冗長化構成Gfarm監視機能

導入・設定マニュアル

第1.2版

作成日：2014年8月27日

変更履歴

|  |  |  |  |
| --- | --- | --- | --- |
| 版数 | 日付 | 変更内容 | 作成者 |
| draft | 2012/01/30 | 新規作成 | SRA |
| 0.1 | 2012/02/08 | 加筆・修正した。 | SRA |
| 0.2 | 2012/02/16 | 加筆・修正した。 | SRA |
| 1.0 | 2012/03/16 | 加筆・修正した。 | SRA |
| 1.0.1 | 2012/10/10 | 以下のファイル名の誤記を修正した。  ・userparameter\_gfarm\_redundant.conf  ・register.php | SRA |
| 1.0.2 | 2012/10/12 | * 「ファイル一覧」の表を、Zabbix公式サイト提供分とgfarm\_zabbixパッケージ提供分で分割した。 * 「zabbix\_gfarm2.zip」という表記を、「gfarm\_zabbixパッケージ」に改めた。 * 「Gfarm\_zabbix監視項目一覧.xls」というファイル名の誤記を修正した。 * 細かな誤植を修正した。 | SRA |
| 1.0.3 | 2012/11/21 | ・gfarm\_zabbix用インストールスクリプトを用意したので、本書もそのスクリプトを用いた手順を記述した。 | SRA |
|  | 2012/12/06 | ・2012/11/2の変更で、zabbix\_serverの起動に関する記述を削除してしまったため、直した。 | SRA |
| 1.1 | 2013/03/22 | ・CentOS6に対応した。  ・章立てを変更した。 | SRA |
|  | 2014/05/23 | ・マクロMONITOR\_GFMD\_DIRECTORY, MONITOR\_GFSD\_DIRECTORY についての記述を追加した。 | SRA |
| 1.2 | 2014/08/27 | ・gfarm\_zabbix 1.2用に改訂した。 | SRA |

目次

[1. はじめに 1](#_Toc396914287)

[1.1. gfarm\_zabbixパッケージの構成 1](#_Toc396914288)

[1.2. 動作環境 1](#_Toc396914289)

[2. システム構成 3](#_Toc396914290)

[2.1. Zabbix基本構成 3](#_Toc396914291)

[2.2. Gfarm構成 4](#_Toc396914292)

[2.3. Zabbix分散監視構成 4](#_Toc396914293)

[3. インストール 6](#_Toc396914294)

[3.2. Zabbixサーバのインストール 6](#_Toc396914295)

[3.3. Zabbixエージェントのインストール 15](#_Toc396914296)

[3.4. gfarm\_zabbixパッケージのインストール 16](#_Toc396914297)

[3.4.1. install.confの編集 16](#_Toc396914298)

[3.4.2. Zabbixエージェント用ファイルのインストール 17](#_Toc396914299)

[3.4.3. クライアント設定ファイル編集機能のインストール 19](#_Toc396914300)

[4. 各ノードの設定 20](#_Toc396914301)

[4.1. zabbixユーザの登録と共通認証鍵の作成 20](#_Toc396914302)

[4.2. 監視サーバの設定 20](#_Toc396914303)

[4.2.1. Zabbixサーバの設定 20](#_Toc396914304)

[4.2.2. Zabbixエージェントの設定 (分散監視構成の場合) 21](#_Toc396914305)

[4.2.3. クライアント設定ファイル編集機能の設定 22](#_Toc396914306)

[4.3. 監視サーバ以外の設定 23](#_Toc396914307)

[4.3.1. Zabbixエージェントの設定 23](#_Toc396914308)

[4.3.2. gfarm\_zabbixスクリプトの設定 24](#_Toc396914309)

[4.4. zabbix\_getによる動作確認 24](#_Toc396914310)

[5. 監視設定 27](#_Toc396914311)

[5.1. 監視項目の設定 27](#_Toc396914312)

[5.1.1. Gfarm監視用テンプレートの導入 27](#_Toc396914313)

[5.1.2. ホストグループの設定 29](#_Toc396914314)

[5.1.3. ホストの追加 31](#_Toc396914315)

[6. 分散監視構成設定 36](#_Toc396914316)

[6.1. 分散監視設定の準備 36](#_Toc396914317)

[6.2. マスターノードの分散監視設定 37](#_Toc396914318)

[6.3. 子ノードの分散監視設定 39](#_Toc396914319)

[6.4. 相互監視構成設定 41](#_Toc396914320)

[7. フェイルオーバ実行機能の設定 42](#_Toc396914321)

[7.1. SSH公開鍵の生成と配布 42](#_Toc396914322)

[7.2. zabbixユーザのsudo権限の設定 43](#_Toc396914323)

[7.3. フェイルオーバスクリプトの設定ファイルの編集 43](#_Toc396914324)

[7.4. Webインターフェース上での設定 45](#_Toc396914325)

[8. その他の注意点 47](#_Toc396914326)

[8.1. SELinux環境での問題 47](#_Toc396914327)

# はじめに

本ドキュメントは、Gfarmファイルシステム (以降、Gfarmとする) における統合監視ソフトウェアZabbix (http://www.zabbix.com/) で構成された障害監視システム(以降、gfarm\_zabbix) を導入する際の、手順および設定について記載したものである。

Zabbixによる障害監視システムの導入から、Gfarmの障害監視を行うためのZabbixの初期設定までを対象とする。導入後の管理・利用方法等については、「冗長化構成Gfarm監視機能 管理・利用マニュアル」を参照のこと。

なお、チケット管理システムのインストールに関しては、別途「異常時チケット登録機能」の「導入・設定マニュアル」を、運用に関しては「冗長化構成Gfarm監視機能 管理・利用マニュアル」を参照されたい。

本ドキュメントは、gfarm\_zabbixバージョン1.2に対応している。

## gfarm\_zabbixパッケージの構成

gfarm\_zabbixパッケージは、以下の内容で構成されている。

* **Zabbix向けGfarm監視モジュール**

監視モジュールはさらに、Zabbix向けの監視テンプレート、監視用の外部スクリプトおよびフェイルオーバスクリプトで構成される。これらを導入することで、Gfarmの稼働状況をZabbixで監視できるようになる。また、フェイルオーバスクリプトを用いることで、Gfarmに障害が発生した祭、メタデータサーバを自動的にフェイルオーバできるようになる。

* **クライアント設定ファイル編集機能**

Gfarmクライアントの設定ファイル (gfarm2.conf) をWeb上で編集する機能。

* **ドキュメント**

Zabbix向けGfarm監視モジュールや、クライアント設定ファイル編集機能に関するドキュメント。

## 動作環境

gfarm\_zabbixの動作環境は、次のものを対象としている。

表 1‑1 動作環境の要件一覧

|  |  |
| --- | --- |
| 区分 | 要件 |
| OS | Red Hat Enterprise Linux 6 またはCentOS 6 |
| Zabbix | 1.8系または2.2系 |
| 監視対象とするGfarm | 2.5.8.10以上 |

本書の解説は主にZabbix 1.8系を対象に行なっている。スクリーンショット等もすべて1.8系のものである。2.2系において操作手順が異なる場合、必要な箇所ではその旨を説明してあるが、多くは本書の読者が独力で容易に対処できる部分であり、特に説明はしていない。

# システム構成

Gfarm にZabbixを導入するにあたり、Zabbixの基本構成とGfarm上での構成について説明する。

## Zabbix基本構成

Zabbixは以下の要素により構成されている。

* **Zabbixサーバ**

監視項目や収集した監視データを管理し、障害の検出や通知等を行う。監視項目や、収集した監視データを、データベース上に保存する。

* **Zabbixエージェント**

監視対象ノード上で動作し、監視データの収集およびZabbixサーバへの送信を行う。

* **Zabbix Webインターフェース**

監視項目の設定や監視データの閲覧等を行うためのWebインターフェースを提供する。

以下に構成図を示す。

**監視対象ノード (1台以上)**

**監視サーバ**

設定意

監視データ閲覧意

監視データ収集

DB

取得/保存

監視設定意

監視データ意

図 2‑1 Zabbix基本構成

## Gfarm構成

gfarm\_zabbixでは、GfarmのサーバおよびクライアントをZabbixの監視対象ノードとすることでGfarmの監視を行う。具体的には、Gfarm側は次のような構成となる。

