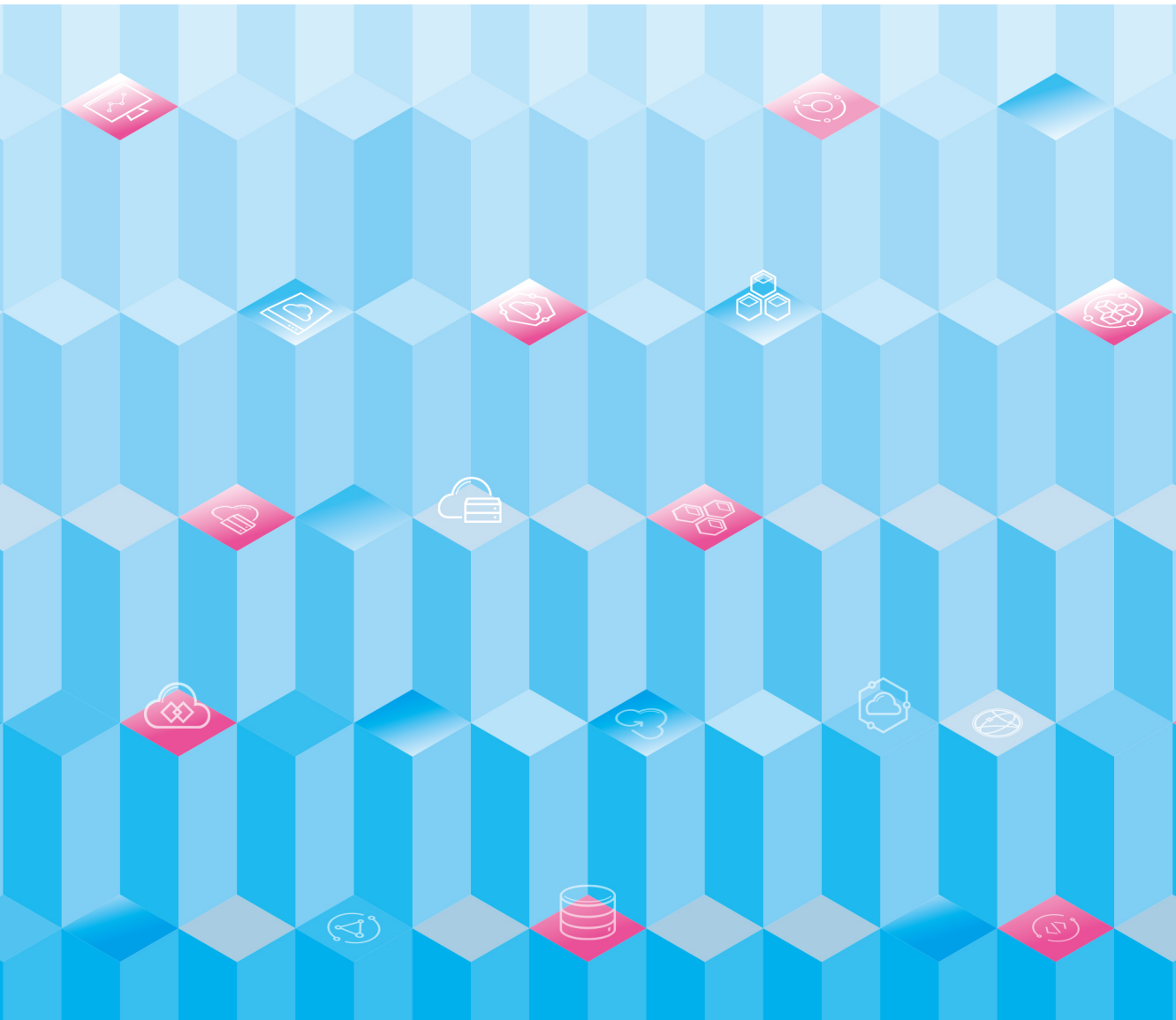
京东智联云

京东智联云

专有云安全白皮书

2019



版权声明

商标声明

京东智联云及其它京东智联云服务相关的商标均为北京京东叁佰陆拾度电子商务有限公司及其关联公司所有。

本文档提及的其他所有商标或注册商标，由各自的所有人拥有。

法律声明

本文档仅供用户使用京东智联云产品及服务的参考性指引，本文档中的所有陈述、信息和建议以及内容的准确性、适用性等不构成任何明示或暗示的担保。任何主体和个人因使用和信赖本文档而发生任何差错或经济损失的，京东智联云不承担任何法律责任。

