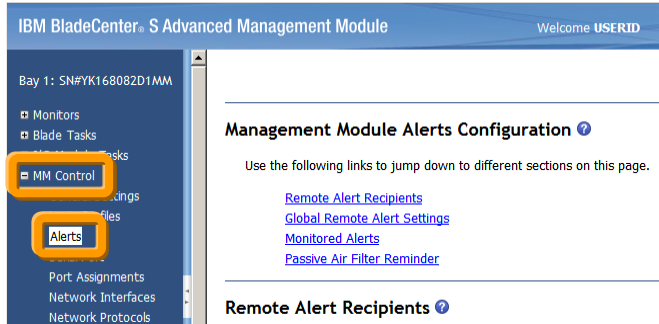
SNMPv3 agent§ Disabled

§ If you enabled the SNMPv3 agent, you must configure SNMPv3 settings for active login profiles in order for the interaction between the SNMPv3 manager and SNMPv3 agent to work properly. You can configure these settings at the bottom of the individual login profile pages which can be reached via the Login Profiles page. Click the link for the login profile to configure, scroll to the bottom of the page and then click the "Configure SNMPv3 User" link.

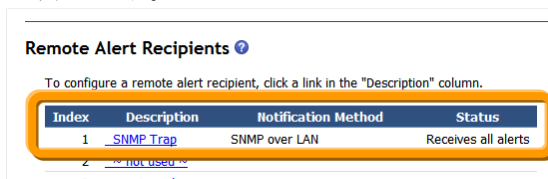
Save

当ガイドでは 3 番目の Community Name に BOFM 4.1 で使用される「trap」、IFM サーバーの IP アドレス: 192.168.70.231 を設定しています。

5. AMM Web インターフェース画面左側にある「MM Control」の「Alerts」を選択します。



6. 画面右側の「Remote Alert Resipients」に「SNMP over LAN」の設定が作成済みで有効に設定あることを確認します。



「SNMP over LAN」の設定が作成されていない場合は「Description」に表示されている一覧の「~ not used ~」をクリックして作成してください。

「SNMP over LAN」の設定が有効であることを確認するには「SNMP over LAN」の「Description」に表示されている名前をクリックし、「Status」欄が「Enabled」であることを確認します。

Remote Alert Recipient 1

1. If you enable a SNMP over LAN recipient, you also need to complete the SNMP section on the [Network Protocols](#) page.
2. If you enable an E-mail over LAN recipient, you also need to complete the SMTP section on the [Network Protocols](#) page.

By entering an email or SNMP address not assigned to your company, you are consenting to share hardware serviceable events and data with the owner of that email or SNMP address not assigned to your company. In sharing this information, you warrant that you are in compliance with all import/export laws.

Status:

Name:

Notification method:

Receives critical alerts only: ☐

7. 「MM Control」の「Alerts」選択後、画面右側を下方へスクロールし、「Monitored Alerts」の「Critical Alerts」、「Warning Alerts」、「Informational Alerts」のチェック・ボックスがオンにして「Save」ボタンをクリックします。

	<input checked="" type="checkbox"/> Critical Alerts	<input checked="" type="checkbox"/> Warning Alerts	<input checked="" type="checkbox"/> Informational Alerts
Chassis/System Management	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Cooling Devices	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Power Modules	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Blades	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
I/O Modules	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Storage Modules	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Event Log		<input checked="" type="checkbox"/>	
Power On/Off			<input checked="" type="checkbox"/>
Inventory change			<input checked="" type="checkbox"/>
Network change			<input checked="" type="checkbox"/>
User activity			<input checked="" type="checkbox"/>

BOFM Advanced 4.1 の設定では「Blades」の「Critical Alerts」、「Warning Alerts」、「Informational Alerts」と、「Power On/Off」の「Informational Alerts」チェック・ボックスのみオンになっていますが、当ガイドでは IFM ユーザーズ・ガイドの記述に従い「Monitored Alerts」の「Critical Alerts」、「Warning Alerts」、「Informational Alerts」のチェック・ボックスすべてオンにします。

3.3. 構成ファイル (bofm.csv) のダウンロード

AMMから現在使用中のBOFM構成ファイル「bofm.csv」をダウンロードします。ここでダウンロードしたファイルはBOFM構成のバックアップとなります。また、IFMにて新規に作成する各テンプレートのベースとなります。

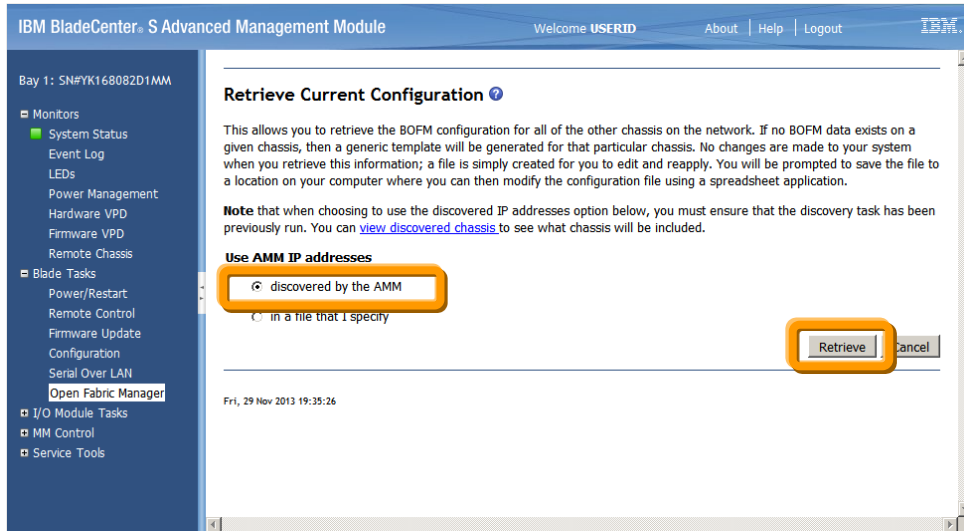
この構成ファイルにはフェイルオーバー・モニターの構成が含まれておりませんので、BOFM Advanced を使用中の場合には、別途IFMにて構成を行う必要がある点にご注意ください。

BOFM Basicのみを使用している場合には、この構成ファイルだけでIFMに移行することができます。

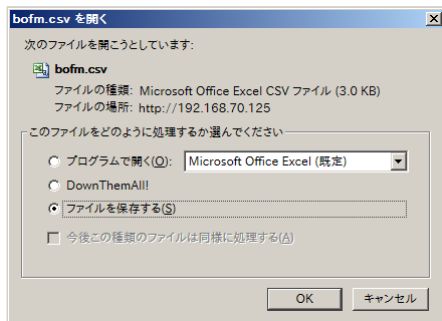
構成ファイルのダウンロードは次からの手順で行います。

1. AMM の Web インターフェースにログイン後、画面左側のナビゲーション・エリアより「Blade Tasks」-「Open Fabric Manager」をクリックし、「Open Fabric Manager Configuration Management」画面表示後、「Retrieve the Current Configuration」をクリックします。

2. 「Retrieve Current Configuration」画面表示後、「discovered by the AMM」が選択されていることを確認し、「Retrieve」をクリックします。

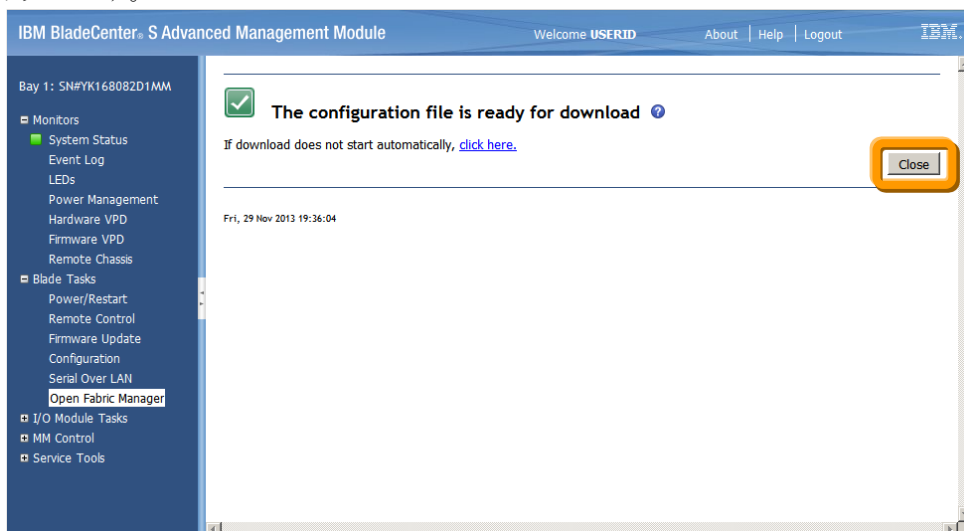


3. 「bofm.csv」ファイルに対する操作選択画面が表示されますので、必要な場合にはファイル名を変更し、任意の場所に保存してください。



(画面は Firefox での操作例です)

4. 「bofm.csv」ファイルの保存完了後、「The configuration file is ready for download」画面にて「Close」をクリックします。



(保存に失敗した場合など、「click here」から再度保存処理を実行できます。)

5. AMM の Web インターフェースからログアウトします。

当ガイドの環境にて保存した「bofm.csv」ファイルの内容は次の通りです。

```
// EXTRACTED FILE STARTS

// Blade Center 192.168.70.125
//IP          Type (Center) Mode
192.168.70.125 BladeCenter  apply

//IP          Type(Slot)  Slot  Mode  Profile
192.168.70.125 Slot          1  enable  Primary

//IP          Type      Slot  Offset  Port          MAC_1          VLAN1          MAC_2          VLAN2
192.168.70.125 Ethernet  1      0          1 00:1a:64:76:00:00      0
192.168.70.125 Ethernet  1      0          2 00:1a:64:76:00:01      0

//IP          Type      Slot  Priority WWPN          LUN
192.168.70.125 FCTarget  1  first  20:06:00:xx:xx:xx:3a      0
192.168.70.125 FCTarget  1  second 20:06:00:xx:xx:xx:3b      0

//IP          Type      Slot  Offset  Port          WWNN          WWPN          Boot-order
192.168.70.125 FC          1      0          3          21:80:00:e0:8b:00:00:00  first
192.168.70.125 FC          1      0          4          21:81:00:e0:8b:20:00:00  second

//IP          Type(Slot)  Slot  Mode  Profile
192.168.70.125 Slot          2  enable  Primary

//IP          Type      Slot  Offset  Port          MAC_1          VLAN1          MAC_2          VLAN2
192.168.70.125 Ethernet  2      0          1 00:1a:64:76:00:02      0
192.168.70.125 Ethernet  2      0          2 00:1a:64:76:00:03      0

//IP          Type      Slot  Priority WWPN          LUN
192.168.70.125 FCTarget  2  first  20:06:00:xx:xx:xx:3a      0
192.168.70.125 FCTarget  2  second 20:06:00:xx:xx:xx:3b      0

//IP          Type      Slot  Offset  Port          WWNN          WWPN          Boot-order
192.168.70.125 FC          2      0          3          21:80:00:e0:8b:00:00:01  first
192.168.70.125 FC          2      0          4          21:81:00:e0:8b:20:00:01  second

//IP          Type(Slot)  Slot  Mode  Profile
192.168.70.125 Slot          3  disable  Profile: 192.168.70.125 Slot-3

//IP          Type(Slot)  Slot  Mode  Profile
192.168.70.125 Slot          4  disable  Profile: 192.168.70.125 Slot-4

//IP          Type(Slot)  Slot  Mode  Profile
192.168.70.125 Slot          5  disable  Profile: 192.168.70.125 Slot-5

//IP          Type(Slot)  Slot  Mode  Profile
192.168.70.125 Slot          6  disable  Profile: 192.168.70.125 Slot-6

// EXTRACTED FILE ENDS
```

※ 各項目や値に関しましては、ご利用の環境により異なる点にご注意ください。

3.4. 仮想アドレスのフェイルオーバー設定確認

BOFM Basicの機能でIFMを使用する(仮想アドレスのフェイルオーバーを使用しない)場合には、こちらの手順を行う必要はありません。

BOFM Advancedを使用している場合、仮想アドレスのフェイルオーバーを実行するトリガーとなるイベント、フェイルオーバーの監視対象システム、フェイルオーバー先のシステム、フェイルオーバーの動作条件を確認します。

当ガイドでは次の構成で仮想アドレスのフェイルオーバーを移行します。

仮想アドレス・フェイルオーバー監視対象システム (仮想アドレスが適用されているシステムが前提です。)	<input checked="" type="checkbox"/> ベイ1 (slot1) <input checked="" type="checkbox"/> ベイ2 (slot2) <input type="checkbox"/> ベイ3 (slot3) <input type="checkbox"/> ベイ4 (slot4) <input type="checkbox"/> ベイ5 (slot5) <input type="checkbox"/> ベイ6 (slot6)
仮想アドレス・フェイルオーバー・システム (仮想アドレスが適用されていないシステムが前提です。)	<input type="checkbox"/> ベイ1 (slot1) <input type="checkbox"/> ベイ2 (slot2) <input checked="" type="checkbox"/> ベイ3 (slot3) <input type="checkbox"/> ベイ4 (slot4) <input type="checkbox"/> ベイ5 (slot5) <input type="checkbox"/> ベイ6 (slot6)
仮想アドレス・フェイルオーバー動作条件 (フェイルオーバー実行時のオプションです。)	<input type="checkbox"/> Ignore model
	<input type="checkbox"/> Ignore type
	<input type="checkbox"/> Ignore width
	<input type="checkbox"/> Ignore power state
	<input type="checkbox"/> Ignore partition
	<input type="checkbox"/> Failover VLAN
仮想アドレス・フェイルオーバー・トリガー・イベント (選択したイベントが監視対象システムで発生した時にフェイルオーバーを行います。)	<input checked="" type="checkbox"/> Power off
	<input checked="" type="checkbox"/> Removal
	<input checked="" type="checkbox"/> CPU failure
	<input checked="" type="checkbox"/> Hard drive failure
	<input checked="" type="checkbox"/> Memory failure
	<input checked="" type="checkbox"/> Communication error
	<input checked="" type="checkbox"/> No power
	<input checked="" type="checkbox"/> Voltage warning
	<input checked="" type="checkbox"/> PFA

各項目の確認方法はBOFMのバージョンにより異なります、次からの手順を参考に確認してください。

3.4.1. BOFM 3.x を使用している場合

BOFM 4.xより、IBM Systems Directorのプラグインではなく単体のアプリケーションとして機能するように再設計されました。そのため、既存のIBM Systems Directorにて使用している仮想アドレスのフェイルオーバーに関するイベント自動化プランが使用できなくなります。

仮想アドレスのフェイルオーバー先となるスタンバイ・システム、フェイルオーバーの監視対象システムを、IBM Systems Director の Web インターフェースより確認してください。

次の一覧からフェイルオーバーのトリガーとして使用するイベントを検討してください。

Power off	サーバーの電源がオフになっているときに検出したとき
Removal	サーバーがシャーシから物理的に除かれたとき
CPU failure	CPUハードウェア障害を検出したとき
Hard drive failure	ハードディスクドライブの障害を検出したとき
Memory failure	メモリハードウェア障害を検出したとき
Communication error	AMMとブレードサーバー上のシステム管理プロセッサの通信障害のとき
No power	電源障害時に検出します。
Voltage warning	異常な電圧のとき
PFA	事前障害分析は、差し迫った障害を検出し、それ以上の損傷を防ぐために、サーバーをシャットダウンするとき

必要な場合にはフェイルオーバー時の動作条件を、次の一覧から検討してください。

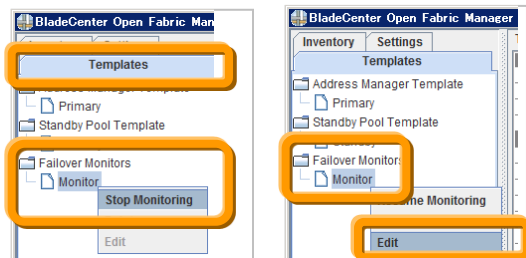
Ignore model	モデルを無視します。
Ignore type	タイプを無視します。
Ignore width	ベイ幅を無視します。
Ignore power state	電源の状態を無視します。
Ignore partition	パーティションを無視します。
Failover VLAN	VLAN設定をフェイルオーバーします。

これらの項目を元に、IFMで仮想アドレスのフェイルオーバーを使用するための「Monitors」構成が必要です。

3.4.2. BOFM 4.1 を使用している場合

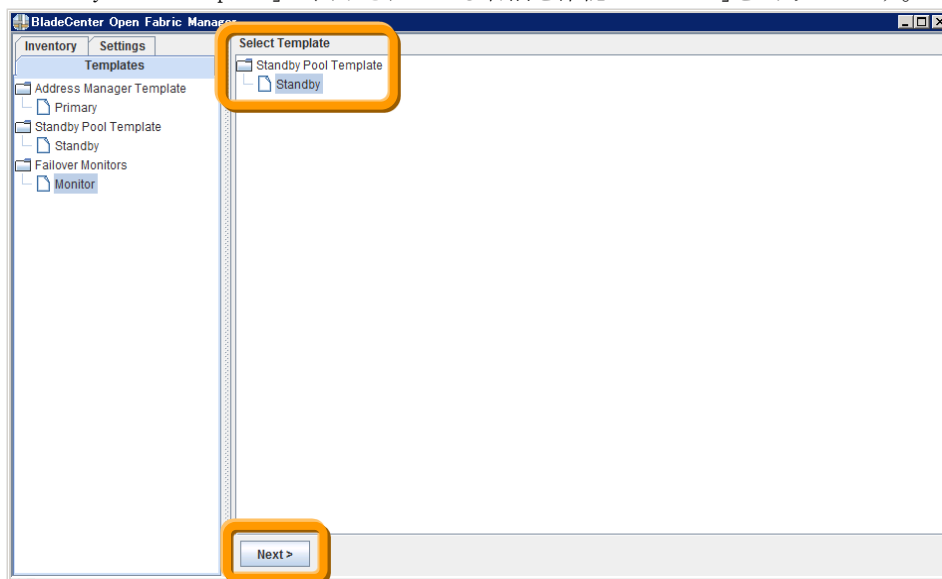
BOFM 4.1を使用している場合、「Failover Monitors」より仮想アドレスのフェイルオーバーでトリガーとするイベントの確認、「Standby Pool Template」より仮想アドレスのフェイルオーバー先となるシステムと動作条件、フェイルオーバーの監視対象システムを次の手順で確認します。

1. BladeCenter Open Fabric Manager ユーザー・インターフェースで、画面左側の「Templates」タブを選択後に「Failover Monitor」の対象となる設定を右クリックして「Stop Monitoring」を選択し、再度「Failover Monitor」の対象となる設定を右クリックして「Edit」を選択します。



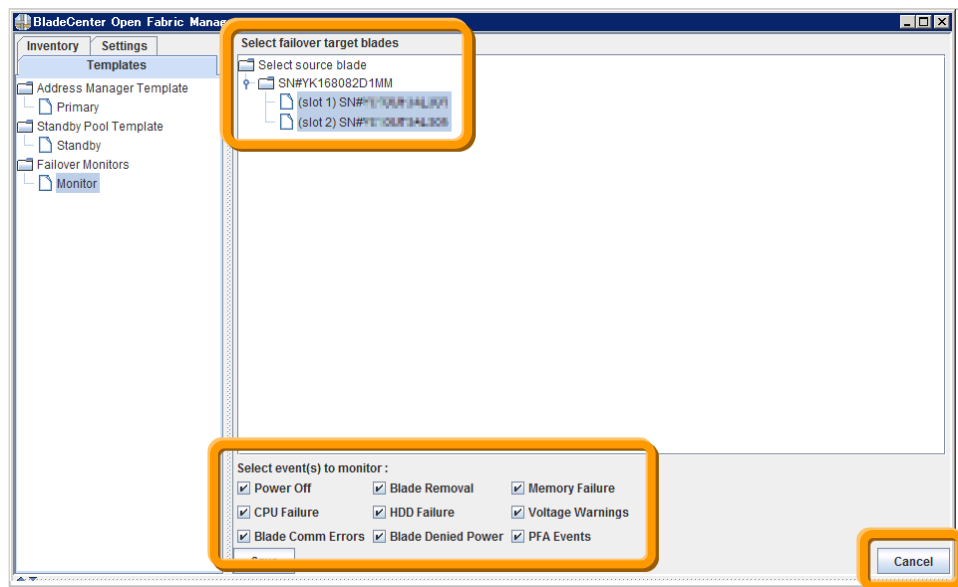
当ガイドでは【Monitor】という名前で設定を作成しています。

2. 画面右側に「Select Template」画面表示後、仮想アドレスのフェイルオーバー先となるシステムとして「Standby Pool Template」に表示されている名前を確認して「Next」をクリックします。



