△完全公开

奇安信网神安全分析与管理系统 V4.0(NGSOC-BD&NGSOC-LV)_R4.14.1_安装部署环境要求手册_V1.0

创建时间：2024 年 5 月 7 日

修改时间：2025 年 5 月 12 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

奇安信集团，保留所有权利。
奇安信集团及其关联公司对其发行的或与合作伙伴共同发行的产品享有版权，本文中出现的任何文字叙述、文档格式、插图、照片、方法、过程描述等内容，除另有特别注明外，所有版权均属奇安信集团及其关联公司所有；受各国版权法及国际版权公约的保护。
对于上述版权内容，任何个人、机构未经奇安信集团或其关联公司的书面授权许可，不得以任何方式复制或引用本文的任何片断；超越合理使用范畴、并未经上述公司书面许可的使用行为，奇安信集团或其关联公司均保留追究法律责任的权利。
由于产品版本升级或其它原因，本手册内容会不定期进行更新。除非另有约定，本手册仅作为使用指导，本手册中的所有陈述、信息和建议不构成任何明示或暗示的担保。

● 免责声明

本免责声明（“**本声明**”）适用于奇安信集团（包括但不限于奇安信科技集团股份有限公司、奇安信网神信息技术（北京）股份有限公司、北京网康科技有限公司，以及前述主体直接或者间接控制的法律实体）旗下推出的全部产品和/或服务（以下统称“**本产品**”）。**如您使用前述产品，即表示您同意接受本声明的一切内容。如果您不同意接受，请立即停止使用相关产品。**

奇安信集团有权随时自行决定修改、添加或删除本声明的全部或部分内容。**您有责任定期检查免责声明部分的内容**，以了解是否发生了变更。**如您在我们发布变更后继续使用本产品，即表示您接受并同意这些变更。**

1. 您明确理解并同意，**本产品按“现状”提供**，不存在任何形式的明示或暗示保证，并且在适用法律允许的最大范围内，奇安信集团不提供任何明示或暗示的陈述或保证，包括但不限于有关适销性、适用于特定目的以及不侵犯第三方权利的保证。奇安信集团不保证产品中所含的功能将满足您的全部要求，也不保证您对本产品的使用不会中断或出错。**选择本产品来达到预期结果，以及安装、使用本产品并获取结果所带来的所有责任和风险由您承担。**

2. 奇安信集团承诺致力于不断提升产品的质量，本产品是在现有技术水平基础上提供的，但奇安信集团无法保证您使用本产品将完全符合您的期望，包括但不限于不能保证您【通过使用产品能够发现所有的安全漏洞以及能检测到所有的入侵威胁，检测到的入侵威胁不保证完全正确】，**您理解并同意，出现前述不符合您对产品期望的情形不视为奇安信集团违约。**

3. 您明确理解并同意，**您在使用本产品过程中可能发生不可抗力或不可预见的情形，包括但不限于：1)被某些未经许可的个人、团体或机构通过某种渠道获得或篡改；2)因通信繁忙出现延迟，或因其他原因出现中断、停顿或数据不完全、数据错误等情况，从而使交易出现错误、延迟、中断或停顿；3)因地震、火灾、台风及其他各种不可抗力因素引起的停电、网络系统故障、电脑故障等；4)计算机系统可能因存在性能缺陷、质量问题、计算机病毒、硬件故障及其他原因；黑客攻击、计算机病毒侵入或发作等非可归责于奇安信集团的原因；5）政府管制、网络故障、国家政策变化、法律法规之变化等。如发生不可抗力或不可预见的情形，奇安信集团将尽最大努力予以补救，但奇安信集团对于因不可抗力和不可预见的情形造成的各类直接或间接损失，均不承担任何责任。**

