**Linux agent使用手册**

**文档版本：V2.0**

**发布日期：2020/07/28**

# 目录

[目录 2](#_Toc47973217)

[一、本文档适用范围 3](#_Toc47973218)

[二、安装前准备 3](#_Toc47973219)

[2.1 环境说明 3](#_Toc47973220)

[2.2 安装环境确认 4](#_Toc47973221)

[2.3 安装前注意事项 4](#_Toc47973222)

[三、Agent配置说明 5](#_Toc47973223)

[3.1 上传并解压Linux agent包 5](#_Toc47973224)

[3.2 目录结构说明 5](#_Toc47973225)

[3.3 配置文件说明 6](#_Toc47973226)

[四、Agent相关功能操作 6](#_Toc47973227)

[4.1 启动和终止Agent程序 6](#_Toc47973228)

[4.2 日志目录说明 7](#_Toc47973229)

[4.3 Agent运行状况的确认及检查 7](#_Toc47973230)

[五、设置或取消开机启动服务 9](#_Toc47973231)

[5.1 设置开机启动服务 9](#_Toc47973232)

[5.2 取消开机启动服务 9](#_Toc47973233)

[六、卸载Linux agent 9](#_Toc47973234)

[七、常见问题说明 10](#_Toc47973235)

# 一、本文档适用范围

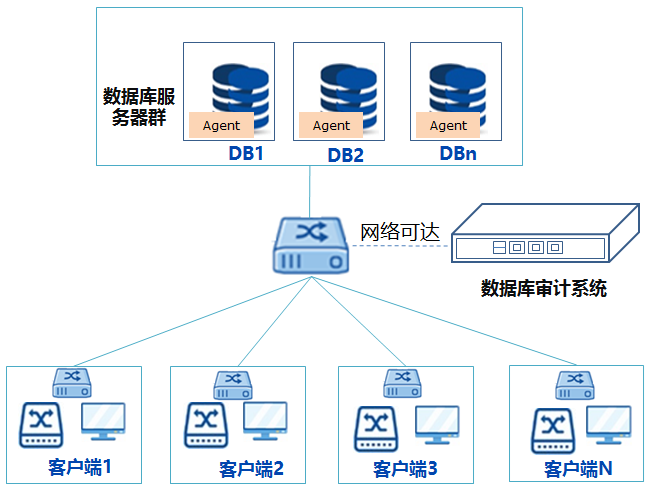
|  |  |
| --- | --- |
| **类型** | **版本** |
| 适用Agent版本 | Linux agent-5.1.1-Auth |
| 适用数审版本 | AAS V6.0及以上版本 |
| 适用操作系统 | Redhat5.8 32位  Redhat6.5 64位  Redhat6.7 64位  Redhat7.0 64位  Redhat7.3 64位  Redhat7.4 64位  CentOS6.5 32位  CentOS6.5 64位  CentOS6.8 64位  CentOS7.0 64位  CentOS7.1 64位  CentOS7.2 64位  CentOS7.3 64位  CentOS7.4 64位  CentOS7.5 64位  CentOS7.6 64位  Ubuntu16.04 64位  Ubuntu12.04 64位 |

# 二、安装前准备

## 2.1 环境说明

1. Agent插件部署在数据库服务器上，它负责将数据库指定的数据库流量转发到数据库审计设备，Agent引流环境中，数据库服务器和数审设备需网络可达
2. Agent插件部署在应用服务器上，它负责将应用服务器到指定数据库的流量转发到数据库审计设备，Agent引流环境中，应用服务器和数审设备需网络可达
3. 环境示例（Agent部署在数据库服务器）：

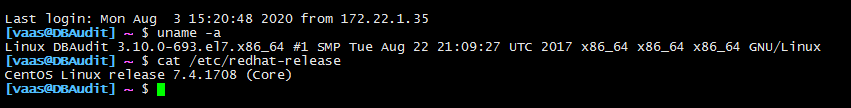
数据库审计设备的IP地址是172.24.1.115， MySQL数据库安装Linux服务器上，服务器的地址是172.21.1.10，所以，需要将Linux agent放在172.21.1.10服务器上运行