当ガイドでは【Standby】という名前で Standby Pool Template を作成しています。後ほどの手順にて、ここで確認しました Standby Pool Template「Standby」の設定値（フェイルオーバー先となるシステムと動作条件）を参照します。

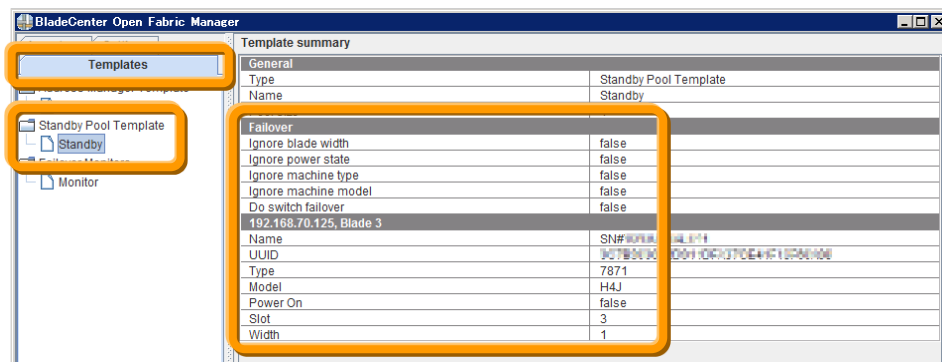
- 画面右側に「Select source blade」画面表示後、「Select source blade」にフェイルオーバーの監視対象となるシステムが表示されていること、「Select event(s) to monitor」にチェックされているフェイルオーバーのトリガーとなるイベントを確認し、「Cancel」をクリックします。



BOFM 4.1 の「Select event(s) to monitor」項目は、IFM で次のように表示されます。選択可能なイベントに違いはありません

BOFM	IFM	
Power off	Power off	サーバーの電源がオフになっているときに検出したとき
Blade Removal	Removal	サーバーがシャーシから物理的に除かれたとき
Memory failure	Memory failure	メモリハードウェア障害を検出したとき
CPU failure	CPU failure	CPUハードウェア障害を検出したとき
HDD failure	Hard drive failure	ハードディスクドライブの障害を検出したとき
Voltage Warnings	Voltage warning	異常な電圧のとき
Blade Comm Errors	Communication error	AMMとブレードサーバー上のシステム管理プロセッサの通信障害のとき
Blade Denied Power	No power	電源障害時に検出します。
PFA Events	PFA	事前障害分析は、差し迫った障害を検出し、それ以上の損傷を防ぐために、サーバーをシャットダウンするとき

- BladeCenter Open Fabric Manager ユーザー・インターフェースで、画面左側の「Templates」タブを選択後に「Standby Pool Template」の対象となるテンプレートをクリックし、「failover」欄よりフェイルオーバーの動作条件と、フェイルオーバーの対象となるシステムの「Slot」を確認します。



当ガイドでは 2 の手順で確認した【Standby】という名前のテンプレートを作成しています。
BOFM 4.1 の「Failover」項目は、IFM で次のように表示されます。

BOFM 4.1	IFM	
Ignore blade width	Ignore width	ベイ幅を無視します。
Ignore power state	Ignore power state	電源の状態を無視します。
Ignore machine type	Ignore type	タイプを無視します。
Ignore machine model	Ignore model	モデルを無視します。
Do switch failover	Failover VLAN	VLAN設定をフェイルオーバーします。
-	Ignore partition	パーティションを無視します。 (IFMで新しく追加された項目です)

4. BOFM Advanced のアンインストール

同じシステムにIFMをインストールする場合、BOFM環境に対するアップグレードをサポートしておりません。お使いのBOFMバージョンに応じて次からの手順を参考にアンインストールを行ってください。

4.1. BOFM 3.x Advanced のアンインストール

IFM はBOFM の後継製品ですが、アップグレードではなく、新規導入にて導入する必要があります。また、IBM Fabric Manager を導入する前に、BOFM 3.x Advancedをアンインストールする必要があります。BOFM 3.x Advanced/IBM Director 環境では、IBM Systems Director サーバーにて BOFM 関連の設定（イベント自動化プランなど）を削除し、IBM Systems DirectorサーバーからBOFM 3.x Advanced/IBM Director をアンインストールします。

当ガイドでは、Windows Server 2008 R2 SP1 でのアンインストール手順となります。

注意:BOFM 3.x Advanced アンインストールの際は、IBM Systems Director サーバーが停止します。アンインストール終了後、システムの再起動が自動的に行われる場合があります（再起動が自動的に行われなない場合は、手動でシステムを再起動してください）。システム再起動後、IBM Systems Director サーバーが起動するまで、IBM Systems Director サーバーを使用した管理・監視を行うことはできません。

5. イベント自動化プランの削除

BOFM をアンインストールする前に、BOFM 関連の設定（イベント自動化プラン）を削除します。Web ブラウザーを起動し、IBM Systems Director サーバーにアクセスします。

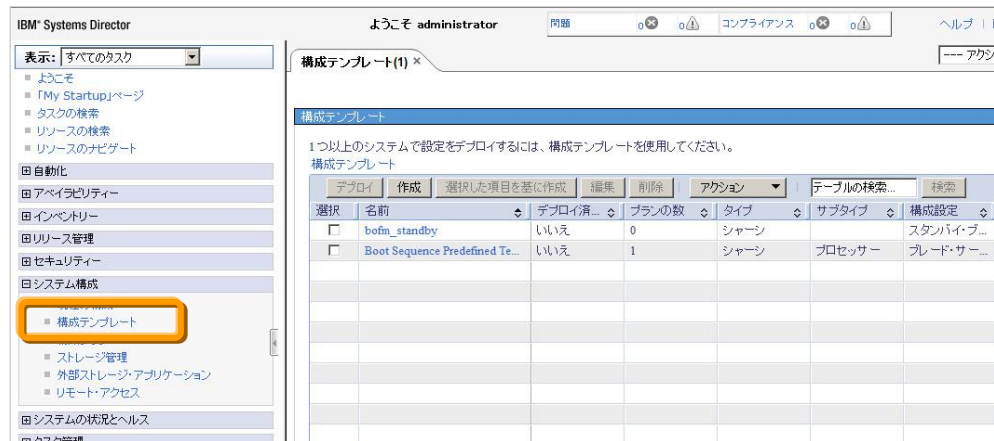
6. IBM Systems Director コンソール左メニューの「自動化」項目より、BOFM に関連するイベント類を削除します。

- イベント自動化プラン
- イベント・アクション
- イベント・フィルター



7. IBM Systems Director コンソール・メニューの「システム構成」項目より、「構成テンプレート」をクリックし、フェイルオーバー設定時に作成したテンプレートを削除します。

➤ 構成テンプレート



8. 関連項目削除後、IBM Systems Director コンソールよりログアウトします。
9. 「スタート」―「コントロール パネル」をクリックします。
10. “コントロール パネル”画面にて「プログラムのアンインストール」をクリックし、「IBM Open Fabric Manager Advanced Upgrade」を選択し、「アンインストールと変更」をクリックします。



11. “IBM BladeCenter Open Fabric Manager Advanced Upgrade のアンインストール”が起動しますので、指示に従いアンインストールを行います。
12. アンインストール処理が完了し、“IBM BladeCenter Open Fabric Manager Advanced Upgrade のアンインストール”画面にて「完了」ボタンをクリックします。
※システムが自動的に再起動しますので、起動後サーバー (IBM Systems Director サーバー) にログインします。
13. 「プログラムのアンインストール」画面を開き、“IBM BladeCenter Open Fabric Manager Advanced Upgrade”が表示されていないことを確認します。
14. IBM Systems Director コンソールにログインし、「管理」タブ内に、“BladeCenter Open Fabric Manager”が表示されていないことを確認します。

以上で、BOFM 3.x Advanced/IBM Director のアンインストールは終了です。

4.2. BOFM 4.1 Advanced のアンインストール

BOFM 4.1のアンインストールを行います。

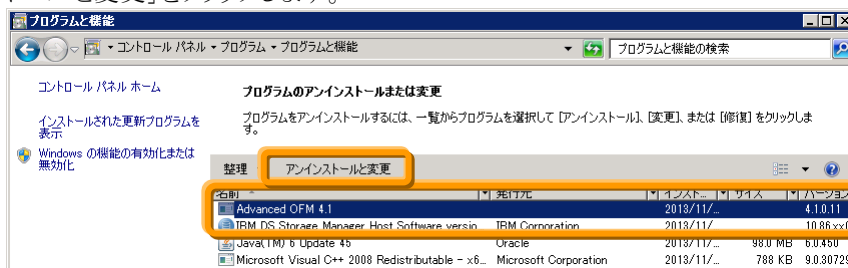
BOFM 4.1のアンインストール完了後は「C:\¥ofm」フォルダーを削除する必要があります。「C:\¥ofm」フォルダーを削除せずにIFMのインストールを行うと、IFMが正常に起動しません。

次からの手順を参考に、BOFM 4.1のアンインストールと「C:\¥ofm」フォルダーの削除を行ってください。

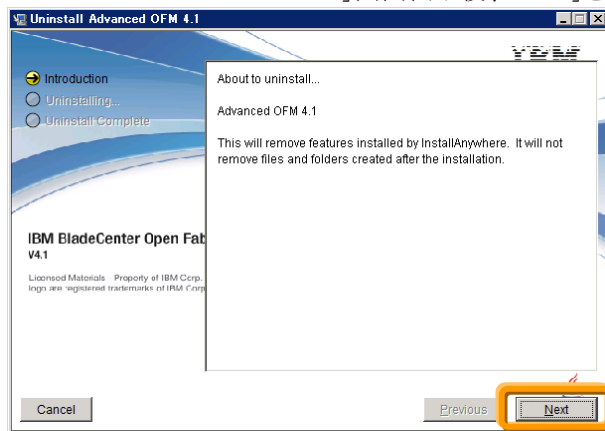
4.2.1. BOFM 4.1 Advanced のアンインストール

アンインストールの作業を開始する前に、BOFM 4.1 Advanced を終了しておきます。

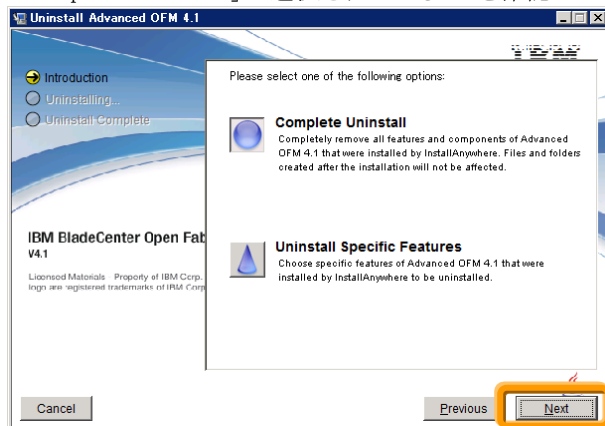
1. 「スタート」から「コントロール パネル」を選択し、「コントロール パネル」画面表示後に「プログラムのアンインストール」をクリックし、「プログラムと機能」画面にて「Advanced OFM 4.1」を選択後に「アンインストールと変更」をクリックします。



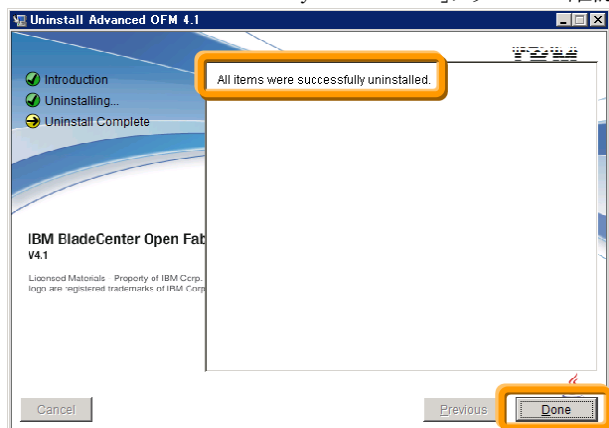
2. 「Uninstall Advanced OFM 4.1」画面表示後、「Next」をクリックします。



3. 「Complete Uninstall」が選択されていることを確認して「Next」をクリックします。



4. 「All items were successfully uninstalled」メッセージ確認後、「Done」をクリックします。



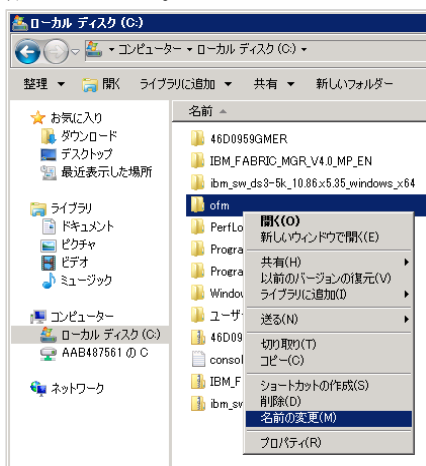
4.2.2. BOFM 4.1 Advanced 「C:\ofm」フォルダーの削除

「C:\ofm」フォルダー内にはBOFM 4.1の構成情報やログが保存されており、このフォルダーは BOFM 4.1 Advancedをアンインストールしても削除されません。

「C:\ofm」フォルダーはIFMでも構成情報やログを保存するために使用され、BOFM 4.1の「C:\ofm」フォルダーが存在する状態でIFMをインストールすると、IFMが正常に起動しませんが、IFMをインストールする前に「C:\ofm」フォルダーを削除してください。

BOFM 4.1の「C:\ofm」フォルダーが存在する状態でIFMをインストール後、IFMが起動できなかった場合は「C:\ofm」フォルダーの削除とIFMの再インストールが必要です。

BOFM 4.1の構成情報やログが必要な場合には「C:\ofm」フォルダーの名前を変更し、バックアップとして保存してください。



5. IFM のインストールと初期設定

5.1. IFM インストール前の確認事項

IFM を導入する前に次の項目を確認します。

5.1.1. IFM ライセンスの確認

AMMのWeb インターフェースにログインし、「MM Control」－「License Manager」をクリックし、BOFM ライセンスが適用されているか確認します。BOFM ライセンスが適用されていない場合、IFM ライセンスを購入し、AMM にライセンスを適用してください。IFM ライセンスに関しましては、“1.2. IFM ライセンス”を参照ください。

※AMM にBOFM ライセンスが適用済みの場合、IFM ライセンスは購入する必要はありますが、AMM にライセンスを再適用する必要はありません。

5.1.2. AMM 構成情報のバックアップ

AMM 構成情報のバックアップを取得します。AMM Web インターフェースにて「MM Control」－「Configuration Mgmt」－「Backup Config to File」をクリック、「Backup」ボタンをクリックしてAMM の構成情報を取得します。

5.1.3. ファームウェアの更新

IFM 4.1では、AMMのファームウェア・バージョンBPET64G以降をサポートします。(最新のIFMでサポートするAMMのファームウェア・バージョンに関しましてはダウンロード・パッケージに含まれる

ibm_ifm_vXX_chg_hist.chg (XXはバージョンにより異なります)を確認してください)

そのため、AMM のファームウェアがIFMの要件を満たしていない場合、Fix Centralサイトより、AMMのファームウェアをダウンロードし、適用してください。(Fix Central からのダウンロードにはIBM IDでのログインが必要です)

Fix Central

<http://www.ibm.com/support/fixcentral/>

※ ファームウェアにつきましては、ダウンロード時点での最新バージョンを適用することを推奨いたします。

5.1.4. IFM をインストールするシステムの Java 確認

IFM をインストールするサーバーには、Java 1.7 がインストールされている必要があります。

インストールされていない場合には、Oracle サイトよりJava 1.7 を入手し、IFM をインストールするサーバーにインストールします。

5.1.5. IFM をインストールするシステムのファイアーウォール確認

IFMをインストールするシステムでは、仮想アドレスのフェイルオーバーを監視するためのSNMP trapを受信するためのUDPポート、IFMの管理や構成を行うためのWebインターフェースに接続するためのTCPポートからの受信を許可しておく必要があります。

当ガイドの構成では次のポートからの受信を許可しています。

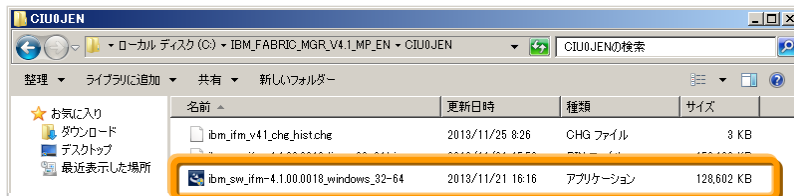
- SNMP trap 受信 : UDP 50990 (UDP)
- IFM Web インターフェース接続 : 8044 (TCP)

5.2. IFM 4.1 のインストール

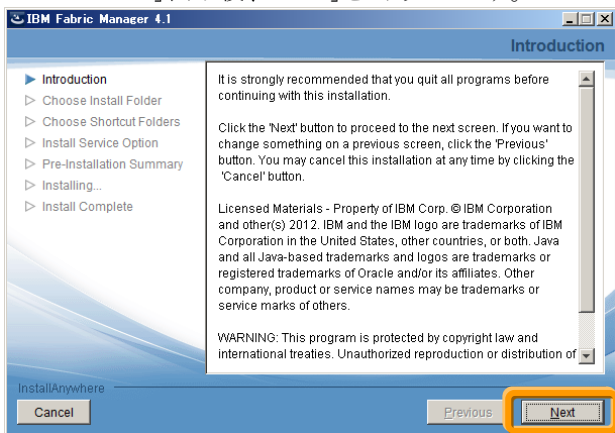
次の手順を参考に、IFM 4.1のインストールを行います。

当ガイドではWindows Server 2008 R2 SP1 へのインストール手順を説明しております。

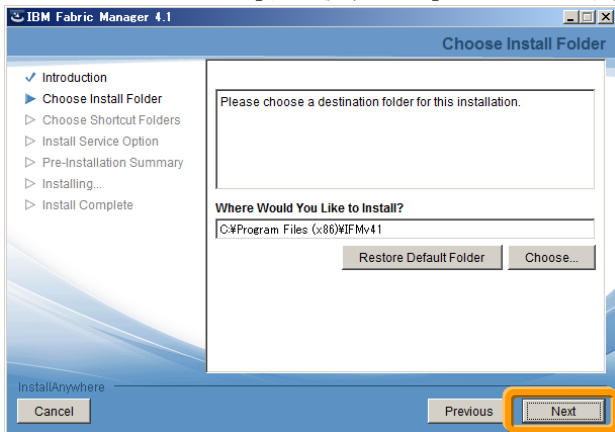
1. 入手したパッケージに含まれる「ibm_sw_ifm-4.1.00.0018_windows_32-64」を実行します。



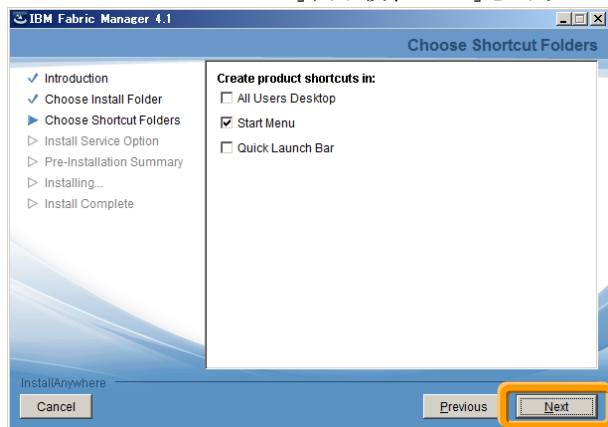
2. 「Introduction」表示後、「Next」をクリックします。



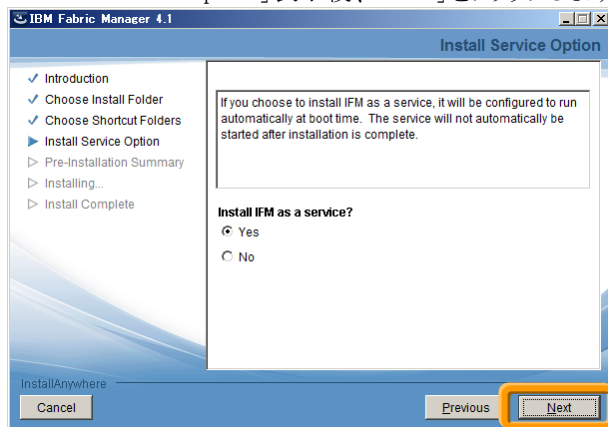
3. 「Choose Install Folder」表示後、「Next」をクリックします。



