



MongoDB 企业管理软件

系统整合书

Version 3.6.1.0

1. 被监控对象端

1.1. 建立 Linux Service Account

此内容是本文件 "2.2 以 SSH 公钥认证" 的前置作业。

被监控对象的主机 OS 为 Linux 时，需在此建立一个 gudab 专用的 Linux Service Account (例如: gudab)。

由于 gudab 的 SSH 公钥认证，采用同一组 Account，因此被监控的所有主机需建立相同的 Service Account。

```
$ sudo useradd gudab
$ sudo passwd gudab
```

1.2. 建立 MongoDB Service Account

被监控对象 (mongod instances) 需在 admin 数据库，建立一个 gudab 专用的 MongoDB Service Account (例如: root)，方能加入 Gudab 监控服务器列表。

由于 Auto Discovery 采用同一组 Account，因此丛集的所有成员需建立相同的 Service Account。

```
> use admin
> db.createUser(
  {
    user:"root",
    pwd:"gudab",
    roles:["root"]
  }
)
```

PS. 建议此 Account 具有 root role 权限，避免 gudab 权限不足无法操作。

1.3. 编辑 hosts file

确认 gudab 的 IP 可以对应其 Hostname，这会影响全备功能。

- Windows：C:\Windows\System32\drivers\etc\hosts
- Linux：/etc/hosts

```
GNU nano 2.3.1                               File: /etc/hosts
127.0.0.1    localhost localhost.localdomain localhost4 localhost4.localdomain4
::1         localhost localhost.localdomain localhost6 localhost6.localdomain6
192.168.1.121 server1
192.168.1.122 server2
192.168.1.123 server3
192.168.1.64 gudabSvr
```

1-3 hosts file (Linux 为例)

检查方式 (Windows 为例)

```
[root@server1 ~]$ ping gudabSvr
PING gudabSvr (192.168.1.64) 56(84) bytes of data.
64 bytes from gudabSvr (192.168.1.64): icmp_seq=1 ttl=128 time=0.920 ms
```

