长城擎天系列服务器
基础设施管理平台

鹰眼(EagleEyes)

产品白皮书

版本：V1.0

中国长城科技集团股份有限公司

声明

环境保护

请将我方产品的包装物交废品收购站回收利用，以利于污染预防，共同营造绿色家园。

商标说明

本文档中提及的所有商标或注册商标，由各自的所有人拥有。

安全声明

账户密码的声明

产品支持不同设备的集中管理，会使用到设备的账户密码，相关密码已经在数据库中加密存储。密码支持文件格式导出，导出文件中的密码未加密，建议您导出后进行必要的安全措施，防止密码被泄露。

个人数据的声明

出于您方便运维的目的，在使用过程中可按需采集个人数据，例如：运维人员信息、驻场人员信息、告警邮箱等。对于这部分信息，本产品提供了如下保护途径：

- 加密存储，个人数据信息在数据库中加密存储。
- 权限控制，Web 界面上个人数据查看等功能仅提供给具有对应权限的管理员使用。

建议您根据所适用国家或地区的法律法规制定必要的用户隐私政策并采取足够的措施以确保用到的个人数据受到充分的保护。

协议使用的声明

- 本产品支持通过 LDAP 认证。LDAP 支持 LDAP over SSL（LDAPS），进行加密传输，建议您使用 636 端口，使用 LDAPS 安全认证。

- 本产品支持通过 syslog 协议转储日志。syslog 支持 syslog over SSL，进行加密传输，建议您使用 syslog over SSL 方式进行日志转储，保证日志数据传输安全。

- 本产品支持通过 SNMP 协议发现设备。SNMP 协议共有三个版本 SNMPv1、SNMPv2c 和 SNMPv3。使用 SNMPv1、SNMPv2c 版本存在安全风险，建议您使用 SNMPv3 方式进行设备发现。

升级、补丁的声明

本产品进行版本升级或补丁安装前，建议您核对产品哈希值或数字签名，校验升级软件的合法性，避免软件被非法篡改或替换，给您带来安全风险。

安全响应的声明

长城已全面建立产品安全漏洞应急和处理机制，确保第一时间处理产品安全问题。若您在本产品使用过程中发现安全问题，或者寻求有关产品安全漏洞的必要支持，请直接联系我司客户服务人员。

长城将一如既往的严密关注产品与解决方案的安全性，为客户提供更满意的服务。

内容声明

您购买的产品、服务或特性等应受长城商业合同和条款的约束。本文档中描述的全部或部分产品、服务或特性可能不在您的购买或使用范围之内。除非合同另有约定，我司对本文档的所有内容不做任何明示或默示的声明或保证。文档中的示意图与产品实物可能有差别，请以实物为准。本文档仅作为使用指导，不对使用我们产品之前、期间或之后发生的任何损害负责，包括但不限于利益损失、信息丢失、业务中断、人身伤害，或其他任何间接损失。本文档默认读者对服务器产品有足够的认识，获得了足够的培训，在操作、维护过程中不会造成个人伤害或产品损坏。文档所含内容如有升级或更新，恕不另行通知。

技术支持

技术服务电话：400-811-8888

地址：深圳市南山区科技园科发路长城大厦

网址：https://www.greatwall.com.cn

前言

摘要

本文档主要介绍长城擎天系列服务器运维软件/工具的产品主要功能、基础操作、常见问题等相关内容。

本文档指导用户了解基础设施管理平台鹰眼（EagleEyes）的功能特性，鹰眼（EagleEyes）在文中表述为“EagleEyes”。

目标受众

本手册主要适用于：

- 技术支持工程师
- 产品维护工程师
- 企业售前工程师
- 企业管理员

注意

- 如您未采购装机服务，请在设备开箱前自行检查外包装箱。如发现包装箱严重损坏、水浸、封条或压敏胶带已开封，请视购机方式进行问题反馈。若您是通过供应商渠道购入设备，请直接与您的供应商联系；若您是通过长城直营渠道购入设备，请直接拨打服务电话 400-811-8888，联系长城技术支持处理。
- 请不要随意拆装服务器组件、请不要随意扩配及外接其它设备。如需操作，请务必在长城的官方授权和指导下进行。

- 在拆装服务器组件前，请务必断开服务器连接的所有电缆。

- 请使用长城认证的驱动程序进行 OS 环境搭建。您可联系我司进行驱动下载。如使用非长城认证的驱动程序，可能会引起兼容性问题并影响产品的正常使用，对此我司将不承担任何责任或义务。

- BIOS、BMC 的设置对配置您的服务器至关重要，如果没有特殊的需求，请您使用系统出厂时的默认值，请勿随意更改参数设置。首次登录时，请及时修改 BMC 用户密码。

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。

图标	说明
 危险	如不当操作，可能会导致死亡或严重的人身伤害。
 警告	如不当操作，可能会导致轻微或中度人身伤害。
 注意	如不当操作，可能会导致设备损坏或数据丢失。
 提示	为确保设备成功安装或配置，而需要特别关注的操作或信息。
 说明	对文档内容的描述进行必要的补充和说明。

版本说明

版　本	发布日期	说　明
V1.0	2025.4.10	初始版本

目　录

1 基础设施管理平台概述

基础设施管理平台定义

在数字化转型的关键时期，数据中心作为一种关键的基础设施，扮演着重要的角色。数据中心是用于集中存储、管理和处理大量数据的设施，它提供高性能的计算和存储资源，满足数字化转型所需的巨大数据处理需求。

随着数据量的不断增长，数据中心的规模也在不断扩大，对基础设施的管理变得愈发困难。数据中心基础设施管理是指对数据中心的计算设备、网络设备、存储设备、安全设施等基础设施进行全方位的管理，功能包括资产管理、监测管理、告警管理、日志网关管理、配置管理、知识库管理、能效管理、报表管理、流程管理、远程管理和系统管理等。

应用场景

长城擎天系列服务器基础设施管理平台主要是管理数据中心基础设施，可应用于大中小规模的数据中心基础设施管理，如大型数据中心、小型自建机房等场景。

企业数据中心：对于大型企业，基础设施管理平台关键在于监控和管理庞大的服务器和网络设备，确保数据处理的高效性和安全性。

云服务提供商：云计算服务提供商利用基础设施管理平台优化资源配置，提高服务的可靠性和资源利用率。

中小型企业：中小企业通过平台以成本效益高的方式管理 IT 资源，确保设备的稳定运行和有效监控，提高运维效率和响应速度。

行业发展现状

随着数据量和数据中心规模的快速增长，基础设施管理软件市场迅速扩大。各大厂商推出了多种数据中心基础设施管理软件。但由于数据中心基础设施的多样性和复杂性，现有的管理软件面临一系列挑战，如缺乏标准化、一体化和智能化，导致软件间协同困难，影响管理效率。此外，现有技术在满足其他行业特定需求方面存在不足，限制了应用范围。

基础设施管理平台管理价值

市场上众多基础设施管理软件的存在，使得现有管理工具缺乏标准化、一体化和智能化，这对数据中心的运营成本、稳定性、可维护性和可扩展性构成了挑战。基础设施管理系统旨在满足数据中心基础设施数字化的需求，通过高效的数据采集与存储，集成资产管理、监测管理、告警管理、日志网关管理、配置管理、知识库管理、能效管理、报表管理、流程管理、远程管理和系统管理等功能，实现数据中心基础设施的全面统一管理。

2 EagleEyes 产品介绍

2.1 产品定位

基础设施管理平台 EagleEyes，是面向金融、通信、互联网等行业数据中心的一体化基础设施管理平台，实现云边数据中心服务器、存储、网络设备及动环等基础设备的统一智能化管理。

该平台覆盖市面多品牌 IT 设备，具备线上+线下资产统一管理、大规模告警实时监控、基于 AI 的硬盘和内存故障预测、性能预测、能效管理、报表统计、流程管理等功能。EagleEyes 可统一管理服务器、存储、网络、安全等异构设备，真正促进了数据中心智能化管理，可帮助客户打造无人值守数据中心，提高运维效率、降低运维成本，保障数据中心安全、可靠、稳定的运行。

EagleEyes 可广泛应用于公有云、私有云、数据中心、运营商和企业客户，在 AI、HPC、互联网、智慧城市等多场景下部署，同时提供 Restful、SNMP、Prometheus 等接口，便于用户集成与对接。

2.2 产品特性

多场景轻量化部署，全生命周期管理

EagleEyes 提供多种部署能力，从虚拟机（KVM/VMware）到裸机场景部署（支持长城擎天 RF6260 V5），可满足小型企业、大中型企业对于全网设备特别是服务器全生命周期管理的要求。

具备高可靠能力，1-N 的数据采集、分析节点按需扩展

EagleEyes 可满足多业务场景需求，提供高可靠能力，并具备采集、分析节点数从 1 到 N 的平滑扩展能力，以应对用户扩容及多数据中心的场景且不影响原有监控业务。

智能资产管理功能，资产变更实时跟踪

EagleEyes 提供全自动、端到端的资产管理能力，包括：合同盘点、设备上架、配置核查、部件变更、设备下架、资产流程审批管理等，实现资产全生命周期管理。

全方位监控与故障预警，把控业务全局

EagleEyes 提供全方位告警监控与故障预警服务，结合先进的 AI 技术，实现服务器硬盘和内存故障预测，以智赋维，确保企业基础设施的高效稳定运行。

性能秒级监控与智能预测，掌握设备健康状况

EagleEyes 通过与 Driver 系统的无缝对接，实现了秒级的实时性能采集，确保设备运行性能指标的即时接收，借助自研的性能分析核心组件，系统能够支持大规模服务器的秒级性能数据监控与告警。同时融合分析数据中心设备性能，全面监测和分析多个关键指标，为管理员提供有效的运维决策支持，实现数据中心的高效管理。

