★完全公开

网神 SecFox 日志收集与分析系统 V5.0 分布式计算存储节点-快速上线部署手册 V1.0-软件版

创建时间：2024 年 5 月 14 日

修改时间：2024 年 5 月 14 日

网络安全服务热线：95015

公司网址：https://www.qianxin.com/

联系地址：北京市西城区西直门外南路 26 号院 1 号楼

邮编：100044

版权声明

目录

1 产品概述 4
1.1 产品简介 4
1.2 适用产品 4
1.3 读者对象 4
1.4 符号约定 4
2 设备上架 6
2.1 安装前准备 6
2.1.1 工具准备 6
2.1.2 安装环境确认 6
2.2 设备上架 7
3 首次使用 8
3.1 存储节点访问 8
3.2 存储节点管理 8
3.2.1 注册/修改日志采集器需要配置 9
3.2.2 存储节点卡片列表 9
4 软件维护 11
4.1 系统升级 11
4.1.1 通过升级包升级 11

1 产品概述

1.1 产品简介

网神 SecFox 日志收集与分析系统 V5.0R7.4.0 是奇安信网神信息技术（北京）股份有限公司（以下简称“奇安信网神”）基于在安全分析和审计技术的长期积累，结合中国政企行业的客户需求，自主研发的基于大数据技术和机器学习技术的日志审计产品，满足了客户针对日志的集中采集、存储、审计、分析和展示的需求。

网神 SecFox 日志收集与分析系统作为一个统一日志监控与审计平台，能够实时不间断地将政企客户 IT 网络中来自不同厂商的安全设备、网络设备、主机、操作系统、数据库系统、用户业务系统的日志、警报等信息汇集到审计中心，实现全网综合日志审计。

网神 SecFox 日志收集与分析系统能够实时地对采集到的不同类型的日志信息进行归一化处理和实时关联分析，协助安全管理人员从海量日志中迅速准确地识别安全事件，大幅降低了日志分析和管理对安全管理人员的技术能力要求，提高了工作效率。日志收集与分析系统为用户在统一的控制台界面进行实时、动态的可视化呈现，消除了管理员在多个控制台之间来回切换的烦恼。 日志收集与分析系统帮助用户满足安全审计的合规要求，可帮助用户快速出具满足国家法律法规，行业标准的多种合规报表和报告，帮助安全人员对内部管理的合规情况一览无余。

网神 SecFox 日志收集与分析系统实现了针对海量、高速、异构日志和事件的高吞吐量采集、高效的长期存储和快速实时的数据分析。系统采集和存储日志事件，支持搜索、检索和报告。系统记录原始日志，支持未修改数据的即席查询，以获取高质量的调查取证数据。

网神 SecFox 日志收集与分析系统既可以单机部署，也可以分布式部署，有多种可选的分布式组件，包括分布式日志采集器软件、分布式计算与存储节点软件、流量采集器设备、日志采集代理程序等。

1.2 适用产品

本手册适用于软件版本为网神 SecFox 日志收集与分析系统 V5.0R7.4.0 的分布式计算计算与存储节点软件，简称为 LAS-DCS。

1.3 读者对象

本文适用于使用奇安信网神信息技术（北京）股份有限公司网神 SecFox 日志收集与分析系统 V5.0R7.4.0 的使用人员，包括企业和组织的安全管理人员、安全分析员、安全审计人员和安全运维人员。

1.4 符号约定

在本文中可能出现下列标志，它们所代表的含义如下。

符号名称	说明
 警告	以本标志开始的文本表示有潜在危险，如果不能避免，可能导致人员伤害。
 注意	以本标志开始的文本表示有潜在风险，如果忽视这些文本，可能导致设备损坏、数据丢失、设备性能降低或不可预知的结果。
 说明	以本标志开始的文本是正文的附加信息，是对正文的强调和补充。
 窍门	以本标志开始的文本能帮助您解决某个问题或节省您的时间。

2 设备上架

2.1 安装前准备

2.1.1 工具准备

表 2-1 工具说明

工具名称	数量	用途
网线	1	用于连接设备的以太网接口和其他设备，例如连接 PC 用来调试设备。或连接其他设备用于检查设备是否配置正确。

2.1.2 安装环境确认

2.1.2.1 服务器硬件要求

硬件配置需要保持一致，标准配置如下：

表 2-2 硬件要求说明

配置	描述
内存	最低要求 32G，推荐 64G
CPU	x86 架构多核多线程 CPU，最低配置为双核 4 线程，推荐使用 Intel i5 以上 CPU，支持超线程 HT
SSD 硬盘	建议一块 SSD 固态硬盘，用来安装操作系统
SATA 硬盘	一块 4TB 企业级 SATA 硬盘及以上（硬盘容量需根据日志采集规模和保存周期确定）
网卡	1000Base-T 及以上

2.1.2.2 操作系统版本要求

目前支持 CentOS_7.X_x64、 Redhat_7.X_x64、Ubuntu18_serve_x64 或 Ubuntu20_server_x64 操作系统。要求为“基础设施服务器安装”，具体安装过程请参考《网神 SecFox 日志收集与分析系统 V5.0-操作系统安装手册 V1.1》文档。