**監視サーバ**

**監視対象ノード**

**(メタデータサーバ)**

DB

監視

設定

監視

データ

**監視対象ノード**

**(メタデータサーバ)**

**監視対象ノード**

**(ファイルシステムノード)**

**監視対象ノード**

**(ファイルシステムノード)**

**監視対象ノード**

**(代表クライアント)**

**監視対象ノード**

**(一般クライアント)**

**監視対象ノード**

**(一般クライアント)**

図 2‑2 Gfarm監視対象ノード構成

gfarm\_zabbixにはクライアントに「代表クライアント」と「一般クライアント」の2種類がある。代表クライアントは、サーバの動作状況に関する監視をその他のクライアントよりも詳しく行う。Gfarmのクライアントとして稼働しているホストの中から1台を選んで代表クライアントとし、その他は一般クライアントという位置付けにする。メタデータサーバもしくはファイルシステムノードが、代表クライアントを兼任しても良い。

## Zabbix分散監視構成

gfarm\_zabbixは、Zabbixによる分散監視構成に対応している。この構成では、親子関係にある監視サーバ間 (マスターノード－子ノード間) で相互監視を行うことで、監視サーバ自体の障害監視も行うことが可能である。以下に、ホスト構成を示す。

**監視サーバ**

**(マスターノード)**

**監視対象ノード**

**(1台以上)**

DB

監視

設定

監視

データ

参照

**監視サーバ**

**(子ノード)**

DB

監視データ

監視

設定

監視データ

監視

設定

監視設定

監視データ

図 2‑3 Zabbix分散監視構成

監視サーバは、それぞれ以下のような役割を持つ。

* **マスターノード**

全ての子ノードの監視設定および、監視データの参照を行う。

* **子ノード**

自身の配下の監視対象ノードの監視設定と、監視データを管理する。単独で動作可能であり、障害通知も行う。子ノード側の監視設定は、マスターノードでも閲覧や変更が可能であり、定期的に同期している。

# インストール

本章では、Zabbixサーバ、Zabbixエージェント、gfarm\_zabbixパッケージのインストール手順について記載する。本ドキュメントで扱うZabbixのバージョンは、1.8.20とする。また、ZabbixサーバおよびZabbix Webインターフェースで利用するデータベースは、Zabbixで推奨されているMySQLを利用するものとする。

本章ではインストールする必要のあるアプリケーションのインストール作業手順を記述してある。本章は確認する程度に読み進め、実際の作業は「4 各ノードの設定」に進み、その内容に応じて本章を参照して作業を行うこと。

* 1. **インストール対象とインストールするソフトウェア**

インストールする必要のあるソフトウェアは、ノードの種類毎に異なる。

表 3‑1 インストールするソフトウェア一覧

|  |  |
| --- | --- |
| ノード | インストールするソフトウェア |
| 監視サーバ | Zabbixサーバ  Zabbix Webインターフェース  Zabbixエージェント (分散監視構成の場合)  gfarm\_zabbixパッケージ |
| Gfarmメタデータサーバ | Zabbixエージェント  gfarm\_zabbixパッケージ |
| Gfarmファイルシステムノード | Zabbixエージェント  gfarm\_zabbixパッケージ |
| 代表クライアント | Zabbixエージェント  gfarm\_zabbixパッケージ |
| 一般クライアント | Zabbixエージェント  gfarm\_zabbixパッケージ |

## Zabbixサーバのインストール

監視サーバ各機に対して、Zabbixサーバをインストールする手順を示す。なお、手順は全てrootユーザで実行する。

1. yumリポジトリ登録用RPMを取得する。

|  |
| --- |
| # wget http://repo.zabbix.com/zabbix/1.8/rhel/6/x86\_64/zabbix-release-1.8-1.el6.noarch.rpm |

1. yumリポジトリ登録用RPMをインストールする。

|  |
| --- |
| # rpm -ivh zabbix-release-1.8-1.el6.noarch.rpm |

1. httpd、MySQL,Zabbixサーバ、Zabbix Webインターフェースをインストールする。

|  |
| --- |
| # yum -y install zabbix zabbix-server zabbix-server-mysql \  zabbix-web zabbix-web-mysql zabbix-get mysql-server |

1. /etc/my.cnfの変更を行う。(赤字の部分を追加する。)

|  |
| --- |
| [mysqld]  datadir=/var/lib/mysql  socket=/var/lib/mysql/mysql.sock  user=mysql  # Disabling symbolic-links is recommended to prevent assorted security risks  symbolic-links=0  character-set-server=utf8  skip-character-set-client-handshake  [mysqld\_safe]  log-error=/var/log/mysqld.log  pid-file=/var/run/mysqld/mysqld.pid |

1. MySQL を起動する。

|  |
| --- |
| # service mysqld start |

1. Zabbixデータベースを作成する。

|  |
| --- |
| # mysqladmin create zabbix --default-character-set=utf8 |

1. データベースへの接続ユーザzabbixを作成する。

|  |
| --- |
| # mysql -uroot  mysql> grant all privileges on zabbix.\* to zabbix@localhost identified by 'zabbix';  mysql> flush privileges;  mysql> quit |

1. Zabbixの初期データをインポートする。

(インストールしたZabbixサーバのバージョンに応じて、SQLファイルのパスは適宜修正する。)

|  |
| --- |
| $ mysql -uroot zabbix \  < /usr/share/doc/zabbix-server-mysql-1.8.20/create/schema/mysql.sql  $ mysql -uroot zabbix \  < /usr/share/doc/zabbix-server-mysql-1.8.20/create/data/data.sql  $ mysql -uroot zabbix \  < /usr/share/doc/zabbix-server-mysql-1.8.20/create/data/images\_mysql.sql |

ただしZabbix 2.2系では、代わりに次のようにすること。(ただしやはり、SQLファイルのパスは適宜修正する。)

|  |
| --- |
| $ mysql -uroot zabbix \  < /usr/share/doc/zabbix-server-mysql-2.2.5/create/schema.sql  $ mysql -uroot zabbix \  < /usr/share/doc/zabbix-server-mysql-2.2.5/create/images.sql  $ mysql -uroot zabbix \  < /usr/share/doc/zabbix-server-mysql-2.2.5/create/data.sql |

1. /etc/php.iniファイルを編集し、date.timezoneを設定する。タイムゾーンがAsia/Tokyoだとすると、[Date] セクション中に赤字で記した行を置く。(date.timezone設定行は、初期状態ではコメントアウトされている。)

|  |
| --- |
| [Date]  ; Defines the default timezone used by the date functions  ; http://www.php.net/manual/en/datetime.configuration.php#ini.date.timezone  date.timezone = Asia/Tokyo |

1. httpd を起動する。

|  |
| --- |
| # service httpd start |

1. iptablesでHTTP、HHTPSのアクセスを制限している場合は、/etc/sysconfig/iptablesに下記 (赤字の部分) を、他の “-A INPUT” 行よりも前に追加する。

|  |
| --- |
| # Firewall configuration written by system-config-firewall  # Manual customization of this file is not recommended.  \*filter  :INPUT ACCEPT [0:0]  :FORWARD ACCEPT [0:0]  :OUTPUT ACCEPT [0:0]  -A INPUT -p tcp -m tcp --dport 443 -j ACCEPT  -A INPUT -p tcp -m tcp --dport 80 -j ACCEPT  -A INPUT -m state --state ESTABLISHED,RELATED -j ACCEPT  (略)  COMMIT |

1. 前項でiptablesの設定を変更した場合は、下記コマンドでiptablesを再起動する。

|  |
| --- |
| # service iptables restart |

1. ブラウザで下記URIにアクセスする。

|  |
| --- |
| http://*Zabbixサーバのホスト名*/zabbix/ |

1. 「Introduction」画面が表示されるので、「Next」ボタンを押下する。



図 3‑1 Introduction画面

1. 「Licence agreement」画面が表示される。「I agree」をチェックし、「Next」ボタンを押下する。



図 3‑2 Licence agreement画面

1. 「Check of pre-requisites」画面が表示される。「Next」ボタンを押下する。



図 3‑3 Check of pre-requisites画面

1. 「Configure DB connection」画面が表示される。下記表の値を入力し、「Test connection」を押下し、「OK」が表示された後「Next」ボタンを押下する。