双通道批量化配置，缩短上线周期

EagleEyes 提供批量固件升级、硬件配置、软件部署等功能，可显著提升服务器上线运维效率。

版本管理，提升版本管理效率

EagleEyes 提供固件及 OS 镜像本地管理与远程官网自动同步的能力，提升数据中心设备软硬件版本管理效率。

标准化的北向接口，方便用户集成对接

EagleEyes 提供标准 Redfish、SNMP 接口，在此基础上可扩展其他功能，便于用户集成对接。

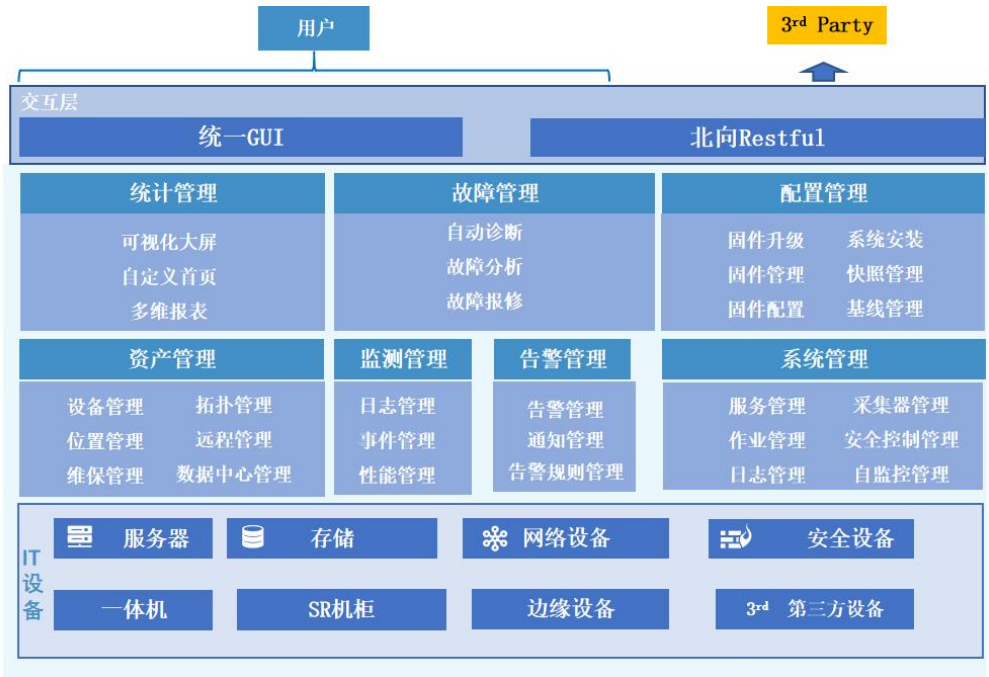
3 系统架构

3.1 软件架构

3.1.1 系统功能架构

EagleEyes 整体功能架构涵盖统计管理、故障管理、配置管理、资产管理、监测管理、告警管理、系统管理等多个模块。

图 3-1 EagleEyes 功能架构



集中管理调度中心

- **基础特性：**监测、告警、升级、安全、DFX 等。
- **七大功能：**统计管理、故障管理、配置管理、资产管理、监测管理、告警管理、系统管理。

支持全网设备管理

- 支持长城擎天 RF6260 V5 服务器，更多长城产品适配中。
- 异厂商产品，包括服务器、存储设备、网络设备等多种设备类型，可定制开发。

高可用、高扩展、灵活的技术架构

- 支持单体和分布式架构，分布式部署支持横向扩展。
- “探针式”采集，多数据中心统一管理。
- 多种部署方式，EagleEyes 支持多种部署方式，灵活适应从百台至万台不等的管理规模。

灵活的技术架构

EagleEyes 面向多种客户群体，如互联网、金融和通信行业，客户资源规模从几台服务器到数万台不等。为了在不同的场景下为这些不同的客户群体提供一致的服务体验，EagleEyes 采用了模块化的技术架构，即 Module-Oriented Architecture（MOA）。这种架构方式使得产品能够灵活适应不同规模和需求的客户，通过模块化组件来满足各种特定的需求。

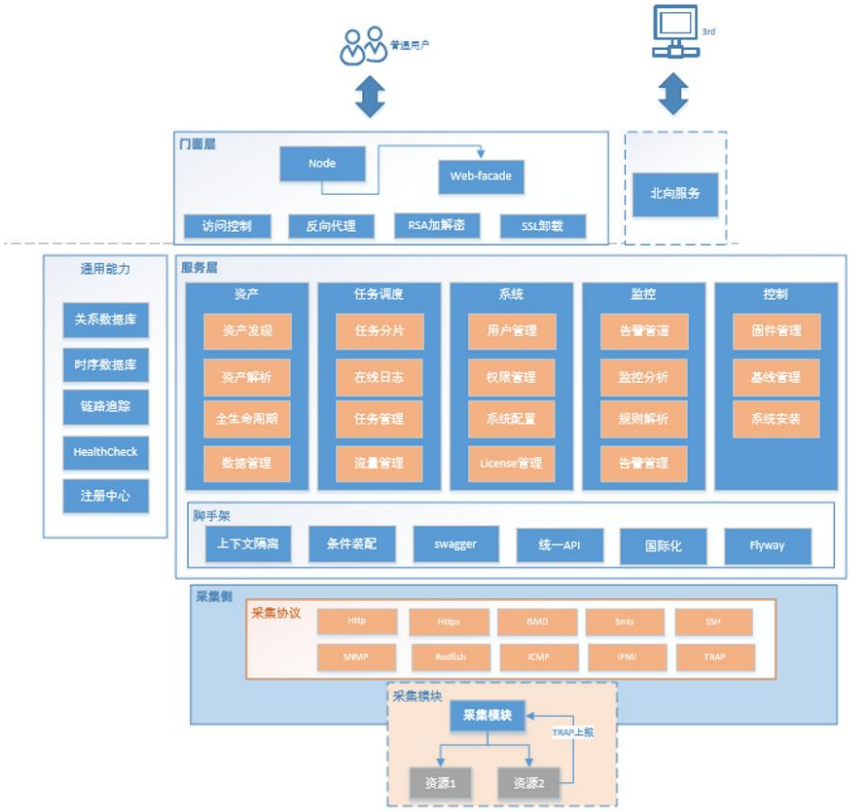
面向模块的技术架构通过区分技术模块（负责系统级功能如调用管理、缓存、队列处理等）和业务模块（针对特定业务需求如订单处理、库存管理等），提供了高度的灵活性和可扩展性。这种架构允许模块的自由组装和合并部署，以适应不同的业务场景，并在面对高负载时支持对特定模块的横向扩展，使其特别适合于复杂、动态的大型企业级应用环境。

以下基于 Module-Oriented-Architecture 的典型的两种常规技术架构：分布式架构和单体式架构。

3.1.2 系统技术架构

技术架构上自上而下分为三层：门面层、服务层和采集层；运行时主要由两个服务组成：Node 和 Mono，Node 负责前端业务和渲染；Mono 负责后端所有业务，采用合并部署的方式，合并所有后端业务到同一个进程中。整体架构如下：

图 3-2 EagleEyes 单体式技术架构



Node：负责前端业务和页面渲染，通过 Node 提供用户的 Web GUI 页面。它处理 SSL 卸载和部分安全问题，主要负责与用户交互的部分；

Mono：包含了门面层、服务层和采集层的所有功能，将这三层的逻辑合并到一个进程中。Mono 处理后端的所有业务逻辑，其内部各模块的职责与在分布式架构中相同，但都集中在单一的服务中。

采集层：采集层负责和设备间的通讯，通过自研的任务调度器触发采集任务，从采集器网关获取绑定关系后，交付给采集器进行信息的采集并上报。同时设备的回调也由采集器处理，如 SNMP TRAP 和 REDFISH 事件。

注册中心：服务注册、发现、健康检查、集群选主，负责服务的治理和健康检测。

北向服务：为北向集成提供服务，独立部署以隔离主服务资源和运行时，保证接口安全。

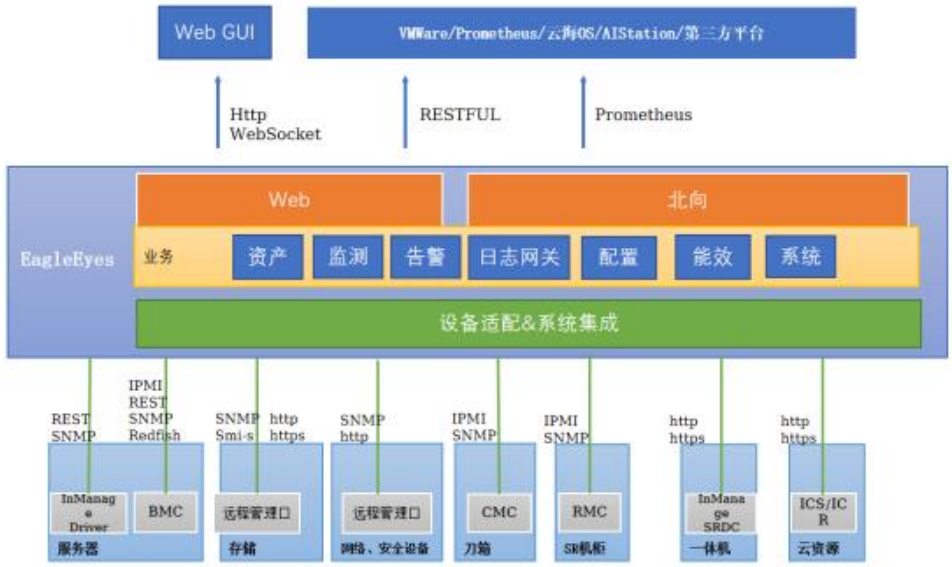
关系型数据库：主要存储资产、监控、系统、控制等配置和业务数据。

时序数据库：存储时序类数据，主要存储性能数据和功耗数据。

3.2 上下文对接方式

作为基础设施管理平台，EagleEyes 支持南北向接口对接，南向对接主要是机型兼容场景及系统接入，北向对接主要是第三方系统集成 EagleEyes 系统。

图 3-3 EagleEyes 上下文对接图



1. 南向对接

- 支持服务器管理，对接 BMC 及 Driver，支持的协议为 IPMI、SNMP、Redfish、http、https 等。
- 支持存储服务器管理，对接管理 Controller，支持的协议为 SNMP、SMI-S。
- 支持网络设备、安全设备管理，对接远程管理口，支持的协议为 http、SNMP。
- 支持刀箱管理，对接 CMC，支持的协议为 IPMI、SNMP。
- 支持 SR 机柜支持，对接 RMC，支持的协议为 IPMI、SNMP。
- 支持管理一体机设备，对接 EagleEyes SRDC，支持的协议为 http、https。