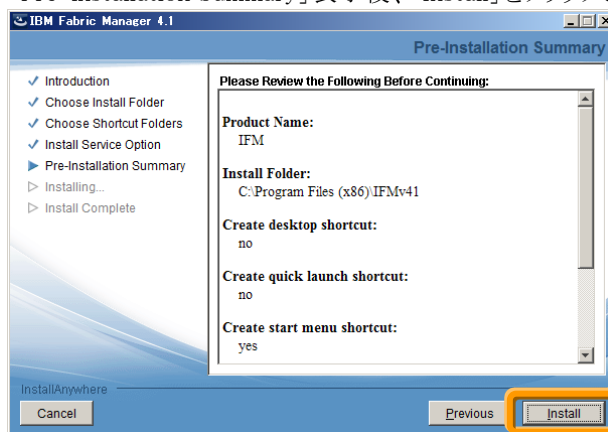
4. 「Choose Shortcut Folders」表示後、「Next」をクリックします。



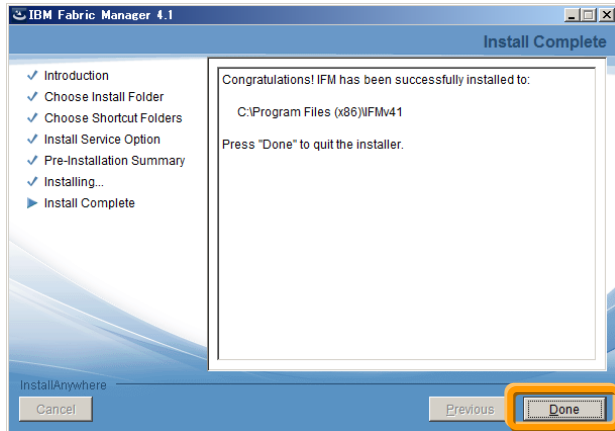
5. 「Install Service Option」表示後、「Next」をクリックします。



6. 「Pre-installation Summary」表示後、「Install」をクリックしてインストール処理を開始します。



7. インストール処理が完了し、「Install Complete」表示後、「Done」をクリックします。



5.3. IFM サービスの開始

IFMのインストール完了後、サーバーマネージャーから構成→サービスを表示後、IBM Fabric Managerを右クリックし、IFMサービスを開始します。



- ※ この操作はインストール完了後のみ行います。これ以降はシステムが起動すると自動的にIFMサービスが開始されます。

5.4. IFM SNMP trap 設定の変更

AMMのSNMP trap構成において、「Community name」の「trap」やポート番号に50990以外を使用する場合には、「C:\ofm\data」フォルダーの「server.prop」内にある次の項目を編集し、IFMサービスの再起動を行ってください。

- SNMPTrapPort=**50990**
- CommunityName=**trap**

- ※ 「C:\ofm\data」フォルダーは、IFMサービス初回起動時に作成されます。

5.5. IFM Web インターフェースへのログイン

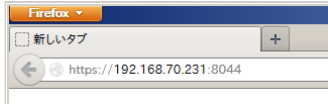
IFMではWebインターフェースから管理や構成を行います。

次からの手順を参考に、IFM Web インターフェースにログインしてください。

当ガイドでは Firefox 17 ESRを使用しております。

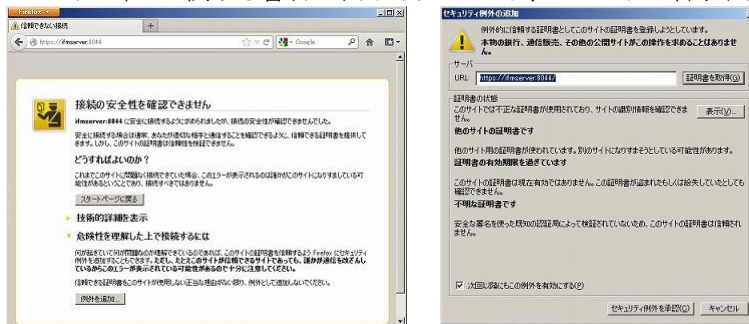
1. アドレス欄に IFM サーバーのホスト名 (適切な DNS 構成を行っている場合)、または IP アドレスを元に次の形式で入力します。

https:// <ホスト名または IP アドレス>:8044



当ガイドでは IFM サーバーの IP アドレスに「192.168.70.231」を設定しております。

セキュリティに関する警告が表示されましたら、「セキュリティ例外を承認」してください。



2. 「IFM Fabric Manager」ログイン画面にてユーザー名とパスワードを入力し、「Log In」をクリックします。



IFM のデフォルト・ユーザー名とパスワードは次の通りです。

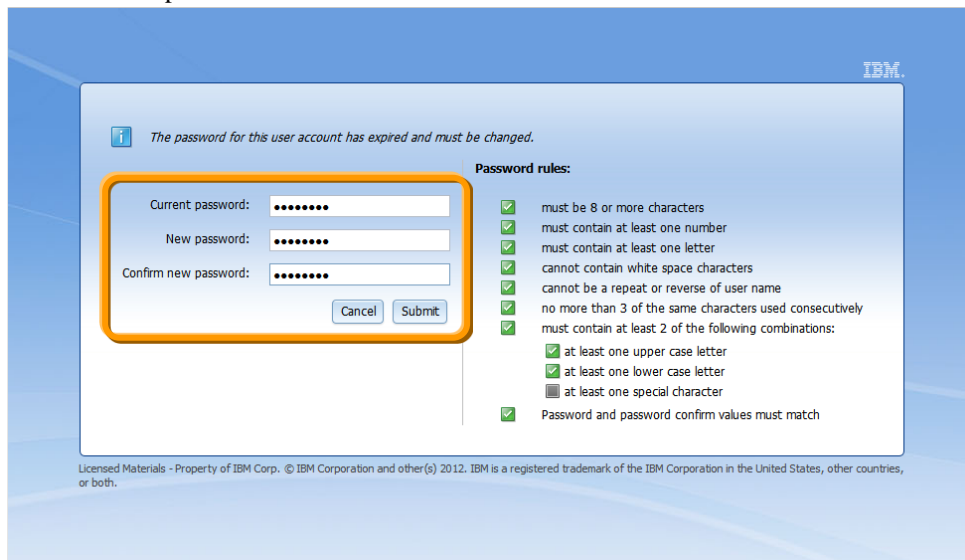
デフォルト・ユーザー名:USERID

デフォルト・パスワード:PASSWORD (0 は数字のゼロ)

5.6. 初回ログイン時のパスワード変更

IFM初回ログイン時にはデフォルト・ユーザーのパスワード変更が必要です。次の手順を参考にパスワードの変更を行ってください。

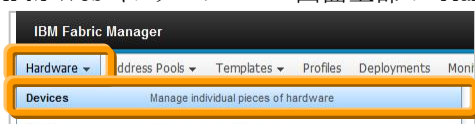
「Current password」に現在のデフォルト・ユーザー・パスワード「PASSWORD(0は数字のゼロ)」を入力し、画面右側に表示されているルールを満たすパスワードを「New password」へ、確認のために同じパスワードを「Confirm new password」へ入力して「Submit」をクリックします。



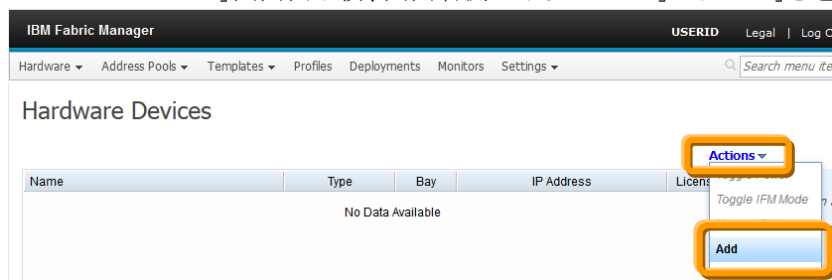
5.7. ハードウェア・デバイス（シャシー）を追加

IFMにシャシーを登録します。

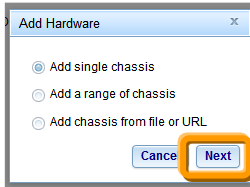
1. IFM Web インターフェース画面上部の「Hardware」から「Device」を選択します。



2. 「Hardware Devices」画面表示後、画面右側にある「Actions」から「Add」を選択します。

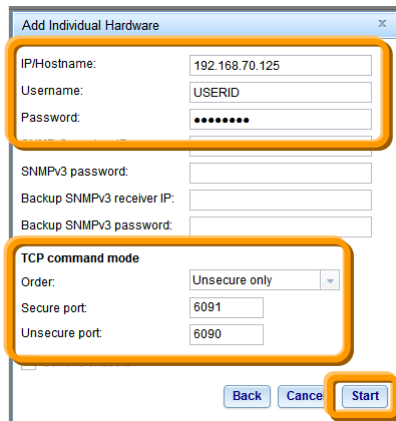


3. 「Add Hardware」画面表示後、適切な項目を選択して「Next」をクリックします。



当ガイドでは 1 台のシャーシを登録しますので「Add single chassis」を選択しています。

4. 登録するシャーシの、管理用 IP アドレスまたはホスト名を「IP /Hostname」、ユーザー名を「Username」、パスワードを「Password」に入力後、「TCP command mode」の項目を適切に設定して「Start」をクリックして登録処理を開始します。



当ガイドでは AMM の設定に合わせて次の値を使用しております。

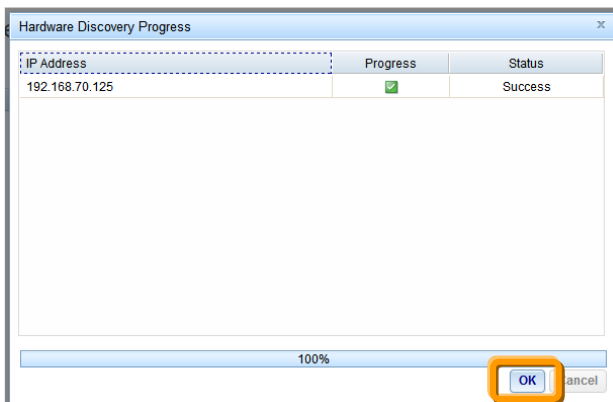
登録するシャーシの管理用 IP アドレス:192.168.70.125

登録するシャーシのユーザー名:USERID

登録するシャーシのユーザー・パスワード:PASSWORD(0 は数字のゼロ)

TCP command mode の Unsecure port:6090

5. 登録処理完了後、「OK」をクリックします。



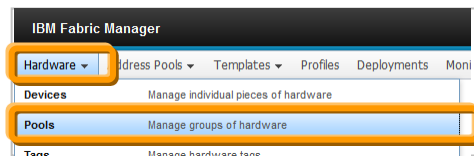
- 登録完了後は「Hardware Devices」画面からシャーシや内部のブレード・サーバー、I/O モジュールの状況を確認することができます。

Name	Type	Bay	IP Address	License	Inventoried	Power	Network	IFM Mode	Source
[1] SNR	BladeCenter	...	192.168.70.125
[2] SNR	BladeCenter
OLLogic 8Gb Fibre Channel Expan...	Daughter card
[2] SNR	BladeCenter
OLLogic 8Gb Fibre Channel Expan...	Daughter card
[3] SNR	BladeCenter
OLLogic 8Gb Fibre Channel Expan...	Daughter card
[1] Ethernet SM	...	1	192.168.70.127
[3] Fibre Channel SM	...	3	192.168.70.129
[4] Fibre Channel SM	...	4	192.168.70.130

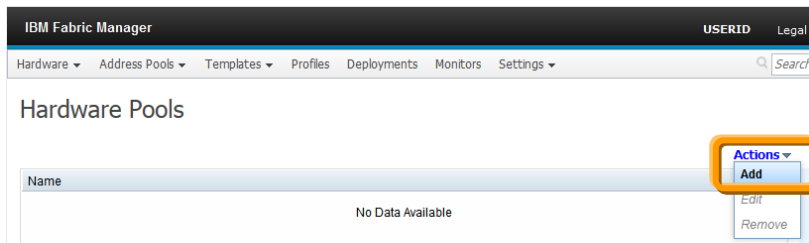
5.8. プライマリー・ハードウェア・プール（仮想アドレスの適用範囲）を追加

仮想アドレスを適用する範囲（BOFMにて仮想アドレス適用済み）のブレード・サーバーをハードウェア・プールに追加します。

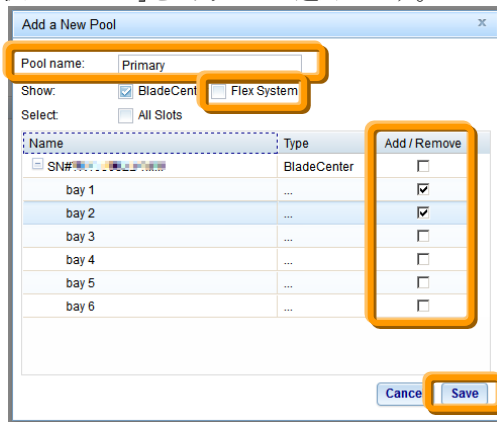
- IFM Web インターフェース上部メニューの「Hardware」から「Pools」を選択します。



- 「Hardware Pools」画面表示後、画面右側の「Actions」から「Add」を選択します。



- 「Add a New Pool」画面表示後、AMM からダウンロードした「bofm.csv」ファイルを元に、「Pool name」を入力後に「Flex System」チェック・ボックスをオフにし、プールに追加するブレード・サーバー・ベイを選択して「Save」をクリックして追加します。



当ガイドでは次の「bofm.csv」ファイルを元に設定しています。

// EXTRACTED FILE STARTS

// Blade Center 192.168.70.125
//IP Type (Center) Mode
192.168.70.125 BladeCenter apply

//IP Type(Slot) Slot Mode Profile
192.168.70.125 Slot 1 enable Primary

//IP	Type	Slot	Offset	Port	MAC_1	VLAN1	MAC_2	VLAN2
192.168.70.125	Ethernet	1	0		1 00:1a:64:76:00:00		0	
192.168.70.125	Ethernet	1	0		2 00:1a:64:76:00:01		0	

//IP	Type	Slot	Priority	WWPN	LUN
192.168.70.125	FCTarget	1	first	20:06:00:xx:xx:xx:xx:3a	0
192.168.70.125	FCTarget	1	second	20:06:00:xx:xx:xx:xx:3b	0

//IP	Type	Slot	Offset	Port	WWNN	WWPN	Boot-order
192.168.70.125	FC	1	0		3	21:80:00:e0:8b:00:00:01	first
192.168.70.125	FC	1	0		4	21:81:00:e0:8b:20:00:01	second

//IP Type(Slot) Slot Mode Profile
192.168.70.125 Slot 2 enable Primary

//IP	Type	Slot	Offset	Port	MAC_1	VLAN1	MAC_2	VLAN2
192.168.70.125	Ethernet	2	0		1 00:1a:64:76:00:02		0	
192.168.70.125	Ethernet	2	0		2 00:1a:64:76:00:03		0	

//IP	Type	Slot	Priority	WWPN	LUN
192.168.70.125	FCTarget	2	first	20:06:00:xx:xx:xx:xx:3a	0
192.168.70.125	FCTarget	2	second	20:06:00:xx:xx:xx:xx:3b	0

//IP	Type	Slot	Offset	Port	WWNN	WWPN	Boot-order
192.168.70.125	FC	2	0		3	21:80:00:e0:8b:00:00:01	first
192.168.70.125	FC	2	0		4	21:81:00:e0:8b:20:00:01	second

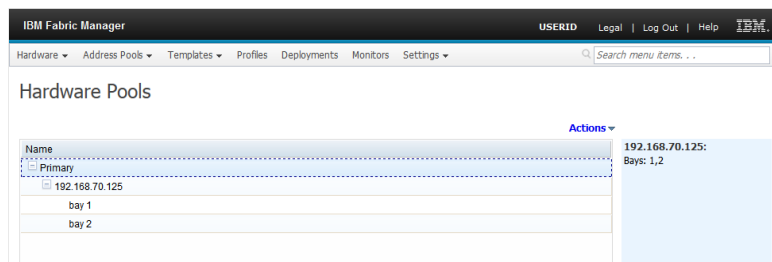
//IP Type(Slot) Slot Mode Profile
192.168.70.125 Slot 3 disable Profile: 192.168.70.125 Slot-3

//IP Type(Slot) Slot Mode Profile
192.168.70.125 Slot 4 disable Profile: 192.168.70.125 Slot-4

BOFMのバージョンによってはbofm.csvの「Profile」が「TempProfile BC-*x*Slot-*x*」というような値が入力されている場合があります。このような場合は仮想アドレスを適用する範囲や仮想アドレスのフェイルオーバー監視対象とする範囲を考慮して任意の名前を入力してください。

当ガイドでは bofm.csv の「Profile」に表示されている「Primary」を「Pool name」に入力し、「Mode」が「enable」の Slot (bay) 1 と 2 を追加します。

4. 「Hardware Pools」画面にて、追加したプールを確認します。



6. IFM にて現在の BOFM 構成を AMM から取り込む移行手順

ここではIFMにて現在使用中のBOFM構成をAMMから取り込む移行手順を説明します。
「現在のBOFM構成を元にIFMにて構成を作成する」場合は、この手順を行わないでください。

	メリット	デメリット
IFMにて現在のBOFM構成をAMMから取り込む	現在の構成を継続して使用するので移行作業時の設定ミスによるトラブルを軽減できます。また、短時間で移行作業を完了できます。	IFMで仮想アドレスの構成に必要な各テンプレートを作成しないので、将来の構成変更が必要となった時にはIFMから行えません。
現在のBOFM構成を元にIFMにて構成を作成する	IFMの構成に必要な各テンプレートから作成するため、将来の構成変更時に対応が容易です。	手作業で現在の構成をIFMに移行するため、作業時の設定ミスによるトラブルが発生する場合があります。また、移行作業に時間がかかります。

当ガイドでは、事前に仮想アドレス設定を取り込む対象となるハードウェア・プールを作成しています。これは、モニター機能による仮想アドレスのフェイルオーバーを使用するための監視対象としてハードウェア・プールを指定する必要があるため、モニター機能を使用しない場合には「Deployments」画面から直接bofm.csvファイルを取り込んで仮想アドレス設定機能のみを使用することもできます。

新しく仮想アドレスの適用範囲にブレード・サーバーを追加する場合は、BOFM Basicの手順を参考にしてbofm.csvファイルを編集後にAMMへ適用後、次からの手順を参考に対応してください。

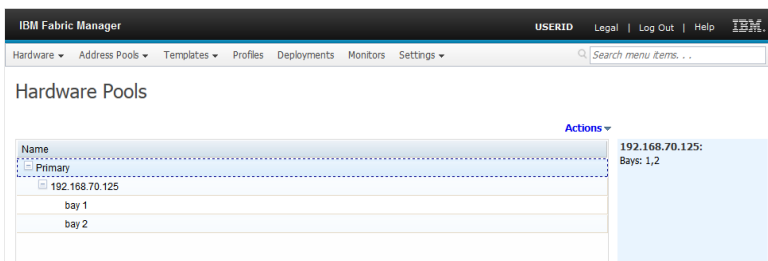
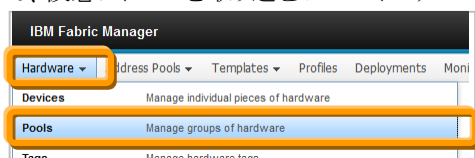
BladeCenter Open Fabric Manager Basic 設定ガイド

<http://www.ibm.com/jp/domino04/pc/support/Sylphd07.nsf/jtechinfo/SYJ0-0473B5B>

6.1. ハードウェア・プールの確認

仮想アドレスを取り込む対象となるブレード・サーバーがハードウェア・プールに追加されているかを確認します。また、ここで確認するハードウェア・プールは、モニター機能による仮想アドレスのフェイルオーバー機能を使用する上での監視対象となります。

