

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
1.1. gfarm_zabbix パッケージの構成	1
1.2. 動作環境	1
2. システム構成	3
2.1. Zabbix 基本構成	3
2.2. Gfarm 構成	4
2.3. Zabbix 分散監視構成	4
3. インストール	6
3.2. Zabbix サーバのインストール	6
3.3. Zabbix エージェントのインストール	15
3.4. gfarm_zabbix パッケージのインストール	16
3.4.1. install.conf の編集	16
3.4.2. Zabbix エージェント用ファイルのインストール	17
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
4. 各ノードの設定	20
4.1. zabbix ユーザの登録と共通認証鍵の作成	20
4.2. 監視サーバの設定	20
4.2.1. Zabbix サーバの設定	20
4.2.2. Zabbix エージェントの設定 (分散監視構成の場合)	21
4.2.3. クライアント設定ファイル編集機能の設定	22
4.3. 監視サーバ以外の設定	23
4.3.1. Zabbix エージェントの設定	23
4.3.2. gfarm_zabbix スクリプトの設定	24
4.4. zabbix_get による動作確認	24
5. 監視設定	27
5.1. 監視項目の設定	27
5.1.1. Gfarm 監視用テンプレートの導入	27
5.1.2. ホストグループの設定	29
5.1.3. ホストの追加	31
6. 分散監視構成設定	36
6.1. 分散監視設定の準備	36
6.2. マスターノードの分散監視設定	37
6.3. 子ノードの分散監視設定	39
6.4. 相互監視構成設定	41
7. フェイルオーバー実行機能の設定	42

7.1.	SSH 公開鍵の生成と配布	42
7.2.	zabbix ユーザの sudo 権限の設定	43
7.3.	フェイルオーバースクリプトの設定ファイルの編集	43
7.4.	Web インターフェース上での設定	45
8.	その他の注意点	47
8.1.	SELinux 環境での問題	47

1. 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。

1.1. 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ー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、フェイルオーバースクリプトを用いることで、Gfarm に障害が発生した際、メタデータサーバを自動的にフェイルオーバーできるようになる。
- 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。