- 支持管理云资源，对接 ICS/ICR，支持的协议为 http、https。

2. 北向对接

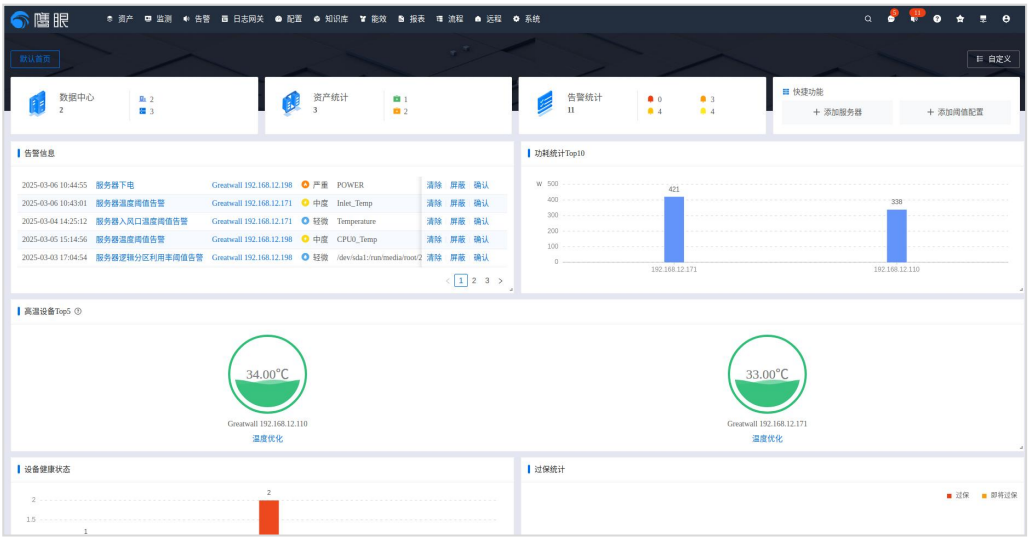
北向支持 Web GUI 对接。

Web GUI 对接：它专为 EagleEyes 页面功能设计，主要服务于运维管理员，通过这种对接，管理员可以有效地进行系统管理和监控。

4 平台功能特性

4.1 首页

图 4-1 EagleEyes 管理平台首页



4.1.1 定义

首页是一个综合信息中心，集中展示数据中心数量、资产统计及告警概况。它不仅是数据概览的窗口，还支持深入查看告警信息、功耗统计及高温设备等细节。用户可在此自定义首页布局，添加新服务器，设置监控阈值，实现个性化管理与高效监控，确保数据中心运营平稳。

4.1.2 价值描述

首页作为 EagleEyes 的核心入口，其价值在于集中、直观地展现数据中心的关键信息，包括数据中心数量、资产及告警统计等，便于用户快速掌握全局。同时，支持查看告警详情、功耗统计及高温设备等关键数据，助力用户及时响应。此外，自定义首页、添加服务器及阈值设置等功能，进一步提升了平台的灵活性和实用性。

4.1.3 功能描述

查看系统默认首页相关信息，执行自定义首页、添加服务器、添加阈值设置等操作。

在首页，用户可以查看基础设施管理平台中的数据中心、资产统计、告警统计等全局概览信息；单击数据中心、资产统计或告警统计对应的统计数字即可跳转至对应的管理页面，查看相关详细信息。

EagleEyes 首页支持查看告警信息、功耗统计、高温设备、设备健康状态、过保统计、设备统计、告警类型信息。将鼠标悬停在各趋势图上，还可以查看指定时刻的机房功耗、温度、告警等指标详情。

4.1.4 原理描述

基础设施管理平台首页的原理在于集成化信息显示与操作管理。它集中汇总并展示数据中心数量、资产及告警统计等关键数据，同时提供告警信息、功耗统计、高温设备的详细查看功能。用户可通过自定义首页布局、添加服务器及设置阈值等操作，实现个性化管理与高效监控，确保数据中心稳定运行。

4.2 资产管理

图 4-2 资产管理

4.2.1 定义

资产管理是指对基础设施系统中的设备进行全生命周期管理，包括从设计、购置、运行、维护的各个环节。它涉及对资产的详细记录、跟踪、优化使用以及定期维护，旨在确保资产的有效利用和长久运转，降低运营成本，提高整体运营效率。

4.2.2 价值描述

通过资产管理，用户可以使用手动添加或自动发现方式发现设备并添加到 EagleEyes 中，实现对不同设备的统一管理。同时，用户可以通过查看 EagleEyes 所管理设备的基本信息和运行状态，及时发现潜在的故障问题，并定位、处理问题和排除系统故障等，从而保障设备正常运行。

4.2.3 功能描述

资产管理提供资产接入和资产监控等功能。

资产接入

资产管理提供多种自动发现设备方式和添加设备方式。

- 支持多种添加设备方式，如自动发现、单个添加设备、批量添加设备。
- 支持分组管理多个设备，如创建分组、查看分组、修改分组、删除分组。
- 支持根据设备侧的协议类型选择相应的协议模板发现设备，并建立与设备间的通信。
- 提供发现任务管理功能。如：
  - 通过任务列表查看所有自动发现任务，包括周期任务和非周期任务。
  - 通过发现结果列表查看所有自动发现结果以及发现设备的基本信息。

资源监控

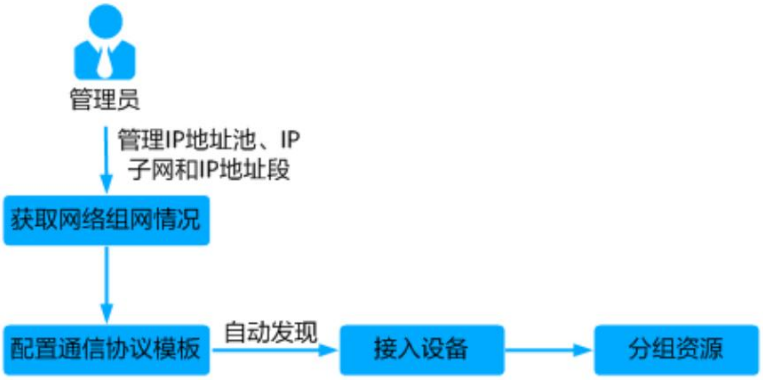
- 支持查看设备的基本信息和协议信息等。

- 支持导出资源信息功能，便于详细了解添加的设备信息。

4.2.4 原理描述

资产管理提供自动发现功能，通过输入某 IP 网段和选择协议类型，定时进行发现设备并添加到网管中。同时也支持单个或批量添加设备。自动发现设备如图 4-3 所示。

图 4-3 自动发现设备



资产添加至 EagleEyes 中时，会默认按设备类型进行分组，但实际应用时，默认提供的分组可能无法满足实际监控设置和授权等要求。因此，可通过自定义资产分组来达成目标。自定义资产分组是通过定义分组规则来实现，被接入的设备会自动匹配所定义的规则完成分组。

4.2.5 关键指标

每添加一个设备至 EagleEyes，即会占用一个 License 容量。

批量导入设备一次支持导入 10000 台设备。

系统最大支持 30 个自定义属性字段可应用在服务器、存储设备、网络设备、安全设备等数据中心 IT 设备上。

4.3 监测管理

图 4-4 监测管理

4.3.1 定义

监测管理是指通过一系列的技术手段和管理方法，对基础设施进行实时或定期的监测、评估和管理，以确保其正常运行、优化性能、预防故障，并满足相关的法规和标准要求。

4.3.2 价值描述

监测管理的价值在于实时掌握基础设施状态，包括健康监测、性能监测、巡检管理以及网络测试工具，预防故障发生，优化运行性能，确保安全性和合规性，同时为决策提供数据支持，提高管理效率，降低运营成本，是保障基础设施稳定运行的重要手段。

4.3.3 功能描述

健康监测

EagleEyes 的健康监测功能为用户提供了监测记录、服务器重启记录以及日志下载功能，该功能方便用户随时掌握设备的运行状况，包括性能、磨损及故障预警等信息。这有助于用户及时采取维护措施，预防设备故障，延长设备寿命，同时优化设备使用效率，确保业务连续性和生产安全。

- **监测记录：**支持服务器、存储、网络设备的健康监测，可查看各部件状态及部件详情。
- **服务器重启记录：**支持服务器的开机、关机、重启事件时间记录、次数统计以及对应的系统事件日志查看。
- **日志下载：**服务器或设备上记录的日志文件传输到本地电脑，以便用户进行查看和分析的过程。