図 3‑4 Configure DB connection画面

各項目に入力すべき値は、次の通り。

**表 3‑2 DB接続設定**

|  |  |
| --- | --- |
| 設定項目 | 設定値 |
| Type | MySQL |
| Host | localhost |
| Port | 0 |
| Name | zabbix |
| User | zabbix |
| Password | zabbix |

1. 「Zabbix server details」画面が表示される。下記表の値を入力し、「Next」ボタンを押下する。



図 3‑5 Zabbix server details画面

各項目に入力すべき値は、次の通り。

**表 3‑3 Zabbix server設定**

|  |  |
| --- | --- |
| 設定項目 | 設定値 |
| Host | localhost |
| Port | 10051 |
| Name | *監視サーバ名* |

1. 「Pre-Installation Summary」画面が表示される。入力内容に間違いがないことを確認し、「Next」ボタンを押下する。



図 3‑6 Pre-Installation summary画面

SELinuxを有効にしている場合はファイルを自動的に保存できないため、設定ファイルの配置に失敗したことを通知する「Install」画面が表示される。



図 3‑7 Install画面

ファイルが自動的に保存された場合は、手順22に進む。

1. 「Save configuration file」ボタンを押下し、設定ファイルを任意の場所に保存する。
2. 設定ファイルをcpコマンドで配置し、「Retry」ボタンを押下する。

|  |
| --- |
| # cp zabbix.conf.php /etc/zabbix |

1. 設定ファイルの配置に成功した「Install」画面が表示される。「Next」ボタンを押下する。



図 3‑8 Install画面

1. 「Finish」画面が表示される。「Next」ボタンを押下する。



図 3‑9 Finish画面

1. Zabbixにログインできるかどうか確認する。

ブラウザでログイン画面:

|  |
| --- |
| http://*Zabbixサーバのホスト名*/zabbix/ |

にアクセスし、ユーザ「Admin」、パスワード「zabbix」でログインする。



図 3‑10 ログイン画面

ログインに成功すると、次のような画面が表示される。



図 3‑11 ログイン成功通知

1. 言語設定を日本語に変える。(省略可)

メニューの「Administration」－「Users」を選択すると、ユーザグループまたはユーザの一覧が表示される。右上の「Users」「User groups」を切り替えるプルダウンメニューがあるので、「Uesrs」を選択する。ユーザ一覧が表示されたら、Alias欄の「Admin」をクリックする。



図 3‑12 ユーザ一覧

Languageに「Japanese (JP)」を選択し、「Save」を押下する。画面を再読み込みすると、言語が日本語に変わる。なお本書では以降、画面に使われている語句は、言語設定を日本語にしたときのもので表記する。



図 3‑13 ユーザ設定画面

1. OS起動時にMySQL、httpdが起動するように設定する。

|  |
| --- |
| # chkconfig --level 345 mysqld on  # chkconfig --level 345 httpd on |

## Zabbixエージェントのインストール

Zabbixエージェントのインストールは、監視対象ノード各機で行う。分散監視構成の場合は、加えて監視サーバ各機にもインストールする。以下に、インストール手順を示す。手順は全てrootユーザで実行する。

1. yumリポジトリ登録用RPMを取得する。(同じホストに、先にZabbixサーバをインストールしている場合、本工程は実施済みなので実行しなくて良い。)

|  |
| --- |
| # wget http://repo.zabbix.com/zabbix/1.8/rhel/6/x86\_64/zabbix-release-1.8-1.el6.noarch.rpm |

1. yumリポジトリ登録用RPMをインストールする。(同上)

|  |
| --- |
| # rpm -ivh zabbix-release-1.8-1.el6.noarch.rpm |

1. Zabbixエージェントをインストールする。

|  |
| --- |
| # yum -y install zabbix zabbix-agent |

1. zabbixユーザの設定を変更する。

ホームディレクトリを「/etc/zabbix」、シェルを「/bin/bash」、任意のパスワードを設定する。

|  |
| --- |
| # usermod -d /etc/zabbix -s /bin/bash -p password zabbix |

1. /etc/zabbixの所有者を変更する。

|  |
| --- |
| # chown zabbix:zabbix /etc/zabbix |

1. visudoコマンドで、zabbixユーザのsudo権限を設定する。

|  |
| --- |
| # visudo |

/etc/sudoersファイルに以下の2行を追加する。

|  |
| --- |
| Defaults:zabbix !requiretty  zabbix ALL=(\_gfarmfs,\_gfarmmd) NOPASSWD: ALL |

## gfarm\_zabbixパッケージのインストール

gfarm\_zabbixパッケージ (“gfarm\_zabbix-*バージョン番号*.tar.gz” というファイル) のインストールは、監視サーバ各機および監視対象ノード各機で行う。以下に、インストール手順を記す。なお、あらかじめ当該ホストでは、Gfarmファイルシステムとしてのインストールおよび設定は完了しているものとする。

### install.confの編集

gfarm\_zabbixパッケージを展開すると、srcディレクトリの下にinstall.confというファイルがあるので、このファイルをエディタで編集する。このファイルは、シェルスクリプトとして解釈されるので、注意すること。このため、たとえば「=」の前後に空白を入れるとエラーになる。

|  |
| --- |
| # Gfarm のコマンド類 (例 gfhost) が置かれているディレクトリ  GFARM\_BINDIR=/usr/local/gfarm/bin  # gfmdの設定ファイル  GFMD\_CONF\_FILE=/etc/gfmd.conf  # gfmd、gfsd、gfarm2fsのログメッセージが記録されるsyslogファイル  GFARM\_SYSLOG\_FILE=/var/log/messages  # Zabbixサーバの設定ファイルが置かれるディレクトリ  # ‘zabbix’ ユーザのホームディレクトリと同じでなくてはならない。  ZABBIX\_CONFDIR=/etc/zabbix  # gfarm\_zabbixがsyslogにエラーを出力する際のファシリティ  ZABBIX\_SYSLOG\_FACILITY=local0  ######################################################  # クライアント設定ファイル編集機能向けの設定  ######################################################  # クライアント設定ファイル編集機能のインストールディレクトリ  EDITOR\_HTMLDIR=/var/www/html/gfarm2-conf-editor  # $EDITOR\_HTMLDIRディレクトリの所有ユーザとグループ  EDITOR\_HTMLDIR\_USER=apache  EDITOR\_HTMLDIR\_GROUP=apache |

### Zabbixエージェント用ファイルのインストール

install.confファイルの置かれたディレクトリをカレントディレクトリとして、root権限で以下のコマンドを実行する。

1. インストールを行う。

|  |
| --- |
| # ./install-agentd.sh |

スクリプトの実行結果として、次のようなメッセージが出力される。

|  |
| --- |
| Install the file: /etc/zabbix/zabbix\_agentd.d/userparameter\_gfarm.conf  Install the file: /etc/zabbix/externalscripts/gfarm\_generic\_client\_gfhost.sh  Install the file: /etc/zabbix/externalscripts/gfarm\_generic\_client\_gfmdhost.sh  Install the file: /etc/zabbix/externalscripts/gfarm\_gfmd\_failover.pl  Install the file: /etc/zabbix/externalscripts/gfarm\_gfmd\_gfhost.sh  Install the file: /etc/zabbix/externalscripts/gfarm\_gfmd\_postgresql.sh  Install the file: /etc/zabbix/externalscripts/gfarm\_gfsd\_gfhost.sh  Install the file: /etc/zabbix/externalscripts/gfarm\_gfsd\_gfsched.sh  Install the file: /etc/zabbix/externalscripts/gfarm\_represent\_client\_gfhost.sh  Install the file: /etc/zabbix/externalscripts/gfarm\_represent\_client\_gfmdhost.sh  Install the file: /etc/zabbix/externalscripts/gfarm\_utils.inc  Install the file: /etc/zabbix/externalscripts/gfarm\_conf.inc  Set mode (= 0644) of the file: /var/log/messages |