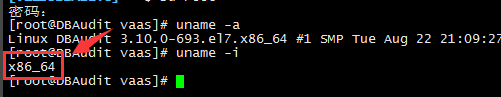
拓扑示意图

## 2.2 安装环境确认

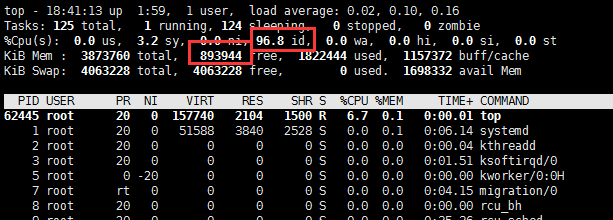
1. 使用uname –a或者cat /etc/redhat-release检查数据库服务器操作系统版本信息（不同操作系统可能命令不相同），确认操作系统是在兼容列表中。



1. 使用uname -i确认系统是32位还是64位，因为后面在配置和操作Agent时，根据系统位数的不同，选择的Agent程序也不相同



1. 使用top命令检查用户数据库服务器资源，如服务器CPU/内存资源占用超过80%，建议不要运行Agent。Agent运行默认最大占用CPU和内存各5%资源，可进行配置，超出阀值启用保护机制。



CPU id值越大代表可用的CPU资源越多；

MEM free值越大代表可用的内存越多；

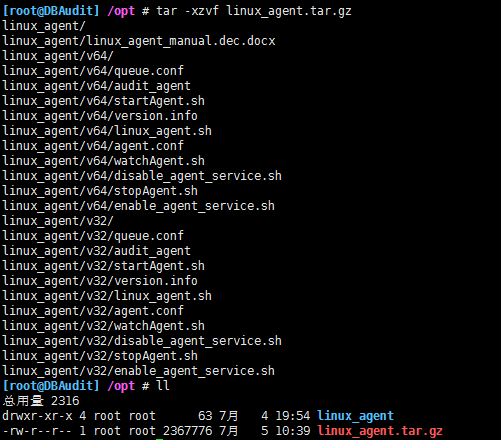
## 2.3 安装前注意事项

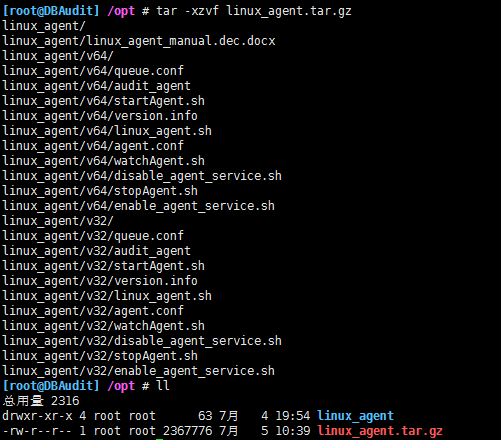
1. Agent不依赖环境，不需要提前安装任何依赖包，支持独立运行
2. 数据库服务器和数审设备之间如果有防火墙，注意要把TCP的9999端口放开。Agent和数审设备之间是通过TCP进行连接的，有时候虽然能ping通，但是中间的防火墙有可能会阻断TCP连接