性能监测

性能监测包括性能视图、指标比对以及性能预测。该功能帮助用户迅速把握整体情况，并支持多种过滤条件以便快速定位特定设备的性能状态。

- **全面的性能指标展示：**性能列表提供了包括服务器名称、IP 地址、带内 IP、序列号、型号、厂商、性能曲线、Driver 状态等在内的多种性能指标。为用户提供了全方位的设备性能信息，帮助用户快速了解设备运行情况。

- **CPU 和内存使用率：**通过监控 CPU 利用率和内存使用率，用户可以识别系统瓶颈和性能热点，进而进行相应的资源调整或优化。

- **支持统一设备类型：**支持同设备的不同时间段的比对，可监测性能变化，优化使用策略，预防故障，提升设备效率和寿命。

- **多组比对配置：**用户可以设置多个比对组，允许同时对不同的设备组或性能指标进行比较。这增加了分析的灵活性，使管理员能够根据需要定制和调整比对方案。

巡检管理

EagleEyes 支持用户自定义添加设备巡检作业，系统会自动对设备状态进行巡检并生成巡检报告，用户可基于巡检记录从系统预览并导出巡检报告到本地。同时支持自动将巡检报告发送给客户，其具体包括以下功能：

- 支持用户自定义巡检周期及巡检设备范围，巡检类型可以选择一次性、区间或每周。支持用户自定义服务器巡检的带外组件，包括：CPU、内存、硬盘、PCIE、电源、风扇、温度等。

- 支持用户自定义服务器巡检的带内指标及期望范围设定，包括：CPU 占用率、内存占用率、硬盘占用率、IO 占用率、交换空间占用率、SELinux、防火墙状态等。

- 支持用户在巡检作业中绑定通知用户，系统将在巡检完成后自动将巡检报告发送至用户。

- 支持用户自定义各类设备部件的健康状态巡检能力。

4.3.4 原理描述

EagleEyes 凭借多种业界标准的管理协议，采用主动与被动相结合的策略，实现设备全天候监控与故障分析，降低业务风险。它全面覆盖带内带外监控，通过可选 Driver 深入服务器采集数据，同时支持网络监测与维保到期告警，满足多样化管理需求。

4.4 告警管理

介绍告警管理的基本信息，包括定义、价值描述、应用场景、功能描述及原理描述等。

图 4-5 告警管理

4.4.1 定义

告警管理提供了告警数据接收、处理、通知等功能，支持告警的全生命周期管理，帮助运维人员根据告警信息快速排除故障。

4.4.2 价值描述

通过告警管理，用户可以集中监控设备自身的告警，快速定位系统和网络中已经发生的故障。

告警管理的价值包括：

- 提供了多样化的告警过滤方式，帮助运维人员快速筛选所关注的告警，实现精准监控。

- 提供告警满处理功能，避免用户所关注的告警被转储。
- 支持灵活的告警规则配置，将海量的告警进行关联和压缩，减少告警噪声，提高监控效率。
- 提供远程通知功能，将上报的告警以邮件或短消息方式发送给 ICT 系统维护人员，方便其及时了解告警情况。
- 用户在实时告警中查看该告警的相关溯源信息及可能引发的预警信息。
- 为用户提供告警相关性分析和告警趋势分析，帮助用户查看告警事件间的内在逻辑与关联。
- 提供告警数据库溢出转储功能，避免因数据库空间不足导致告警丢失。

4.4.3 功能描述

告警管理提供告警订阅、告警规则管理、告警降噪压缩、告警相关性、告警通知等功能。

告警订阅

系统基于用户自定义的订阅策略，自动检查设备订阅状态。用户可随时检测或发起基于 SNMP Trap 及 Redfish 协议的告警订阅。同时，用户可查阅系统接收的设备发送的消息，并能够基于消息内容，自定义 SNMP Trap Oid 的识别能力。其具体包括以下内容：

- 支持告警订阅策略设置，支持自定义协议设置及智能订阅，系统可自动寻找空闲通道进行订阅，不影响其他监控平台。
- 支持被纳管设备的告警订阅状态查询。
- 支持一键订阅、一键检测设备告警订阅状态。
- 支持对未订阅设备自动订阅设置。
- 支持订阅检测周期设置及订阅失败重试次数设置。
- 支持设备订阅状态导出。

- 支持系统各采集器网关告警订阅目标 IP 设置。
- 支持对各个设备的告警订阅日志、订阅状态检测日志查看。
- 支持 SNMP Trap Oid 自定义，Redfish 定义，精准解析识别告警。
- 支持 SNMPv3 USM 的增删改查及消息自动解析。
- 支持 SNMP Trap 及 Redfish 消息的查询。

告警规则管理

告警规则包括告警重定义规则、告警屏蔽规则、告警确认规则等。系统维护人员可根据不同场景灵活设置告警监控规则。用户可以选择对某些设备自定义设置阈值配置，支持各设备类型的告警条件定义，以满足不同的业务需求。

- 支持设置屏蔽规则屏蔽待产生、不关注的告警/事件。
- 支持告警级别重定义和告警名称重定义。
- 支持按级别设置自动确认规则，将处于清除状态的当前告警移入到历史告警列表中。
- 支持用户按照告警级别设定不同的告警提示音功能。
- 支持用户选择是否开启告警提示音功能。

告警降噪压缩

在告警管理中，由于各种因素（如临时性的网络波动、设备短暂不稳定等）可能导致出现大量、重复的告警信息，其中很多可能是并不真正代表问题的“噪音”。通过告警降噪压缩可以实现对“噪音告警”的压缩集中展示，降低干扰以及后续告警处理流程的压力。此外一些已知问题设备频繁产生/恢复的告警信息也会为服务器监控带来困扰和额外的人力成本，可以通过告警降噪压缩设定触发阈值避免该类型告警的产生。这具体包含以下内容：

- 支持降噪规则的灵活创建。支持按照阈值对告警进行产生/恢复计数，对未达到计数的告警进行过滤。
- 支持告警压缩规则的灵活创建。按照不同维度对告警进行压缩处理，并根据用户反馈以及运维经验，内置默认的压缩规则。

- 支持压缩告警/真实告警的集中展示，支持多样化的告警查询。
- 支持压缩告警的压缩范围及其生命周期的统一展示。
- 支持压缩告警按照独立频率进行告警通知。

告警相关性

EagleEyes 内置告警模型及算法，基于系统告警数据动态生成告警相关依赖关系图谱，支持用户在系统中快速查询当前告警的依赖关系及传播路径，帮助迅速洞察告警事件的内在逻辑与关联，为客户提供了告警溯源与告警预测能力。这具体包含以下内容：

- 支持告警相关性自定义能力。
- 支持系统基于实时、历史告警自动更新生成告警相关性图谱。
- 支持用户指定告警类型进行相关告警查询。
- 支持用户导出告警相关性数据。
- 支持用户查询根源告警及衍生告警。
- 支持告警详情中跳转查看根源告警及衍生告警。
- 支持用户在实时告警中查看该告警的相关溯源信息及可能引发的预警信息。

告警通知

EagleEyes 提供邮件、短信、企业微信、钉钉、Slack、飞书、PagerDuty 等多渠道的告警通知方式，以便用户可以根据自己的偏好和可用性来接收通知。同时支持自定义的邮件、短信通知内容模板，可将告警信息按照客户制定的通知策略通知到运维人员。这具体包含以下内容：

- 支持邮件、短信、钉钉、企业微信、Slack、飞书以及 PagerDuty 通知方式，提供自定义配置功能。
- 支持自定义邮件及短信通知内容模板。包括：告警名称、告警位置、告警描述、告警级别、告警类型、清除方式、资产名称、资产序列号、可能原因、修复建议、首次发生时间、最后发生时间、恢复时间、资源归属、业务归属、资产 IP、资产位置、资产机型、资产厂商、部件名称、部件序列号等。

- 支持通知策略的自定义。内容涵盖：通知时间，通知方式，告警类型，告警级别，通知用户，是否携带设备日志通知等。

- 支持对告警通知记录的筛选溯源查看，支持对通知内容、通知方式、通知结果的组合筛选，快速定位到关注的通知记录。

- 支持一键开启/关闭通知功能。

- 支持按照告警级别、告警名称设定通知策略，也可以按照具体告警/事件设定通知策略。

- 支持告警在一定时间内未确认、未解决的，自定义通知相关用户。

告警处理机制

表 4- 1 告警处理机制

功能类型	描述
主被动告警采集	主动轮询加上被动接收告警，提供设备全天候实时监控与故障分析，减少业务隐患。
事件消息解析	支持用户查看系统接收到的 SNMP Trap 及 Redfish 消息。同时，用户可基于定义 Trap Oid 属性来进行自定义消息解析，从而转为设备告警。
告警显示	通过告警台面板、实时历史告警列表，按照告警级别、设备、告警来源、机房、机柜等集中显示告警，实时掌握全网的运行状况。
告警统计	支持告警级别、告警源告警数量、告警类型、设备型号、机房告警数量、告警发生时间分布等多维度统计。
告警确认	用户可以对告警执行<启用/禁用>操作，支持告警延迟或立即确认，支持对确认后的告警信息进行延迟或立即清除。
告警搜索	用户可以根据告警状态、告警级别、告警类型、位置、机房、机柜、逻辑分类、告警来源、部件类型等条件对当前和历史告警进行组合过滤搜索，快速锁定到关注的告警进行处理。
告警重定义	支持告警名称及告警级别的重定义。内容涵盖所有告警类型的名称自定义及针对特定资源的级别自定义。支持各类告警与事件的灵活转换。
告警屏蔽	用户可以通过创建告警屏蔽规则，对某些不重要的或不关心的告警进行屏蔽，避免冗余信息。
告警音效	用户可按照告警级别设定是否开启告警提示音。
故障报修	系统提供告警报修的对接设置及告警的报修策略设置，报修记录跟踪等功能。

