

**闪捷数据库运维安全管理系统**

**V3.0**

**闪捷数据库运维安全管理系统购买指导说明**

**文档版本：01**

**发布日期：2023-05-09**

 版权声明

本手册的所有内容，其版权属于闪捷信息科技有限公司（以下简称:闪捷信息）所有，未经闪捷信息许可，任何人不得仿制、拷贝、转译或任意引用。本手册没有任何形式的担保、立场倾向或其他暗示。

若因本手册或其所提到的任何信息引起的直接或间接的资料流失、利益损失，闪捷信息及其员工恕不承担任何责任。本手册所提到的产品规格及资讯仅供参考，有关内容可能会随时更新，闪捷信息恕不承担另行通知之义务。

**版权所有 © 2023 闪捷信息**

商标声明

本手册中所谈及的产品名称仅做识别之用，而这些名称可能属于其他公司的注册商标或是版权，其他提到的商标，均属各该商标注册人所有，恕不逐一列明。

**Secsmart ® 闪捷信息科技有限公司**

**目 录**

1 闪捷数据库运维安全管理系统购买指导说明书 2

1.1 说明 2

1.2 操作步骤 2

1.3 授权许可说明 5

2 关于SSH登录闪捷数据库运维安全管理系统后台的补充说明 6

2.1 说明 6

2.2 操作方法 6

文档说明

|  |  |
| --- | --- |
| **产品名称** | 闪捷数据库运维安全管理系统 |
| **适用平台/版本** | V3.0 |
| **拟制人**  |  | **评审组** |  |
| **发布人** |  | **备注** |  |

修订记录

|  |  |  |  |
| --- | --- | --- | --- |
| **日期** | **修订版本** | **修改记录** | **修改人** |
| 2023-05-09 | 01 | 初次发布 |  |

# **闪捷数据库运维安全管理系统购买指导说明书**

## 说明

数据库运维安全管理系统，是一款基于数据库协议分析并对数据访问行为进行控制的数据安全产品，对数据库的违规访问和攻击行为进行发现和过滤，提升整体安全防护能力。产品可通过对数据库运维人员操作行为进行安全管控。通过多因素认证、权限管控、操作审批、动态脱敏、本地化防护、误删恢复等技术，可实现对于运维人员的最小化权限控制、危险操作阻断以及行为审计。

## 操作步骤

1. 在市场搜索闪捷数据库运维安全管理系统软件镜像，选择对应的规格和推荐配置，确认购买方式按月或按年进行购买
2. 在自定义购买界面添加一块数据不小于200G的数据盘。



1. 自定义购买界面配置安全组规则，入方向规则中添加TCP 18443以及9000至10000端口范围规则。





1. 设置root用户和密码



1. 确认购买的配置无误后，点击立即购买。



1. 购买后在主机控制台使用控制台提供的VNC方式登录云主机后台，检查数据盘大小，数据盘用于存储数据库运维安全管理系统数据，

确认在云主机后台使用lsblk命令能看到新增的这块新增的大容量数据盘



1. 在控制台，复制云主机的弹性公网 IP 地址，打开浏览器，输入 **https:// 弹性公网 IP 地址 :18443**，进入WEB 界面





点击”下载授权码”，下载授权码。



## 授权许可说明

购买完成后，闪捷数据库运维安全管理系统实例会自动运行，需要购买许可方可使用。

license 购买流程（购买前如有疑问请咨询客服 [客服电话：4008118806]）：

1. 根据您单位情况，选择合适的最大资产数，并购买支付；
2. 支付成功后联系客服核对信息，验证支付；
3. 登录闪捷数据库运维安全管理系统的web管理界面，点击“下载机器码”按钮，会自动下载授权码；
4. 在交付中心提交需求，上传授权码；
5. 服务商在交付中心提供授权文件，进行下载；
6. 在数据库运维安全管理系统的web管理界面，点击“导入授权文件”按钮，上传授权文件；
7. 导入成功后可以看到相应的授权注册信息，请核实，如果有问题请联系客服；

\*\*注意\*\*：购买许可前，请先购买数据库运维安全管理系统软件镜像。

# **关于SSH登录闪捷数据库运维安全管理系统后台的补充说明**

## 说明

由于闪捷数据库运维安全管理系统安全策略SSH服务设置了root用户不能直接SSH登录，必须需要先创建普通用户登录SSH后再su切成root用户

## 操作方法

1、登录云服务器控制台, 使用控制台提供的VNC方式登录。

登录服务器控制台，在弹性云服务器界面选择对应的云主机，点击远程登录

使用控制台提供的VNC方式登录







2、使用SSH登录工具例如MobaXterm通过adg用户登录云主机的SSH后台。



1. 登录成功后，使用su命令切换成sudo su - root用户