上記のメッセージにある通り、インストールスクリプトはsyslogファイル (上記では/var/log/messeges) のパーミッションを0644に変更する。これはzabbix-agentdがsyslogファイルからgfmdやgfsdの出力したログを検出するために、パーミッションを緩めている (ログファイルのローテーション時も、このパーミッションが維持される)。0644では緩すぎるという場合は、適宜変更すること。ただし、zabbixユーザの権限で読めるようにする必要がある。

インストールスクリプトは、当該ノード上の$GFMD\_CONF\_FILE (この値はinstall.confで指定) ファイルの内容を読み取って、PostgreSQLへのアクセス情報を$ZABBIX\_CONFDIRディレクトリ (同上) の下のgfarm\_conf.incというファイルに転記する。PostgreSQLのアクセス情報が正しく書き込まれたか、念のためファイルを確認すること。

|  |
| --- |
| # syslog ファシリティ  SYSLOG\_FACILITY=local0  # PostgreSQLサーバのホスト名  PGHOST=mds-master  # PostgrSQLサーバのTCPポート番号  PGPORT=10602  # PostgreSQLデータベース名  PGDATABASE=gfarm  # PostgreSQLへ接続する際のユーザ名  PGUSER=gfarm  # PostgreSQLへ接続する際のパスワード  PGPASSWORD="MycWlXdJpvyhV52NpMxQzZX3QiJdP=GRCzv2MJCXQBH" |

なお、本ファイルの設定項目は、インストール後に手で編集しても支障なく、その時点からその設定が有効になる。PostgreSQLの接続情報を変えた場合は、忘れずに更新すること。

### クライアント設定ファイル編集機能のインストール

クライアント設定ファイル編集機能は、必要な場合のみインストールを行う。クライアント設定ファイル編集機能に関しての詳細は「冗長化構成Gfarm監視機能 管理・利用マニュアル」を参照のこと。

クライアント設定ファイル編集機能は、監視サーバだけにインストールする。分散構成では、子ノードのほうの監視サーバにインストールする。install.confファイルを編集した後、install.confファイルの置かれたディレクトリをカレントディレクトリとして、root権限で以下のコマンドを実行する。

1. インストールを行う。

|  |
| --- |
| # ./install-editor.sh |

スクリプトの実行結果として下記が出力されるので、出力された内容に従いzabbixユーザのcrontabファイルまたは/etc/cron.d/ディレクトリ下のファイルに/etc/zabbix/gfmdlist.shを定期的に実行する設定を行う。

|  |
| --- |
| Install the file: /var/www/html/gfarm2-conf-editor/common.php  Install the file: /var/www/html/gfarm2-conf-editor/download.php  Install the file: /var/www/html/gfarm2-conf-editor/edit.php  Install the file: /var/www/html/gfarm2-conf-editor/index.php  Install the file: /var/www/html/gfarm2-conf-editor/save.php  Install the file: /etc/zabbix/gfmdlist.sh  Please add the following lines to a crontab file of user 'zabbix':  # Run 'gfmdhost -l' every five minutes.  \*/5 \* \* \* \* /etc/zabbix/gfmdlist.sh  or add the following lines to a file under /etc/cron.d/:  # Run 'gfmdhost -l' every five minutes.  \*/5 \* \* \* \* zabbix /etc/zabbix/gfmdlist.sh |

# 各ノードの設定

本章では、各ノードの設定を記載する。

## zabbixユーザの登録と共通認証鍵の作成

Gfarm上にzabbixユーザを登録する。以下の手順は、Gfarmクライアントとして動作している任意のホスト1台を選び、gfadminユーザで実行する。

1. Gfarm上にzabbixユーザを作成する。

|  |
| --- |
| $ gfuser -c zabbix zabbix "/home/zabbix" "" |

zabbixユーザが作成されたことを確認する。

|  |
| --- |
| $ gfuser –l  gfarmadm:Gfarm administrator:/:  gfadmin:Gfarm administrator:/:  zabbix:zabbix:/home/zabbix: |

1. Gfarm共有認証鍵を生成する。

zabbixユーザのGfarm共有認証鍵の作成を行う。Gfarmクライアントとして動作している任意のホスト上にて、zabbixユーザで実行する。

(-pオプションで指定する有効期限は任意で設定する。)

|  |
| --- |
| $ gfkey -c -p 3156300 |

1. 指定した有効期限でGfarm共有認証鍵が生成されたことを確認する

|  |
| --- |
| $ gfkey –e  expiration time is Fri May 10 06:09:14 2013 |

1. 作成したGfarm共有認証鍵を、すべての監視サーバおよび監視対象ノードにコピーする。

|  |
| --- |
| $ scp -p /etc/zabbix/.gfarm\_shared\_key zabbix@*ホスト名*:/etc/zabbix |

## 監視サーバの設定

監視サーバの設定を行う。

### Zabbixサーバの設定

Zabbixサーバの設定を行う。下記の手順は全てrootユーザで実行する。

1. Zabbixサーバの設定ファイル/etc/zabbix/zabbix\_server.confを編集する。(赤字の箇所は、注意して設定する必要がある。) なお、NodeID のデフォルト値は0 なので、仕様に従えば設定を省略できる筈だが、少なくともZabbix 1.8.20では、再起動時にエラーが発生する。このため、NodeIDは設定しておくことを薦める。

|  |
| --- |
| NodeID=0  LogFile=/var/log/zabbix/zabbix\_server.log  LogFileSize=0  PidFile=/var/run/zabbix/zabbix\_server.pid  DBName=zabbix  DBUser=zabbix  DBPassword=zabbix  Timeout=30  AlertScriptsPath=/etc/zabbix/alertscripts  ExternalScripts=/etc/zabbix/externalscripts |

1. Zabbixサーバを起動する。

|  |
| --- |
| # service zabbix-server start |

1. iptablesでZabbixサーバのアクセスを制限している場合は、/etc/sysconfig/iptablesの下記 (赤字の部分) を、他の “-A INPUT” 行よりも前に追加する。

|  |
| --- |
| # Firewall configuration written by system-config-firewall  # Manual customization of this file is not recommended.  \*filter  :INPUT ACCEPT [0:0]  :FORWARD ACCEPT [0:0]  :OUTPUT ACCEPT [0:0]  -A INPUT -p tcp -m tcp --dport 10051 -j ACCEPT  -A INPUT -p tcp -m tcp --dport 443 -j ACCEPT  (略)  COMMIT |

1. 前項でiptablesの設定を変更した場合は、iptablesを再起動する。

|  |
| --- |
| # service iptables restart |

1. OS起動時にZabbixサーバが起動するように設定する。

|  |
| --- |
| # chkconfig --level 345 zabbix-server on |

1. SELinux環境では、httpdプロセスからのネットワーク接続を許可する。

|  |
| --- |
| # setsebool -P httpd\_can\_network\_connect 1 |

### Zabbixエージェントの設定 (分散監視構成の場合)

分散監視構成では監視サーバ上でもZabbixエージェント動作させることになるので、その設定を行う。下記の手順は全てrootユーザで実行する。

1. Zabbixエージェントの設定ファイル/etc/zabbix/zabbix\_agentd.confを編集する。(赤字の箇所は、注意して設定する必要がある。)

|  |
| --- |
| PidFile=/var/run/zabbix/zabbix\_agentd.pid  LogFile=/var/log/zabbix/zabbix\_agentd.log  LogFileSize=0  Server=192.168.0.1,192.168.0.2 ← 各監視サーバのIPアドレス  Hostname=zabbix-master ← この監視サーバのGUI表示ホスト名  ListenIP=0.0.0.0  Timeout=30  Include= /etc/zabbix/zabbix\_agentd.d/ |

1. Zabbixエージェントを起動する。

|  |
| --- |
| # service zabbix-agent start |

1. iptablesでZabbixエージェントのアクセスを制限している場合は、/etc/sysconfig/iptablesの下記 (赤字の部分) を、他の “-A INPUT” 行よりも前に追加する。

|  |
| --- |
| # Firewall configuration written by system-config-firewall  # Manual customization of this file is not recommended.  \*filter  :INPUT ACCEPT [0:0]  :FORWARD ACCEPT [0:0]  :OUTPUT ACCEPT [0:0]  -A INPUT -p tcp -m tcp --dport 10050 -j ACCEPT  -A INPUT -p tcp -m tcp --dport 10051 -j ACCEPT  (略)  COMMIT |