4.4.4 原理描述

告警管理提供了告警处理机制以精简告警，帮助系统维护人员从海量告警中解放出来，提升处理告警的效率。

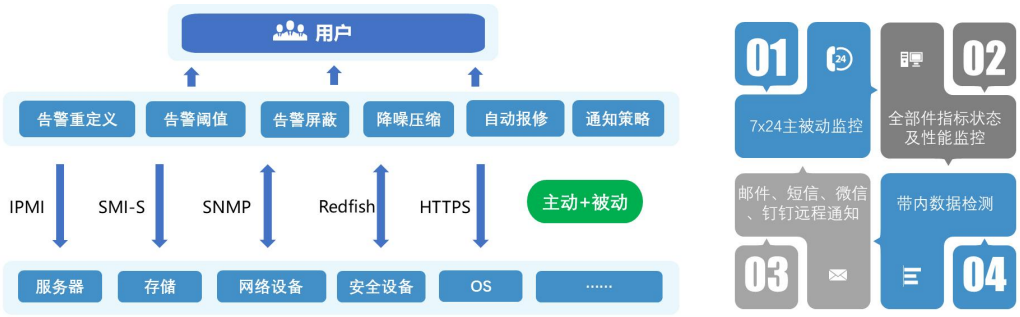
告警级别定义

表 4-2 告警定义级别

告警级别	描述
紧急	使业务中断并需要立即进行故障检修的告警
严重	影响业务并需要立即进行故障检修的告警
中度	不影响现有业务，但需进行检修以阻止恶化的告警
轻微	不影响现有业务，但发展下去有可能影响业务，可视需要采取措施的告警
事件	不影响现有业务的事件

告警全方位监控

图 4-6 告警全方位监控



4.4.5 关键指标

表 4-3 告警管理关键指标

指标项	指标值
实时告警存储容量（条）	10 万

指标项	指标值
历史告警存储容量（条）	30 万
事件告警存储容量（条）	30 万
Trap 报文存储容量（条）	10 万
Redfish 报文存储容量（条）	10 万
告警处理能力（条/秒）	100 **说明：**告警持续处理能力：100 条/秒，告警风暴处理能力：1000 条/秒，最长可支持 15 分钟。若超过该规格，可能导致告警延时上报或丢失。

4.5 日志网关管理

图 4-7 日志网关

4.5.1 定义

日志网关管理为用户提供了全新的解决方案。它能够自动化、智能化地处理日志数据，实现日志的高效收集、过滤、分析和存储，从而大幅提升日志处理的效率和准确性，充分释放基础设施的潜能，为用户创造更大的价值。

4.5.2 价值描述

日志网关管理的核心价值在于其能够有效整合、转发及存储海量日志数据，确保数据的安全性与完整性。它提供强大的过滤与转换功能，满足多样化的日志处理需求。同时，日志网关管理简化了日志管理流程，降低了运维成本，提高了数据查询与分析效率，为故障排查及业务优化提供了有力的数据支持，助力企业实现智能化运维与决策。

4.5.3 功能描述

EagleEyes 支持对纳管设备的日志管理功能，可对设备日志进行关键字检索、日志下载、智能分析，为客户日常运维，问题定位提供有效帮助。

日志检索

- **使用强大的搜索引擎：**选择支持全文搜索和复杂查询条件的搜索引擎，以确保能够快速地检索到所需的日志数据。
- **定义合理的检索字段：**在日志数据中定义清晰的字段，如时间戳、日志级别、来源 IP 等，以便用户可以根据这些字段进行检索。
- **支持多种检索方式：**提供关键词检索、正则表达式检索、时间段检索等多种检索方式，以满足用户不同的检索需求。

索引管理

- **合理划分索引：**根据日志数据的特性和查询需求，合理划分索引，如按时间、按业务类型等。这有助于优化查询性能，减少索引的冗余和浪费。
- **定期清理过期索引：**对于不再需要查询的过期日志数据，应定期清理其对应的索引，以释放存储空间并提升查询效率。
- **使用索引生命周期管理：**借助 Elasticsearch 等搜索引擎提供的索引生命周期管理功能，可以自动管理索引的创建、更新、删除等过程，降低运维成本。

采集模板

- **标准化模板格式：**制定统一的日志格式标准，如 JSON 事件格式等，以确保采集到的日志数据具有一致性和可比性。
- **支持自定义模板：**提供灵活的自定义模板功能，允许用户根据特定的日志源和业务需求定义个性化的采集模板。
- **定期更新模板：**随着业务的发展和日志源的变化，定期更新采集模板，以确保能够准确地采集到所需的日志数据。

采集器

- **选择合适的采集器：**根据日志源的类型和特性选择合适的采集器，这些采集器具有不同的特点和优势，可以满足不同的采集需求。

- **配置采集参数：**根据日志源的实际情况配置采集器的参数，如采集路径、采集频率、过滤条件等。这有助于确保采集到的日志数据具有准确性和完整性。

- **监控采集性能：**定期监控采集器的性能，如采集速度、资源占用情况等。及时发现并解决采集性能问题，以确保日志网关的稳定性和可靠性。

4.5.4 原理描述

当用户在系统上执行操作或系统自动触发任务时，会生成相应的日志条目；随后，采集器根据预设的采集模板，从指定源头实时读取这些日志数据，并将其安全地存储到日志管理数据库中；用户可以通过高效的检索工具快速查找和筛选日志，进行深入分析，以便及时发现安全风险、定位问题。

4.6 配置管理

图 4-8 配置管理

4.6.1 定义

EagleEyes 提供对业务的配置管理能力，配置管理是指对系统硬件、软件及其运行环境的识别、记录、状态监控、变更控制及审计的过程。

4.6.2 价值描述

配置管理的价值在于确保 IT 环境中的硬件、软件及文档得到准确记录、跟踪与变更控制，提升系统稳定性与安全性，优化资源利用，加速故障恢复，促进团队协作与合规性，最终降低运维成本并提升业务效率。

4.7 知识库管理

图 4-9 知识库管理

4.7.1 定义

知识库是一个存储和管理与企业 IT 基础设施相关的各类知识信息的系统，如用户手册、故障排查、常见问题等。通过结构化组织，便于检索、分享与应用，有效提升运维团队效率和问题解决能力。

4.7.2 价值描述

知识库的价值在于集中存储、组织并分享专业知识，提升信息检索效率，加速问题解决，促进团队协作与创新，同时确保知识的持续更新与传承，为组织带来更高的工作效率与决策质量，是推动业务发展与知识管理的关键工具。通过共享知识库中的最佳实践和常见问题解答，减少重复学习和试错成本。

4.7.3 功能描述

知识库检索

知识库检索是一种高效的信息查询方式，通过特定的检索系统或工具，在知识库中快速定位并获取所需的知识或信息。输入关键词或语句，系统运用先进算法，深度扫描各类知识源，帮助用户快速找到相关文档、解决方案或最佳实践。也可以通过系统提供的常见问题进行快速查询。

空间管理

知识库空间是一个专门用于存储、管理和检索知识的集合，以特定的结构和分类方式来组织知识，使得用户可以方便的查找和获取所需的信息。通过对知识库中的知识和信息进行合理规划、整合与优化，提高了知识存储的效率和知识检索的准确性，通过有效的分类、标签、索引等手段，使知识库中的资源得以充分利用。同时，知识库空间管理还关注知识的安全性和时效性，确保用户能够便捷、快速地获取所需知识，为组织的决策制定、问题解决和业务发展提供有力支持。

4.7.4 原理描述

知识库模块基于数据库和搜索引擎技术构建。首先，将各类知识信息以结构化的方式存储到数据库中，包括知识条目的内容、类型、分类标签、创建时间、修改时间等数据。然后，利用搜索引擎技术，对知识库进行索引和分词处理，实现快速的全文搜索和分类检索。

4.8 能效管理

介绍性能管理的功能特性，包括定义、价值、功能、原理和关键指标。

图 4-10 能效管理

4.8.1 定义

能效管理是指通过有效的策略和措施来提高能源利用效率，减少能源消耗和排放的一种管理方法。

4.8.2 价值描述

能效管理通过监测和分析能源使用情况，帮助企业发现能源浪费的环节，并采取相应的节能措施，从而显著降低能源成本，提高经济效益。

4.8.3 功能描述

功耗策略

EagleEyes 允许用户针对单台设备制定相应的功耗限制策略，以限制服务器的最大功耗。策略的内容包括：

- **是否启用：**建立策略后，可以随时单独关停或启用某条策略。
- **时间周期：**策略启用后，会在设定的时间周期内生效。
- **功耗上限：**策略的主要作用是通过降低 CPU 频率等手段限制设备的功耗，当策略启用并生效时，设备的功耗会被限制在设定的功耗上限附近。