# 三、Agent配置说明

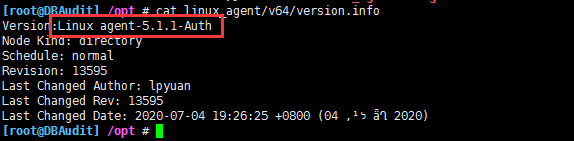
## 3.1 上传并解压Linux agent包

1. 将安装包linux\_agent.tar.gz上传到任意目录（可自定义），如/opt目录，并解压，这时目录下会多出一个解压后的目录linux\_agent



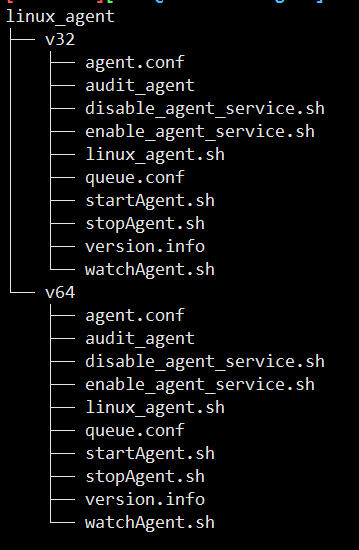


2. 查看版本号。cat linux\_agent/v64/version.info



## 3.2 目录结构说明

1. Linux\_agent主目录结构：



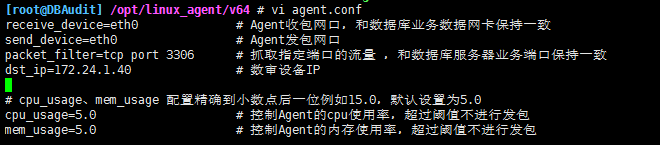
2. linux\_agent的子目录有两个，v32和v64，根据操作系统位数来选择不同的目录进行操作，其中存放agent的可执行程序、配置文件等，详细说明如下：

1. agent.conf：agent插件的配置文件
2. enable\_agent\_service.sh：设置开机自启动
3. disable\_agent\_service.sh：取消开机自启动
4. queue.conf：配置收包队列大小
5. startAgent.sh：agent启动脚本
6. stopAgent.sh：agent停止脚本
7. audit\_agent：Agent运行所需要的程序文件
8. linux\_agent.sh：Agent运行所需要的执行脚本
9. watchAgent.sh：Agent运行所需要的执行脚本

## 3.3 配置文件说明

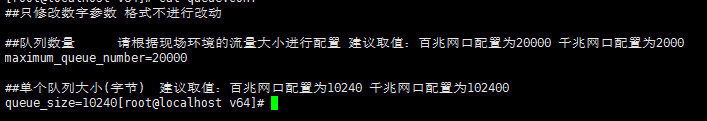
Agent主要有两个配置文件：agent.conf和queue.conf

1. agent.conf文件主要配置Agent运行的必要参数，一定要配置准确。具体配置说明如下：



注：如果receive\_device参数配置为any（receive\_device=any），那么它将采集该服务器所有网口的流量（此功能仅限Linux agent-5.1.1-Auth版本及之后的版本）。 如果要采集多个端口的流量，端口和端口之间用or分隔，如：packet\_filter=tcp port 3306 or 1521 or 50000

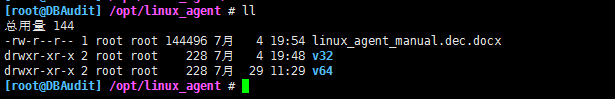
2. queue.conf文件主要配置缓存队列大小的，使用时保持默认的配置就好，如果需要作调整，请联系相关研发人员，以下为默认配置：



# 四、Agent相关功能操作

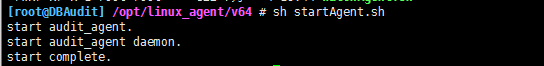
## 4.1 启动和终止Agent程序

1. 如果操作系统为32位，即进入linux\_agent/v32/目录进行参数配置并执行Agent启动脚本，如果操作系统为64位，即进入linux\_agent/v64/目录进行参数配置并执行Agent启动脚本。



2. 配置参数设定好以后，就可以启动Agent程序了。Agent程序操作命令说明如下：

① 启动Agent程序，使用sh执行对应版本目录下的脚本：sh startAgent.sh，效果如下：



② 终止Agent程序，使用sh执行对应版本目录下的脚本：sh stopAgent.sh，效果如下：

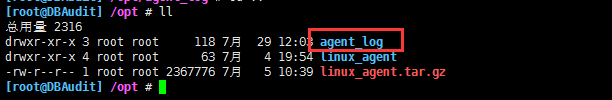


3. 当Agent服务启动后，用命令netstat –anp|grep 9999查看Agent服务器是否和审计设备建立了连接，正常已连接是显示ESTABLISHD状态，如下图所示：