1. 前項でiptablesの設定を変更した場合は、iptablesを再起動する。

|  |
| --- |
| # service iptables restart |

1. OS起動時にZabbixエージェントが起動するように設定する。

|  |
| --- |
| # chkconfig --level 345 zabbix-agent on |

### クライアント設定ファイル編集機能の設定

クライアント設定ファイル編集機能を使用する場合は、監視サーバ (分散監視構成の場合は子ノードのほう) で下記の設定を行う。

1. apacheユーザが、端末を持たない状態でもsudoで任意のコマンドを管理者権限で実行できるよう、visudoで設定する。

|  |
| --- |
| # visudo |

/etc/sudoersファイルに以下の2行を追加する。

|  |
| --- |
| Defaults:apache !requiretty  apache ALL=(ALL) NOPASSWD: ALL |

## 監視サーバ以外の設定

Gfarmメタデータサーバ、Zabbixファイルシステムノード、代表クライアント、一般クライアント各機に対して、本節の設定を行う。

### Zabbixエージェントの設定

Zabbixサーバの設定を行う。下記の手順は全てrootユーザで実行する。

1. Zabbixエージェントの設定ファイル/etc/zabbix/zabbix\_agentd.confを編集する。

(赤字の箇所は注意して設定する必要がある。)

|  |
| --- |
| PidFile=/var/run/zabbix/zabbix\_agentd.pid  LogFile=/var/log/zabbix/zabbix\_agentd.log  LogFileSize=0  Server=192.168.0.2 ← 監視サーバのIPアドレス  (分散監視構成では子ノードのほうを指定)  Hostname=fsn1 ←このホストの表示ホスト名  ListenIP=0.0.0.0  Timeout=30  Include= /etc/zabbix/zabbix\_agentd.d/ |

1. Zabbixエージェントを起動する。

|  |
| --- |
| # service zabbix-agent start |

1. iptablesでZabbixエージェントのアクセスを制限している場合は、/etc/sysconfig/iptablesの下記 (赤字の部分) を、他の “-A INPUT” 行よりも前に追加する。

|  |
| --- |
| # Firewall configuration written by system-config-firewall  # Manual customization of this file is not recommended.  \*filter  :INPUT ACCEPT [0:0]  :FORWARD ACCEPT [0:0]  :OUTPUT ACCEPT [0:0]  -A INPUT -p tcp -m tcp --dport 10050 -j ACCEPT  -A INPUT -p tcp -m tcp --dport 10051 -j ACCEPT  (略)  COMMIT |

1. 前項でiptablesの設定を変更した場合は、iptablesを再起動する。

|  |
| --- |
| # service iptables restart |

OS起動時にZabbixエージェントが起動するように設定する。

|  |
| --- |
| # chkconfig --level 345 zabbix-agent on |

### gfarm\_zabbixスクリプトの設定

必要に応じて、監視サーバおよび監視対象ノード各機の/etc/zabbix/externalscripts/gfarm\_conf.incファイルを編集する。特に、メタデータサーバ機ではPostgreSQLのアクセス情報がこのファイルに転記されているので、正しい情報が記載されているか確認すること。

|  |
| --- |
| # syslog ファシリティ  SYSLOG\_FACILITY=local0  # PostgreSQLサーバのホスト名  PGHOST=mds-master  # PostgrSQLサーバのTCPポート番号  PGPORT=10602  # PostgreSQLデータベース名  PGDATABASE=gfarm  # PostgreSQLへ接続する際のユーザ名  PGUSER=gfarm  # PostgreSQLへ接続する際のパスワード  PGPASSWORD="MycWlXdJpvyhV52NpMxQzZX3QiJdP=GRCzv2MJCXQBH" |

## zabbix\_getによる動作確認

ここまでの設定が正しいかどうかを確認するには、zabbix\_getコマンドを用いると便利である。zabbix\_getコマンドは、Zabbixサーバ (分散監視構成の場合は、子ノードのほう) 上で実行する必要がある。SELinuxを有効にしている環境で、どうしてもうまくいかない場合は、「8.1 SELinux環境での問題」を参照のこと。

1. zabbix\_getコマンドを実行する。

|  |
| --- |
| $ zabbix\_get -s *監視対象ノード* -p 10050 -k *監視アイテム名* |

ここで「監視対象ノード」には、ノードのホスト名もしくはIPアドレスを指定する。監視対象ノード上では、Zabbixエージェントが動作していなければならない。「監視アイテム名」には、様々なものが指定できるが、代表的なものを挙げておく。

表 4‑1 代表的な監視アイテム

|  |  |
| --- | --- |
| 監視アイテム名 | 監視対象ノード種別 |
| 説明 |
| gfarm.gfmd.gfhost | メタデータサーバ |
| 監視対象ノード上にて、\_gfarmmdユーザでgfhostコマンドを実行して成功するかどうかを確認する。成功すると “ok” が、失敗すると失敗理由がそれぞれ表示される。  監視対象ノード上において、ユーザzabbixでgfarm\_gfmd\_gfhost.shを実行するのと同じである。 |
| gfarm.gfsd.gfhost | ファイルシステムノード |
| 監視対象ノード上にて、\_gfarmfsユーザで “gfhost-lv” コマンドを実行して成功するかどうかを確認する。成功すると “ok” が、失敗すると失敗理由がそれぞれ表示される。  監視対象ノード上において、ユーザzabbixでgfarm\_gfsd\_gfhost.shを実行するのと同じである。 |
| gfarm.represent\_client.gfmdhost | 代表クライアント |
| 監視対象ノード上にて、“gfmdhost -l” コマンドを実行して成功するかどうかを確認する。成功すると “ok” が、失敗すると失敗理由がそれぞれ表示される。  監視対象ノード上におて、ユーザzabbixでgfarm\_represent\_client\_gfmdhost.shを実行するのと同じである。 |
| gfarm.generic\_client.gfhost | 一般クライアント |
| 監視対象ノード上にて、“gfhost -lv” コマンドを実行して、認証が通るかどうかを確認する。成功すると “ok” が、失敗すると失敗理由がそれぞれ表示される。  監視対象ノード上におて、ユーザzabbixでgfarm\_generic\_client\_gfhost.shを実行するのと同じである。 |
| proc.num[*プロセス名*] | 全ノード種別 |
| 監視対象ノード上にて、動作中の「*プロセス名*」の個数を表示する。たとえば “proc.num[gfmd]” とすれば、動作中のgfmdのプロセス数が表示される。 |

# 監視設定

本節では、Zabbixの監視設定について記載する。Zabbixサーバの設定、Zabbixエージェントの設定および、監視項目の設定方法について記載する。分散監視構成の場合は、次章「6 分散監視構成設定」の設定も合わせて行うこと。

本章の記載内容は、初期導入時向けである。設定の変更や監視項目の追加を行う場合には、別途ドキュメント「冗長化構成Gfarm監視機能 管理・利用マニュアル」を参照のこと。

## 監視項目の設定

Zabbixでの監視項目の設定は、全てWebインターフェース上で行う。Zabbixでは、以下の項目を設定することにより監視を行う。

表 5‑1 設定項目一覧

|  |  |
| --- | --- |
| 設定項目 | 説明 |
| ホスト | 監視対象の設定。  Gfarm監視では、Gfarmメタデータサーバ、Gfarmファイルシステムノード、Gfarmクライアントノード、監視サーバ(相互監視用)をホストとして設定。 |
| ホストグループ | 監視対象(ホスト)をグループ化する設定。  Gfarm監視では、Gfarmファイルシステムを1ホストグループとして設定。 |
| アイテム | 監視項目の設定。  Zabbixサーバが各監視対象から収集する監視情報を設定。 |
| トリガー | 収集した監視情報に対して、障害検知する際の閾値の設定。 |
| アクション | 障害発生時の障害通知やスクリプト実行等の設定。 |