2.1.2.3 操作系统账户要求

确保使用 root 用户进行安装操作。

2.1.2.4 软件版本要求

快速部署版本对软件的要求：

LAS-DCS-V5.0R7.4.0，当前安装包为：LAS-DCS-V5.0R7.4.0-202308030017-linux-x86-64-singleton.tar.gz

2.1.2.5 安装准备

安装 LAS-DCS 前准备工作：

1、 操作系统禁用 SELinux
禁用 SElinux 命令：sed -i "s/\=enforcing/\=disabled/g" /etc/selinux/config

2、 操作系统禁用防火墙
禁用 firewall 命令：

```
systemctl disable firewalld.service
systemctl stop firewalld.service
```

3、 重启

```
reboot
```

4、 查看 SELinux 和防火墙状态
执行命令：getenforce，查看 SElinux 状态为 Disabled

```
[root@localhost ~]# getenforce
Disabled
```

图 2-1 SELinux 状态图

执行命令：systemctl status firewalld.service，查看防火墙状态为 inactive

```
[root@localhost ~]# systemctl status firewalld.service
● firewalld.service - firewalld - dynamic firewall daemon
   Loaded: loaded (/usr/lib/systemd/system/firewalld.service; disabled; vendor preset: enabled)
   Active: inactive (dead)
     Docs: man:firewalld(1)
```

图 2-2 防火墙状态图

注意：如日志收集与分析系统（管理中心）需要搭配部署分布式计算存储节点，日志收集与分析系统（管理中心）需要开启管理中 3308 端口，供分布式计算存储节点连接。

2.2 设备上架

注意 该章节内容请按照标题顺序执行

3 首次使用

3.1 存储节点访问

LAS-DCS 系统是不提供页面登录功能的，LAS-DCS 系统安装完毕，访问页面展示如下图所示，此种情况说明系统服务启动正常

图 3-1 DCS 访问页面

3.2 存储节点管理

存储节点全称分布式计算存储节点，又称为数据节点，用来支撑大数据量下分布式计算和存储事件。

日志收集与分析系统（管理中心），“配置”—>“节点管理”模块下进行存储节点的注册和管理。（注：标准产品安装完毕不带存储节点授权，从页面看不到存储节点功能，如果客户现场需要，存储节点模块需要单独申请授权）

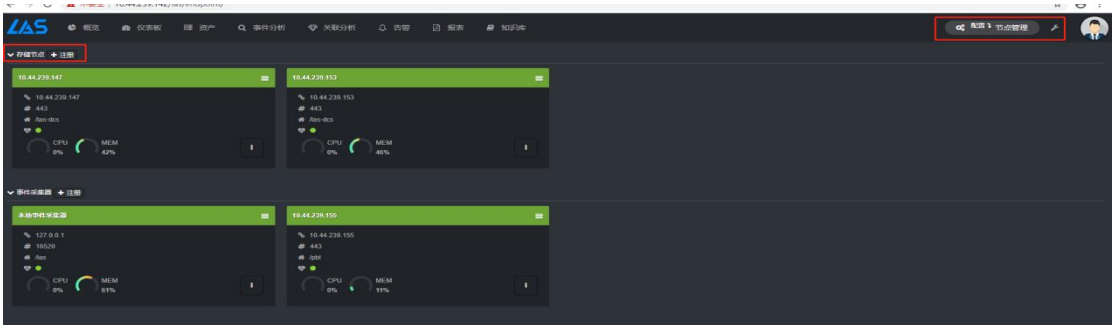

图 3-2 存储节点管理图

3.2.1 注册/修改日志采集器需要配置

1、 第一层

2、 节点类型

3、 名称

4、 描述

5、 主机（存储节点访问地址）

6、 端口（存储节点访问端口）

7、 协议（可选择 http、https）

8、 反向访问主机（需要填写）

9、 反向访问端口

3.2.2 存储节点卡片列表

点击 [配置] - [节点管理] 菜单，即可进入存储节点列表页面。存储节点列表中每个卡片中显示了存储节点的

1、 名称
2、 地址
3、 端口
4、 访问路径
5、 状态（绿色表示正常，红色表示日志采集器出现故障）
6、 CPU 利用率及内存利用率
7、 在卡片右上角可以对该采集器进行操作，对于存储节点可以进行修改、删除操作。
8、 在卡片右下角按钮可以点击查看该采集器的详细监控信息，包括：
   （1） 当前 CPU 利用率及最近 1 小时 CPU 利用率趋势
   （2） 当前内存利用率及最近 1 小时内存利用率趋势
   （3） 当前磁盘使用情况

（4） 当前系统负载情况及最近 1 小时系统负载趋势
（5） 最近 1 小时网卡流量趋势

4 软件维护

4.1 系统升级

4.1.1 通过升级包升级

DCS 未提供页面升级功能，需在后台进行升级操作。

1、 确保使用 root 用户进行安装操作。

2、 通过 sftp 工具使用 root 账户登录系统，上传至/root 目录。

3、 通过命令执行升级

```
cd /root
secfox –U LAS-DCS-R7.4.x-202x-xx-xx_202xxxxxxxx.dat
```

4、 升级完成后，通过命令：`secfox –sv` 查看版本信息，确认升级成功。