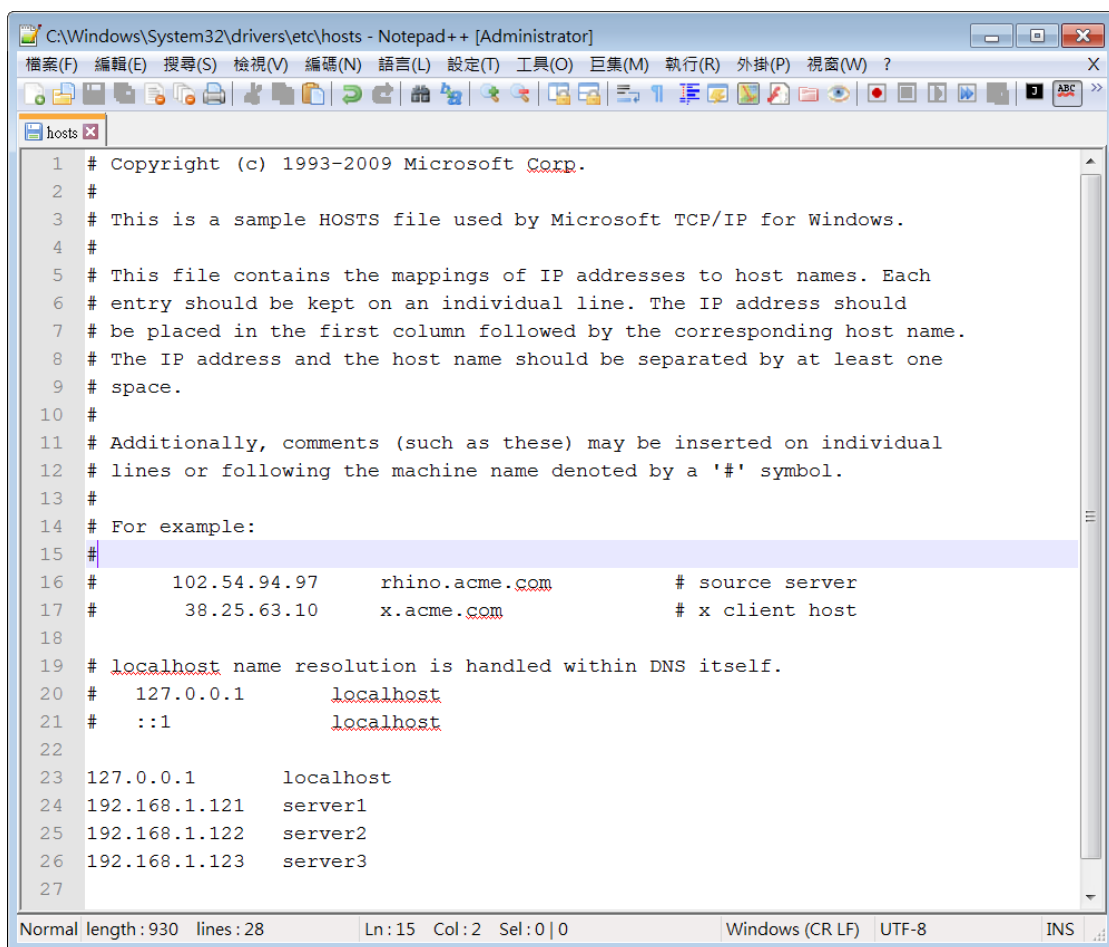
PS. 若已有 DNS 可以对应，则不用编辑 hosts file。

2. gudab 端 (监控端)

2.1. 编辑 hosts file

确认被监控对象的 IP 可以对应其 Hostname，这会影响 gudab 能否监控。

- Windows：C:\Windows\System32\drivers\etc\hosts
- Linux：/etc/hosts



```
1 # Copyright (c) 1993-2009 Microsoft Corp.
2 #
3 # This is a sample HOSTS file used by Microsoft TCP/IP for Windows.
4 #
5 # This file contains the mappings of IP addresses to host names. Each
6 # entry should be kept on an individual line. The IP address should
7 # be placed in the first column followed by the corresponding host name.
8 # The IP address and the host name should be separated by at least one
9 # space.
10 #
11 # Additionally, comments (such as these) may be inserted on individual
12 # lines or following the machine name denoted by a '#' symbol.
13 #
14 # For example:
15 #
16 #      102.54.94.97      rhino.acme.com      # source server
17 #      38.25.63.10      x.acme.com          # x client host
18
19 # localhost name resolution is handled within DNS itself.
20 #      127.0.0.1        localhost
21 #      ::1              localhost
22
23 127.0.0.1      localhost
24 192.168.1.121  server1
25 192.168.1.122  server2
26 192.168.1.123  server3
27
```

2-1 hosts file (Windows 为例)

检查方式 (Windows 为例)

```
C:\> ping server1
Ping server1 [192.168.1.121] (使用 32 字节的数据):
回复自 192.168.1.121: 字节=32 time<1ms TTL=64
```

PS. 若已有 DNS 可以对应，则不用编辑 hosts file。

2.2. 以 SSH 公钥认证、编辑 SSH properties file

● SSH 设定

以 SSH 公钥认证 (Public Key Authentication)，将 gudab 的公钥 (id_rsa.pub) 加入被监控端的信任名单(authorized_keys)，让 gudab 可免密码远程登录，搜集 Host Status 指针 (CPU, Memory, Storage, Swap)。

以下指令，在 gudab 端的主机上操作：

1. 在 gudab 端产生公钥、私钥

```
$ ssh-keygen -t rsa
```

2. 将 gudab 端的公钥，加入被监控端 (*hostname*) 的信任名单。

```
$ ssh-copy-id -i ~/.ssh/id_rsa.pub gudab@<hostname>
```