Zabbixでは、監視項目をテンプレート化して管理する機能を有している。テンプレートには、各種アイテム/トリガーの設定が記述してある。gfarm\_zabbixパッケージではGfarm監視用のテンプレートを用意しており、本書ではこのテンプレートを利用した設定手順について記載する。

次節より、Gfarm監視設定における各手順について説明する。

### Gfarm監視用テンプレートの導入

Gfarm監視用テンプレートの導入手順を以下に示す。

1. Webインターフェースへのログイン

(冗長構成の場合は、子ノードのほうの) 監視サーバのWebインターフェースにアクセスし、Adminユーザでログインする。

1. テンプレート設定画面

メニューの「設定」－「テンプレート」からテンプレート設定画面を表示する。



図 5‑1 テンプレート設定画面

1. インポート画面

「テンプレートのインポート」ボタンを押下し、インポート画面を表示する。



図 5‑2 インポート画面

1. gfarm\_zabbixパッケージを展開したディレクトリ下にあるファイルsrc/templates/Template\_Gfarm\_exported\_all.xmlを選択し、「インポート」ボタンを押下する。成功メッセージが表示されることを確認する。

### ホストグループの設定

ホストグループの設定手順を以下に示す。

1. ログイン

(冗長構成の場合は、子ノードのほうの) 監視サーバのWebインターフェースにアクセスし、Adminユーザでログインする。

1. ホストグループ設定画面

「設定」－「ホストグループ」からホストグループ設定画面を表示する。



図 5‑3 ホストグループ設定画面

1. ホストグループ作成画面

「グループの作成」ボタンを押下し、ホストグループ設定画面を表示する。



図 5‑4 ホストグループ作成画面

1. ホストグループ作成

下記情報を入力後、「保存」ボタンを押下する。

表 5‑2 ホストグループ設定

|  |  |
| --- | --- |
| 入力項目 | 設定値 |
| グループ名 | Gfarm Filesystem |
| ホスト | なし |

「保存」ボタン押下後、成功メッセージが表示され、一覧に追加されていることを確認する。

以上で、テンプレートのインポートおよび、ホストグループの設定が完了となる。次節以降は、監視対象となるサーバ、ノードの追加を行う。

### ホストの追加

監視対象ノードを追加するには、Zabbixにそのノードを「ホスト」としてぞれぞれ追加することになる。追加手順は以下の通りである。なお、分散監視構成においては、監視サーバ自身もホストとして追加する。

1. ログイン

(冗長構成の場合は、子ノードのほうの) 監視サーバのWebインターフェースにアクセスし、Adminユーザでログインする。

1. ホスト一覧画面の表示

メニューの「設定」－「ホスト」からホスト一覧画面を表示する。



図 5‑5 ホスト一覧画面

1. ホスト作成画面の表示

「ホストの作成」ボタンを押下し、ホスト作成画面を表示する。



図 5‑6 ホスト作成画面

1. ホストの作成

下記情報を入力後、「保存」ボタンを押下し、ホストを作成する。「リンクしているテンプレート」は「追加」ボタンを押下すると、テンプレートの一覧が表示されるので、一覧から選択する。

表 5‑3 ホスト設定

|  |  |
| --- | --- |
| 設定項目 | 設定値 |
| 名前 | 任意の名前。  ※ホスト上のzabbix\_agentd.confファイルのHostNameで設定した名前と必ず一致させること。 |
| グループ | Gfarm Filesystem  ※「5.1.2 ホストグループの設定」で追加したグループを選択する。 |
| 新規グループ作成 | 空欄 |
| DNS名 | 空欄 |
| IPアドレス | メタデータサーバのIPアドレス |
| 接続方法 | IPアドレス |
| Zabbixエージェントのポート | 10050 |
| プロキシによる監視 | (プロキシなし) |
| ステータス | 有効 |
| IPMIを使用 | チェックなし |
| リンクするテンプレート | 監視対象ノードの種別によって異なる。詳しくは後述。 |
| マクロ | 監視対象ノードの種別によって異なる。詳しくは後述。 |
| プロファイル | チェックなし  ※チェックすると、項目が表示されるので必要に応じて入力 |
| 拡張ホストプロファイル | チェックなし  ※チェックすると、項目が表示されるので必要に応じて入力 |

「リンクするテンプレート」欄は、監視対象ノードに応じて、次のように選択する。

表 5‑4「リンクするテンプレート」一覧 (1)

|  |  |
| --- | --- |
| 監視対象ノード種別 | リンクするテンプレート |
| メタデータサーバ | Template\_Gfarm\_gfmd |
| ファイルシステムノード | Template\_Gfarm\_gfsd |
| 代表クライアント | Template\_Gfarm\_represent\_client |
| 一般クライアント | Template\_Gfarm\_generic\_client |

ただし、監視対象ノード1台が複数のノード種別を兼任している場合、上記のテンプレートをそれぞれリンクすることはできない。(リンクしようとすると、依存関係のエラーが発生する。) これを回避するためには、リンクするテンプレートを次表のように変更する。どのノード種別もTemplate\_Gfarm\_common\_nodepを選択しているが、リンクするのは一回で良い。(複数回のリンクはできない。) どちらの方法で「リンクするテンプレート」を指定しても、設定自体は等価である。

表 5‑5「リンクするテンプレート」一覧 (2)

|  |  |
| --- | --- |
| 監視対象ノード種別 | 選択するテンプレート |
| メタデータサーバ | Template\_Gfarm\_gfmd\_nodep  Template\_Gfarm\_common\_nodep |
| ファイルシステムノード | Template\_Gfarm\_gfsd\_nodep  Template\_Gfarm\_common\_nodep |
| 代表クライアント | Template\_Gfarm\_represent\_client\_nodep  Template\_Gfarm\_common\_nodep |
| 一般クライアント | Template\_Gfarm\_generic\_client\_nodep  Template\_Gfarm\_common\_nodep |

「マクロ」欄も、監視対象ノードに応じた設定が必要である。次表で、マクロのデフォルト値と異なる値をセットする場合は、そのマクロを「マクロ」欄に設定すること。

表 5‑6ホストマクロ設定

|  |  |
| --- | --- |
| メタデータサーバ | |
| マクロ | 説明 |
| {$GFMD\_LOGFILE} | gfmdのログメッセージを記録しているsyslogファイルのパス。  デフォルト値は/var/log/messages。 |
| {$GFMD\_PGDATA\_DIR} | PostgreSQLのデータ領域ディレクトリへのパス。  デフォルト値は/var/gfarm-pgsql。 |
| ファイルシステムノード | |
| マクロ | 説明 |
| {$GFSD\_LOGFILE} | gfsdのログメッセージを記録しているsyslogファイルのパス。  デフォルト値は/var/log/messages。 |
| {$GFSD\_SPOOL\_DIR} | gfsdのスプールディレクトリへのパス。  デフォルト値は/var/gfarm-spool。 |
| {$GFSD\_HOST\_NAMES} | ファイルシステムノードのホスト名。gfhost –cでファイルシステムノードを登録した際のホスト名でなければならない。ホスト上で複数のgfsdを動作させている場合は、ホスト名を空白で区切って並べること。本マクロの値を- (ハイフン・マイナス) に設定すると、ファイルシステムノード上でhostname –fを実行した際に得られるホスト名を指定したものと看做される。  デフォルト値は、- (ハイフン・マイナス)。 |
| 全ノード種別 | |
| マクロ | 説明 |
| {$KERNEL\_LOGFILE} | カーネルのログメッセージを記録しているsyslogファイルのパス。  デフォルト値は/var/log/messages。 |
| {$MONITOR\_DIR} | このディレクトリの属するファイルシステムの空き容量率を監視する。  デフォルト値は/ (ルートディレクトリ)。 |

「保存」ボタン押下後、ホスト一覧が表示され、作成したホストが追加されていることを確認する。

# 分散監視構成設定

分散監視構成の場合は、前章に続いて本章の設定も合わせて行う必要がある。なお説明上は子ノードが1つだけであることを想定しているが、同じ要領で設定を行うことで、2つ目以降の設定も設定可能である。