4. **对于任何本产品的使用行为，包括但不限于您自身和/或任何第三方的行为，奇安信集团均不承担任何责任。**

5. 对于从**非奇安信集团指定途径以及从非奇安信集团发行的介质上获得的本产品**，奇安信集团无法保证其是否感染计算机病毒、是否隐藏有伪装的特洛伊木马程序或者黑客软件。**使用此类产品，将可能导致不可预测的风险，建**

议用户不要轻易下载、安装、使用，奇安信集团不承担任何由此产生的一切法律责任。

6. **上述免责声明适用于因任何性能故障、错误、遗漏、中断、删除、缺陷、操作或传输延迟、电脑病毒、通信线路故障、失窃、毁坏、未经授权的访问、篡改或使用（无论是出于违约、侵权、疏忽或任何其他诉因）而导致的任何损害、责任或伤害。**
7. 奇安信集团保留在**不发布通知**的情况下随时采取以下行动的权利： **在执行常规或非常规维护、错误纠正或其他更改所必需时，中断或修改本产品的任何组成部分的运行或功能。**
8. 本声明受中华人民共和国法律的约束并依据其解释。
9. 在法律允许的最大范围内，本声明最终解释权归奇安信集团享有。

修订记录

版本	状态	修订理由和内容摘要	修订人	批准人	修订日期
V1.0.0	C	创建	朱保建		2024/05/11

状态：C-创建，A-增加，M-修改，D-删除

数据安全分级标注说明

■ 数据分级	公开数据（Y）	内部数据（）	普通商秘（）	核心商秘（）

*数据分级标注及说明：

1、文档编写前，应标注数据安全级别，默认为内部；

2、请根据文档内容评估数据安全级别，在对应数据级别（）中填写（Y）；

3、分级 TIPS：

【核心商秘】：限于个别人、小范围共享和使用的信息，例如薪酬数据、未公开的产生严重危害的样本等。如泄露将导致法律风险或者影响到社会公众利益或者严重的恶意竞争等；

【普通商秘】：限于特定人群、特定范围内共享和使用的信息，例如公司组织架构、产品样本集等。如泄露存在合规风险或者可能影响社会公众个人利益或者存在一般恶意竞争的风险等；

【内部数据】：限于在公司范围内按需使用，除去公开数据、核心商秘、普通商秘，都为内部数据。如泄露不存在法律合规风险或不存在影响社会公众个人利益的风险，但会产生轻微的恶意竞争风险等；

【公开数据】：对任何方面都无危害的、不会被任何方面进行利用的信息，例如官网上的产品简介等。如泄露对任何方面都无影响。

更多分级 Tips 参考链接: https://sec.qianxin-inc.cn/data-security/data-classification-tips

目录

1 产品概述

1.1 产品简介

奇安信态势感知与安全运营系统（Next Generation Security Operation Center，以下简称 NGSOC）是奇安信科技集团股份有限公司（简称：奇安信集团）基于大数据架构自主构建的一套面向企业用户安全运营中心的安全管理工具。该系统在 ISO 27000 信息安全管理体系和国家等级保护基本要求的指导下设计完成，可以为企业安全管理者提供资产、威胁、脆弱性等相关管理，并具备对威胁的事前预警、事中发现和事后回溯的能力，对威胁进行整体生命周期管理。