1. IFM Web インターフェース上部メニューの「Hardware」から「Pools」を選択し、「Hardware Pools」画面にて、仮想アドレスを取り込むブレード・サーバーの範囲が追加されていることを確認します。



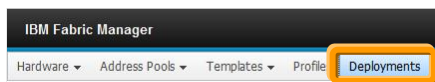
当ガイドでは、ブレード・サーバー・ベイ1と2を追加した「Primary」という名前のハードウェア・プールから、現在適用されている仮想アドレスを取り込みます。

手順に関しましては 35 ページ「5.7. ハードウェア・デバイス(シャーシ)を追加」、37 ページ「5.8. プライマリー・ハードウェア・プール(仮想アドレスの適用範囲)を追加」をご確認ください。

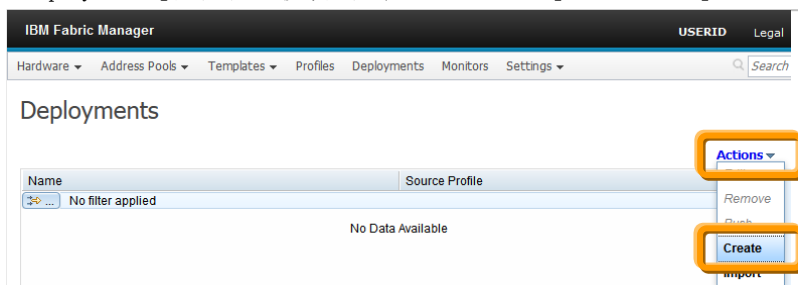
6.2. ハードウェア・プールで使用されている仮想アドレス設定をデプロイメントに取り込む

事前に追加したハードウェア・プールのブレード・サーバーから使用中の仮想アドレス設定を、デプロイメントに取り込みます。

1. IFM Web インターフェース上部メニューの「Deployments」を選択します。

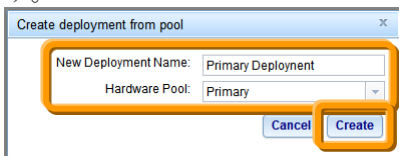


2. 「Deployments」画面表示後、画面右側の「Actions」から「Create」を選択します。



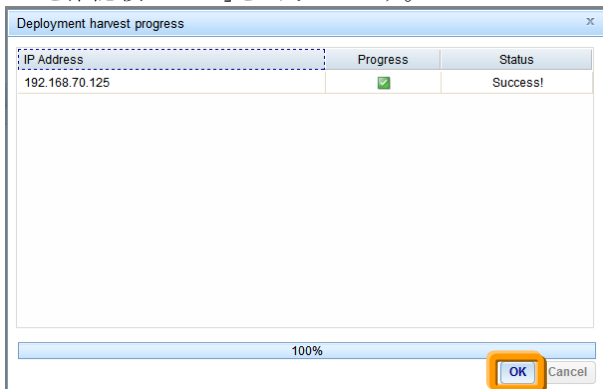
ここで「Actions」から「Import」を選択することで、bofm.csv ファイルから取り込むこともできますが、ハードウェア・プールが追加されていないとモニター機能による仮想アドレスのフェイルオーバーが使用できません。ご注意ください。

3. 「Create deployment from pool」画面表示後、任意の名前を「New Deployment Name」に入力し、仮想アドレスを取り込む対象となる「Hardware Pool」を選択して「Create」をクリックして作成処理を開始します。

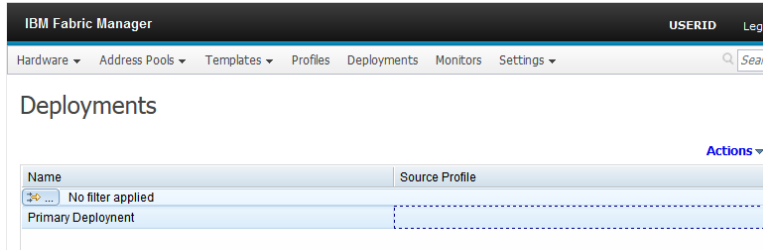


当ガイドでは「New Deployment Name」に「Primary Deployment」を入力し、「Hardware Pool」は「Primary」を選択します。

4. 「Deployment harvest progress」画面表示後、作成処理が完了して「status」に「Success!」が表示されたことを確認後に「OK」をクリックします。



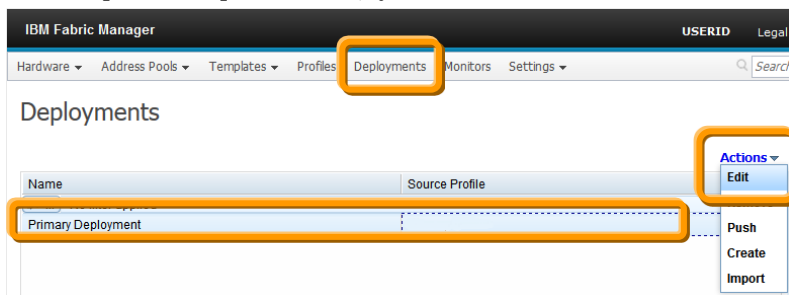
- 「Deployments」画面にて、デプロイメントの項目が作成されたことを確認します。



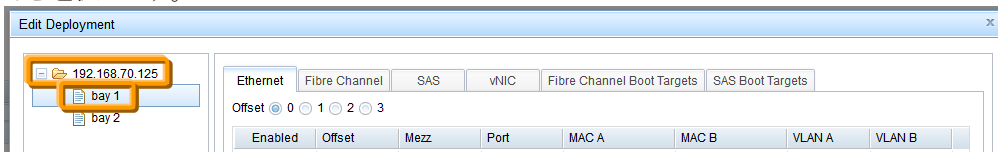
6.3. デプロイメント（仮想アドレス設定）の確認

bofm.csvファイルとブレード・サーバーへ適用する仮想アドレスの確認を行います。
当ガイドでは、各ブレード・サーバー・ベイに対するMACアドレスとQLLogicファイバー・チャンネル拡張カード（CIOv）のWWPN、ファイバーチャンネル・ブート・ターゲットの確認と編集を行います。

- IFM Web インターフェース上部メニューの「Deployments」を選択し、対象となるデプロイを選択後に「Actions」から「Edit」を選択します。



- 「Edit Deployment」画面表示後、画面左側のシャーンを展開表示後に確認の対象となるブレード・ベイを選択します。



bofm.csv ファイル

//IP	Type(Slot)	Slot	Mode	Profile
192.168.70.125	Slot	1	enable	Primary

//IP	Type	Slot	Offset	Port	MAC_1	VLAN1	MAC_2	VLAN2
192.168.70.125	Ethernet	1	0		1 00:1a:64:76:00:00		0	
192.168.70.125	Ethernet	1	0		2 00:1a:64:76:00:01		0	

//IP	Type	Slot	Priority	WWPN	LUN
192.168.70.125	FCTarget	1	first	20:06:00:xx:xx:xx:3a	0
192.168.70.125	FCTarget	1	second	20:06:00:xx:xx:xx:3b	0

//IP	Type	Slot	Offset	Port	WWNN	WWPN	Boot-order
192.168.70.125	FC	1	0		3	21:80:00:e0:8b:00:00:0c	first
192.168.70.125	FC	1	0		4	21:81:00:e0:8b:20:00:0c	second

//IP	Type(Slot)	Slot	Mode	Profile
192.168.70.125	Slot	2	enable	Primary

3. 「Edit Deployment」画面にて対象となるブレード・ベイが選択されていることを確認し、「Ethernet」タブを選択後にオフセット値を含めた各値を bofm.csv ファイルと確認し、必要な場合は編集します。

bofm.csv ファイル

```
//IP      Type(Slot)  Slot  Mode  Profile
192.168.70.125 Slot      1  enable  Primary
```

//IP	Type	Slot	Offset	Port	MAC_1	VLAN1	MAC_2	VLAN2
192.168.70.125	Ethernet	1	0		1 00:1a:64:76:00:00		0	
192.168.70.125	Ethernet	1	0		2 00:1a:64:76:00:01		0	

```
//IP      Type      Slot  Priority  WWPNN      LUN
192.168.70.125 FCTarget  1  first    20:06:00:xx:xx:xx:3a  0
192.168.70.125 FCTarget  1  second   20:06:00:xx:xx:xx:3b  0
```

```
//IP      Type      Slot  Offset  Port      WWNN      WWPNN      Boot-order
192.168.70.125 FC      1      0      3      21:80:00:e0:8b:00:00:00  first
192.168.70.125 FC      1      0      4      21:81:00:e0:8b:20:00:00  second
```

```
//IP      Type(Slot)  Slot  Mode  Profile
192.168.70.125 Slot      2  enable  Primary
```

4. 「Edit Deployment」画面にて対象となるブレード・ベイが選択されていることを確認し、「Fibre Channel」タブを選択後にオフセット値を含めた各値を bofm.csv ファイルと確認し、必要な場合は編集します。

bofm.csv ファイル

```
//IP      Type(Slot)  Slot  Mode  Profile
192.168.70.125 Slot      1  enable  Primary
```

//IP	Type	Slot	Offset	Port	MAC_1	VLAN1	MAC_2	VLAN2
192.168.70.125	Ethernet	1	0		1 00:1a:64:76:00:00		0	
192.168.70.125	Ethernet	1	0		2 00:1a:64:76:00:01		0	

```
//IP      Type      Slot  Priority  WWPNN      LUN
192.168.70.125 FCTarget  1  first    20:06:00:xx:xx:xx:3a  0
192.168.70.125 FCTarget  1  second   20:06:00:xx:xx:xx:3b  0
```

//IP	Type	Slot	Offset	Port	WWNN	WWPN	Boot-order
192.168.70.125	FC	1	0	3	21:80:00:e0:8b:00:00:00	21:80:00:e0:8b:00:00:00	first
192.168.70.125	FC	1	0	4	21:81:00:e0:8b:20:00:00	21:81:00:e0:8b:20:00:00	second

```
//IP      Type(Slot)  Slot  Mode  Profile
192.168.70.125 Slot      2  enable  Primary
```

- 「Edit Deployment」画面にて対象となるブレード・ベイが選択されていることを確認し、「Fibre Channel Boot Targets」タブを選択後に各値を bofm.csv ファイルと確認し、必要な場合は編集後に「Submit」をクリックします。

bofm.csv ファイル

```
//IP      Type(Slot)  Slot  Mode  Profile
192.168.70.125 Slot      1  enable  Primary
```

```
//IP      Type      Slot  Offset  Port      MAC_1      VLAN1      MAC_2      VLAN2
192.168.70.125 Ethernet      1      0      0      1 00:1a:64:76:00:00      0
192.168.70.125 Ethernet      1      0      0      2 00:1a:64:76:00:01      0
```

```
//IP      Type      Slot  Priority WWPN      LUN
192.168.70.125 FCTarget      1  first  20:06:00:xx:xx:xx:3a      0
192.168.70.125 FCTarget      1  second 20:06:00:xx:xx:xx:3b      0
```

```
//IP      Type      Slot  Offset  Port      WWNN      WWPN      Boot-order
192.168.70.125 FC      1      0      0      3      21:80:00:e0:8b:00:00:00 first
192.168.70.125 FC      1      0      0      4      21:81:00:e0:8b:20:00:00 second
```

```
//IP      Type(Slot)  Slot  Mode  Profile
192.168.70.125 Slot      2  enable  Primary
```

- その他のベイに対しても同様の手順で設定値を確認し、「Edit Deployment」画面を終了するには「Submit」をクリックします。
- 追加した仮想アドレスを適用するために、69 ページの「8. 仮想アドレスをブレード・サーバーへ適用 (デプロイメントのプッシュ)」の手順に進みます。

7. 現在のBOFM構成を元にIFMにて構成を作成する移行手順

ここでは現在使用中のBOFM構成を元にIFMにて構成を作成する移行手順を説明します。
「IFMにて現在のBOFM構成をAMMから取り込む」場合は、この手順を行わないでください。

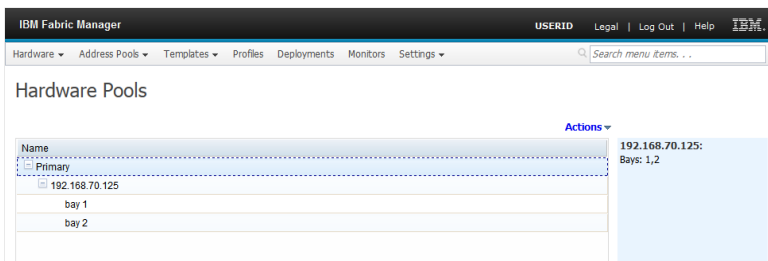
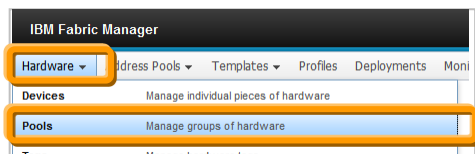
	メリット	デメリット
IFMにて現在のBOFM構成をAMMから取り込む	現在の構成を継続して使用するので移行作業時の設定ミスによるトラブルを軽減できます。また、短時間で移行作業を完了できます。	IFMで仮想アドレスの構成に必要な各テンプレートを作成しないので、将来の構成変更が必要となった時にはIFMから行えません。
現在のBOFM構成を元にIFMにて構成を作成する	IFMの構成に必要な各テンプレートから作成するため、将来の構成変更時に対応が容易です。	手作業で現在の構成をIFMに移行するため、作業時の設定ミスによるトラブルが発生する場合があります。また、移行作業に時間がかかります。

新しく仮想アドレスの適用範囲にブレード・サーバーを追加する場合は、次からの手順を参考にしてください。

7.1. ハードウェア・プールの確認

仮想アドレスを適用する範囲となるブレード・サーバーのベイがハードウェア・プールに追加されているかを確認します。

1. IFM Web インターフェース上部メニューの「Hardware」から「Pools」を選択し、「Hardware Pools」画面にて、仮想アドレスを取り込むブレード・サーバーの範囲が追加されていることを確認します。



当ガイドでは、ブレード・サーバー・ベイ1と2を追加した「Primary」という名前のハードウェア・プールに対して仮想アドレスの適用を行います。

手順に関しましては 35 ページ「5.7. ハードウェア・デバイス(シャーシ)を追加」、37 ページ「5.8. プライマリー・ハードウェア・プール(仮想アドレスの適用範囲)を追加」をご確認ください。

7.2. アドレス・プールの追加

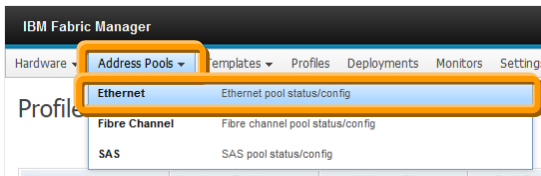
ブレード・サーバーに適用する仮想アドレスの範囲をプールとして定義します。

7.2.1. イーサネット・プールの追加

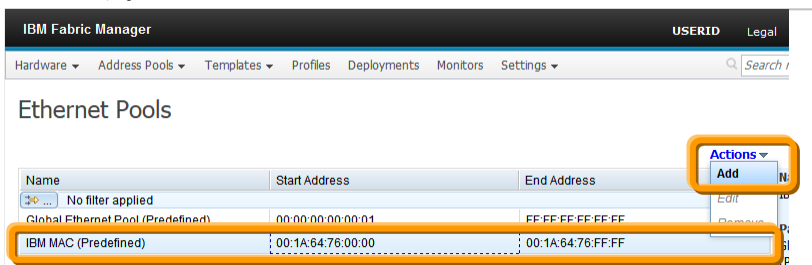
bofm.csv ファイルからMACアドレスの範囲を追加します。当ガイドでは「IBM MAC (Pretended)」をベースに移行するMACアドレスの範囲を追加します。

仮想アドレスとしてMACアドレスを移行しない場合、この手順を行う必要はありません。

1. IFM Web インターフェース上部メニューの「Address Pools」から「Ethernet」を選択します。



2. 「Ethernet Pools」画面表示後、作成するプールのベースになる名前を選択して「Actions」から「Add」を選択します。



当ガイドでは BOFM 環境で使用していた「00:1A:64:76:xx.xx」の範囲で MAC アドレスを移行するため【IBM MAC (Predefined)】を選択します。異なる範囲で定義する場合は「Global Ethernet Pool (Predefined)」を選択してください。

何も選択していない状態では「Actions」から「Add」を選択できませんのでご注意ください。

- 「Add Ethernet Pool」画面表示後、任意の名前で「Pool name」を入力し、「Max server offset」、「Chassis count」、「Start address」を設定後に「Save」をクリックします。

「Calculated last address」の値は「Max server offset」、「Chassis count」、「Start address」の値を元に自動で算出されます。

当ガイドでは「Pool name」に【Primary MAC】を入力します。

「Max Server offset」はブレード・サーバーのベイ幅になります。bofm.csv ファイルより「mode」が「enable」のブレード・サーバーの「Offset」に表示されている最大値を指定してください。当ガイドでは【0】を使用します。

「Chassis count」は仮想アドレスを適用するブレード・サーバーが搭載されるシャーシの台数になります。当ガイドでは 1 台のシャーシ内へ適用するために【1】を使用します。

「Start address」は使用する仮想アドレス範囲の開始値になります。bofm.csv ファイルより「MAC_1」に表示されているアドレスの最小値を設定してください。当ガイドでは【00:1A:64:76:00:00】を使用します。

// EXTRACTED FILE STARTS

```
// Blade Center 192.168.70.125
//IP      Type (Center) Mode
192.168.70.125 BladeCenter apply

//IP      Type(Slot) Slot Mode Profile
192.168.70.125 Slot 1 enable Primary

//IP      Type Slot Offset Port
192.168.70.125 Ethernet 1 0
192.168.70.125 Ethernet 1 0

//IP      Type Slot Priority WWPN LUN
192.168.70.125 FCTarget 1 first 20:06:00:xx:xx:xx:3a 0
192.168.70.125 FCTarget 1 second 20:06:00:xx:xx:xx:3b 0

//IP      Type Slot Offset Port WWNN WWPN Boot-order
192.168.70.125 FC 1 0 3 21:80:00:e0:8b:00:00:01 first
192.168.70.125 FC 1 0 4 21:81:00:e0:8b:20:00:01 second

//IP      Type(Slot) Slot Mode Profile
192.168.70.125 Slot 2 enable Primary

//IP      Type Slot Offset Port
192.168.70.125 Ethernet 2 0
192.168.70.125 Ethernet 2 0

//IP      Type Slot Priority WWPN LUN
192.168.70.125 FCTarget 2 first 20:06:00:xx:xx:xx:3a 0
192.168.70.125 FCTarget 2 second 20:06:00:xx:xx:xx:3b 0

//IP      Type Slot Offset Port WWNN WWPN Boot-order
192.168.70.125 FC 2 0 3 21:80:00:e0:8b:00:00:01 first
192.168.70.125 FC 2 0 4 21:81:00:e0:8b:20:00:01 second

//IP      Type(Slot) Slot Mode Profile
192.168.70.125 Slot 3 disable Profile: 192.168.70.125 Slot-3

//IP      Type(Slot) Slot Mode Profile
192.168.70.125 Slot 4 disable Profile: 192.168.70.125 Slot-4
```

「Offset」の最大値を「Max Server offset」に指定

最小値を「Start address」に指定

MAC_1 LAN1 MAC_2 VLAN2

1 00:1a:64:76:00:00 0

2 00:1a:64:76:00:01 0

MAC_1 LAN1 MAC_2 VLAN2

1 00:1a:64:76:00:02 0

2 00:1a:64:76:00:03 0

4. 「Ethernet Pools」画面にて、追加した仮想アドレス・プールを確認します。

Name	Start Address	End Address
Global Ethernet Pool (Predefined)	00:00:00:00:00:01	FF:FF:FF:FF:FF:FF
IBM MAC (Predefined)	00:1A:64:76:00:00	00:1A:64:76:FF:FF
Primary MAC	00:1A:64:76:00:00	00:1A:64:76:1E:84

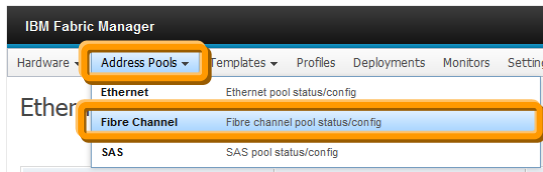
7.2.2. ファイバーチャネル・プールの追加

bofm.csv ファイルからFC拡張カードに適用するWWNの範囲を定義します。当ガイドではQLogicファイバー・チャネル拡張カードのポート1で使用していたWWPNを移行するために「QLOGIC WWPNA (Predefined)」を、ポート2で使用していたWWPNを移行するために「QLOGIC WWPNB (Predefined)」をベースにして作成します。