## 分散監視設定の準備

Zabbixでの分散監視では、各Zabbixサーバに対し識別子であるノードIDを割り振る必要がある。

1. ノードIDの決定

各Zabbixサーバに対しノードIDを割り振る。割り振るノードIDは任意の値で問題ないが、重複しないように注意すること。分散監視時のノードIDとして指定可能な範囲は、1～999である。以降の手順では、以下のノードIDを割り振ったものとして説明する。

* + マスターノード：1
  + 子ノード ：2

1. ノードIDの設定

手順1で設定したノードIDを、各監視サーバ上の設定ファイル/etc/zabbix/zabbix\_server.confに設定する。以下の赤字箇所を追加する (下記例は、マスターノードの場合)。

|  |
| --- |
| ### Option: NodeID  # Unique NodeID in distributed setup.  # 0 - standalone server  #  # Mandatory: no  # Range: 0-999  # Default:  # NodeID=0  NodeID=1 |

1. データベースの変換

分散監視を行う際には、データベースのデータを分散監視用に変換する必要があるので、以下を実施する。-nオプションでノードIDを指定する。Zabbixサーバが起動中の場合は、停止してから実施すること。(下記例はマスターノードの場合)

|  |
| --- |
| # /usr/sbin/zabbix\_server -c /etc/zabbix/zabbix\_server.conf -n 1  Converting tables .........................................................done.  Conversion completed. |

マスターノード側、子ノード側双方で上記手順を実施後、Zabbixサーバの起動を行い、Webインターフェースより分散監視設定を行う。

## マスターノードの分散監視設定

まず、マスターノード側の分散監視設定を行う。

1. Webインターフェースへのログイン

マスターノードのWebインターフェースにアクセスし、Adminユーザでログインする。

1. 分散監視管理画面の表示

メニューの「管理」－「分散監視」から分散監視管理画面を表示する。初期状態では、自分自身がLocal Nodeとして登録されている。



図 6‑1 分散監視管理画面

1. 子ノードの追加

右側のプルダウンメニューから「ノード」を選択し、「新規ノード」ボタンを押下で設定画面が表示されるので、下記情報を設定する。

表 6‑1 子ノード設定

|  |  |
| --- | --- |
| 設定項目 | 設定値 |
| 名前 | 任意の名称 |
| ID | 2  ※子ノードのノードIDを指定 |
| タイプ | 子 |
| マスターノード | Local node  ※自分自身を指定 |
| タイムゾーン | GMT+09:00 |
| IPアドレス | 追加する子ノードのIPアドレス |
| ポート | 10051 |
| ヒストリの保存期間(日) | 90 |
| トレンドの保存期間(日) | 365 |



図 6‑2 ノード作成画面

ノード情報を入力後、「保存」ボタンを押下すると、下記画面が表示され、Local node/の配下に、子ノードが追加されていることを確認する。



図 6‑3 分散監視管理画面(子ノード追加後)

このとき、Local node(マスターノード)の設定でタイムゾーンがデフォルト設定のGMT+00:00になっているので、GMT+09:00に変更しておくこと。

以上で、マスターノード側での子ノードの追加は完了となる。別の子ノードを追加する際には、同様の手順を実施する。

## 子ノードの分散監視設定

次に、子ノード側の分散監視設定を行う。

1. Webインターフェースへのログイン

子ノードのWebインターフェースにアクセスし、Adminユーザでログインする。

1. 分散監視管理画面の表示

メニューの「管理」－「分散監視」から分散監視管理画面を表示する。初期状態では、自分自身がLocal Nodeとして登録されている。



図 6‑4 分散監視管理画面

1. マスターノードの追加

右側のプルダウンメニューから「ノード」を選択し、「新規ノード」ボタンを押下で設定画面が表示されるので、下記情報を設定する。

表 6‑2 マスターノード設定

|  |  |
| --- | --- |
| 設定項目 | 設定値 |
| 名前 | 任意の名称 |
| ID | 1  ※マスターノードのノードIDを指定 |
| タイプ | マスター |
| タイムゾーン | GMT+09:00 |
| IPアドレス | 追加するマスターノードのIPアドレス |
| ポート | 10051 |
| ヒストリの保存期間(日) | 90 |
| トレンドの保存期間(日) | 365 |



図 6‑5 ノード作成画面

ノード情報を入力後、「保存」ボタンを押下すると、下記画面が表示され、自分自身が、追加したマスターノードの配下になっていることを確認する。



図 6‑6 分散監視管理画面(マスターノード追加後)

このとき、Local node(子ノード)の設定でタイムゾーンがデフォルト設定のGMT+00:00になっているので、GMT+09:00に変更しておくこと。

以上で、子ノード側でのマスターノードの追加は完了となる。

## 相互監視構成設定

相互監視によって、マスターノードで子ノードの監視、子ノードでマスターノードを監視する。相互監視の設定手順として以下を実施する。

1. Zabbizサーバのホスト追加

Zabbixサーバの監視設定手順は、「5.1.3 ホストの追加」と同様の手順を踏む。ホスト設定情報の内で、異なる部分を以下に示す。

表 6‑3 Zabbixサーバ ホスト設定

|  |  |
| --- | --- |
| 設定項目 | 設定値 |
| グループ | Zabbix Servers |
| DNS名 | ZabbixサーバのDNS名 |
| IPアドレス | ZabbixサーバのIPアドレス |
| リンクするテンプレート | Template\_Gfarm\_zabbix |

ただし、Zabbixサーバが他の監視対象ノード種別いずれか (メタデータサーバ、ファイルシステムノード、代表クライアント、一般クライアント) を兼ねている場合は、上記のテンプレートをリンクしようとすると、依存関係でエラーになる。その場合は、代わりに次のテンプレートをリンクすること。(「5.1.3 ホストの追加」も合わせて参照のこと。)

表 6‑4 「リンクするテンプレート」代替設定

|  |  |
| --- | --- |
| 設定項目 | 代替設定値 |
| リンクするテンプレート | Template\_Gfarm\_zabbix\_nodep  Template\_Gfarm\_common\_nodep |

相互監視を行うため、上記設定手順は、マスターノード、子ノードそれぞれで実施する。マスターノード側では、子ノードの情報。子ノード側では、マスターノードの情報を設定する必要があるので注意すること。

# フェイルオーバ実行機能の設定

Gfarmでメタデータサーバが冗長化されている場合、マスターサーバの障害時に、フェイルオーバさせてスレーブサーバをマスターサーバに昇格させることが可能である。本機能では、Zabbixがマスターサーバの致命的な障害を検出した場合、自動的にマスターサーバを停止し、昇格可能なスレーブメタデータサーバをマスターに昇格させる自動フェイルオーバ実行機能を実現する。

ただし、ZabbixサーバがZabbixエージェントに対して、マスターサーバの状態を問い合わせたものの動作中であるという応答が得られなかった場合、それが以下のどの理由なのかを、正しく判断するのは難しい。

* マスターメタデータサーバが停止している
* マスターメタデータサーバは一旦停止したが、再起動の起動処理中である
* マスターメタデータサーバは動作中だが、非常に高負荷である
* マスターメタデータサーバは動作中だが、ネットワーク障害が起きている

本章で紹介するフェイルオーバ実行機能は、上記の理由如何によらず、マスターサーバのフェイルオーバを試みるものである。(フェイルオーバ実行は、最初は無効になっているため、本章の手順を実施しないと機能しない。)

以下、設定手順について説明する。インストールするホストにZabbixエージェント、Gfarmクライアント、メタデータサーバリスト管理機能が導入済みであることを前提とする。

## SSH公開鍵の生成と配布

下記の手順を、代表クライアント上のzabbixユーザで実行する。

この手順は代表クライアントからGfarmメタデータサーバにsshログインできることを確認すると共に、ssh先のメタデータサーバのエントリをknown\_hostsファイルに登録するために行う。known\_hostsファイルにエントリが未登録の場合は、パスフレーズなしでSSHログインができずフェイルオーバ実行が失敗するので、注意が必要である。また、known\_hostsに登録するホスト名は、gfmdhost -lコマンドで表示されるものと一致している必要がある点も、合わせて注意すること。下記の手順は全てzabbixユーザで実行する。この手順により、代表クライアントから各メタデータサーバにSSHでログインできることを可能にする。