由于产品版本升级、调整或其他原因，本文档内容有可能变更。京东智联云保留在没有任何通知或者提示下对本文档的内容进行修改的权利。

本文档未授予用户任何京东智联云产品的任何知识产权的法律权利。

引言 Introduction

以云计算、大数据、人工智能、区块链、物联网等为标志的新兴科技正在推动着数字化变革。随着数字化转型的不断深化，政府和企业的 IT 架构日益复杂，单一形式的云计算服务难以满足客户多样化的需求，混合云架构成为新的趋势。这意味着搭建可以与私有云良好协同互动的专有云平台将变得至关重要。

为了更好地理解客户对专有云的需求，京东智联云与全球权威咨询机构 Forrester 展开合作，对 157 家正在数字化转型的大中型企业（包括政府、金融、能源、制造、物流等行业）展开专项调研，并联合发布了《京东智联云专有云思想指导力白皮书》。调研结果显示，近 7 成企业或政府机构未来对云计算的投入将全部集中在专有云平台建设方面，可见建设专有云平台对企业的数字化转型起到了举足轻重的作用。

新一代专有云平台除了具有公有云亲和性和更高的企业级水准，对于关键任务系统和数据主权也更为安全可控， 架构设计与部署模式灵活多样，可以同时满足行业标准和专业化要求，是政府和企业原有资产虚拟化向云化转型的新起点，是支撑其数字化转型的有效手段。

基于京东智联云公有云自研云计算架构，经过海量用户实践和验证，京东智联云推出新一代专有云平台 JDStack，将京东智联云成熟、稳定的产品能力延伸至客户自有数据中心，通过建立一个安全、稳定、可信赖的专有云平台，助力客户的数字化转型。

作为面向政府和企业客户的大规模商业化全栈云平台，JDStack 具有“超大规模”、“灵活部署”、“安全可靠”三大核心优势。2018 可信云大会，JDStack 助力宿迁市电子政务办公室获得“可信云十大用户奖”， 并同时通过“政务云综合水平评估”、“可信政务云评估”。宿迁政务云更作为优秀案例入选云计算开源产业联盟《中国政务云发展白皮书，2018》及 IDC《政务云建设模式及典型案例研究，2018》报告。此外，在 2018 安全可控技术应用推进大会上，基于安全、可信、高可用的特性，京东智联云“JDStack 专有云”产品荣获“2017-2018 年度安全可控优秀解决方案”奖项。2019 中国国际大数据产业博览会，京东智联云“JDStack 专有云平台”凭借领先的云计算技术创新、丰富的实践和场景应用获得“2019 领先科技成果奖—新产品”奖项。

在数字化浪潮席卷而来的当下，京东智联云致力于为政府、企业和合作伙伴提供一体化、专业化、现代化和生态化的专有云平台，在保障安全、可靠、敏捷、高效的同时，提升用户体验，推动客户数字化转型并与其共建数字化生态。

目录 Contents

1 概要

在安全可靠、稳定可用作为云计算服务的必要条件的背景下，相对于大多基于不够成熟稳定的开源框架或同质化的解决方案搭建而成传统的专有云，新一代专有云平台具有公有云亲和性和更高的企业级水准，对于关键任务系统和数据主权更为安全可控，架构设计与部署模式灵活多样，同时满足行业标准和专业化要求。

依托于京东集团海量业务和用户的实践及验证，京东智联云在技术研发方面不断沉淀与积累经验。京东智联云专有云以最佳实践为基础，从底层架构设计到应用策略安全架构设计，实现从基础设施、物理环境、网络架构、访问控制、配置管理、运营管理、产品服务等各个环节的安全控制要求，提供多维度的安全防护。

本白皮书从安全合规、隐私保护、权责归属、专有云安全架构、专有云产品安全和专有云安全产品服务几个方面介绍了京东智联云专有云安全体系。

京东智联云专有云为用户提供安全、稳定、高可用的云计算服务，旨在利用技术创新助力政府与企业客户加速数字化转型的进程，并致力于保护用户的数据及业务安全。

2 京东智联云专有云介绍

2.1 专有云简介

京东智联云专有云（即“JDStack 专有云”）平台是京东智联云公有云核心产品与服务的私有化部署版本，在保证产品能力和使用体验与公有云一致的前提下，其根据私有化场景特点对整个平台的硬件、网络和服务分布等架构设计进一步优化，能确保在常见故障和运维场景下，提供连续的可用服务。产品采用“1+N”模式（“1”为最小化云平台底座，“N”为其它可选装产品集合）实现灵活部署，不断将公有云的成熟产品和服务持续更新集成到新的专有云版本。JDStack 天然亲和公有云的特性，可以让用户将业务扩展到京东公有云和其它 JDStack 专有云。

不同于当前国内外其他同类项目，JDStack 专有云平台利用技术创新解决了传统企业 Openstack 集群运维成本高、弹性能力弱、灵活度低、安全可控性差等诸多痛点。