1.2 适用产品

本手册适用产品型号 NGSOC-BD、NGSOC-LV，系统软件版本 R4.14.1 版本。

1.3 读者对象

本用户手册供客户、交付代表使用。

1.4 配套手册

《奇安信网神安全分析与管理系统 V4.0(NGSOC-BD)_R4.14.1_安装部署手册》

《奇安信网神安全分析与管理系统 V4.0(NGSOC-LV)_R4.14.1_安装部署手册》

1.5 符号约定

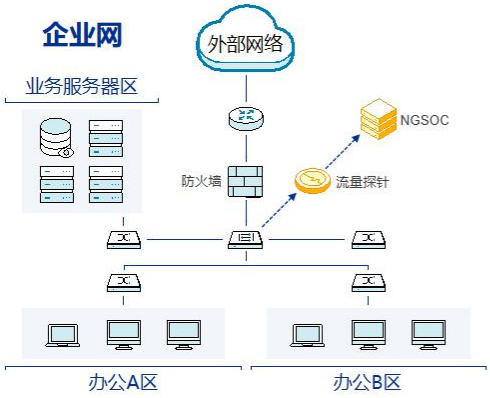
在本文中可能出现下列标志，它们所代表的含义如下。

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。

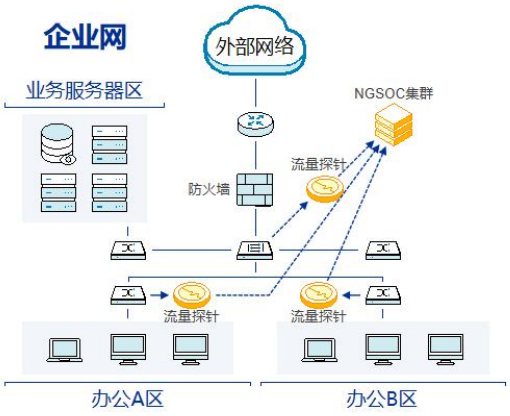
2 系统要求

2.1 网络拓扑

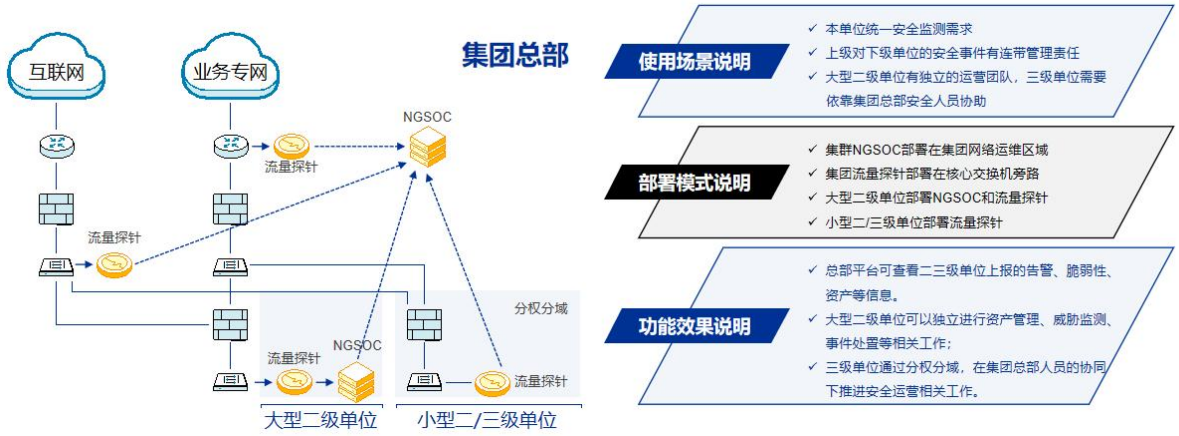
单集群部署



分权分域部署



上下级联部署



2.2 网络环境要求

NGSOC 部署时要求集群内所有节点部署在同一机房，集群内节点间开放所有网络端口访问权限。

NGSOC 部署后需要对集群外或有条件地开放如下端口。

服务（或组件）	端口	协议	端口用途
Web 页面访问	443	TCP	用于访问奇安信网神安全分析与管理系统
NOAH-Collector	514	UDP	采集日志
NOAH-Collector	162	UDP	采集日志
NOAH-Collector	161	UDP	采集日志
NOAH-Collector	29996	UDP	采集日志
Kafka	9092	TCP	用于接收流量探针发送的日志
Kafka	9094	TCP	用于接收流量探针发送的日志
级联服务	22	TCP	用于级联数据传输
级联服务	443	TCP	用于级联数据传输