1.2. 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。

2. 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。

2.1. 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。

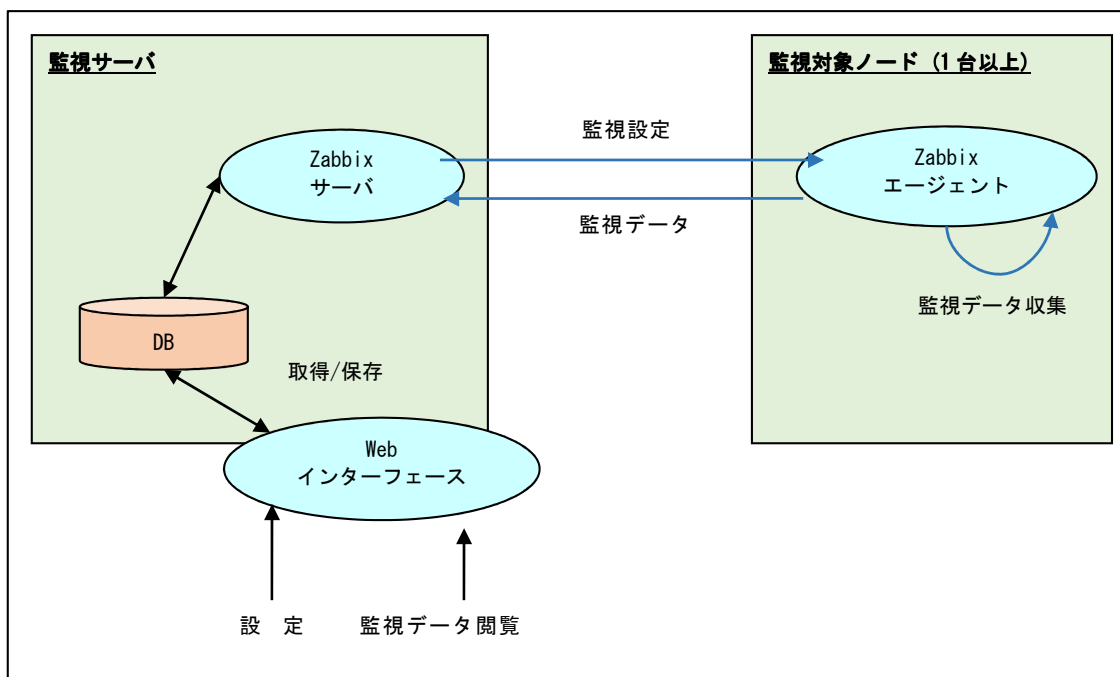


図 2-1 Zabbix 基本構成

2.2. 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。

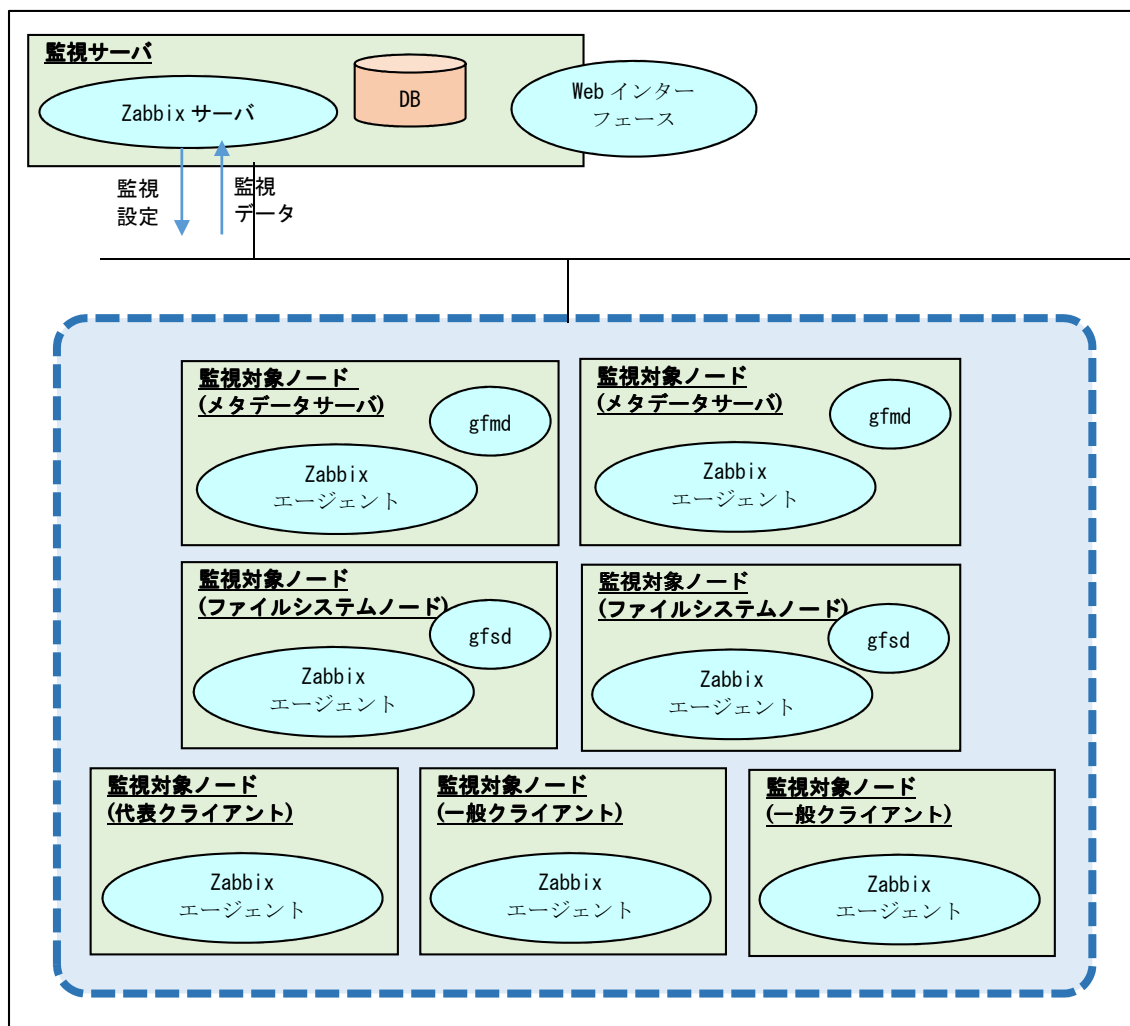


図 2-2 Gfarm 監視対象ノード構成

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。

2.3. 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（マスターノードー子ノード間）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。