首先，JDStack 专有云平台可实现超大规模部署。传统企业的信息化平台通常运行多个 OpenStack 集群，不仅难以应对大型私有云平台场景，而且运维成本过高。京东智联云专有云通过技术创新，不仅实现了可支持超大规模集群、超多用户量以及超大规模请求量，且同时提供统一的运维管理平台和监控平台，降低了日常运维成本。

其次，JDStack 专有云平台可提供丰富的产品类型，供用户根据业务场景自由选择。可以帮助不同规模、不同使用场景的用户轻松搭建专有云平台，并根据典型客户的需求场景，提供了不同产品。如，针对政府客户及大型企业客户提供包含所有云产品的全栈专有云平台；面向有数据计算与分析场景的客户，提供包含离线计算、实时计算、数字大屏等产品的大数据专有云平台；面向中小型企业的轻量级开发场景， 提供容器平台、DevOps 等产品及面向安全防护、流量接入、网络互联等诸多应用场景。

JDStack 专有云平台架构如下图所示：

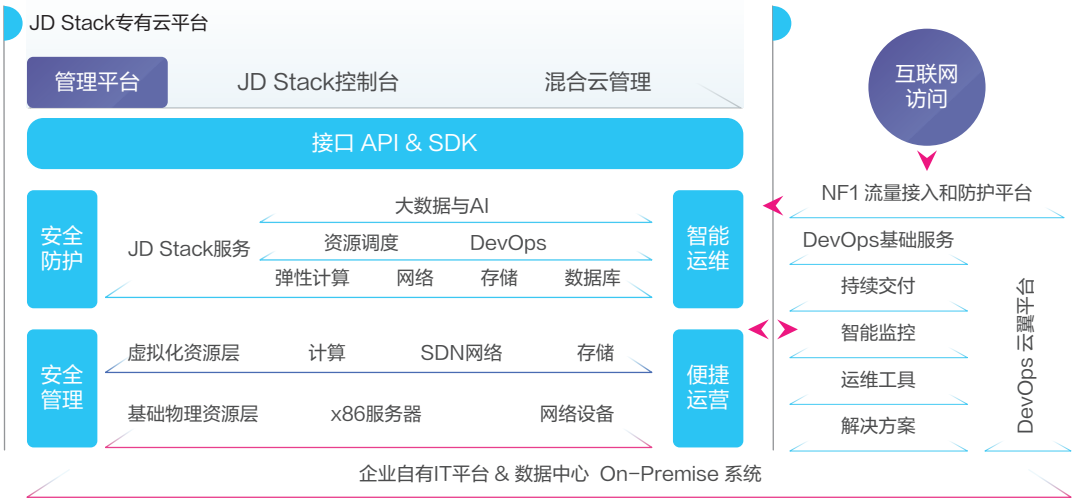


图 1 JDStack 专有云平台架构

2.2 专有云安全需求

传统的自建私有云平台难以满足现阶段政府和企业在稳定可靠、安全合规、广泛资源协同等方面的更高要求。专有云从物理环境上保障了应用和数据的安全可控，但在安全层面仍会面临诸多来自内外部的挑战。

· 企业部署云平台面临的安全挑战

安全合规：在部署专有云平台的过程中需要系统性地解决安全合规的问题，达到与公有云同样的安全合规能力。

安全策略：由虚拟化产生的流量模型的变化和因业务变化带来的虚机迁移，使得企业的安全策略需要动态 适应系统和应用带来的变化。

访问控制：除了现有的企业级云安全方案在应对传统终端漏洞带来的威胁以外，虚拟化环境所产生的跨域访问、多个虚机之间的资源调用和防护等问题仍为薄弱环节。

数据安全：如果不同保密层级的核心数据资源存储在同一介质内，可能存在不同安全级别跨级访问的风险。

稳定性和可靠性：企业在建设专有云过程中面临的挑战还来自于“是否具有和公有云相当的稳定性和可靠性”。

· 端到端安全合规一体化需求

端到端的安全合规需要涵盖平台安全、应用安全、数据安全以及业务安全等层面。在平台层面，需要从安全防护、可用性以及可靠性等维度，对软件平台、主机平台以及网络互联等进行全面保护；在应用层面，应注重事前、事中和事后的全周期安全防护； 在数据层面，需要加强数据治理和加密措施，防范各种漏洞风险；在业务层面，需要借助技术能力以外的经验，建立完善的管控流程并通过技术手段进行固化。