注意

由于 NGSOC 系统采集并存储了客户现网中的安全数据信息，对访问安全性要求较高。用户需要将 NGSOC 系统部署在单位出口防火墙以内，且避免使用公网 IP。

2.3 硬件环境

2.3.1 物理服务器

NGSOC-BD 系统需要 3 台或以上服务器组成的服务器集群; NGSOC-LV 系统支持单机部署，最多支持 2 台服务器集群安装部署，为保障性能和稳定性，每台服务器配置需保持一致，且不低于推荐的标准配置。

配置项	说明
CPU	X86架构CPU，CPU核数（包含逻辑核）不低于40核（例如：2颗Intel Xeon Silver 4114 ）
内存	256GB DDR4及以上。
系统盘	2块960GB及以上的SSD硬盘做RAID1，保障系统的高可用性（注：告警级联时，需要扩大系统盘，按每个下级300G）。
数据盘	12块4TB或以上容量的SATA或SAS硬盘单盘做RAID0，磁盘转速不低于7200rpm（注：单盘容量不能低于4TB）。
网卡	2个万兆以太网口或4个千兆以太网口（注：集群内部流量较大，需要使用万兆网卡以保障带宽）。

2.3.2 虚拟化服务器

NGSOC-BD 系统需要 3 台或以上服务器组成的服务器集群; NGSOC-LV 系统支持单机部署，最多支持 2 台服务器集群安装部署，为保障性能和稳定性，每台服务器配置需保持一致，且不低于推荐的标准配置。

规格一：64G 规格

配置项	说明
CPU	X86架构CPU，16核(逻辑核)
内存	64GB
系统盘	600GB以上
数据盘	4TB*2
网卡	千兆网卡

说明

- 64G 规格 NGSOC-BD 安装部署最少 6 节点起。
- 64G 规格 NGSOC-LV 不支持安装部署。

规格二： 128G 规格

配置项	说明
CPU	X86架构CPU，32核(逻辑核)
内存	128GB
系统盘	600GB以上
数据盘	4TB*8
网卡	万兆网卡

说明

- 128G 规格部署 NGSOC-LV 单机不支持安全编排、高级情报检测功能。

规格三：256G 规格

配置项	说明
CPU	X86架构CPU，64核(逻辑核)
内存	256GB
系统盘	600GB以上
数据盘	4TB*12
网卡	万兆网卡

2.4 软件环境

2.4.1 操作系统配置要求

NGSOC 产品支持的操作系统

操作系统类型	版本号	内核版本	操作系统位数	备注
Openeuler	22.03 LTS SP3	5.10	64 位	X86 版本且最小化安装
麒麟 V10	V10 SP2	4.19	64 位	X86 版本且最小化安装

说明

- 麒麟 V10 操作系统为商业化产品，选择该操作系统需客户要自行采购或者在公司 CRM 系统单独购买并激活。

2.4.2 操作系统账号要求

NGSOC 需要使用 root 账户进行安装部署。需确保拥有服务器的 root 权限，且集群内所有节点服务器的 root 密码保持一致。若不一致，请使用 root 账户登录各节点服务器后台执行 passwd 命令，将密码修改为一致。

注意

在进行安装部署与扩容前，root 账户密码中不能包含‘:’、‘!’、‘\’、‘$’、‘”’、‘’’（中英文）、‘#’、‘（’、‘）’等特殊字符，否则会造成安装部署失败。**建议在进行安装部署与扩容前，临时修改 root 用户密码，使用数字+字母组合，待部署或扩容完成后修改为安全级别高的密码。**

2.4.3 浏览器配置要求

NGSOC 产品支持的浏览器

浏览器名称	版本号	位数
谷歌 Chrome 浏览器	89 及以上版本	64 位
奇安信可信浏览器	v1.0 以上	64 位

3 产品支持的数据规格表

NGSOC 产品支持数据规格表

配置	数量	备注
BD 三节点	数据处理 20000EPS	在标准物理服务器下的性能
LV 单节点	数据处理 11000EPS	在标准物理服务器下的性能
LV 双节点	数据处理 15000EPS	在标准物理服务器下的性能