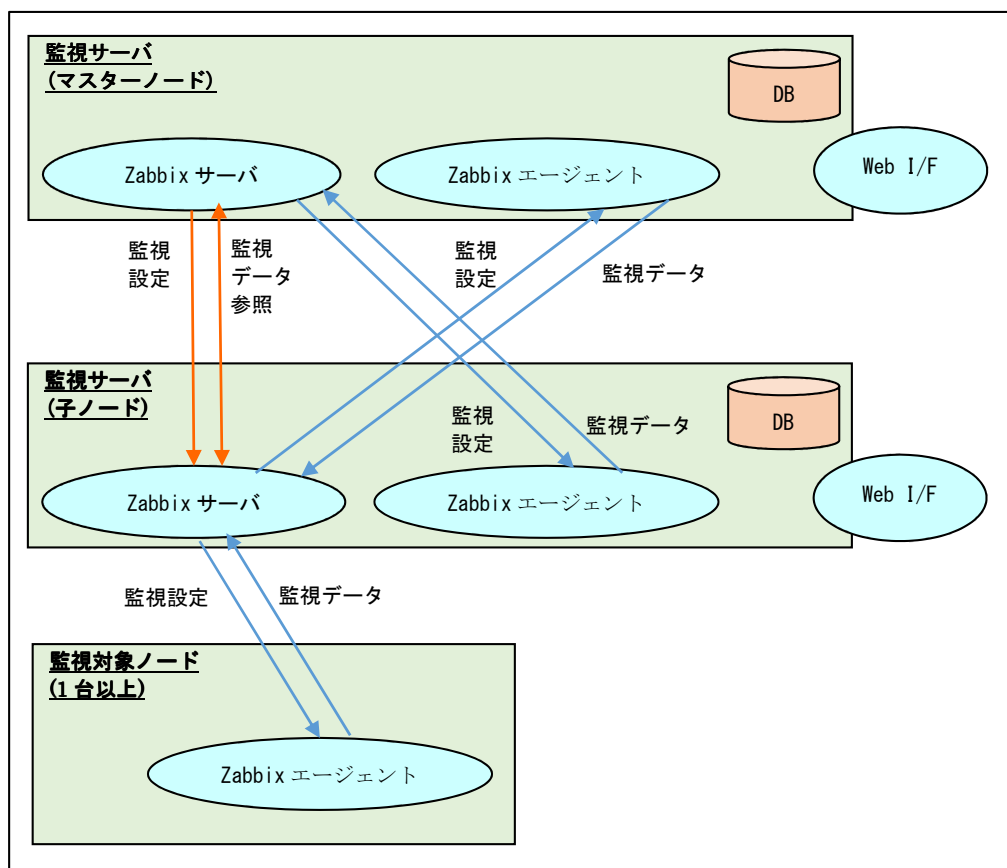


図 2-3 Zabbix 分散監視構成

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。

3. 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。

3.1. 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) <code>gfarm_zabbix</code> パッケージ
Gfarm メタデータサーバ	Zabbix エージェント <code>gfarm_zabbix</code> パッケージ
Gfarm ファイルシステムノード	Zabbix エージェント <code>gfarm_zabbix</code> パッケージ
代表クライアント	Zabbix エージェント <code>gfarm_zabbix</code> パッケージ
一般クライアント	Zabbix エージェント <code>gfarm_zabbix</code> パッケージ

3.2. 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
```

2. 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
```

3. 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
```

4. /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
```

5. MySQL を起動する。

```
# service mysqld start
```

6. Zabbix データベースを作成する。

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

7. 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
```

8. 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
```

9. /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
```

10. httpd を起動する。

```
# service httpd start
```

11. iptables で HTTP、HTTPS 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
```

12. 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
```

13. 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/
```