Brocade、Emulex ファイバー・チャネル拡張カードの場合、WWNNも必要となりますので、次からの手順を参考に追加してください。

仮想アドレスとしてファイバー・チャネルのWWNを移行しない場合、この手順を行う必要はありません。

1. IFM Web インターフェース上部メニューの「Address Pools」から「Fibre Channel」を選択します。



2. 「Fibre Channel Pools」画面表示後、追加するファイバー・チャネル拡張カードのポート1 (WWPNA) のプールのベースになる名前を選択して「Actions」から「Add」を選択します。

Name	Start Address	End Address
Global Fibre Channel Pool (Predefined)	00:00:00:00:00:00:00:01	FF:FF:FF:FF:FF:FF:FF:FF
IBM WWNNA (Predefined)	20:80:00:50:76:00:00:00	20:80:00:50:76:0F:FF:FF
IBM WWNNB (Predefined)	20:81:00:50:76:20:00:00	20:81:00:50:76:2F:FF:FF
IBM WWPNA (Predefined)	21:80:00:50:76:00:00:00	21:80:00:50:76:0F:FF:FF
QLOGIC WWPNA (Predefined)	21:80:00:E0:8B:00:00:00	21:80:00:E0:8B:0F:FF:FF
QLOGIC WWPNB (Predefined)	21:81:00:E0:8B:20:00:00	21:81:00:E0:8B:2F:FF:FF

当ガイドではBOFM環境でQLogicファイバー・チャネル拡張カードのポート1で使用していた「21:80:00:E0:8B:00:xx:xx」の範囲でアドレスを移行するため【QLOGIC WWPNA (Predefined)】を選択します。使用する範囲に応じて適切な名前を選択してください。

何も選択していない状態で「Actions」から「Add」を選択できませんのでご注意ください。

- 「Add Fibre Channel Pool」画面表示後、任意の名前で「Pool name」を入力し、「Max server offset」、「Chassis count」、「Start address」を設定後に「Save」をクリックします。

当ガイドでは「Pool name」に【Primary WWPNA】を入力します。

「Max Server offset」はブレード・サーバーのベイ幅になります。bofm.csv ファイルより「mode」が「enable」のブレード・サーバーの「Offset」に表示されている最大値を指定してください。当ガイドでは【0】を使用します。

「Chassis count」は仮想アドレスを適用するブレード・サーバーが搭載されるシャーシの台数になります。当ガイドでは 1 台のシャーシ内へ適用するために【1】を使用します。

「Start address」は使用する仮想アドレス範囲の開始値になります。bofm.csv ファイルよりポート 3 の「WWPN」に表示されているアドレスの最小値を設定してください。当ガイドでは【21:81:00:E0:8B:00:00:00】を使用します。

// EXTRACTED FILE STARTS

```
// Blade Center 192.168.70.125
//IP          Type (Center) Mode
192.168.70.125 BladeCenter apply

//IP          Type(Slot) Slot Mode
192.168.70.125 Slot 1 enable Primary

//IP          Type Slot Offset Port MAC_1 VLAN1 MAC_2 VLAN2
192.168.70.125 Ethernet 1 0 1 00:1a:64:76:00:00 0
192.168.70.125 Ethernet 1 0 2 00:1a:64:76:00:01 0

//IP          Type Slot Priority WWPN LUN
192.168.70.125 FCTarget 1 first 20:06:00:xx:xx:xx:xx:3a 0
192.168.70.125 FCTarget 1 second 20:06:00:xx:xx:xx:xx:3b 0

//IP          Type Slot Offset Port WWNN WWPN port-order
192.168.70.125 FC 1 0 3 21:80:00:e0:8b:00:00:00 first
192.168.70.125 FC 1 0 4 21:81:00:e0:8b:20:00:00 second

//IP          Type(Slot) Slot Mode Profile
192.168.70.125 Slot 2 enable Primary

//IP          Type Slot Offset Port MAC_1 VLAN1 MAC_2 VLAN2
192.168.70.125 Ethernet 2 0 1 00:1a:64:76:00:02 0
192.168.70.125 Ethernet 2 0 2 00:1a:64:76:00:03 0

//IP          Type Slot Priority WWPN LUN
192.168.70.125 FCTarget 2 first 20:06:00:xx:xx:xx:xx:3a 0
192.168.70.125 FCTarget 2 second 20:06:00:xx:xx:xx:xx:3b 0

//IP          Type Slot Offset Port WWNN WWPN port-order
192.168.70.125 FC 2 0 3 21:80:00:e0:8b:00:00:01 first
192.168.70.125 FC 2 0 4 21:81:00:e0:8b:20:00:00 second

//IP          Type(Slot) Slot Mode Profile
192.168.70.125 Slot 3 disable Profile: 192.168.70.125 Slot-3

//IP          Type(Slot) Slot Mode Profile
192.168.70.125 Slot 4 disable Profile: 192.168.70.125 Slot-4
```

「Offset」の最大値を「Max Server offset」に指定

「Port」3 の最小値を「Start address」に指定

WWNN WWPN port-order
3 21:80:00:e0:8b:00:00:00 first
4 21:81:00:e0:8b:20:00:00 second

WWNN WWPN port-order
3 21:80:00:e0:8b:00:00:01 first
4 21:81:00:e0:8b:20:00:00 second

4. 「Fibre Channel Pools」画面にて、追加した仮想アドレス・プールを確認します。

Name	Start Address	End Address
IBM WWPNB (Predefined)	21:81:00:50:76:20:00:00	21:81:00:50:76:2F:FF:FF
QLOGIC WWPNA (Predefined)	21:80:00:E0:8B:00:00:00	21:80:00:E0:8B:0F:FF:FF
QLOGIC WWPNB (Predefined)	21:81:00:E0:8B:20:00:00	21:81:00:E0:8B:2F:FF:FF
EMULEX WWNNA (Predefined)	2F:FE:00:00:C9:00:00:00	2F:FE:00:00:C9:FF:FF:FF
EMULEX WWPNA (Predefined)	2F:FF:00:00:C9:00:00:00	2F:FF:00:00:C9:FF:FF:FF
EMULEX WWPNA (Predefined)	2F:FC:00:00:C9:00:00:00	2F:FC:00:00:C9:FF:FF:FF
EMULEX WWPNB (Predefined)	2F:FD:00:00:C9:00:00:00	2F:FD:00:00:C9:FF:FF:FF
BROCADE WWNNA (Predefined)	2B:FA:00:05:1E:00:00:00	2B:FA:00:05:1E:FF:FF:FF
BROCADE WWPNA (Predefined)	2B:FB:00:05:1E:00:00:00	2B:FB:00:05:1E:FF:FF:FF
BROCADE WWPNA (Predefined)	2B:FC:00:05:1E:00:00:00	2B:FC:00:05:1E:FF:FF:FF
BROCADE WWPNB (Predefined)	2B:FD:00:05:1E:00:00:00	2B:FD:00:05:1E:FF:FF:FF
Primary WWPNA	21:80:00:E0:8B:00:00:00	21:80:00:E0:8B:00:00:E0

5. 「Fibre Channel Pools」画面表示後、追加するファイバー・チャネル拡張カードのポート2(WWPNB)のプールのベースになる名前を選択して「Actions」から「Add」を選択します。

Name	Start Address	End Address
IBM WWPNB (Predefined)	21:81:00:50:76:20:00:00	21:81:00:50:76:2F:FF:FF
QLOGIC WWPNB (Predefined)	21:81:00:E0:8B:20:00:00	21:81:00:E0:8B:2F:FF:FF

当ガイドでは BOFM 環境で QLogic ファイバー・チャネル拡張カードのポート2 で使用していた「21:80:00:E0:8B:20:xx:xx」の範囲でアドレスを移行するため【QLOGIC WWPNB (Predefined)】を選択します。使用する範囲に応じて適切な名前を選択してください。

6. 「Add Fibre Channel Pool」画面表示後、任意の名前を「Pool name」に入力し、「Max server offset」、「Chassis count」、「Start address」を設定後に「Save」をクリックします。

当ガイドでは「Pool name」に【Primary WWPNB】を入力します。

「Max Server offset」はブレード・サーバーのベイ幅になります。bofm.csv ファイルより「mode」が「enable」のブレード・サーバーの「Offset」に表示されている最大値を指定してください。当ガイドでは【0】を使用します。

「Chassis count」は仮想アドレスを適用するブレード・サーバーが搭載されるシャーシの台数になります。当ガイドでは 1 台のシャーシ内へ適用するために【1】を使用します。

「Start address」は使用する仮想アドレス範囲の開始値になります。bofm.csv ファイルよりポート 4 の「WWPN」に表示されているアドレスの最小値を設定してください。当ガイドでは【21:81:00:E0:8B:20:00:00】を使用します。

// EXTRACTED FILE STARTS

// Blade Center 192.168.70.125

//IP Type (Center) Mode
192.168.70.125 BladeCenter apply

//IP Type(Slot) Slot Mode Pr
192.168.70.125 Slot 1 enable Primary

//IP	Type	Slot	Offset	Port	MAC_1	VLAN1	MAC_2	VLAN2
192.168.70.125	Ethernet	1	0		1 00:1a:64:76:00:00		0	
192.168.70.125	Ethernet	1	0		2 00:1a:64:76:00:01		0	

//IP	Type	Slot	Priority	WWPN	LUN
192.168.70.125	FCTarget	1	first	20:06:00:xx:xx:xx:xx:3a	0
192.168.70.125	FCTarget	1	second	20:06:00:xx:xx:xx:xx:3b	0

//IP	Type	Slot	Offset	Port	WWNN	WWPN	Boot-order
192.168.70.125	FC	1	0		2	21:80:00:e0:8b:00:00:01	first
192.168.70.125	FC	1	0		4	21:81:00:e0:8b:20:00:01	second

//IP Type(Slot) Slot Mode Profile
192.168.70.125 Slot 2 enable Primary

//IP	Type	Slot	Offset	Port	MAC_1	VLAN1	MAC_2	VLAN2
192.168.70.125	Ethernet	2	0		1 00:1a:64:76:00:02		0	
192.168.70.125	Ethernet	2	0		2 00:1a:64:76:00:03		0	

//IP	Type	Slot	Priority	WWPN	LUN
192.168.70.125	FCTarget	2	first	20:06:00:xx:xx:xx:xx:3a	0
192.168.70.125	FCTarget	2	second	20:06:00:xx:xx:xx:xx:3b	0

//IP	Type	Slot	Offset	Port	WWNN	WWPN	Boot-order
192.168.70.125	FC	2	0		2	21:80:00:e0:8b:00:00:01	first
192.168.70.125	FC	2	0		4	21:81:00:e0:8b:20:00:01	second

//IP Type(Slot) Slot Mode Profile
192.168.70.125 Slot 3 disable Profile: 192.168.70.125 Slot-3

//IP Type(Slot) Slot Mode Profile
192.168.70.125 Slot 4 disable Profile: 192.168.70.125 Slot-4

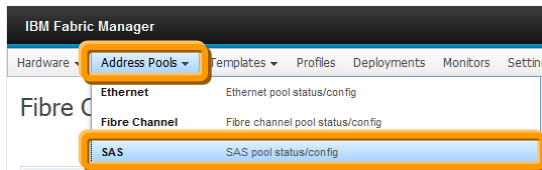
- 「Fibre Channel Pools」画面にて、追加した仮想アドレス・プールを確認します。

Name	Start Address	End Address
No filter applied		
QLOGIC WWPNA (Predefined)	21:80:00:E0:8B:00:00:00	21:80:00:E0:8B:0F:FF:FF
QLOGIC WWPNB (Predefined)	21:81:00:E0:8B:20:00:00	21:81:00:E0:8B:2F:FF:FF
EMULEX WWPNA (Predefined)	2F:FE:00:00:C9:00:00:00	2F:FE:00:00:C9:FF:FF:FF
EMULEX WWPNB (Predefined)	2F:FF:00:00:C9:00:00:00	2F:FF:00:00:C9:FF:FF:FF
EMULEX WWPNA (Predefined)	2F:FC:00:00:C9:00:00:00	2F:FC:00:00:C9:FF:FF:FF
EMULEX WWPNB (Predefined)	2F:FD:00:00:C9:00:00:00	2F:FD:00:00:C9:FF:FF:FF
BROCADE WWPNA (Predefined)	2B:FA:00:05:1E:00:00:00	2B:FA:00:05:1E:FF:FF:FF
BROCADE WWPNB (Predefined)	2B:FB:00:05:1E:00:00:00	2B:FB:00:05:1E:FF:FF:FF
BROCADE WWPNA (Predefined)	2B:FC:00:05:1E:00:00:00	2B:FC:00:05:1E:FF:FF:FF
BROCADE WWPNB (Predefined)	2B:FD:00:05:1E:00:00:00	2B:FD:00:05:1E:FF:FF:FF
Primary WWPNA	21:80:00:E0:8B:00:00:00	21:80:00:E0:8B:00:00:E0
Primary WWPNB	21:81:00:E0:8B:20:00:00	21:81:00:E0:8B:20:00:E0

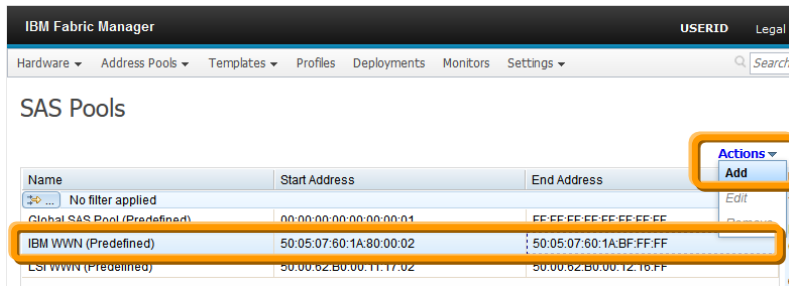
7.2.3. SASプールの追加

当ガイドでは移行対象に含んでおりません。必要な場合には、ここまでの手順を参考に追加してください。仮想アドレスとしてSASのアドレスを移行しない場合、この手順を行う必要はありません。

- IFM Web インターフェース上部メニューの「Address Pools」から「SAS」を選択します。

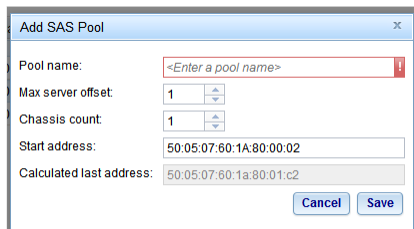


- 「SAS」画面表示後、追加するプールのベースになる名前を選択して「Actions」から「Add」を選択します。



何も選択していない状態で「Actions」から「Add」を選択できませんのでご注意ください。

3. 「Add Fibre Channel Pool」画面表示後、任意の名前で「Pool name」を入力し、「Max server offset」、「Chassis count」、「Start address」を設定後に「Save」をクリックします。



The screenshot shows a dialog box titled "Add SAS Pool" with a close button (X) in the top right corner. The dialog contains the following fields and controls:

- Pool name:** A text input field with the placeholder text "<Enter a pool name>" and a red error icon on the right.
- Max server offset:** A numeric input field with the value "1" and up/down arrow buttons.
- Chassis count:** A numeric input field with the value "1" and up/down arrow buttons.
- Start address:** A text input field containing the MAC address "50:05:07:60:1A:80:00:02".
- Calculated last address:** A text input field containing the MAC address "50:05:07:60:1a:80:01:c2".
- Buttons:** "Cancel" and "Save" buttons at the bottom right.

7.3. テンプレートの追加

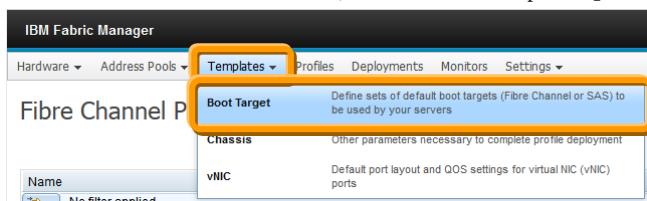
シャーシ内のブレード・サーバーの構成や、ブート・ターゲットを定義するテンプレートを追加します。

7.3.1. ブート・ターゲット・テンプレートの追加

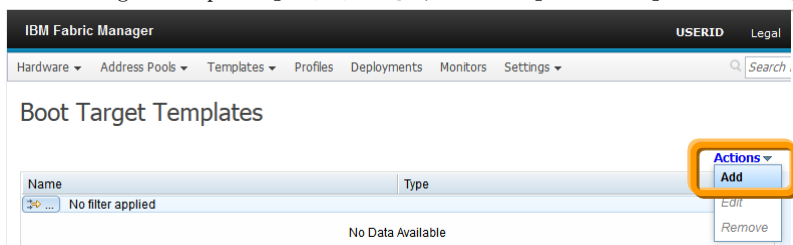
FCまたはSASブート・ターゲットのテンプレートを追加します。

当ガイドではシャーシ外部ストレージ装置のコントローラーAのアドレス「20:06:00:xx:xx:xx:xx:3a」をプライマリー、コントローラーBのアドレス「20:06:00:xx:xx:xx:xx:3b」をセカンダリーとしてテンプレートに追加します。ブート・ターゲットを移行しない場合、この手順を行う必要はありません。

1. IFM Web インターフェース上部メニューの「Templates」から「Boot Target」を選択します。



2. 「Boot Target Templates」画面表示後、「Actions」から「Add」を選択します。



- 「Create Boot Targets」画面表示後、任意の名前を「Name」に入力し、「Type」でファiber・チャネルか SAS を選択後、「Primary boot targets」、「Secondary boot targets」の各値を設定して「Save」をクリックします。

当ガイドでは「Name」に【Primary Boot Target】を入力し、「Type」は【Fibre Channel】を選択します。「Primary boot targets」の Order 1 にある Address には、bofm.csv ファイルより「Priority」が「first」に設定されているアドレスを、「Secondary boot targets」の Order 1 にある Address には「Priority」が「Second」に設定されているアドレスを入力します。当ガイドでは「Primary boot targets」に【20:06:00:xx:xx:xx:3a】を「Secondary boot targets」に【20:06:00:xx:xx:xx:3b】を使用します。

// EXTRACTED FILE STARTS

// Blade Center 192.168.70.125
//IP Type (Center) Mode
192.168.70.125 BladeCenter apply

//IP Type (Slot) Slot
192.168.70.125 Slot

IP	Type	Slot	Priority	WWPN	LUN	VLAN2
192.168.70.125	Ethernet	1	0	1 00:1a:64:76:00:00	0	
192.168.70.125	Ethernet	1	0	2 00:1a:64:76:00:01	0	

//IP Type Slot Priority WWPN LUN
192.168.70.125 FCTarget 1 first 20:06:00:xx:xx:xx:3a 0
192.168.70.125 FCTarget 1 second 20:06:00:xx:xx:xx:3b 0

//IP Type Slot Offset Port WWNN WWPN Boot-order
192.168.70.125 FC 1 0 3 21:80:00:e0:8b:00:00:01 first
192.168.70.125 FC 1 0 4 21:81:00:e0:8b:20:00:01 second

//IP Type (Slot) Slot Mode Profile
192.168.70.125 Slot 2 enable Primary

//IP Type Slot Offset Port MAC_1 VLAN1 MAC_2 VLAN2
192.168.70.125 Ethernet 2 0 1 00:1a:64:76:00:02 0
192.168.70.125 Ethernet 2 0 2 00:1a:64:76:00:03 0

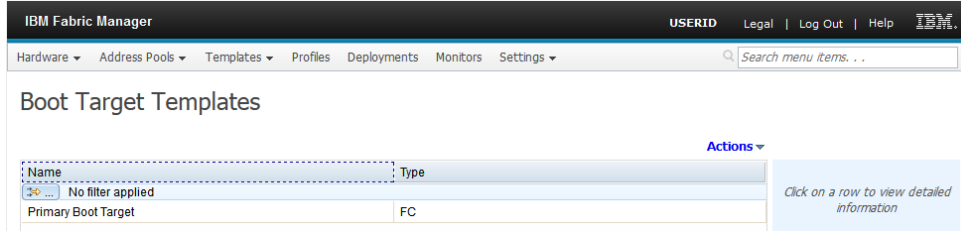
//IP Type Slot Priority WWPN LUN
192.168.70.125 FCTarget 2 first 20:06:00:xx:xx:xx:3a 0
192.168.70.125 FCTarget 2 second 20:06:00:xx:xx:xx:3b 0