## 4.2 日志目录说明

1. 当Agent服务启动以后，linux\_agent主目录的同级目录下会生成一个agent\_log目录：

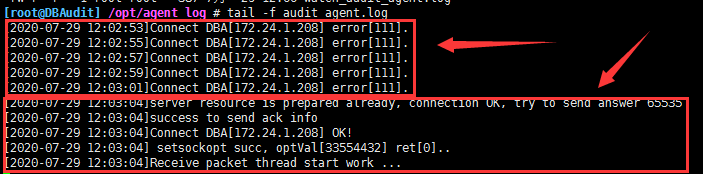


2. 日志目录各文件说明：

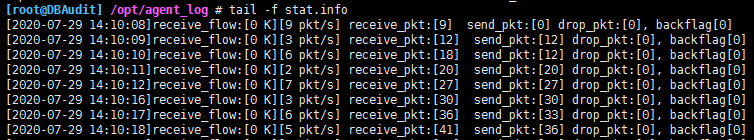
1. audit\_agent.log文件：agent连接DBA是否正常
2. watch\_audit\_agent.log文件：audit\_agent启动停止记录。
3. stat.info文件：agent流量收发情况记录。
4. resource\_usage.log: audit\_agent运行时一些相关资源占用的信息。

## 4.3 Agent运行状况的确认及检查

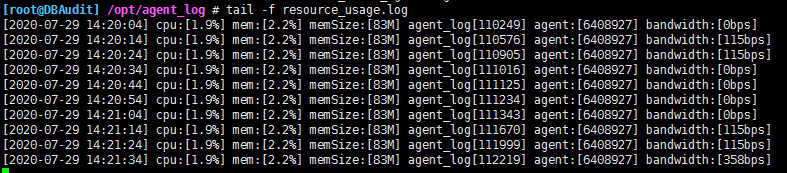
1. 使用tail –f audit\_agent.log命令查看日志，如果Agent启动失败，audit\_agent.log中会报错error，如果启动成功，则会显示start work，如下图所示：



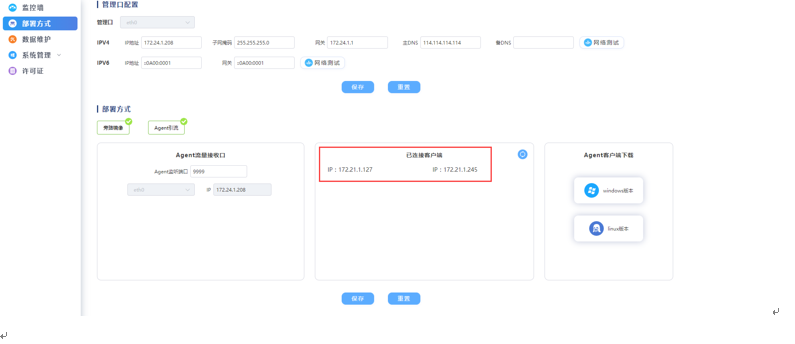
2. Agent正常工作后，stat.info日志文件将会实时每秒记录流量转发情况，如下：



3. Agent占用内存、CPU和带宽监控。Agent开始运行后，使用tail -f resource\_usage.log可监控Agent占用的CPU和内存等资源信息，刷新间隔范围10S



4. Agent正常运行后，在数据库审计系统使用sysadmin登录，可以在部署模式中，查看已连接数据库服务器客户端

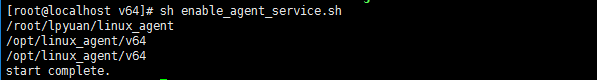


# 五、设置或取消开机启动服务

## 5.1 设置开机启动服务

如果需要数据库服务器每次重启后，audit\_agent能自动运行。执行对应版本目录下脚本。

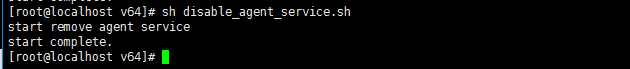
添加开机自启动，可执行命令：sh enable\_agent\_service.sh