碳排放管理

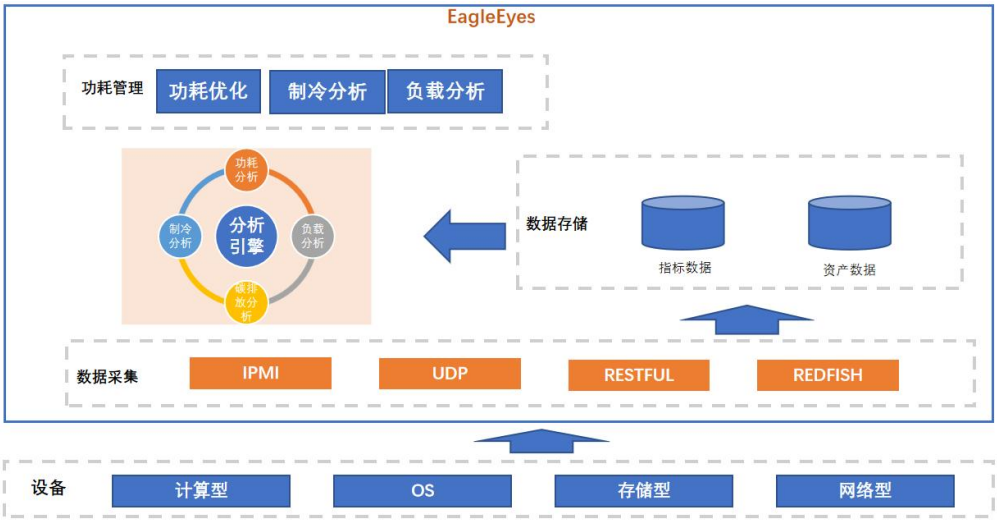
EagleEyes 提供碳排放管理，可以对数据中心进行碳资产和碳排放管理。用户录入碳资产后，碳排放管理可以对数据中心的碳排放量进行计算、分析、核减，产生碳排放趋势图。

- **碳资产：**用户根据自身实际情况，录入碳资产信息，录用后可得知数据中心的碳资产使用情况、分布类型等。
- **碳排放管理：**碳排放管理中需要维护数据中心相关信息，包括 PUE、配额、碳排放系数信息，EagleEyes 将根据维护信息，计算出碳排放趋势图，碳配额月使用率，碳资产预计使用天数。

4.8.4 原理描述

能耗管理

图 4-11 能耗管理原理图



4.8.5 关键指标

制冷分析

- ASHRAE 推荐温度 18℃-27℃。
- ASHRAE 一级许可温度 15℃-32℃。
- ASHRAE 二级许可温度 10℃-35℃。

4.9 报表管理

介绍报表管理的功能特性，包括定义、价值、功能、原理和关键指标。

图 4-12 报表管理

4.9.1 定义

报表管理提供端到端的数据分析框架和报表展现平台，支撑管理员从不同的维度查看、对比数据并生成所需的报表。

4.9.2 价值描述

报表管理通过整合、分析并可视化展示海量数据，帮助管理层全面了解系统运行状态，及时发现并解决潜在问题。同时，报表管理还支持多维度分析和数据挖掘，为优化资源配置、提升运维效率提供有力支持，是企业实现智能化、系统化管理的关键工具。

4.9.3 功能描述

资产报表

展示基础设施中各类资产的详细信息，包括机房信息、厂商信息、型号信息、部件信息等。

服务器报表

实时监控服务器的运行状态，包括 CPU、内存、网卡、磁盘、网口等。

告警报表

记录当前和历史告警信息，包括告警名称、级别、告警源、发生时间等，帮助运维团队快速响应和处理问题。

维保报表

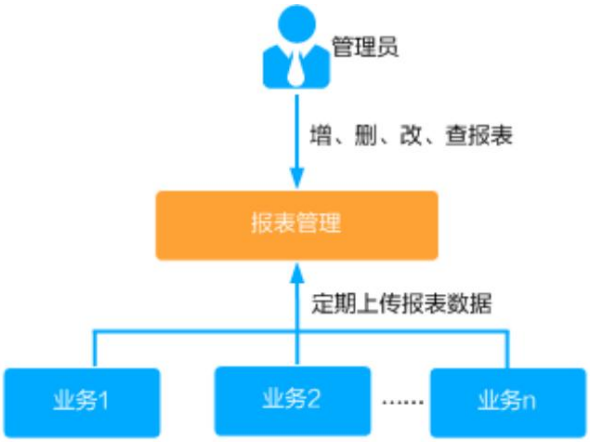
记录设备的维保状态、维保类型、采购时间、即将过保时间等，提醒运维团队及时进行设备维保，确保设备稳定运行。

4.9.4 原理描述

报表模块在基础设施管理平台上的原理是通过收集资产、服务器、告警、存储、性能及维保等各类数据，运用数据处理技术对这些原始数据进行整理、统计与分析。用户可根据实际需求，选择预设报表模板或自定义报表内容，并设置定时任务。系统则根据设定自动生成报表，以直观、准确的方式展示数据，帮助管理者及时洞察系统状态，优化资源配置，确保基础设施高效稳定运行。

各业务模块定期上报报表数据，经过报表管理模块处理后以图表方式进行展示，报表管理的实现原理如图 4-13 所示。

图 4-13 报表原理



4.10 流程管理

图 4-14 流程管理

4.10.1 定义

流程定义是指对资产管理的各个环节进行全面管理和控制的流程。这些流程旨在确保基础设施项目的质量和安全，提高投资效益，并实现项目的可持续发展。

4.10.2 价值描述

基础设施管理平台中的流程的价值在于提高管理效率、优化资源配置、确保项目质量和安全。通过流程化管理，可以实现基础设施项目的全生命周期监控，及时发现并解决潜在问题，降低运营风险，提升整体投资效益，为城市的可持续发展提供有力支持。

4.10.3 功能描述

我的服务单

我的服务单支持服务申请，服务列表，保存草稿。服务申请包括设备上下架，问题处理和变更服务；服务列表包括工单编号，申请原因，状态等信息。

- 支持批量上架、下架能力。
- 支持上架过程中进行机柜一键上架规划能力。

工作台

工作台是一个核心组件，它为用户提供了一个集中、直观的管理界面，使用户能够高效地监控、配置和管理基础设施。用户在工作台申请信息，处理信息，流程信息，查看到我的待办和我的已办。通过图表、仪表盘等形式，用户可以直观地了解相关的流程信息。

4.10.4 原理描述

远程管理在基础设施管理平台上的原理是利用 KVM 或 Terminal 技术，实现对不同资源设备的远程访问与控制。用户通过平台界面发起连接请求，平台根据请求类型和资源设备信息，建立安全的远程会话通道，使用户能够像操作本地设备一样对远程设备进行管理和维护，提高管理效率和响应速度。

4.11 远程管理

图 4-15 远程管理

4.11.1 定义

远程管理功能可以使用户能够实时访问、监控、配置和维护平台所管理的 IT 基础设施。

4.11.2 价值描述

远程管理不仅大幅提高了运维团队的工作效率，降低了因现场访问而产生的成本，还增强了组织在运维管理上的灵活性和响应速度，同时通过集成多重安全认证和加密技术，确保了远程操作的安全性和可靠性，为组织的数字化转型和业务发展提供了坚实的技术支撑。

4.11.3 功能描述

远程连接

实时监控基础设施的运行状态，包括服务器、网络设备、存储设备等，提供详细的性能数据和告警信息。

4.11.4 原理描述

管理员通过客户端发起连接请求，经过身份验证后，与服务器端的远程管理服务建立安全通道。连接建立后，管理员就可以通过命令行界面（CLI）对基础设施进行远程操作。这些操作指令通过网络传输到服务器端的设备或系统，执行相应的管理任务。

4.11.5 关键指标

EagleEyes 同时最多远程连接 5 台设备。

4.12 系统管理

图 4-16 系统管理

4.12.1 定义

系统管理通过一系列功能和技术手段，对平台的用户、日志、通知、巡检、作业、视频审计、服务、安全和升级进行全面而高效的管理。它确保平台的稳定运行，优化资源利用，并保障数据安全。

4.12.2 价值描述

系统管理通过自动化和集成化的管理功能，减少手动操作，提高管理效率；同时，它还为数据安全提供了坚实的保障，借助严格的安全控制和审计功能，确保系统数据的机密性、完整性和可用性不受侵害；此外，系统管理还能通过深入的数据分析和监控，实现资源的优化配置，有效降低运营成本。

4.12.3 功能描述

用户管理

实现用户账户的创建、修改、删除和权限分配，确保用户能够根据自己的角色和权限访问系统资源。

日志管理

记录和存储系统运行过程中用户的操作日志，提供日志查询和下载功能。

通知管理

通过邮件、短信、微信、钉钉、Slack、飞书、PagerDuty 方式，向用户发送系统通知、告警信息等。

作业中心

作业中心包括系统作业和用户作业，记录系统周期性执行的作业和用户自定义的作业。

系统巡检

定期对系统进行全面检查，包括服务巡检、模块巡检、资源巡检等，生成巡检报告，用户可以添加和管理巡检任务，并且可以预览和下载巡检报告。

KVM 视频审计

对 KVM 操作进行记录和审计，确保操作合规性和安全性，提供下载和在线播放视频功能。

安全控制

系统安全控制策略为数据中心安全管理带来了新方案。用户可轻松选择适合的周期（如日、周、月），满足不同安全需求。同时，策略提供多项禁止操作选项，用户可根据实际禁止特定操作或访问，有效预防安全风险。

此外，策略还具备申请与审批功能。用户可提交策略申请，详细说明需求及原因，经审批后生成执行依据。这既提升了策略灵活性，又避免了不当控制导致的资源浪费和效率降低。

- 安全策略设置，支持禁止操作项设置、操作时间段设置，应用资源范围支持全部和自定义设置。
- 策略申请单，支持普通用户向管理员申请资源的操作项及操作时间段权限，审批通过后生效。
- 策略审批单，支持超级管理员对普通用户申请单进行通过和驳回操作。

4.12.4 原理描述

系统管理的原理在于通过集成多种管理功能于基础设施管理平台，实现对 IT 环境的全面监控与维护。它涵盖用户权限分配、日志记录与分析、通知推送、作业调度、系统健康巡检、许可证管理、KVM 视频审计等关键环节，确保资源高效运行与安全可控。同时，通过系统集成功能，实现与其他系统的无缝对接与自动化服务。安全控制与在线升级机制保障系统稳定与数据安全，而灵活的设置选项则满足个性化需求，共同构成了一个综合性的系统管理框架。