//IP Type Slot Offset Port WWNN WWPN Boot-order
192.168.70.125 FC 2 0 3 21:80:00:e0:8b:00:00:01 first
192.168.70.125 FC 2 0 4 21:81:00:e0:8b:20:00:01 second

//IP Type (Slot) Slot Mode Profile
192.168.70.125 Slot 3 disable Profile: 192.168.70.125 Slot-3

//IP Type (Slot) Slot Mode Profile
192.168.70.125 Slot 4 disable Profile: 192.168.70.125 Slot-4

4. 「Boot Target Template」画面にて、追加したテンプレートを確認します。

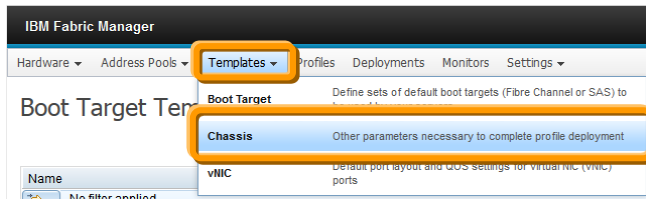


7.3.2. シャーシ・テンプレートの追加

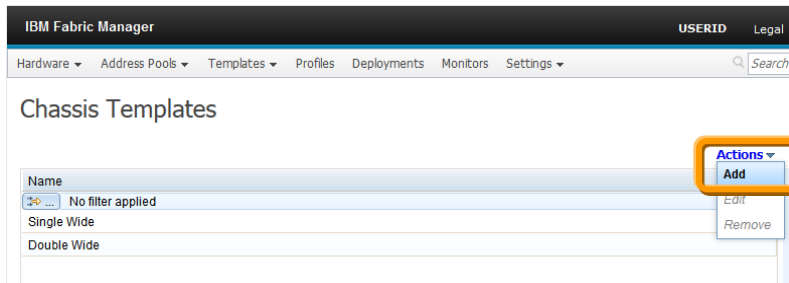
シャーシ内に搭載されたブレード・サーバーのベイ幅や、仮想アドレスを適用するポートを指定するためのテンプレートを作成します。

当ガイドでは、ブレード・サーバーのベイ幅を1、オンボードNICのポート1と2、CIOv拡張カードのポート1と2に仮想アドレスを適用するためのテンプレートを作成します。

1. IFM Web インターフェース上部メニューの「Templates」から「Chassis」を選択します。



2. 「Chassis Templates」画面表示後、「Actions」から「Add」を選択します。



- 「Edit Chassis Template」画面表示後、任意の名前を「Name」に入力後に「Max server offset」を指定して、「Ports to configure」の一覧から仮想アドレスを適用するブレード・サーバーのポート番号のチェック・ボックスをオンにした後、必要に応じて「VALN」、「Port Ranging」の設定を行います。

当ガイドでは「Name」に【Primary Chassis Template】を入力し、「Max server offset」は bofm.csv ファイルより【0】を指定します。

「Double density bays」は Flex System 用の設定項目となりますので、BladeCenter で設定する必要はありません。

当ガイドでは「Port to configure」の各チェック・ボックスは、bofm.csv ファイルより「type」が「Ethernet」の「port」に表示された値【1】と【2】、「Type」が「FC」の「Port」に表示された値【3】と【4】をオンにします。

```
// EXTRACTED FILE S
// Blade Center 192.1
//IP          Type (
192.168.70.125 BladeC

//IP          Type(S
192.168.70.125 Slot

1 enable Primary

//IP          Type      Slot  Offset  Port          MAC_1          LAN1          MAC_2          VLAN2
192.168.70.125 Ethernet  1      0      1 00:1a:64:76:00:00
192.168.70.125 Ethernet  1      0      2 00:1a:64:76:00:01

//IP          Type      Slot  Priority WWPN          LUN
192.168.70.125 FCTarget  1  first  20:06:00:xx:xx:xx:3a  0
192.168.70.125 FCTarget  1  second 20:06:00:xx:xx:xx:3b  0

//IP          Type      Slot  Offset  Port          WWNN          WWPN          port-order
192.168.70.125 FC        1      0      3          21:80:00:e0:8b:00:00:00  first
192.168.70.125 FC        1      0      4          21:81:00:e0:8b:20:00:00  second

//IP          Type(Slot) Slot  Mode  Profile
192.168.70.125 Slot      2  enable Primary

//IP          Type      Slot  Offset  Port          MAC_1          LAN1          MAC_2          VLAN2
192.168.70.125 Ethernet  2      0      1 00:1a:64:76:00:02
192.168.70.125 Ethernet  2      0      2 00:1a:64:76:00:03

//IP          Type      Slot  Priority WWPN          LUN
192.168.70.125 FCTarget  2  first  20:06:00:xx:xx:xx:3a  0
192.168.70.125 FCTarget  2  second 20:06:00:xx:xx:xx:3b  0

//IP          Type      Slot  Offset  Port          WWNN          WWPN          port-order
192.168.70.125 FC        2      0      3          21:80:00:e0:8b:00:00:01  first
192.168.70.125 FC        2      0      4          21:81:00:e0:8b:20:00:01  second

//IP          Type(Slot) Slot  Mode  Profile
192.168.70.125 Slot      3  disable Profile: 192.168.70.125 Slot-3

//IP          Type(Slot) Slot  Mode  Profile
192.168.70.125 Slot      4  disable Profile: 192.168.70.125 Slot-4
```

「Offset」の最大値を「Max server offset」に指定
仮想アドレスを適用する「Port」に表示された
番号のチェック・ボックスをオンにする。

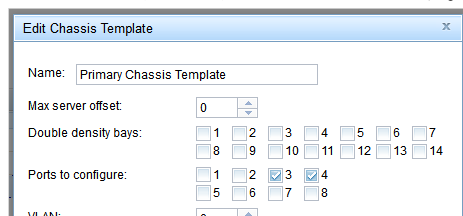
「VLAN」はPXEブート(ネットワーク・ブート)使用時に、UEFIに対して設定される値です。OSには反映されませんのでご注意ください。当ガイドでは移行しません。

「Port Ranging」は各イーサネット・ポートでMAC 2(MAC B)を使用する場合などに指定します。当ガイドでは移行しません。

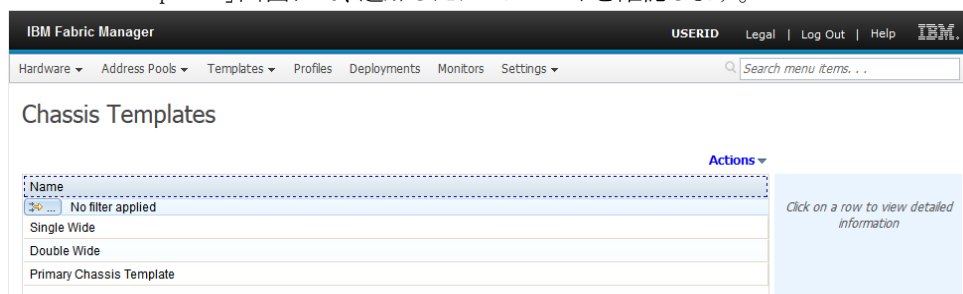
※ 「Port to configure」は次の表を確認して、仮想アドレスを適用するポートに応じて選択してください。

Port to configure	適用対象ポート	シャーシごとの接続先 I/Oモジュール・ベイ番号		
		BCE	BCS	BCH/HT
1	オンボードNICポート1	1	1	1
2	オンボードNICポート2	2	1	2
3	CIOv拡張カード・ポート1	3	3	3
4	CIOv拡張カード・ポート2	4	4	4
5	CFFh拡張カード・ポート1	N/A	2	7
6	CFFh拡張カード・ポート2	N/A	2	8
7	CFFh拡張カード・ポート3	N/A	N/A	9
8	CFFh拡張カード・ポート4	N/A	N/A	10

たとえば、SAS やファイバー・チャネルの CIOv 拡張カードに対する仮想アドレスのみ適用する場合は、3 と 4 のチェック・ボックスをオンにします。



- 「Chassis Templates」画面にて、追加したテンプレートを確認します。

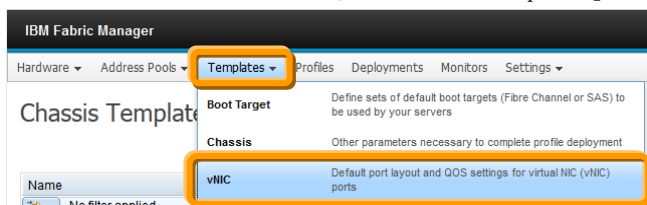


7.3.3. vNIC テンプレートの追加

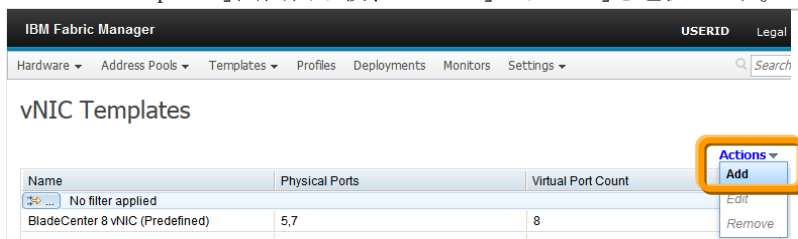
当ガイドでは移行対象に含んでおりません。必要な場合には、ここまでの手順を参考に追加してください。シャーン内に搭載されたブレード・サーバーのvNICテンプレートを作成します。各vNICポートの帯域やVLAN設定を行うことができます。

vNIC設定を移行しない場合、この手順を行う必要はありません。

1. IFM Web インターフェース上部メニューの「Templates」から「vNIC」を選択します。



2. 「Chassis Templates」画面表示後、「Actions」から「Add」を選択します。



3. 「Add vNIC Template」画面表示後、任意の名前を「Name」に入力後、「Chassis family」を「BladeCenter」に「Port count」を「8」に変更後、必要に応じて「VLAN」、「Min Bandwidth」、「Max Bandwidth」、「Priority」をダブルクリックして値を変更し、「Save」をクリックします。

Virtual Port	ASIC	Physical Port	VLAN	Min Bandwidth	Max Bandwidth	Priority
1	1	5	0	10	25	1
2	1	7	0	10	25	1
3	1	5	0	10	25	2
4	1	7	0	10	25	2
5	1	5	0	10	25	3
6	1	7	0	10	25	3
7	1	5	0	10	25	4
8	1	7	0	10	25	4

7.4. 仮想アドレスを適用するためのプロファイル作成とデプロイメント

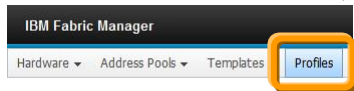
作成済みのハードウェア・プールやアドレス・プール、テンプレートを組み合わせ、仮想アドレスを適用するためのプロファイルを作成します。

プロファイル作成後にデプロイメントを行いますが、仮想アドレスは適用されません。デプロイメント後の各設定をプッシュすることで仮想アドレスが適用されますのでご注意ください。

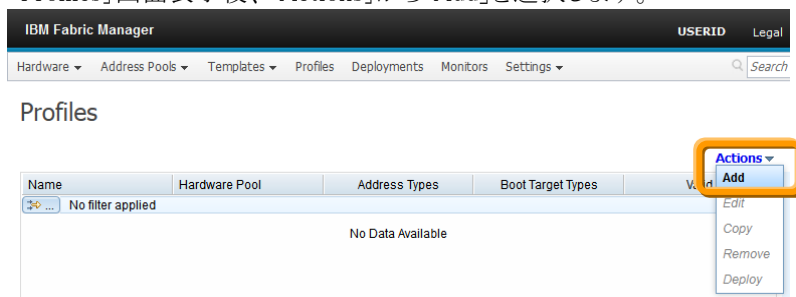
7.4.1. プロファイルの作成

当ガイドでは、ここまでの手順で作成したハードウェア・プール「Primary」と、イーサネット・プール「Primary MAC」、ファイバーチャネル・プール「Primary WWPNA」、「Primary WWPNB」、シャーシ・テンプレート「Primary Chassis Template」、ブート・ターゲット・テンプレート「Primary Boot Target」を組み合わせます。

1. IFM Web インターフェース上部メニューの「Profiles」を選択します。



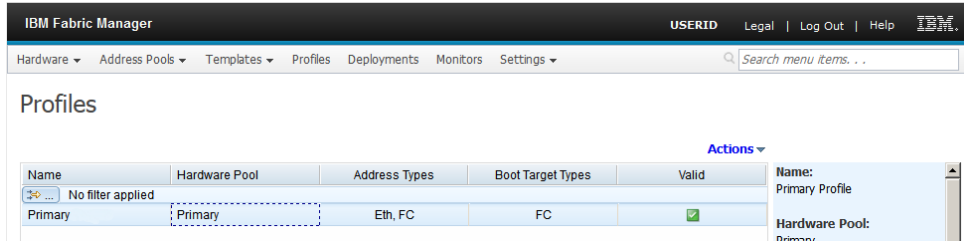
2. 「Profiles」画面表示後、「Actions」から「Add」を選択します。



3. 「Create Profile」画面にて、任意の名前を「Profile Name」に入力し、仮想アドレスを適用するブレード・サーバーの範囲を「Hardware Pool」から選択、ブレード・サーバーのベイ幅などを定義したテンプレートを「Chassis Template」から選択後、必要なアドレス・プールやテンプレートを選択し、「Save」をクリックします。

当ガイドでは「Profile Name」に【Primary】を入力し、「Hardware Pool」に【Primary】、「Ethernet Address Pool」に【Primary MAC】、「FC WWPNA Address Pool」に【Primary WWPNA】、「FC WWPNB Address Pool」に【Primary WWPNB】、「Chassis Template」に【Primary Chassis Template】、「FC Boot Target Template」に【Primary Boot Target】を選択します。

- 「Profiles」画面にて、プロファイルが作成されたことを確認します。

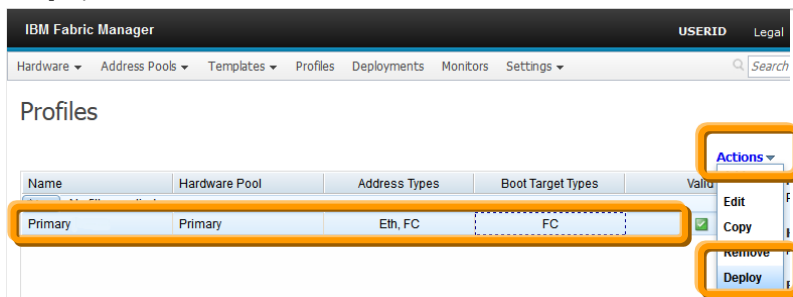


7.4.2. プロファイルのデプロイメント

作成したプロファイルを元に、各ブレード・サーバーへ仮想アドレスが適用できるよう、デプロイメントを実行します。

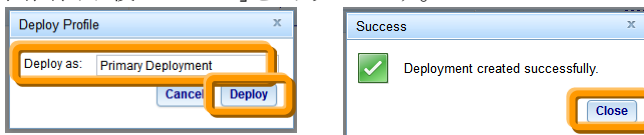
デプロイメントした内容をプッシュするまでは、仮想アドレスが適用されませんのでご注意ください。

- 「Profiles」画面にて、デプロイするプロファイル(作成したプロファイル)を選択して「Actions」から「Deploy」を選択します。



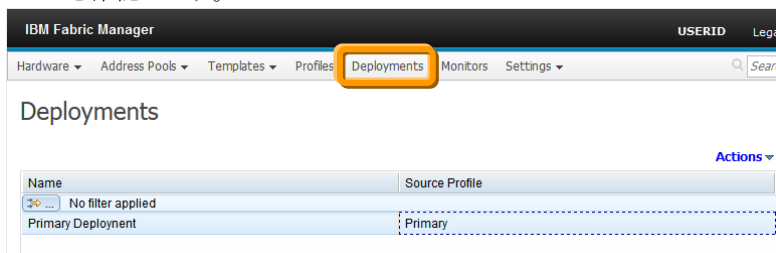
当ガイドでは【Primary】をデプロイします。

- 「Deploy Profile」画面表示後、任意の名前を「Deploy as」へ入力後に「Deploy」をクリックし、「Success」画面表示後に「Close」をクリックします。



当ガイドでは「Deploy Profile」に【Primary Deployment】を入力します。

- IFM Web インターフェース上部メニューの「Deployments」を選択し、プロファイルがデプロイメントされたことを確認します。



7.5. デプロイ後の仮想アドレスをブレード・サーバーに適用

デプロイしたプロファイルから仮想アドレスをブレード・サーバーに適用します。

新規に仮想アドレスを適用する場合には、プロファイルからデプロイした設定をそのまま適用することも可能ですが、BOFM から仮想アドレスを移行する場合にはデプロイの内容を確認し、編集する必要があります。

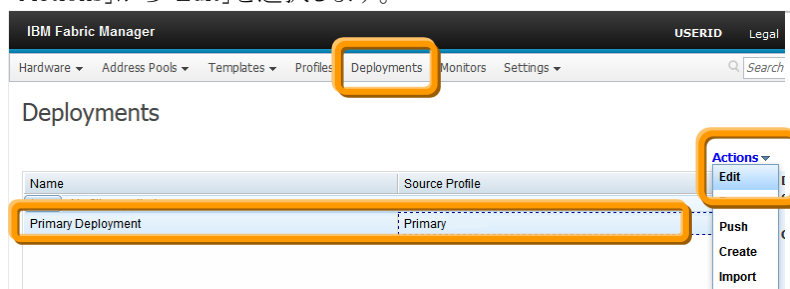
当ガイドではデプロイした設定と bofm.cfg ファイルとを確認後に編集し、ブレード・サーバーに適用（プッシュ）する手順を説明します。

7.5.1. デプロイメント内容の確認

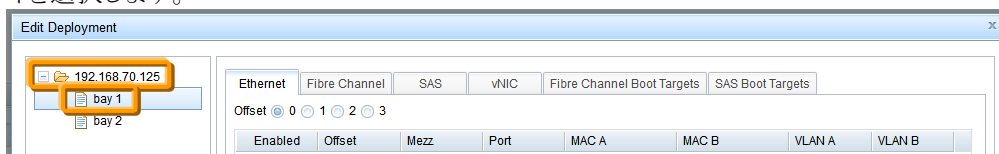
bofm.csvファイルとブレード・サーバーへ適用する仮想アドレスの確認と編集を行います。

当ガイドでは、各ブレード・サーバー・ベイに対するMACアドレスとQLogicファイバー・チャネル拡張カード（CIOv）のWWPN、ファイバーチャネル・ブート・ターゲットの確認と編集を行います。

1. IFM Web インターフェース上部メニューの「Deployments」を選択し、対象となるデプロイを選択後に「Actions」から「Edit」を選択します。



2. 「Edit Deployment」画面表示後、画面左側のシャーンを展開表示後に確認の対象となるブレード・ベイを選択します。



bofm.csv ファイル

//IP	Type(Slot)	Slot	Mode	Profile
192.168.70.125	Slot	1	enable	Primary

//IP	Type	Slot	Offset	Port	MAC_1	VLAN1	MAC_2	VLAN2
192.168.70.125	Ethernet	1	0		1 00:1a:64:76:00:00		0	
192.168.70.125	Ethernet	1	0		2 00:1a:64:76:00:01		0	

//IP	Type	Slot	Priority	WWPN	LUN
192.168.70.125	FCTarget	1	first	20:06:00:xx:xx:xx:xx:3a	0
192.168.70.125	FCTarget	1	second	20:06:00:xx:xx:xx:xx:3b	0

//IP	Type	Slot	Offset	Port	WWNN	WWPN	Boot-order
192.168.70.125	FC	1	0		3	21:80:00:e0:8b:00:00:0c	first
192.168.70.125	FC	1	0		4	21:81:00:e0:8b:20:00:0c	second

//IP	Type(Slot)	Slot	Mode	Profile
192.168.70.125	Slot	2	enable	Primary

3. 「Edit Deployment」画面にて対象となるブレード・ベイが選択されていることを確認し、「Ethernet」タブを選択後にオフセット値を含めた各値を bofm.csv ファイルと確認し、必要な場合は編集します。

bofm.csv ファイル

```
//IP      Type(Slot)  Slot  Mode  Profile
192.168.70.125 Slot      1  enable  Primary
```