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

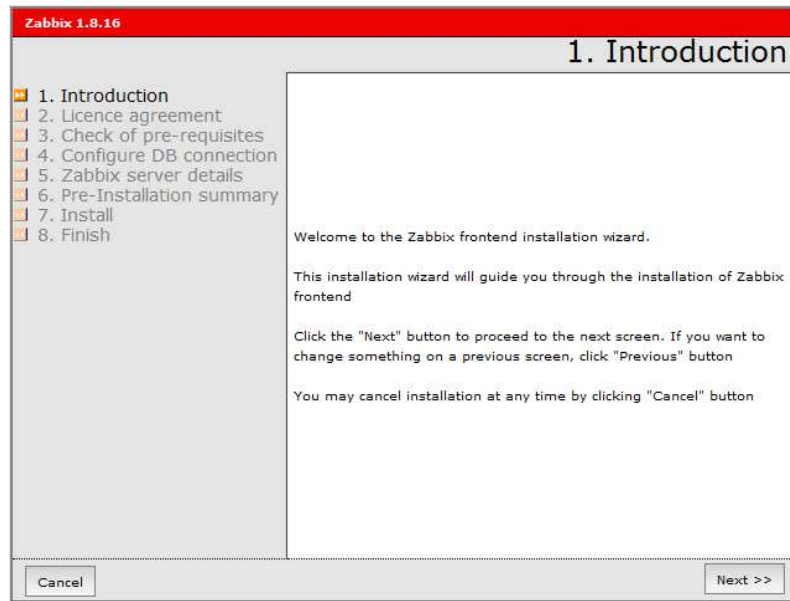


図 3-1 Introduction 画面

15. 「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。

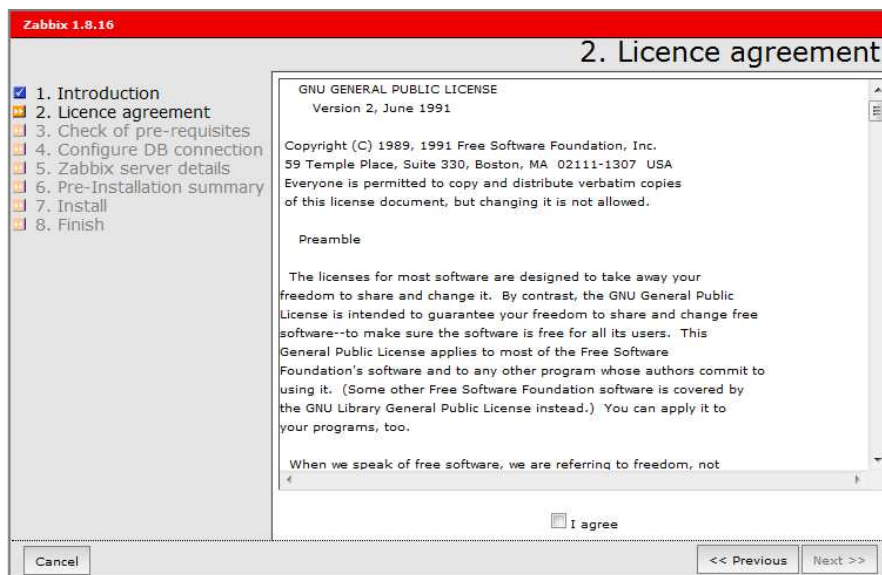


図 3-2 Licence agreement 画面

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

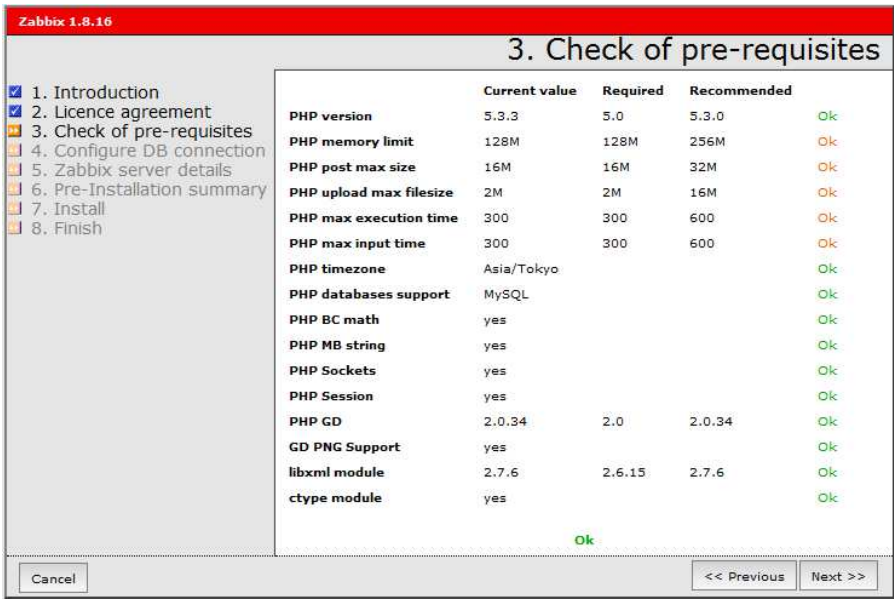


図 3-3 Check of pre-requisites 画面

17. 「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。

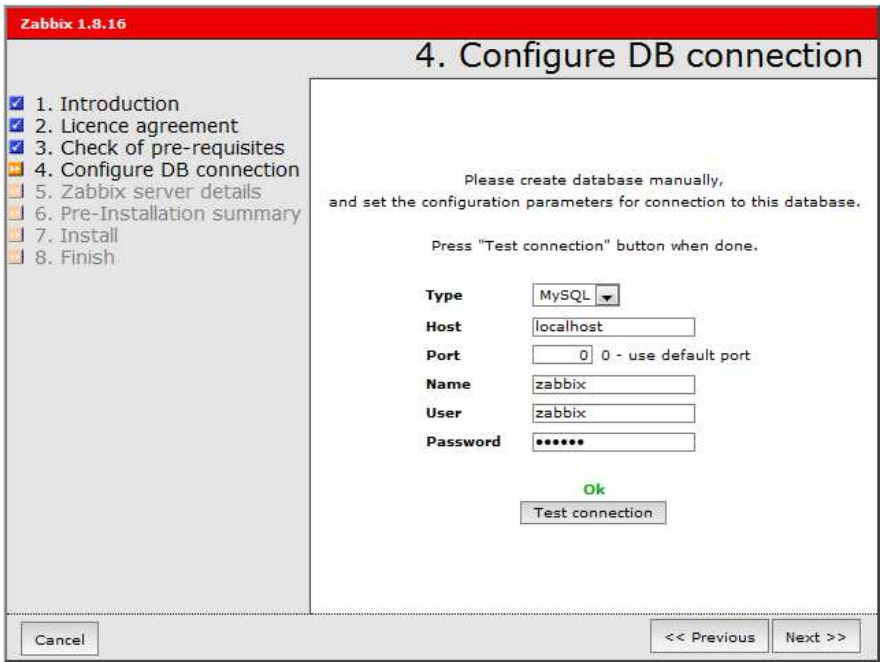


図 3-4 Configure DB connection 画面

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

18. 「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。

Zabbix 1.8.16

5. Zabbix server details

- ☒ 1. Introduction
- ☒ 2. Licence agreement
- ☒ 3. Check of pre-requisites
- ☒ 4. Configure DB connection
- ☒ 5. Zabbix server details
- ☐ 6. Pre-Installation summary
- ☐ 7. Install
- ☐ 8. Finish

Please enter host name or host IP address and port number of Zabbix server, as well as the name of the installation (optional).

Host:

Port:

Name:

Cancel << Previous Next >>

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

19. 「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。

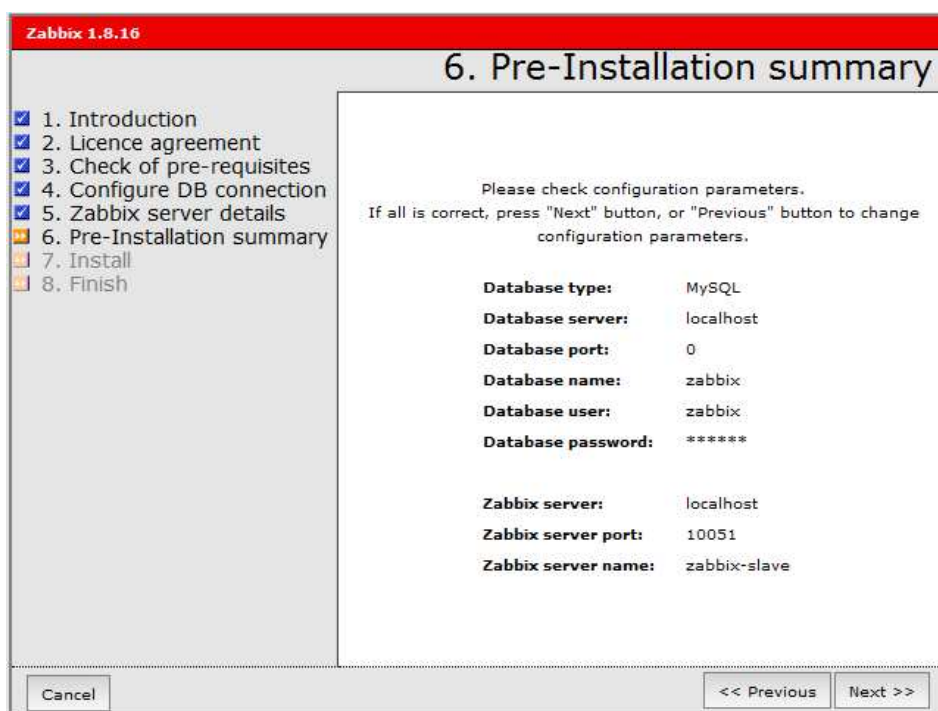


図 3-6 Pre-Installation summary 画面

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。

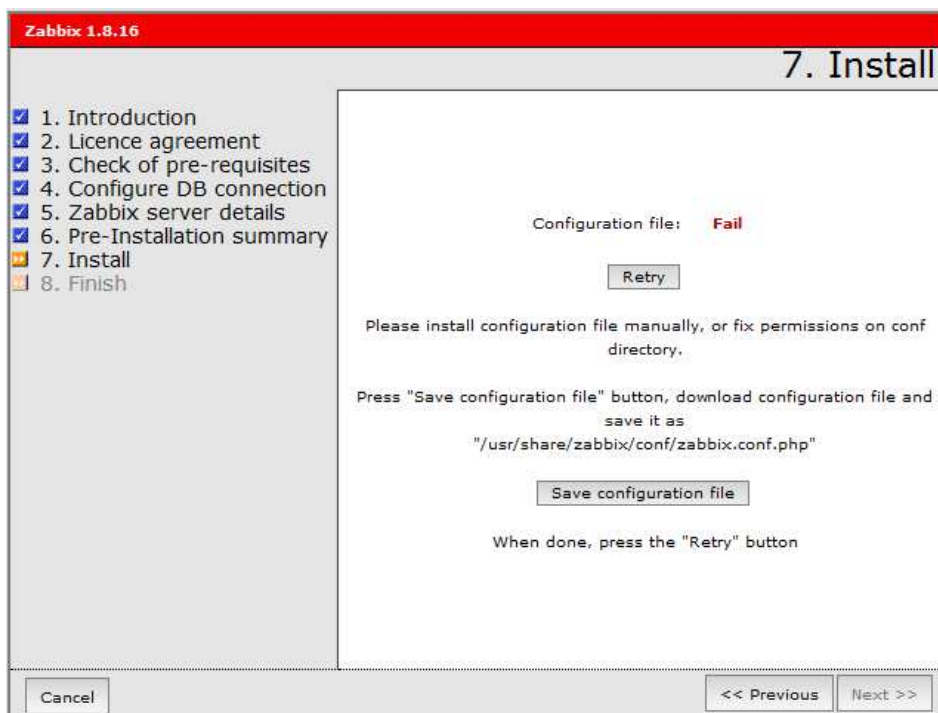


図 3-7 Install 画面

ファイルが自動的に保存された場合は、手順 22 に進む。

20. 「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。
21. 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
```

22. 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

23. 「Finish」画面が表示される。「Next」ボタンを押下する。



図 3-9 Finish 画面

24. 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

25. 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

ユーがあるので、「Users」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。

USERS

Displaying 1 to 2 of 2 found

User group

All

<input type="checkbox"/>	Alias	Name	Surname	User type	Groups	Is online?	Login	GUI access	API access	Debug mode	Status
<input type="checkbox"/>	Admin	Zabbix	Administrator	Zabbix Super Admin	Zabbix administrators	Yes (Fri, 08 Aug 2014 11:15:03 +0900)	Ok	System default	Disabled	Disabled	Enabled
<input type="checkbox"/>	guest	Default	User	Zabbix User	Guests	No (Fri, 08 Aug 2014 10:53:55 +0900)	Ok	System default	Disabled	Disabled	Enabled

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。

User "Admin" ?

Alias

Admin

Name

Zabbix

Surname

Administrator

Password

Change password

Groups

Zabbix administrators

Add Delete selected

Language

Japanese (JP)

Theme

System default

Auto-login

☐

Auto-logout (min 90 seconds)

☐ 90

Refresh (in seconds)

30

Rows per page

50

URL (after login)

Media

☐ Email m-kasahr@sra.co.jp 1-7,00:00-23:59; NIWAHD Enabled Edit

Add Delete selected

User rights (Show)

Save Delete Cancel

図 3-13 ユーザ設定画面

26. 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
```

3.3. 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
```

2. 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
```

3. Zabbix エージェントをインストールする。

```
# yum -y install zabbix zabbix-agent
```

4. 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
```

5. /etc/zabbix の所有者を変更する。

```
# chown zabbix:zabbix /etc/zabbix
```

6. 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
```

3.4. 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。

3.4.1. 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
```

3.4.2. 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
```

```
# PostgreSQL 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="MycWIXdJpvyhV52NpMxQzZX3QiJdP=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。

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

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` を定期的に行う設定を行う。