1. zabbixユーザの認証用の鍵を生成する。

|  |
| --- |
| $ ssh-keygen -N "" -t rsa |

1. メタデータサーバ各機に、鍵をコピーする。

|  |
| --- |
| $ ssh-copy-id zabbix@*メタデータサーバのホスト名* |

代表クライアントからメタデータサーバ各機に、パスフレーズ無しでssh接続ができることを確認する。

|  |
| --- |
| $ ssh*メタデータサーバ*の*ホスト名* |

## zabbixユーザのsudo権限の設定

メタデータサーバ各機で、下記の手順をrootユーザで実行する。

1. zabbixユーザが、任意のコマンドを管理者権限で実行できるよう設定する。

visudoコマンドを使用し、/etc/sudoersファイルを編集する。

|  |
| --- |
| # visudo |

zabbixユーザに関する設定行を以下のように修正する。(赤字が修正部分)

|  |
| --- |
| zabbix ALL=(ALL) NOPASSWD: ALL |

## フェイルオーバスクリプトの設定ファイルの編集

下記の手順を、代表クライアントのzabbixユーザで実行する。

1. フェイルオーバスクリプトファイルの設定ファイルを編集する。

エディタで、ファイル/etc/zabbix/externalscripts/gfarm\_gfmd\_failover.confを開いて編集する。メタデータサーバ1台毎に、[gfmd1]、[gfmd2]、....とセクションに分けて記述する。

|  |
| --- |
| ssh=/usr/bin/ssh -i /home/zabbix/ssh/id\_rsa\_nopass  log-to-syslog=false  [gfmd1] ← Gfarmメタデータサーバ1台目の設定  host=mds-master ← ホスト名  gmd\_listen\_port=10601 ←listenしているTCPポート番号  gfmd\_pid\_file=/var/run/gfmd.pid ←PIDファイルのパス  gfarm\_bindir=/usr/bin ←一般コマンドのディレクトリへのパス  [gfmd2] ← Gfarmメタデータサーバ2台目の設定 (以下同様)  host=mds-slave  gmd\_listen\_port=10601  gfmd\_pid\_file=/var/run/gfmd.pid  gfarm\_bindir=/usr/bin |

構文はINIファイルと同じである。記述可能な設定項目は、下記の通り。

表 7‑1 フェイルオーバスクリプト設定項目一覧

|  |  |
| --- | --- |
| 設定項目 | 説明 |
| セクション共通部 | |
| log\_to\_syslog | syslog にメッセージを書き込むかどうかのフラグ。trueないしyesを指定すると、syslogへの書き込みが行われる。  デフォルト値はtrue。 |
| syslog\_facility | syslogにメッセージを書き込む際に使用するファシリティ。  デフォルト値はuser。 |
| lock\_file | フェイルオーバスクリプトの二重起動を防止するために使用する、ロックファイルのパス。  デフォルト値は/var/tmp/gfarm\_gfmd\_failover.lock。 |
| promotion\_timeout | フェイルオーバを開始してから、完了 (クライアント向けにポートをlistenしているのを確認できた状態) までの最大待ち時間。これを越えると、時間切れになった旨のメッセージ が出力され、フェイルオーバスクリプト自体もエラー終了する。  デフォルト値はnever (タイムアウトしない)。 |
| 各セクション | |
| host | gfmdの動作するホスト。  デフォルト値はセクション名。 |
| gfarm\_bindir | host上にインストールされたGfarmのbindir (一般コマンドの置かれたディレクトリへのパス)。  デフォルト値は/usr/local/bin。 |
| gfmd\_journal\_file | host上のgfmdが読み書きするジャーナルファイルへのパス。  デフォルト値は/var/gfarm-metadata/journal/0000000000.gmj。 |
| gfmd\_pid\_file | host上のgfmdが作成するPIDファイルへのパス。  デフォルト値は/var/run/gfmd.pid。 |
| gfmd\_listen\_address | host上のgfmdがlistenしているアドレス。  デフォルト値は0.0.0.0。 |
| gfmd\_listen\_port | host上のgfmdがlistenしているポートの番号。  デフォルト値は601。 |
| ssh | hostに対してsshで接続する際のsshコマンド名およびオプション。フェイルオーバスクリプトはZabbixから自動実行されるため、パスフレーズの入力無し で接続できるようになっている必要がある。  デフォルト値はssh。 |
| sudo | hostにsshで接続したとき、スーパユーザ権限でコマンドを実行する際に使用するsudoコマンドのコマンド名およびオプション。フェイルオーバスクリプトはZabbixから自動実行されるため、パスワード入力無しでsudoが実行できるようになっている必要がある。  デフォルト値はsudo。 |

1. zabbixユーザでフェイルオーバスクリプトのドライランを実行する。

設定ファイルの記述が終わったら、確認のためフェイルオーバスクリプトのドライランを行う。下記の手順はzabbixユーザで実行する。(実行した際、全てのGfarmメタデータサーバのRunがyesになっていればGfarmメタデータサーバと正しく通信が行われている。)

|  |
| --- |
| $ /etc/zabbix/externalscripts/gfarm\_gfmd\_failover.pl -t  try to get the current status of gfmd on gfmd1  try to get the current status of gfmd on gfmd2  RUN LISTEN MAX\_SEQNO ID  yes yes - gfmd1  yes - - gfmd2  gfarm\_gfmd\_failover.pl: notice: master gfmd is running |

## Webインターフェース上での設定

Zabbix上でのフェイルオーバの設定は下記になる。下記の手順は全てZabbix のWebインターフェース (分散監視構成の場合は、子ノードのほう) 上で行う。

1. Webインターフェースへのログイン

子ノードのWebインターフェースにアクセスし、Adminユーザでログインする。

1. メニューの「設定」－「アクション」からアクション一覧画面を表示する。
2. 「アクションの作成」ボタンを押下する。
3. 次表の設定を行い、「保存」を押下する。

表 7‑2 アクション設定

|  |  |
| --- | --- |
| アクション | |
| 設定項目 | 設定値 |
| 名前 | フェイルオーバ実行 |
| イベントソース | トリガー |
| エスカレーションを有効 | チェックなし |
| デフォルトの件名 | 変更なし(デフォルト値のまま) |
| デフォルトのメッセージ | 変更なし(デフォルト値のまま) |
| リカバリメッセージ | チェックなし |
| ステータス | 有効 |
| アクションのコンディション | |
| 設定項目 | 設定値 |
| 計算のタイプ | (A) and (B) and (C) |
| コンディション | (A)トリガーの値 = “障害”  (B)メンテナンスの状態  期間外 “メンテナンス”  (C)トリガー =  “Template\_Gfarm\_represent\_client\_nodep:Problem of gfmd ({ITEM.LASTVALUE})” |
| アクションのオペレーション | |
| 設定項目 | 設定値 |
| オペレーションのタイプ | リモートコマンド |
| リモートコマンド | zabbix-slave:/etc/zabbix/externalscripts/gfarm\_gfmd\_failover.pl |

以上で、フェイルオーバ実行機能の設定は完了である。

# その他の注意点

Zabbixの導入・設定に関して、当該する章で書ききれなかった点をここで補足する。

## SELinux環境での問題

SELinuxを有効にしている環境では、Zabbixエージェントが/etc/zabbix/externalscripts/の下にある外部スクリプトの実行に失敗したり、/var/log/messages等のログファイルの読み込みに失敗したりすることがある。

/var/log/zabbix/zabbix\_agentd.logに以下のようなメッセージが出力されていれば、この問題が起きている可能性が高い。

|  |
| --- |
| sh: /etc/zabbix/externalscripts/gfarm\_gfmd\_gfhost.sh: Permission denied  27376:20140826:113633.587 cannot open [/var/log/messages]: [13] Permission denied |

問題を回避するには、SELinuxのZabbix用セキュリティポリシーの定義を修正して、Zabbixエージェントによるこれらの処理が許可されるようにするか、もしくはZabbix用のセキュリティポリシー定義を無効にする必要がある。無効にするには、Zabbixエージェントの動作しているホスト上で、root権限で以下のコマンドを実行する。

|  |
| --- |
| # semodule -r zabbix |

Zabbixエージェントが動作中であれば、無効にした後でいったん起動し直すこと。

|  |
| --- |
| # service zabbix-agent restart |