//IP	Type	Slot	Offset	Port	MAC_1	VLAN1	MAC_2	VLAN2
192.168.70.125	Ethernet	1	0		1 00:1a:64:76:00:00		0	
192.168.70.125	Ethernet	1	0		2 00:1a:64:76:00:01		0	

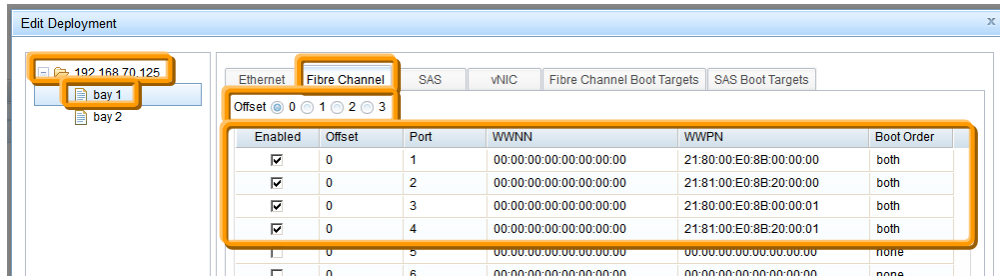
```
//IP      Type      Slot  Priority  WWPN      LUN
192.168.70.125 FCTarget  1  first    20:06:00:xx:xx:xx:3a
192.168.70.125 FCTarget  1  second  20:06:00:xx:xx:xx:3b
```

//IP	Type	Slot	Offset	Port	WWNN	WWPN	Boot-order
192.168.70.125	FC	1	0		3	21:80:00:e0:8b:00:00:0c	first
192.168.70.125	FC	1	0		4	21:81:00:e0:8b:20:00:0c	second

```
//IP      Type(Slot)  Slot  Mode  Profile
192.168.70.125 Slot      2  enable  Primary
```

当ガイドでは Port 3、4 の「Enabled」欄にあるチェック・ボックスをオフにして MAC A の欄をダブルクリック後に【00:00:00:00:00:00】へ変更します。

4. 「Edit Deployment」画面にて対象となるブレード・ベイが選択されていることを確認し、「Fibre Channel」タブを選択後にオフセット値を含めた各値を bofm.csv ファイルと確認し、必要な場合は編集します。



bofm.csv ファイル

```
//IP      Type(Slot)  Slot  Mode  Profile
192.168.70.125 Slot      1  enable  Primary
```

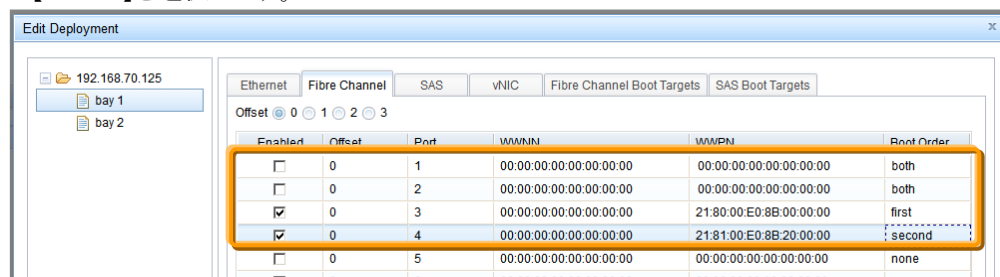
```
//IP      Type      Slot  Offset  Port      MAC_1      VLAN1      MAC_2      VLAN2
192.168.70.125 Ethernet  1      0      1      00:1a:64:76:00:00      0
192.168.70.125 Ethernet  1      0      2      00:1a:64:76:00:01      0
```

```
//IP      Type      Slot  Priority  WWPN      LUN
192.168.70.125 FCTarget  1  first  20:06:00:xx:xx:xx:3a      0
192.168.70.125 FCTarget  1  second 20:06:00:xx:xx:xx:3b      0
```

```
//IP      Type      Slot  Offset  Port      WWNN      WWPN      Boot-order
192.168.70.125 FC      1      0      3      00:00:00:00:00:00:00:00      21:80:00:e0:8b:00:00:00:00 first
192.168.70.125 FC      1      0      4      00:00:00:00:00:00:00:00      21:81:00:e0:8b:20:00:00:00 second
```

```
//IP      Type(Slot)  Slot  Mode  Profile
192.168.70.125 Slot      2  enable  Primary
```

当ガイドでは Port 1、2 の「Enabled」欄にあるチェック・ボックスをオフにして WWPN の欄をダブルクリック後に【00:00:00:00:00:00:00:00】へ変更し、Port 3 の「WWPN」をダブルクリック後に【21:80:00:E0:8B:00:00:00:00】へ変更後に「Boot Order」をダブルクリックして【first】を選択し、Port 4 の「WWPN」をダブルクリック後に【21:81:00:E0:8B:20:00:00:00】へ変更後に「Boot Order」をダブルクリックして【second】を選択します。



5. 「Edit Deployment」画面にて対象となるブレード・ベイが選択されていることを確認し、「Fibre Channel Boot Targets」タブを選択後に各値を bofm.csv ファイルと確認し、必要な場合は編集後に「Submit」をクリックします。

bofm.csv ファイル

```
//IP      Type(Slot)  Slot  Mode  Profile
192.168.70.125 Slot          1 enable Primary
```

```
//IP      Type      Slot  Offset  Port          MAC_1      VLAN1      MAC_2      VLAN2
192.168.70.125 Ethernet  1      0        0          1 00:1a:64:76:00:00      0
192.168.70.125 Ethernet  1      0        0          2 00:1a:64:76:00:01      0
```

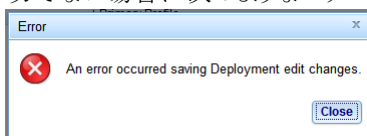
```
//IP      Type      Slot  Priority WWPN          LUN
192.168.70.125 FCTarget  1 first  20:06:00:xx:xx:xx:3a      0
192.168.70.125 FCTarget  1 second 20:06:00:xx:xx:xx:3b      0
```

```
//IP      Type      Slot  Offset  Port          WWNN      WWPN      Boot-order
192.168.70.125 FC          1      0        0          3          21:80:00:e0:8b:20:00:00 first
192.168.70.125 FC          1      0        0          4          21:81:00:e0:8b:20:00:00 second
```

```
//IP      Type(Slot)  Slot  Mode  Profile
192.168.70.125 Slot          2 enable Primary
```

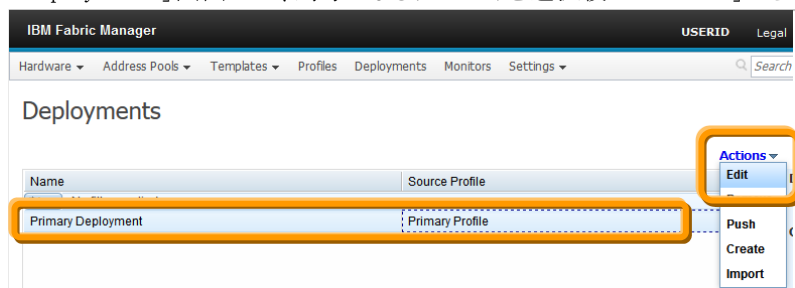
当ガイドでは「Primary Boot Targets」の 1 〜 bofm.csv ファイルの「Priority」が「first」と表示されている「WWPN」の値【20:06:00:xx:xx:xx:3A】が、「Secondary Boot Targets」の 1 〜 bofm.csv ファイルの「Priority」が「second」と表示されている「WWPN」の値【20:06:00:xx:xx:xx:3B】が入力されていることを確認します。

- ※ すべてのブレード・サーバー・ベイに対する編集を行った後に「Submit」をクリックして設定を反映させることもできますが、各ブレード・サーバー・ベイのMACアドレスやWWPNが重複するなど入力項目が適切でない場合に次のようなエラー画面が表示されます。

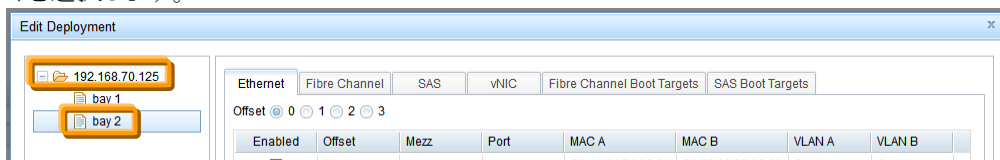


このエラー画面が表示されると、IFMのWebインターフェースからログアウト後に再度ログインするまで、正しい値に修正しても表示され続けます。また、それまでの編集内容が失われる場合もありますので、各ベイで編集を行った後に「Submit」をクリックして、個々に反映することをお勧めします。

6. 「Deployments」画面にて、対象となるデプロイを選択後に「Actions」から「Edit」を選択します。



7. 「Edit Deployment」画面表示後、画面左側のシャーシを展開表示後に確認の対象となるブレード・ベイを選択します。



bofm.csv ファイル

//IP	Type(Slot)	Slot	Mode	Profile
192.168.70.125	Slot	2	enable	Primary

//IP	Type	Slot	Offset	Port	MAC_1	VLAN1	MAC_2	VLAN2
192.168.70.125	Ethernet	2	0		1 00:1a:64:76:00:02		0	
192.168.70.125	Ethernet	2	0		2 00:1a:64:76:00:03		0	

//IP	Type	Slot	Priority	WWPN	LUN
192.168.70.125	FCTarget	2	first	20:06:00:xx:xx:xx:3a	0
192.168.70.125	FCTarget	2	second	20:06:00:xx:xx:xx:3b	0

//IP	Type	Slot	Offset	Port	WWNN	WWPN	Boot-order
192.168.70.125	FC	2	0		3	21:80:00:e0:8b:00:00:01	first
192.168.70.125	FC	2	0		4	21:81:00:e0:8b:20:00:01	second

//IP	Type(Slot)	Slot	Mode	Profile
192.168.70.125	Slot	3	disable	Profile: 192.168.70.125 Slot-3

8. 「Edit Deployment」画面にて対象となるブレード・ベイが選択されていることを確認し、「Ethernet」タブを選択後にオフセット値を含めた各値を bofm.csv ファイルと確認し、必要な場合は編集します。

Enabled	Offset	Mezz	Port	MAC A	MAC B	VLAN A	VLAN B
<input checked="" type="checkbox"/>	0	1	1	00:1A:64:76:00:04	00:00:00:00:00:00	0	0
<input checked="" type="checkbox"/>	0	1	2	00:1A:64:76:00:05	00:00:00:00:00:00	0	0
<input checked="" type="checkbox"/>	0	1	3	00:1A:64:76:00:06	00:00:00:00:00:00	0	0
<input checked="" type="checkbox"/>	0	1	4	00:1A:64:76:00:07	00:00:00:00:00:00	0	0
<input type="checkbox"/>	0	1	5	00:00:00:00:00:00	00:00:00:00:00:00	0	0
<input type="checkbox"/>	0	1	6	00:00:00:00:00:00	00:00:00:00:00:00	0	0

bofm.csv ファイル

```
//IP      Type(Slot)  Slot  Mode  Profile
192.168.70.125 Slot      2 enable Primary
```

//IP	Type	Slot	Offset	Port	MAC_1	VLAN1	MAC_2	VLAN2
192.168.70.125	Ethernet	2	0	1	00:1a:64:76:00:02		0	
192.168.70.125	Ethernet	2	0	2	00:1a:64:76:00:03		0	

```
//IP      Type      Slot  Priority WWPN      LUN
192.168.70.125 FCTarget 2 first 20:06:00:xx:xx:xx:3a 0
192.168.70.125 FCTarget 2 second 20:06:00:xx:xx:xx:3b 0
```

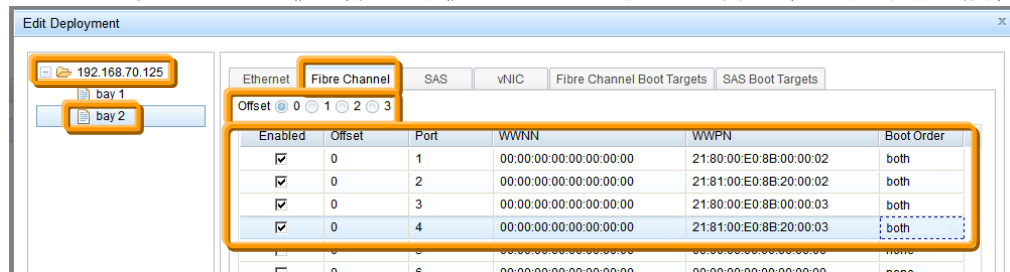
```
//IP      Type      Slot  Offset Port      WWNN      WWPN      Boot-order
192.168.70.125 FC      2      0      3      21:80:00:e0:8b:20:00:01 first
192.168.70.125 FC      2      0      4      21:81:00:e0:8b:20:00:01 second
```

```
//IP      Type(Slot)  Slot  Mode  Profile
192.168.70.125 Slot      3 disable Profile: 192.168.70.125 Slot-3
```

当ガイドでは Port 1 の MAC A 欄をダブルクリック後に【00:1A:64:76:00:02】に変更し、Port 2 の MAC A 欄をダブルクリック後に【00:1A:64:76:00:03】に変更し、Port 3、4 の「Enabled」欄にあるチェック・ボックスをオフにして MAC A 欄をダブルクリック後に【00:00:00:00:00:00】へ変更します。

Enabled	Offset	Mezz	Port	MAC A	MAC B	VLAN A	VLAN B
<input checked="" type="checkbox"/>	0	1	1	00:1A:64:76:00:02	00:00:00:00:00:00	0	0
<input checked="" type="checkbox"/>	0	1	2	00:1A:64:76:00:03	00:00:00:00:00:00	0	0
<input type="checkbox"/>	0	1	3	00:00:00:00:00:00	00:00:00:00:00:00	0	0
<input type="checkbox"/>	0	1	4	00:00:00:00:00:00	00:00:00:00:00:00	0	0
<input type="checkbox"/>	0	1	5	00:00:00:00:00:00	00:00:00:00:00:00	0	0
<input type="checkbox"/>	0	1	6	00:00:00:00:00:00	00:00:00:00:00:00	0	0

9. 「Edit Deployment」画面にて対象となるブレード・ベイが選択されていることを確認し、「Fibre Channel」タブを選択後にオフセット値を含めた各値を bofm.csv ファイルと確認し、必要な場合は編集します。



bofm.csv ファイル

```
//IP      Type(Slot)  Slot  Mode  Profile
192.168.70.125 Slot      2  enable  Primary

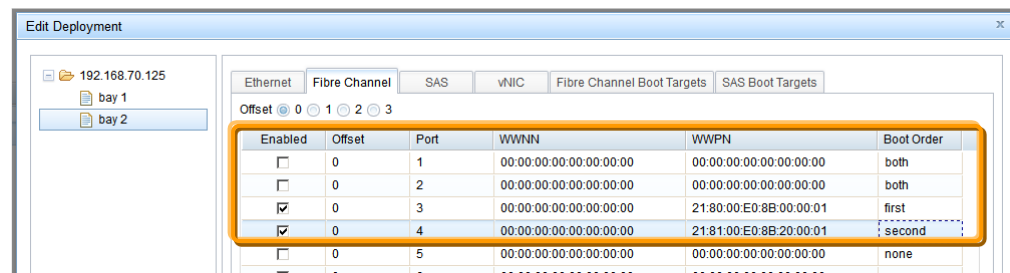
//IP      Type      Slot  Offset  Port      MAC.1      VLAN1      MAC.2      VLAN2
192.168.70.125 Ethernet  2      0      1      00:1a:64:76:00:02      0
192.168.70.125 Ethernet  2      0      2      00:1a:64:76:00:03      0

//IP      Type      Slot  Priority  WWPN      LUN
192.168.70.125 FCTarget  2  first  20:06:00:xx:xx:xx:xx:3a      0
192.168.70.125 FCTarget  2  second 20:06:00:xx:xx:xx:xx:3b      0

//IP      Type      Slot  Offset  Port      WWNN      WWPN      Boot-order
192.168.70.125 FC      2      0      3      00:00:00:00:00:00:00:00      21:80:00:e0:8b:00:00:00:01 first
192.168.70.125 FC      2      0      4      00:00:00:00:00:00:00:00      21:81:00:e0:8b:20:00:00:01 second

//IP      Type(Slot)  Slot  Mode  Profile
192.168.70.125 Slot      3  disable  Profile: 192.168.70.125 Slot-3
```

当ガイドでは Port 1、2 の「Enabled」欄にあるチェック・ボックスをオフにして WWPN の欄をダブルクリック後に【00:00:00:00:00:00:00:00】へ変更し、Port 3 の「WWPN」をダブルクリック後に【21:80:00:E0:8B:00:00:01】へ変更後に「Boot Order」をダブルクリックして【first】を選択し、Port 4 の「WWPN」をダブルクリック後に【21:81:00:E0:8B:20:00:01】へ変更後に「Boot Order」をダブルクリックして【second】を選択します。



10. 「Edit Deployment」画面にて対象となるブレード・ベイが選択されていることを確認し、「Fibre Channel Boot Targets」タブを選択後に各値を bofm.csv ファイルと確認し、必要な場合は編集後に「Submit」をクリックします。

bofm.csv ファイル

```
192.168.70.125 FCtarget      1 second 20:06:00:xx:xx:xx:3b      0

//IP      Type      Slot  Offset  Port      WWNN      WWPN      Boot-order
192.168.70.125 FC      1      0      3      21:80:00:e0:8b:00:00:0f first
192.168.70.125 FC      1      0      4      21:81:00:e0:8b:20:00:0f second

//IP      Type(Slot)  Slot  Mode  Profile
192.168.70.125 Slot      2 enable Primary

//IP      Type      Slot  Offset  Port      MAC_1      VLAN1      MAC_2      VLAN2
192.168.70.125 Ethernet      2      0      1 00:1a:64:76:00:02      0
192.168.70.125 Ethernet      2      0      2 00:1a:64:76:00:03      0

//IP      Type      Slot  Priority WWPN      LUN
192.168.70.125 FCtarget      2 first  20:06:00:xx:xx:xx:3a      0
192.168.70.125 FCtarget      2 second 20:06:00:xx:xx:xx:3b      0
```

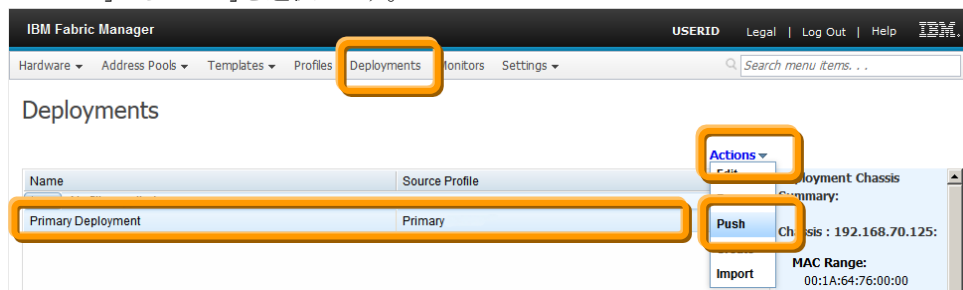
当ガイドでは「Primary Boot Targets」の 1 へ bofm.csv ファイルの「Priority」が「first」と表示されている「WWPN」の値【20:06:00:xx:xx:xx:3A】が、「Secondary Boot Targets」の 1 へ bofm.csv ファイルの「Priority」が「second」と表示されている「WWPN」の値【20:06:00:xx:xx:xx:3B】が入力されていることを確認します。