```
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
```

4. 各ノードの設定

本章では、各ノードの設定を記載する。

4.1. 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:
```

2. 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
```

3. 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
```

4. 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
```

4.2. 監視サーバの設定

監視サーバの設定を行う。

4.2.1. 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

```

2. Zabbix サーバを起動する。

```
# service zabbix-server start
```

3. 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

```

4. 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
```

5. 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
```

6. 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
```

4.2.2. 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/
```

2. Zabbix エージェントを起動する。

```
# service zabbix-agent start
```

3. 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
```

4. 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
```

5. 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
```

4.2.3. 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
```

4.3. 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。

4.3.1. 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/
```

2. Zabbix エージェントを起動する。

```
# service zabbix-agent start
```

3. 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
```

4. 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
```

4.3.2. 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

# PostgreSQL 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="MycWIXdJpyyhV52NpMxQzZX3QiJdP=GRCzv2MJCXQBH"
```

4.4. 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、 <code>_gfarmmd</code> ユーザで <code>gfhost</code> 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 <code>zabbix</code> で <code>gfarm_gfmd_gfhost.sh</code> 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、 <code>_gfarmfs</code> ユーザで “ <code>gfhost-lv</code> ” 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 <code>zabbix</code> で <code>gfarm_gfsd_gfhost.sh</code> 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、“ <code>gfmdhost-l</code> ” 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 <code>zabbix</code> で <code>gfarm_represent_client_gfmdhost.sh</code> 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、“ <code>gfhost-lv</code> ” コマンドを実行して、認証が通るかどうかを確認す

	<p>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。</p> <p>監視対象ノード上において、ユーザ <code>zabbix</code> で <code>gfarm_generic_client_gfhost.sh</code> を実行するのと同じである。</p>
proc.num[プロセス名]	全ノード種別
	<p>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</p> <p>“proc.num[gfmd]” とすれば、動作中の gfmd のプロセス数が表示される。</p>

5. 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。

5.1. 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。

5.1.1. 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。
2. 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。