## 5.2 取消开机启动服务

如果数据库服务器每次重启后，不需要audit\_agent自动运行。则执行对应版本目录下脚本。

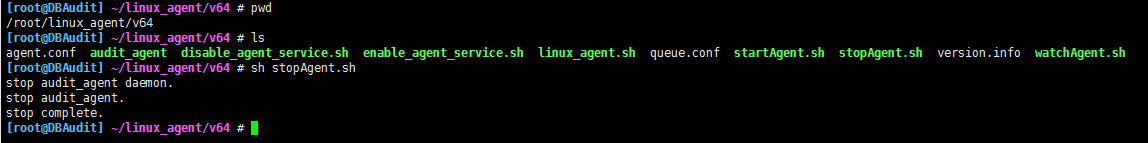
移除开机自启动，可执行命令：sh disable\_agent\_service.sh



# 六、卸载Linux agent

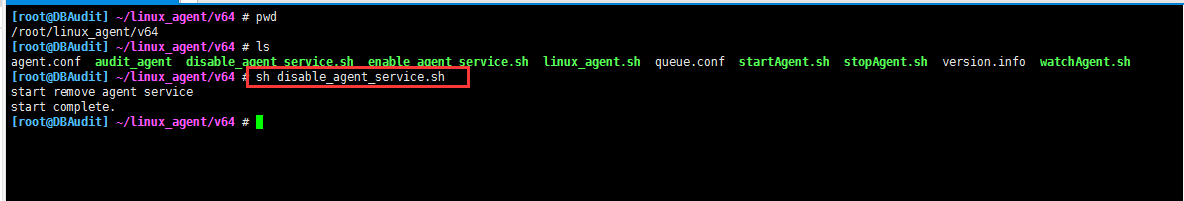
1. 若不使用Agent需要卸载Agent服务；则切换到linux\_agent/v64/目录下（如果为32位系统，则切换到linux\_agent/v32/），使用sh执行目录下的脚本： stopAgent.sh

命令如下：“sh stopAgent.sh”停止Agent程序

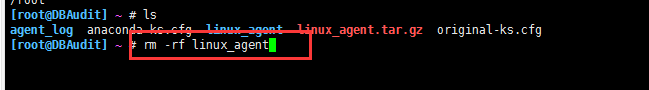


2. 取消开机自动启动，同样在linux\_agent/v64目录下（如果为32位系统，则切换到linux\_agent/v32/），使用sh执行目录下的脚本： disable\_agent\_service.sh

命令如下“sh disable\_agent\_service.sh”



3. 使用rm -rf linux\_agent 删除目录



# 七、常见问题说明

1. Linux agent是否支持多个Agent与一台数审设备对接？

答：支持

2. Linux agent是否支持一个Agent与多个数审设备对接？

答：不支持

3. Linux agent的存储是否会无限制增长？

答：不会。Linux agent客户端只会转发流量，但并不会保存流量数据到磁盘。唯一会引起存储量变化的就是日志目录。但日志目录的存储已做限制，audit\_agen.log、resource\_usage.log、stat.info这三个日志文件的存储最高为20M左右，当超过20M时会自动转成一个备份文件，并重新创建一个新的日志文件。备份文件最多只能有两个，再有新的备份文件则会自动覆盖最早的备份文件。

4. Agent是否会因为网络原因或者服务端异常，导致流量数据一直阻塞？

答：当网络原因或者服务端异常时，接收到的流量数据会逐渐写满设置的缓存空间，当缓存空间无空闲时，Agent会直接丢包处理，以保障Agent和数据库服务器的正常运行

5. Agent启动后，用netstat –anp|grep 9999查询端口信息时无结果

答：是因为数审端的部署方式没有设置成Agent引流方式

6. Agent启动成功，但是无法转发数据

答：先确认Agent 的收发包网口是否设置正确，再确认Agent的数审服务端IP、及端口信息是否设置正确

7. Agent启动后，用nestat –anp|grep 9999查询端口信息时有时无

答：确认数据库服务器的网关、子网掩码等网卡信息是否设置有误

8. 对配置文件进行了修改，但是并没有生效

答：对配置文件进行修改后，需要重启Agent