11. 追加した仮想アドレスを適用するために、69 ページの「8. 仮想アドレスをブレード・サーバーへ適用 (デプロイメントのプッシュ)」の手順に進みます。

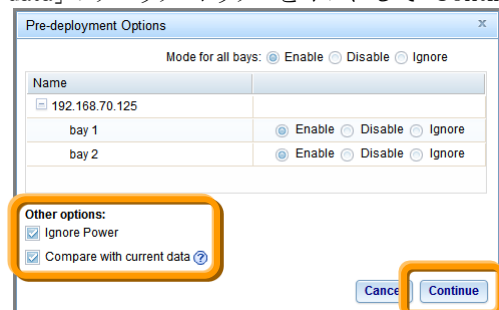
8. 仮想アドレスをブレード・サーバーへ適用（デプロイメントのプッシュ）

確認および編集後のデプロイメント設定をブレード・サーバーへ適用します。

1. IFM Web インターフェース上部メニューの「Deployments」を選択し、対象となるデプロイを選択後に「Actions」から「Push」を選択します。

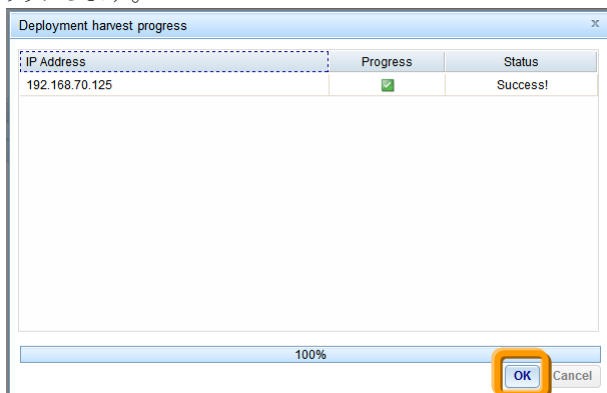


2. 「Pre-deployment Options」画面表示後、「Other options」の「Ignore Power」と「Compare with current data」のチェック・ボックスをオンにして「Continue」をクリックします。

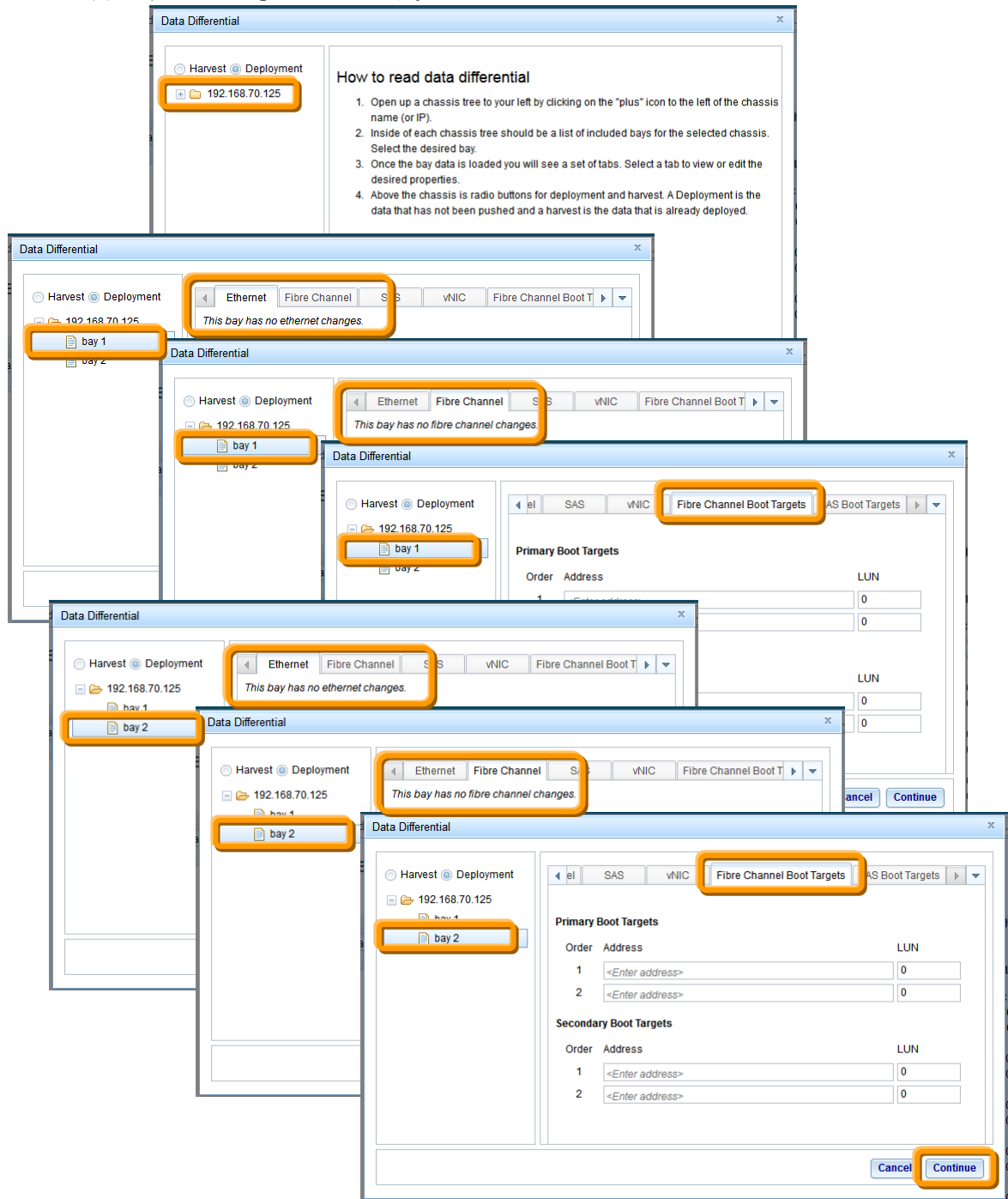


当ガイドでは、起動中のブレード・サーバーを考慮して「Ignore Power」チェック・ボックスをオンにし、電源の状態を無視します。また、「Compare with current data」のチェック・ボックスをオンにして現在使用中の仮想アドレス構成と違いがないかを確認します。

3. 「Deployment harvest progress」画面にて、「Status」に「Success」と表示されたことを確認し、「OK」をクリックします。

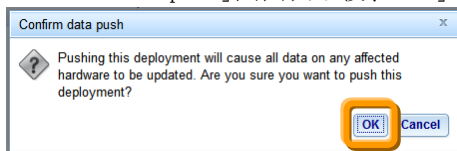


4. 「Data Differential」画面表示後、各ベイの仮想アドレスを適用するタブを確認し、何も表示されていないことを確認し、「Continue」をクリックします。

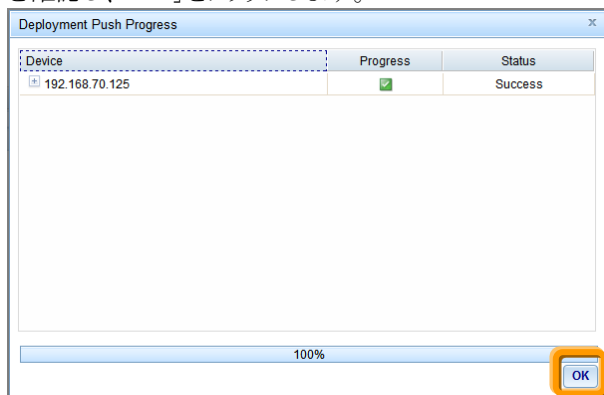


※ 現在使用中の構成と異なる部分のみ表示されます。異なる部分が表示されている場合には「Cancel」をクリックし、42ページ「6.3. デプロイメント (仮想アドレス設定) の確認」、または、61ページ「7.5. デプロイ後の仮想アドレスをブレード・サーバーに適用」の手順を参考に修正を行ってください。

5. 「Confirm data push」画面表示後、「OK」をクリックしてプッシュ処理を開始します。



6. 「Deployment Push Progress」画面にて、「Status」に「Success」と表示され、プッシュ処理が完了したことを確認し、「OK」をクリックします。



7. 仮想アドレスのフェイルオーバー機能を使用する場合は、次のページに進みます。

9. フェイル・オーバー・モニター（仮想アドレスのフェイルオーバー）設定

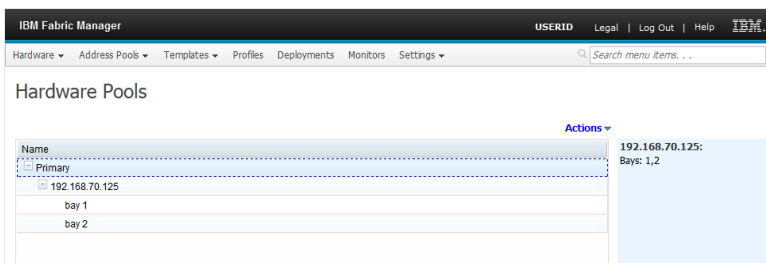
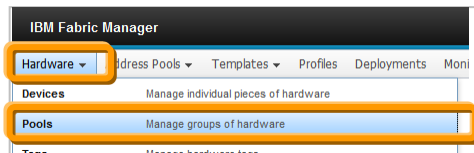
仮想アドレスのフェイルオーバーを使用するには、管理対象となるプライマリー・ハードウェア・プールと、フェイルオーバー時の切り替え先となるスタンバイ・ハードウェア・プール、それぞれにブレード・サーバーを追加しておく必要があります。

プライマリー・ハードウェア・プールのブレード・サーバーにて、モニターの作成時に選択したイベントが発生した場合にスタンバイ・ハードウェア・プールに追加済みのブレード・サーバーに仮想アドレスをフェイルオーバーします。

9.1. プライマリー・ハードウェア・プールの確認

ハードウェア・プールに仮想アドレスのフェイルオーバーで監視対象となるブレード・サーバーが追加されているか確認します。

1. IFM Web インターフェース上部メニューの「Hardware」から「Pools」を選択し、「Hardware Pools」画面にて、仮想アドレスのフェイルオーバーで監視対象となるブレード・サーバーの範囲が追加されていることを確認します。



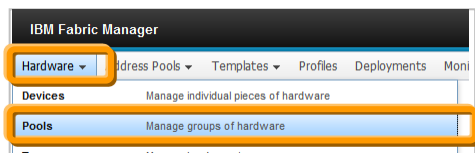
当ガイドでは、ブレード・サーバー・ベイ1と2を追加した「Primary」という名前のハードウェア・プールを、仮想アドレスのフェイルオーバーで監視対象とします。

このハードウェア・プールはデプロイメント機能により仮想アドレスを適用済みです。

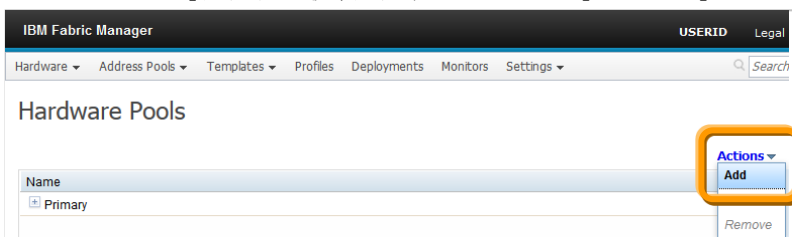
9.2. スタンバイ・ハードウェア・プールの追加

仮想アドレスのフェイルオーバー先となるブレード・サーバーをハードウェア・プールに追加します。

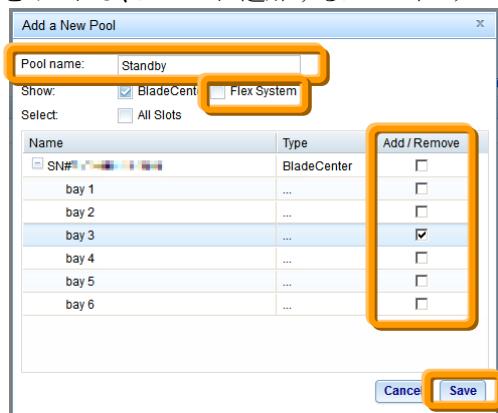
1. IFM Web インターフェース上部メニューの「Hardware」から「Pools」を選択します。



2. 「Hardware Pools」画面表示後、画面右側の「Actions」から「Add」を選択します。

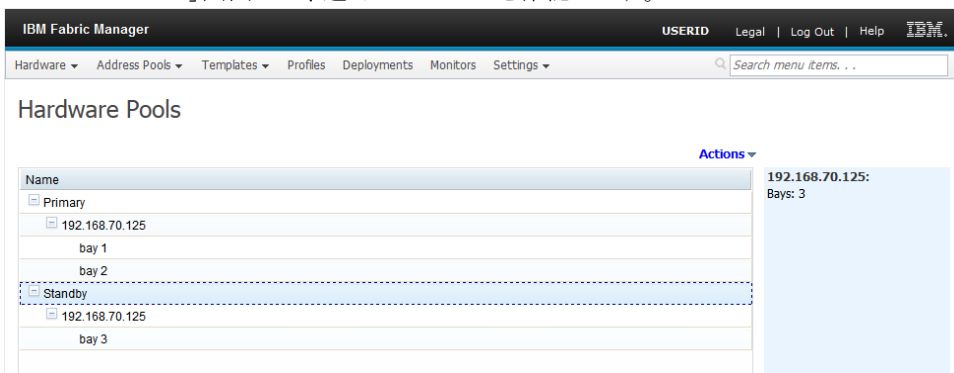


3. 「Add a New Pool」画面表示後、任意の名前で「Pool name」を入力後に「Flex System」チェック・ボックスをオフにし、プールに追加するブレード・サーバー・ベイを選択して「Save」をクリックして追加します。



当ガイドでは、「Pool name」に「Standby」を入力し、ベイ 3 のブレード・サーバーを仮想アドレスのフェイルオーバー先として追加します。

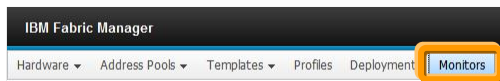
4. 「Hardware Pools」画面にて、追加したプールを確認します。



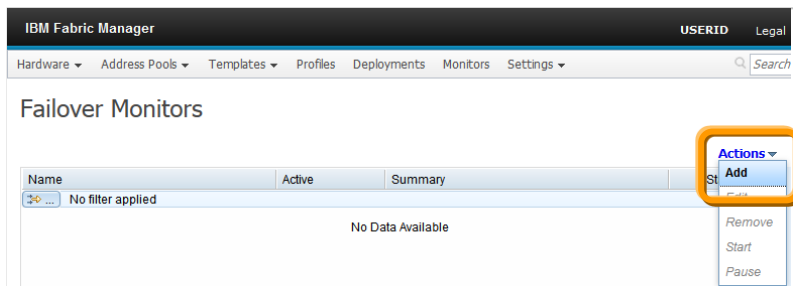
9.3. フェイルオーバー・モニターの追加

監視対象となるハードウェア・プールと仮想アドレスのフェイルオーバー先となるハードウェア・プールに、フェイルオーバーのトリガーとなるイベントを設定してモニターへ追加します。

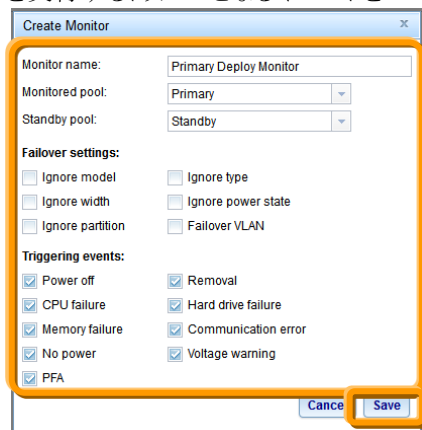
1. IFM Web インターフェース上部メニューの「Monitors」を選択します。



2. 「Failover Monitors」画面表示後、画面右側の「Actions」から「Add」を選択します。

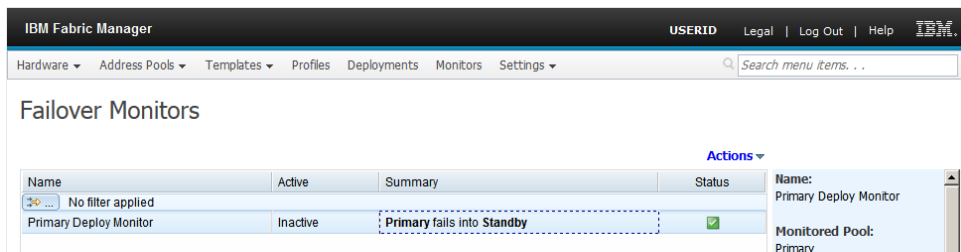


3. 「Create Monitor」画面表示後、任意の名前を「Monitor name」に入力後、監視対象となるハードウェア・プールを「Monitored pool」に選択して仮想アドレスのフェイルオーバー先となるハードウェア・プールを「Standby pool」に選択し、フェイルオーバー時の設定を「Failover settings」で、フェイルオーバーを実行するトリガーとなるイベントを「Triggering events」の一覧から選択して「Save」をクリックします。



当ガイドでは「Monitor name」に【Primary Deploy Monitor】を入力し、「Monitored Pool」には【Primary】、「Standby pool」には【Standby】を選択後、すべての「Triggering events」を選択しています。

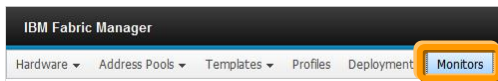
4. 「Failover Monitors」画面にて、モニターが追加されたことを確認します。



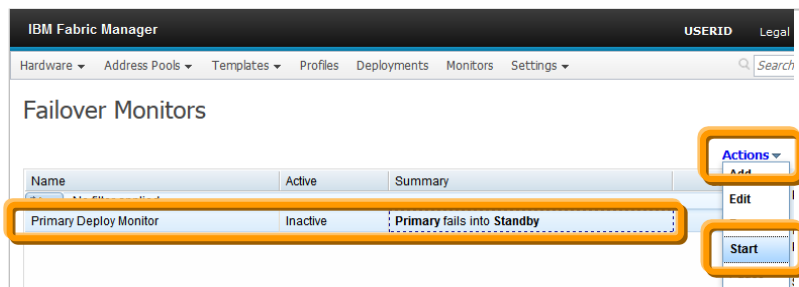
9.4. フェイルオーバー・モニターを開始

プライマリ・ハードウェア・プール内のブレード・サーバーにてトリガー・イベントが発生した場合に、自動的にスタンバイ・ハードウェア・プール内のブレード・サーバーへ仮想アドレスがフェイルオーバーするようにモニター機能を開始します。

1. IFM Web インターフェース上部メニューの「Monitors」を選択します。



2. 「Failover Monitors」画面表示後、開始するモニターの名前を選択して「Actions」から「Start」を選択し、モニター機能を開始します。



開始後のモニター機能を停止する場合は「Pause」から実行できます。

10. 参考資料

各製品マニュアルやガイドへのリンクとなります。

IBM Fabric Manager (インフォメーション・センター)

http://pic.dhe.ibm.com/infocenter/flexsys/information/topic/com.ibm.acc.iofm.doc/dw1li_product_page.html

IBM Fabric Manager 初期導入_設定ガイド (Flex System / BladeCenter 編)

<http://www.ibm.com/jp/domino04/pc/support/Sylphd07.nsf/jtechinfo/SYJ0-02C4792>

IBM Fabric Manager for Flex System / BladeCenter FAQ

<http://www-06.ibm.com/jp/domino04/pc/support/Sylphd07.nsf/jtechinfo/SYJ0-0317C29>

Feature on Demand (FOD) ライセンス・アクティベーション・ガイド

<http://www.ibm.com/jp/domino04/pc/support/Sylphd07.nsf/jtechinfo/SYJ0-03B4811>

Features on Demand

<http://www.ibm.com/systems/x/fod/>

IBM BladeCenter Open Fabric Manager Basic 設定ガイド

<http://www.ibm.com/jp/domino04/pc/support/Sylphd07.nsf/jtechinfo/SYJ0-0473B5B>

IBM BladeCenter Open Fabric Manager v3.x FAQ

<http://www.ibm.com/jp/domino04/pc/support/sylphd07.nsf/jtechinfo/syj0-0473b5f>

IBM BladeCenter Open Fabric Manager v3.0 Advanced Upgrade 設定ガイド

<http://www.ibm.com/jp/domino04/pc/support/Sylphd07.nsf/jtechinfo/SYJ0-0473B5A>

IBM BladeCenter Open Fabric Manager v3.0 Advanced Upgrade VLAN 設定ガイド

<http://www.ibm.com/jp/domino04/pc/support/Sylphd07.nsf/jtechinfo/SYJ0-0473B5V>

IBM BladeCenter Open Fabric Manager 4 Advanced Upgrade FAQ

<http://www.ibm.com/jp/domino04/pc/support/Sylphd07.nsf/jtechinfo/SYJ0-0309DD9>

IBM BladeCenter Open Fabric Manager v4.x Advanced Upgrade 導入ガイド

<http://www-.ibm.com/jp/domino04/pc/support/Sylphd07.nsf/jtechinfo/SYJ0-038E11C>

IBM BladeCenter Open Fabric Manager v4.x Advanced Upgrade 設定ガイド

<http://www.ibm.com/jp/domino04/pc/support/Sylphd07.nsf/jtechinfo/SYJ0-02D701F>

Installation and User's Guide - IBM BladeCenter Open Fabric Manager (BOFM)

<http://www.ibm.com/support/entry/portal/docdisplay?Indocid=MIGR-5086714>