テンプレート	アプリケーション	アイテム	トリガー	グラフ	リンクしているテンプレート	次にリンク
Template_3COM_3824	アプリケーション (0)	アイテム (168)	トリガー (24)	グラフ (24)	-	-
Template_3COM_4400	アプリケーション (0)	アイテム (175)	トリガー (25)	グラフ (25)	-	-
Template_AIX	アプリケーション (12)	アイテム (102)	トリガー (44)	グラフ (0)	-	-
Template_APC_Automatic_Transfer_Switch	アプリケーション (0)	アイテム (18)	トリガー (0)	グラフ (3)	-	-
Template_APC_Battery	アプリケーション (0)	アイテム (7)	トリガー (6)	グラフ (0)	-	-
Template_App_httpd	アプリケーション (1)	アイテム (13)	トリガー (7)	グラフ (1)	-	-
Template_App_MySQL	アプリケーション (0)	アイテム (6)	トリガー (0)	グラフ (0)	-	-
Template_C3750-48TS	アプリケーション (2)	アイテム (759)	トリガー (1)	グラフ (104)	-	-
Template_Cisco_837	アプリケーション (0)	アイテム (35)	トリガー (0)	グラフ (3)	-	-
Template_Cisco_877	アプリケーション (0)	アイテム (45)	トリガー (0)	グラフ (3)	-	-
Template_Cisco_2960	アプリケーション (0)	アイテム (54)	トリガー (0)	グラフ (26)	-	-
Template_Cisco_PIX	アプリケーション (0)	アイテム (9)	トリガー (1)	グラフ (1)	-	-
Template_Cisco_PIX515E	アプリケーション (4)	アイテム (48)	トリガー (7)	グラフ (9)	-	-
Template_Cisco_PIX_525	アプリケーション (0)	アイテム (35)	トリガー (0)	グラフ (0)	-	-
Template_Dell_OpenManage	アプリケーション (0)	アイテム (15)	トリガー (15)	グラフ (0)	-	-
Template_Dell_PowerConnect_S224	アプリケーション (2)	アイテム (216)	トリガー (3)	グラフ (24)	-	-
Template_Dell_PowerConnect_S324	アプリケーション (2)	アイテム (262)	トリガー (3)	グラフ (24)	-	-

図 5-1 テンプレート設定画面

3. 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

4. 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。

5.1.2. 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。
2. 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。

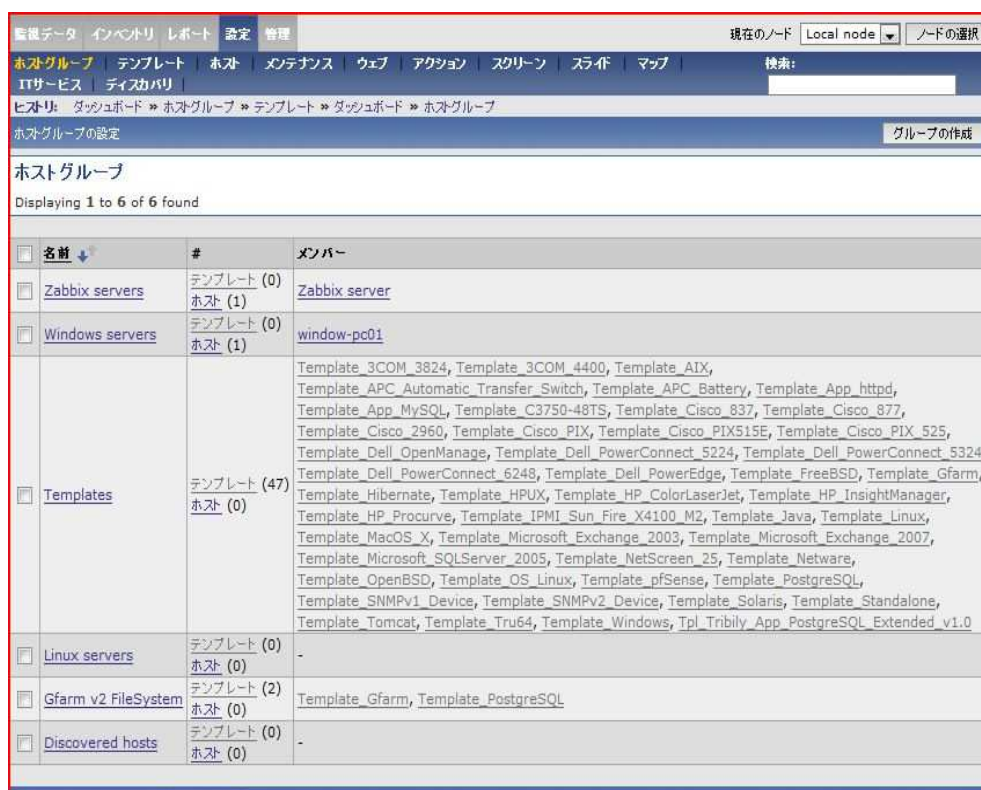


図 5-3 ホストグループ設定画面

3. 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。

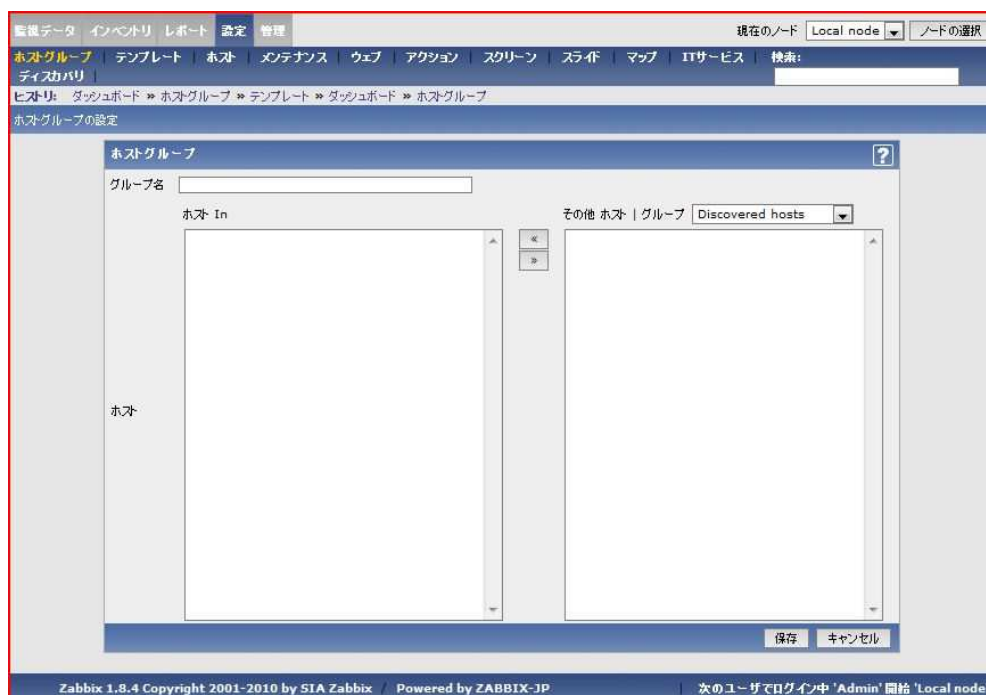


図 5-4 ホストグループ作成画面

4. 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。

5.1.3. 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」としてそ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。

2. 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

3. 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。

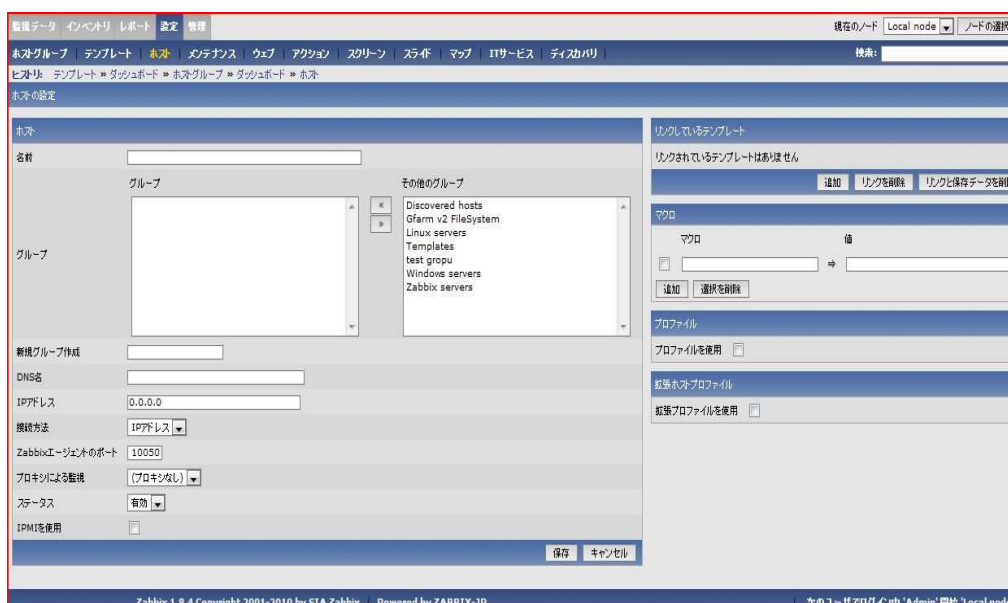


図 5-6 ホスト作成画面

4. 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、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-psql。
ファイルシステムノード	
マクロ	説明
{GFS_D_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。
{GFS_D_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。
{GFS_D_HOST_NAMES}	ファイルシステムノードのホスト名。gfhost -c でファイ

	<p>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。</p> <p>デフォルト値は、- (ハイフン・マイナス)。</p>
全ノード種別	
マクロ	説明
{ \$KERNEL_LOGFILE }	<p>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。</p> <p>デフォルト値は/var/log/messages。</p>
{ \$MONITOR_DIR }	<p>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。</p> <p>デフォルト値は/ (ルートディレクトリ)。</p>

「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。

6. 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。

6.1. 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

2. 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
```