3. 测试 gudab 端可以免密码直接连到被监控端

```
$ ssh gudab@<hostname>
```

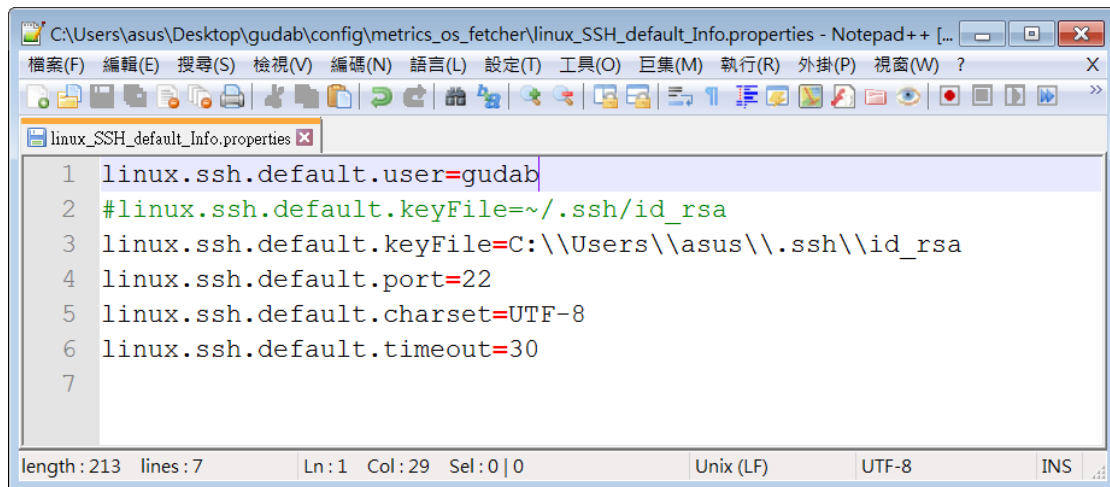
PS. 被监控对象的主机 OS 为 Windows，暂不支持监控其 Host Status 指标。

● 编辑 gudab 的 SSH properties file

在 gudab/config/metrics_os_fetcher/linux_SSH_default_Info.properties 档案，设定 Linux Service Account。

字段设定

1. linux.ssh.default.user：被监控端的 Linux Service Account。
2. linux.ssh.default.keyFile：gudab 端的私钥，路径请依实际修改。