4.13 IOPS

4.13.1 定义

IOPS 是指负责处理服务器设备每秒输入/输出操作（IOPS）的后台管理系统。它涵盖概览、服务器列表、数据库运维、数据收集和备份还原等功能模块，用于全面监控和设备的性能，确保数据的高效读写、安全存储与快速恢复。通过 IOPS，用户可以实时了解设备状态，优化性能，保障业务连续性。

4.13.2 价值描述

IOPS 页面作为一个综合管理工具，其价值在于全面而深入地关注存储设备的性能与运维。通过概览功能，用户可以迅速掌握存储系统的整体状况；服务器列表则提供了详细的存储设备信息，便于用户进行性能对比和故障排查。数据库运维功能确保了数据库的高效运行，而数据收集功能则帮助用户收集并分析存储设备的性能数据，为优化决策提供有力支持。此外，备份还原功能保障了数据的安全性和完整性。综上所述，IOPS 页面的价值在于通过全面的功能与数据支持，提升存储设备的性能与运维效率。

4.13.3 功能描述

在 IOPS 页面展示各组件状态以及组件运行情况。

展示服务器列表，在该页面用户可以查看服务器的名称，ip 地址，在线状态，cpu 使用率，内存使用率，磁盘使用率，CPU 内核，内存总容量，磁盘总容量等指标。

展示数据库运维，在该页面用户可以查看数据库类型，ip 地址，端口，数据库名称，SQL 语句、执行结果等指标。

数据收集界面，用户可以选择收集的数据，包括日志、SQL 记录、机型映射

IOPS 备份与还原，进入备份还原界面，可以进行自动备份，手动备份，执行回滚的操作，在备份还原过程会有基础设施管理平台系统服务的重启。

4.13.4 原理描述

在基础设施管理平台上，IOPS 通过记录服务器的详细信息和进程、数据库运维、数据收集（包括日志、SQL 记录、机型映射）以及支持备份还原操作，方便用户在 IOPS 页面查看和管理到后台的相关信息。其原理在于集中管理资源，优化资源分配，提升系统响应速度，确保数据完整性与业务连续性。

5 部署方案

5.1 部署方式

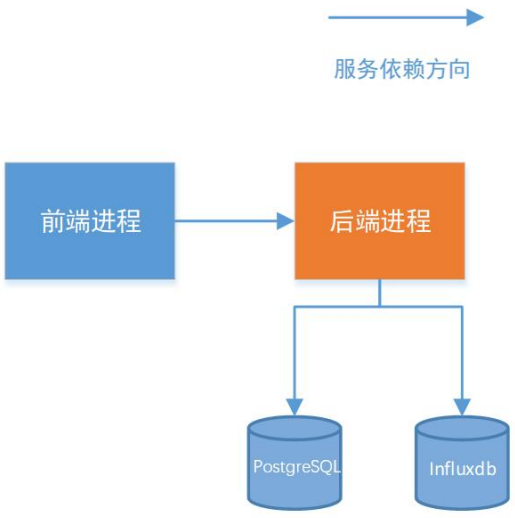
EagleEyes 基于面向模块的架构，可根据纳管的节点数量、业务场景、客户提供的服务器资源配置，提供多种部署方案。

5.1.1 单节点部署

单机部署指 EagleEyes 所有功能都部署在同一台服务器上。

单机部署方案适用于网络规模不大，可靠性要求不高的场景。

图 5-1 单节点部署示意图



5.2 升级方式

- EagleEyes 提供版本升级包，一键升级，安全可靠。升级成功会自动重启 EagleEyes 服务，时间大约 10 分钟。

6 安全性

6.1 组网约束

由于 EagleEyes 内部已经占用了 3306、8086、32314、32315、32316、32317、32318、32319、32320、32321、32322、32323、32324、32325、32326、32327、32229、161、162、623 端口，在规划端口时，和 EagleEyes 业务相关的设备的其他业务需要避开这些端口。

表 6-1 组网约束

源设备	源 IP	源端口	目的设备	目的 IP	目的端口（监听）	协议	端口说明	认证方式
本机	127.0.0.1	Socket 随机分配[1-65535]	本机	127.0.0.1	9200	TCP/UDP	ElasticSearch 数据存储服务	用户名、密码认证
ElasticSearch 节点	127.0.0.1	Socket 随机分配[1-65535]	本机	127.0.0.1	9300	TCP/UDP	ElasticSearch 节点之间通讯	用户名、密码认证
本机	127.0.0.1	Socket 随机分配[1-65535]	本机	127.0.0.1	6379	TCP/UDP	Redis 数据存储服务	用户名、密码认证
Redis 节点	127.0.0.1	Socket 随机分配[1-65535]	本机	127.0.0.1	26379	TCP/UDP	Redis 高可用数据同步服务	用户名、密码认证
RabbitMQ	127.0.0.1	Socket 随机分配[1-65536]	本机	127.0.0.1	5672	TCP/UDP	RabbitMQ 消息队列服务	用户名、密码认证
本机	127.0.0.1	Socket 随机分配[1-65535]	本机	127.0.0.1	3306	TCP/UDP	PostgreSQL 存储服务端口	用户名、密码认证
本机	127.0.0.1	Socket 随机分配[1-65535]	本机	127.0.0.1	8086	TCP/UDP	InfluxDB 性能数据存储服务端口	用户名、密码认证

源设备	源 IP	源端口	目的设备	目的 IP	目的端口（监听）	协议	端口说明	认证方式
本机	任意	Socket 随机分配[1-65535]	被管理节点	任意	161	UDP	采集器通过 SNMP 协议获取硬件数据	SNMPv1 和 SNMPv2c 使用团体字；SNMPv3 使用 usm-user/md5 和 sha 认证密码。
EagleEyes 管理节点	任意	Socket 随机分配[1-65535]	本机	任意	162	UDP	采集器接收 SNMP TRAP 告警信息	SNMPv1 和 SNMPv2c 使用团体字；SNMPv3 使用 usm-user/md5 和 sha 认证密码。
本机	任意	Socket 随机分配[1-65535]	被管理节点	任意	623	UDP	采集器通过 IPMI 协议获取硬件数据	用户名、密码认证
EagleEyes 管理节点	任意	Socket 随机分配[1-65535]	本机	本机任意地址，可以指定目的地址	514	UDP	采集器接收 SysLog 端口	
任意	任意	Socket 随机分配[1-65535]	本机	本机任意地址，可以指定目的地址	22	TCP	安全外壳协议（SSH）服务	用户名、密码认证

源设备	源 IP	源端口	目的设备	目的 IP	目的端口（监听）	协议	端口说明	认证方式
任意	任意	Socket 随机分配[1-65535]	本机	本机任意地址，可以指定目的地址	9141	TCP	北向 HTTPS 接口服务	用户名、密码认证
任意	任意	Socket 随机分配[1-65535]	本机	本机任意地址，可以指定目的地址	80	TCP	Node 页面访问 HTTP 服务（默认跳转到 443 端口）	用户名、密码认证
任意	任意	Socket 随机分配[1-65535]	本机	本机任意地址，可以指定目的地址	443	TCP	Node 页面访问 HTTPS 服务	用户名、密码认证
EagleEyes 管理节点	127.0.0.1	Socket 随机分配[1-65535]	本机	127.0.0.1	30100	TCP	web-facade	用户名、密码认证
EagleEyes 管理节点	127.0.0.1	Socket 随机分配[1-65535]	本机	127.0.0.1	32301	TCP		
EagleEyes 管理节点	127.0.0.1	Socket 随机分配[1-65535]	本机	127.0.0.1	32310	TCP	asset	

源设备	源 IP	源端口	目的设备	目的 IP	目的端口（监听）	协议	端口说明	认证方式
EagleEyes 管理节点	127.0.0.1	Socket 随机分配[1-65535]	本机	127.0.0.1	32311	TCP		
EagleEyes 管理节点	127.0.0.1	Socket 随机分配[1-65535]	本机	127.0.0.1	32326	TCP	monitor	
EagleEyes 管理节点	127.0.0.1	Socket 随机分配[1-65535]	本机	127.0.0.1	32327	TCP		
EagleEyes 管理节点	127.0.0.1	Socket 随机分配[1-65535]	本机	127.0.0.1	32330	TCP	system	
EagleEyes 管理节点	127.0.0.1	Socket 随机分配[1-65535]	本机	127.0.0.1	32331	TCP		
EagleEyes 管理节点	127.0.0.1	Socket 随机分配[1-65535]	本机	127.0.0.1	32340	TCP	job-schedule	
EagleEyes 管理节点	127.0.0.1	Socket 随机分配[1-65535]	本机	127.0.0.1	32341	TCP		
EagleEyes 管理节点	127.0.0.1	Socket 随机分配[1-65535]	本机	127.0.0.1	32350	TCP	control	
EagleEyes 管理节点	127.0.0.1	Socket 随机分配[1-65535]	本机	127.0.0.1	32351	TCP		
EagleEyes 管理	127.0.0.1	Socket 随机分配[1-65535]	本机	127.0.0.1	32360	TCP	collector-gateway	