3. 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。

6.2. 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。

2. 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

3. 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

履歴の保存期間(日)	90
トレンドの保存期間(日)	365

ノードの設定

ノード

名前: Child_Node_1

ID: 2

タイプ: 子

マスターノード: Local node

タイムゾーン: GMT+09:00

IPアドレス: 127.0.0.1

ポート: 10051

履歴の保存期間(日): 90

トレンドの保存期間(日): 365

保存 キャンセル

Zabbix 1.8.4 Copyright 2001-2010 by SIA Zabbix

次のユーザでログイン中 'Admin' 開始 'Local node'

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。

ノードを追加しました

ノードの設定

ノード

ID	名前	タイムゾーン	IPアドレス:ポート
1	/Local node	GMT+00:00	127.0.0.1:10051
2	/Local node/Child_Node_1	GMT+09:00	127.0.0.1:10051

Zabbix 1.8.4 Copyright 2001-2010 by SIA Zabbix

次のユーザでログイン中 'Admin' 開始 'Local node'

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。

6.3. 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。

2. 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

3. 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
履歴の保存期間(日)	90
トレンドの保存期間(日)	365

現在のノード: Local node | ノードの選択

一般設定 | 分散監視 | 認証 | ユーザ | メディアタイプ | スクリプト | 監査 | キュー | 通知レポート | ロケール | 検索:

インストール |

履歴: アクションの設定 » ダッシュボード » ノード » ダッシュボード » ノード

ノードの設定 | ノード

ノード

名前: Master Node

ID: 1

タイプ: マスター

タイムゾーン: GMT+09:00

IPアドレス: 127.0.0.1

ポート: 10051

履歴の保存期間(日): 90

トレンドの保存期間(日): 365

保存 | キャンセル

Zabbix 1.8.4 Copyright 2001-2010 by SIA Zabbix / Powered by ZABBIX-JP | 次のユーザでログイン中 'Admin' 開始 'Local node'

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。

現在のノード: Local node | ノードの選択

一般設定 | 分散監視 | 認証 | ユーザ | メディアタイプ | スクリプト | 監査 | キュー | 通知レポート | ロケール | 検索:

インストール |

履歴: アクションの設定 » ダッシュボード » ノード » ダッシュボード » ノード

ノードを追加しました

ノードの設定 | ノード | 新規ノード

ノード

ID	名前	タイムゾーン	IPアドレス:ポート
1	/Master Node	GMT+09:00	127.0.0.1:10051
2	/Master Node/Local node	GMT+00:00	127.0.0.1:10051

Zabbix 1.8.4 Copyright 2001-2010 by SIA Zabbix / Powered by ZABBIX-JP | 次のユーザでログイン中 'Admin' 開始 'Local node'

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。

6.4. 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. Zabbix 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、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。

7. フェイルオーバー実行機能の設定

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、フェイルオーバー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ー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ー実行機能は、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ーを試みるものである。(フェイルオーバー実行は、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。

7.1. 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ー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
```

2. 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
```

7.2. 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
```

7.3. フェイルオーバー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. フェイルオーバー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	フェイルオーバーを開始してから、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

	<p>ョン。フェイルオーバースクリプトは Zabbix から自動実行されるため、パスワードの入力無し で接続できるようになっている必要がある。</p> <p>デフォルト値は ssh。</p>
sudo	<p>host に ssh で接続したとき、スーパー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。フェイルオーバースクリプトは 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。</p> <p>デフォルト値は sudo。</p>

2. zabbix ユーザでフェイルオーバー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ー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
```

7.4. 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ー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。

- 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。
- 「アクションの作成」ボタンを押下する。
- 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	フェイルオーバー実行
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、フェイルオーバー実行機能の設定は完了である。

8. 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。

8.1. 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
```