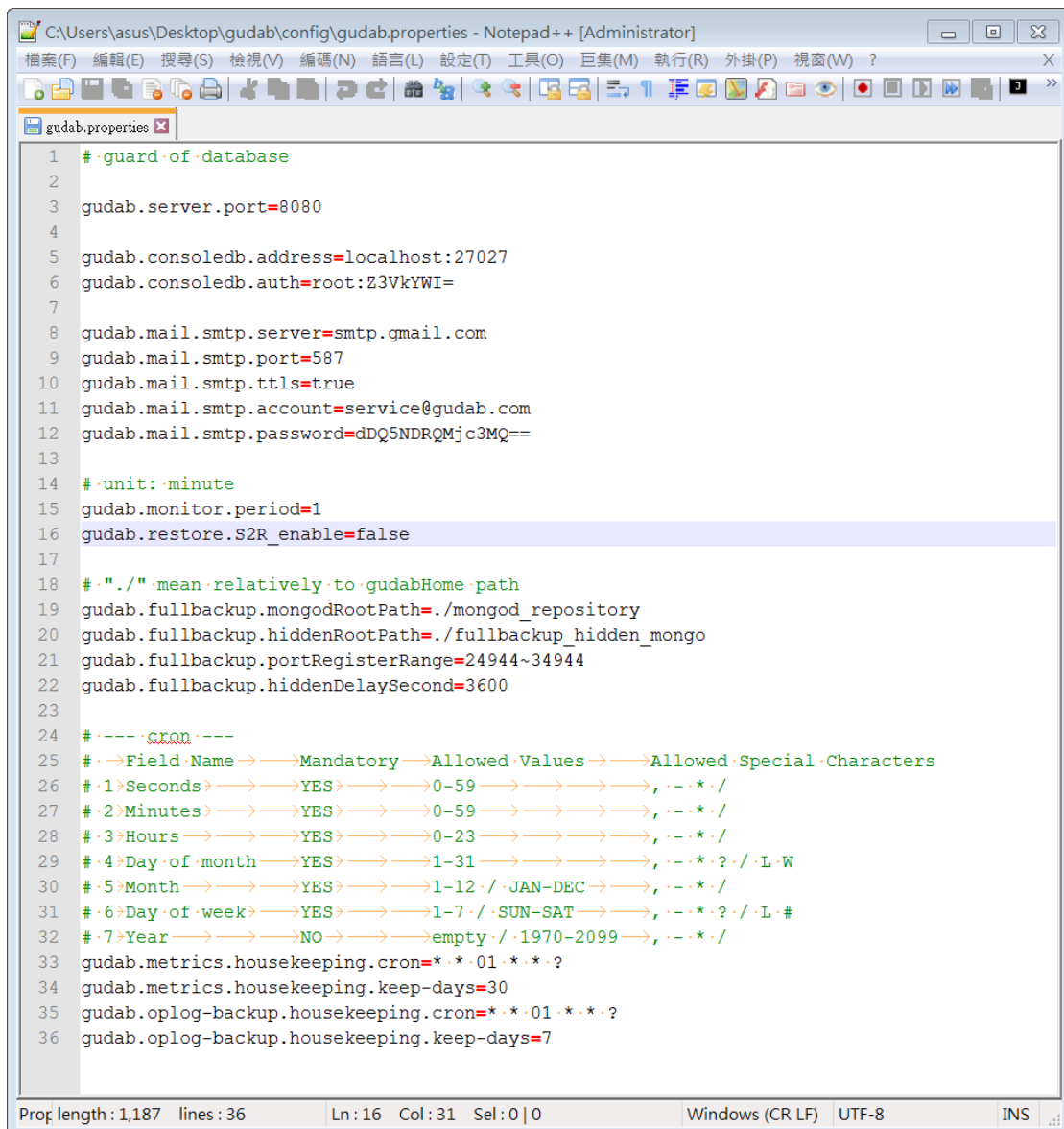
```
1 linux.ssh.default.user=gudab
2 #linux.ssh.default.keyFile=~/.ssh/id_rsa
3 linux.ssh.default.keyFile=C:\\Users\\asus\\.ssh\\id_rsa
4 linux.ssh.default.port=22
5 linux.ssh.default.charset=UTF-8
6 linux.ssh.default.timeout=30
7
```

2-2 SSH properties file (Windows 为例)