源设备	源 IP	源端口	目的设备	目的 IP	目的端口（监听）	协议	端口说明	认证方式
节点								
EagleEyes 管理节点	127.0.0.1	Socket 随机分配[1-65535]	本机	127.0.0.1	32361	TCP		
EagleEyes 管理节点	127.0.0.1	Socket 随机分配[1-65536]	本机	127.0.0.1	32380	TCP	iops	
任意	127.0.0.1	Socket 随机分配[1-65535]	本机	本机任意地址，可以指定目的地址	32370	TCP	collector-worker	
任意	127.0.0.1	Socket 随机分配[1-65535]	本机	本机任意地址，可以指定目的地址	32371	TCP		
任意	127.0.0.1	Socket 随机分配[1-65535]	本机	本机任意地址，可以指定目的地址	32372	TCP		

源设备	源 IP	源端口	目的设备	目的 IP	目的端口（监听）	协议	端口说明	认证方式
任意	127.0.0.1	Socket 随机分配[1-65535]	本机	本机任意地址，可以指定目的地址	32373	TCP		
任意	127.0.0.1	Socket 随机分配[1-65535]	本机	本机任意地址，可以指定目的地址	32374	TCP		
任意	127.0.0.1	Socket 随机分配[1-65535]	本机	本机任意地址，可以指定目的地址	32320	TCP		
EagleEyes 管理节点	127.0.0.1	Socket 随机分配[1-65536]	本机	127.0.0.1	32333	TCP	logs	
本机	任意	Socket 随机分配[1-65535]	远端	任意	32390	TCP(https)	HingeClient	License+认证凭证
本机	127.0.0.1	Socket 随机分配[1-65535]	本机	127.0.0.1	32391	TCP		
本机	127.0.0.1	Socket 随机分配[1-65535]	本机	127.0.0.1	111	TCP/UDP	rpcbind	用户名、密码认证

源设备	源 IP	源端口	目的设备	目的 IP	目的端口（监听）	协议	端口说明	认证方式
任意	任意	Socket 随机分配[1-65535]	本机	本机任意地址，可以指定目的地址	9140	TCP	北向 HTTP 接口服务	用户名、密码认证
本机	127.0.0.1	Socket 随机分配[1-65535]	远端	任意	18081	TCP	centerhub	用户名、密码认证
本机	127.0.0.1	Socket 随机分配[1-65535]	本机	127.0.0.1	20048	TCP/UDP	rpc.mount	用户名、密码认证
本机	127.0.0.1	Socket 随机分配[1-65535]	本机	127.0.0.1	30100	TCP	momo	用户名、密码认证

6.2 系统安全

EagleEyes 选用安全稳定的数据库版本和其他中间件版本，以解决最基本的安全问题。操作系统安全对 EagleEyes 安全至关重要，部署 EagleEyes 的操作系统请遵循如下原则进行安全加固。

- 关闭不使用的端口和服务，依据最小授权原则，默认关闭非必要的访问通道，关闭不使用的服务，关闭不需要开启的 TCP/UDP 端口，如禁止 Telnet 登录。
- 文件权限最小化，系统关键文件和目录进行安全配置加固。
- 访问控制，如禁止 root 远程访问，添加 IP 地址黑白名单等
- 认证和授权，如设置账号口令安全策略、登录和审计等。
- 访问协议安全，使用安全的访问通道、使用安全配置的 SSH 服务。
- 系统设置安全，如屏蔽登录 banner 信息、设置系统 core dump 禁止产生 core 文件等。
- 漏洞管理，进行定期的系统漏洞修复，针对高危应急响应漏洞进行及时修复。

6.3 应用安全

为了保护 EagleEyes 的应用安全，引入安全策略，主要体现在认证鉴权、数据保护、协议安全、会话管理和日志审计安全这五个方面。

6.3.1 认证鉴权

用户通过 Web 对 EagleEyes 的访问,本地认证采用“用户+密码”的方式进行认证，使用强密码规则和密码修改策略，提供登录失败锁定机制，防止密码攻击和暴力破解。

- 强密码规则，包括：
  - 密码长度不能短于 8 位。
  - 必须同时包含大写字母、小写字母、数字和特殊字符中至少三种。

- 密码修改策略，包括：
  - 提示管理员用户修改初始密码。
  - 修改自己密码需验证旧密码
  - 界面密码不能明文显示。
  - 密码不能和用户名一致。
  - 密码进行密文保存。
- 登录失败锁定机制，某一用户连续 5 次密码错误，该用户将被锁定 20 分钟。超级管理员可对锁定用户进行解锁。

6.3.2 数据保护

EagleEyes 系统中敏感数据包括：系统关键参数数据、账户信息、用户隐私数据等，都进行了加密保护、并使用 SHA-256/HMAC-SHA-256/AES/PBKDF2 等复杂加密算法。除了对保存在 EagleEyes 中的敏感数据进行加密保护还对在系统运行过程中产生的，堆、栈、数据段中的未加密的敏感数据，使用类似 memset 函数覆盖或清空。

6.3.3 协议安全

- 用户登录 EagleEyes 时使用 Https(Http over SSL)协议。
- 支持使用 SNMPv3、Https、IPMI2.0 等安全协议访问设备
- 用户上传下载支持使用安全加密的 SFTP 协议。

6.3.4 会话管理

- 使用 token 维持会话。
- 防会话固定机制。
- 会话超时机制，会话静置 10 分钟，会话超时退出，并清除会话信息。

- 提供用户“注销\退出”菜单。
- 用户退出清除会话信息。

6.3.5 日志审计

- 提供操作日志审计能力，对 EagleEyes 的安全实践及操作记录日志。
- 日志信息包括用户名、用户 IP 地址、操作时间、操作内容等信息。

6.4 发布安全

代码安全扫描：编码安全是系统安全的基础，EagleEyes 发布版本通过代码扫描工具 fortify、Coverity 扫描，无、高、中级别漏洞。

安全工具扫描：EagleEyes 发布版本通过漏洞扫描工具 NESSUS、AppSca、绿盟扫描，无高、中级别漏洞。

版本安全：EagleEyes 发布版本，提供哈希值和数字签名，版本升级或补丁安装前，可以校验产品哈希值或数字签名，检验软件的合法性，避免软件被非法篡改或替换。

7 可靠性

7.1 集群可靠性

EagleEyes 提供 3 节点的集群部署能力，集群节点正常运行时，各节点为多活状态。若其中 1 个节点发生故障，其他节点将分担这个故障节点的负载能力，继续均衡地提供服务。

7.1.1 业务微服务可靠性

EagleEyes 各个业务微服务均部署两个或更多实例，分布 3 个节点；各个节点之间相互独立处理业务，单个节点或业务服务实例故障后可以自动切换到其他节点。

7.1.2 数据库可靠性

PostgreSQL 数据库采用主从复制模式部署于集群的第 1、2、3 节点，实时进行数据的冗余备份；当主节点或主数据库实例故障后，可以自动切换到备节点数据库实例，原主节点实例降为备节点。

7.2 数据可靠性

备份与恢复功能是保证系统在出现异常情况时，能够快速恢复正常运行的重要保证。

EagleEyes 支持数据库的备份与恢复，可根据系统情况设置备份策略为自动备份或手动备份。可以设置定期备份的周期和备份的路径。

EagleEyes 在应用层规划了高可用性保护方案，可用于防范由于硬件或软件故障导致的未知风险，保障 EagleEyes 的安全、稳定运行。

8 配置要求

EagleEyes 可以安装到虚拟机或者物理机上，关于服务器的配置要求如表 8-1 所示。

表 8-1 EagleEyes 服务器配置说明

项目	说明
操作系统	CentOS7.9
CPU	100 节点以下≥2 核 200 节点以下≥4 核 500 节点以下≥8 核 2000 节点以下≥16 核
内存	100 节点以下≥4GB 200 节点以下≥8GB 500 节点以下≥16GB 2000 节点以下≥64GB
硬盘	≥500GB 【说明】当管理规模大于 1000 节点时，建议每 1000 节点增加 100GB
网卡	≥1 个
IP	静态 IP 一个

说明

- 部署 EagleEyes 前，请先部署好 Kylin V10 SP3 操作系统。
- 部署完操作系统后，用 tar 包进行 EagleEyes 的安装。

A. 如何获取帮助

A.1 收集必要的故障信息

在进行故障处理前，需要收集必要的故障信息。

收集的信息包括：

- 客户详细名称、地址。
- 联系人姓名、电话号码。
- 故障发生的具体时间。
- 故障现象的详细描述。
- 设备类型及软件版本。
- 故障后已采取的措施和结果。
- 问题的级别及希望解决的时间。

A.2 如何使用文档

长城提供全面的随设备发货的指导文档。指导文档能解决您在日常维护或故障处理过程中遇到的常见问题。为了更好的解决故障，在寻求长城技术支持前，建议充分使用指导文档。

A.3 获取技术支持

中国长城科技集团股份有限公司（简称：中国长城）提供全国联保，由分布在全国各地长城专业售后服务网点提供“一站式”服务响应与支持。

如果您在使用我们的产品的过程中遇到任何疑问或者无法解决的问题，请您采取以下方式进行咨询。

客服服务中心和技术支持联系方式：热线服务电话（400-811-8888）。

网址：https:// www.greatwall.com.cn

提示：

文中所涉及到的相关信息，如因产品升级或其他原因而导致的变更，恕不另行通知。本文中所涉及的图片仅供参考。

B. 术语和缩略语

术语	说明性定义
EagleEyes	鹰眼，长城擎天系列服务器基础设施管理平台
BMC	Baseboard Management Controller，基板管理控制器
BIOS	Basic Input Output System，基本输入输出系统
RAID	Redundant Arrays of Independent Drives，磁盘阵列
DHCP	Dynamic Host Configuration Protocol，动态主机设置协议
DNS	Domain Name System，域名系统
IPMI	Intelligent Platform Management Interface，智能平台管理接口
SNMP	Simple Network Management Protocol，简单网络管理协议

中国长城科技集团股份有限公司

CEC中国电子

CGT中国长城