2.3. 编辑 gudab properties file

在 gudab/config/gudab.properties 档案，有许多重要设定。

1. gudab.server.port：是 Web Server 对外的埠，可调整数值，避免与其他占用程序冲突。
2. gudab.consoledb.*：gudab 将收集的指针和信息，存在此 MongoDB，为了与被监控对象区隔，将其命名为 consoleDB，可透过 changePwd.sh (.bat)修改密码。
3. gudab.mail.smtp.*：设定信箱信息，让 gudab 透过此信箱，转发系统 mail (例. "忘记密码"、"告警通知")。下图信箱以 gamil 为例，其 password 仅为示意，无法使用。可透过 encryptedPwd.sh(.bat)，将加密后的密码贴上。
4. gudab.monitor.period：监控间隔 (单位：分钟)
5. gudab.restore.S2R_enable：让 oplog 还原对象改为 mongos (router)，给特殊情境使用，预设 false。
6. gudab.fullbackup.*：全备时，delayed 成员档案的根目录、端口范围和同步延迟秒钟。
7. gudab.metrics.*：采用 Quartz 排程框架，预设每天凌晨 1 点执行作业，确保 metrics 只保留 30 天。
8. gudab.oplog-backup.*：参考 7. gudab.metrics.* 描述。



```
1 #guard-of-database
2
3 gudab.server.port=8080
4
5 gudab.consoledb.address=localhost:27027
6 gudab.consoledb.auth=root:Z3VkYWI=
7
8 gudab.mail.smtp.server=smtp.gmail.com
9 gudab.mail.smtp.port=587
10 gudab.mail.smtp.ttls=true
11 gudab.mail.smtp.account=service@gudab.com
12 gudab.mail.smtp.password=dDQ5NDRQMjc3MQ==
13
14 #unit: minute
15 gudab.monitor.period=1
16 gudab.restore.S2R_enable=false
17
18 # "." mean relatively to gudabHome.path
19 gudab.fullbackup.mongodRootPath=./mongod_repository
20 gudab.fullbackup.hiddenRootPath=./fullbackup_hidden_mongo
21 gudab.fullbackup.portRegisterRange=24944~34944
22 gudab.fullbackup.hiddenDelaySecond=3600
23
24 # --- CRON ---
25 # -->Field Name-->Mandatory-->Allowed Values-->Allowed Special Characters
26 # 1>Seconds-->YES-->0-59-->*,-.*./
27 # 2>Minutes-->YES-->0-59-->*,-.*./
28 # 3>Hours-->YES-->0-23-->*,-.*./
29 # 4>Day of month-->YES-->1-31-->*,-.*?./L.W
30 # 5>Month-->YES-->1-12./JAN-DEC-->*,-.*./
31 # 6>Day of week-->YES-->1-7./SUN-SAT-->*,-.*?./L.#
32 # 7>Year-->NO-->empty./1970-2099-->*,-.*./
33 gudab.metrics.housekeeping.cron=*. * .01.*.*?
34 gudab.metrics.housekeeping.keep-days=30
35 gudab.oplog-backup.housekeeping.cron=*. * .01.*.*?
36 gudab.oplog-backup.housekeeping.keep-days=7
```

2-2 gudab properties file (Windows 为例)

2.4. 防火墙端口设定(可选-全备用)

现阶段的 gudab 全备功能，是透过在 gudab Server 建立 delayed 成员，所以需要让部分埠开放给被监控对象，让被监控对象成员能够连接 delayed 成员。

参考 "2.3. 编辑 gudab properties file" 可以发现，
gudab.fullbackup.portRegisterRange 的范围介于 24944~34944，从数字小的开始使用。

2.5. 准备档案到指定路径(可选-全备用)

Production 环境，不论是 ReplicaSet 或 Shard，设定 Access control 是基本条件。因此，建立 delayed 成员时，就需要 Keyfile 辨识身分，并且要使用与被监控对象相同的 mongod 执行文件来启动。

- fullbackup_hidden_mongo 目录

放入 Keyfile，命名规则为 <primary hostport>.keyfile。

例. 假设要在某 ReplicaSet 加入 delayed 成员，其 primary 成员的 hostname = server1、port = 20011，则 Keyfile 路径如下

`./gudab/fullbackup_hidden_mongo/server120011.keyfile`

- mongod_repository 目录

放入对应版本的 mongod，路径只算到第二位。

例 1. 被监控对象的 MongoDB 版本是 v3.4.10，Gudab 所在的 OS 是 linux，则将下载 v3.4 的 mongod，放在下列路径：

`./gudab/mongod_repository/3.4/linux/mongod`

例 2. 被监控对象的 MongoDB 版本是 v3.6.2，Gudab 所在的 OS 是 windows，则将下载 v3.6 的 mongod.exe，放在下列路径：

`.\gudab\mongod_repository\3.6\windows\mongod.exe`

注. windows 需包含 libeay32.dll 和 ssleay32.dll (msi 下载时会提供)