· 京东智联云专有云安全

京东智联云专有云的架构和产品源于公有云，京东公有云通过对历次 618、11.11 大促的成功支持，具备坚如磐石的稳定性。作为同源产品 JDStack 在产品稳定性、平台易用性、安全性等方面，具备与京东智联云公有云同级别的成熟度。在网络安全方面，面对大流量攻击，DDoS 防护迅速扩展安全防护能力，轻松解决用户本地防护能力不足的问题，结合可扩展的 Web 应用防火墙模块，多维度保护业务安全；在数据安全方面，通过京东智联云自研的对象存储产品，支持超大规模存储量，同时存储数据三副本备份，能够提供数据可靠性和服务可用性。用户可以在任何应用、任何时间、任何地点存储和访问任意类型的数据。

3 安全合规/隐私保护/权责归属

3.1 安全合规

京东智联云在努力完善业界标准认证体系的同时，致力于建立高效的安全内控体系，务求更好的向用户展示京东智联云的合规实践。

京东智联云权威安全资质认证：

· ISO27001 信息安全管理体系国际认证

· 公安部 “信息系统安全三级等级保护认证”

· 中国信息通信研究院 “可信云服务认证”

· 工业和信息化部 “ITSS 云计算服务能力标准符合性证书”

· 支付卡行业数据安全标准认证 (PCI DSS)

· CSA STAR 云安全认证

· C STAR 云计算安全评估认证

ISO27001
信息安全管理体系
国际认证

公安部
信息系统安全三级
等保认证

中国信息通信研究院
可信云服务认证

工业和信息化部
云计算服务能力标准
符合性证书

支付卡行业数据安全
标准认证
（ PCI DSS ）

CSA STAR
云安全认证

C STAR
云计算安全评估认证

图 2 京东智联云安全资质认证

3.2 隐私保护

京东智联云将依照《用户服务协议》、《隐私政策》予以尊重和保护用户信息。京东智联云采用符合业界标准的安全防护措施，包括建立合理的制度规范、安全技术来防止用户的个人信息遭到未经授权的访问、使用、修改，避免数据的损坏或丢失。保护用户对于个人信息访问、更正、删除以及撤回同意的权利，以使用户拥有充分的能力保障用户的隐私和安全。

专有云环境中，用户对项目规划建设的用户数据、运维过程中产生的运行数据、转移到云环境中的业务数据等均拥有所有权。京东智联云对确保用户数据隐私的特定策略、操作实践和技术保持透明。未经用户授权许可，京东智联云不会触碰用户数据，并确保用户对其信息具有唯一的所有权和控制权。

3.3 权责归属

参考国家标准《GBT 31168-2014 信息安全技术 云计算服务安全能力要求》中“云计算环境的安全性由云服务商和客户共同保障。云计算的设施层（物理环境）、硬件层（物理设备）、资源抽象和控制层都处于云服务商的完全控制下，所有安全责任有云服务商承担。应用软件层、软件平台层、虚拟化计算资源层的安全责任由双方共同承担”。同时，参考国家标准《GBT 31167-2014 信息安全技术 – 云计算服务安全指南》中“信息安全管理责任不应随服务外包而转移，无论客户数据和业务是位于内部信息系统还是云服务商的云计算平台上，客户都是信息安全的最终责任人。”

专有云场景下，云平台的软件开发商、运维服务方、服务使用者实现安全责任共担与能力共建。

- A：云平台的软件开发商：负责云平台的软件设计与实现
- B：云平台的运维服务方：负责云平台自身的稳定和安全的运行
- C：云平台的服务使用者：负责云平台上的应用和数据安全

通常作为云服务商的京东智联云会担任 A+B 角色，负责基础设施、物理设备资源、云操作系统及云服务产品的安全控制和管理，并基于安全合规、高可用最佳实践、安全的云产品及安全服务，构建基础设施、平台及应用和身份管理与资源访问控制的多维立体安全防护体系，并保障其运维运营安全。同时，用户担任 C 角色，基于京东智联云提供的服务构建云端应用系统，并运用京东智联云安全的云产品和安全服务以及安全生态服务保护自己的业务系统。

4

京东智联云专有云安全架构

4.1 专有云安全架构概述

京东智联云专有云提供了成熟的网络安全架构及多层防护安全方案，对业务网络和管理网络、虚拟网络和物理网络进行了安全隔离和严格的访问控制。在云平台侧，专有云从底层云平台基础架构安全性入手，结合大数据处理的能力，实现云平台、网络、系统、数据和应用系统安全的全面覆盖。在云用户（租户）侧，为了确保用户在使用云服务的过程中数据和业务系统受到实时的保护，京东智联云在各个层面提供了为租户安全保驾护航的云安全产品与服务，以帮助用户快速高效地部署云端安全防护。

专有云安全架构如下图所示：

图 3 专有云安全架构

专有云的安全产品为云平台及用户提供从网络--系统--应用--数据--管理综合防护及安全运维运营管理能力。

专有安全产品部署示意图如下所示：

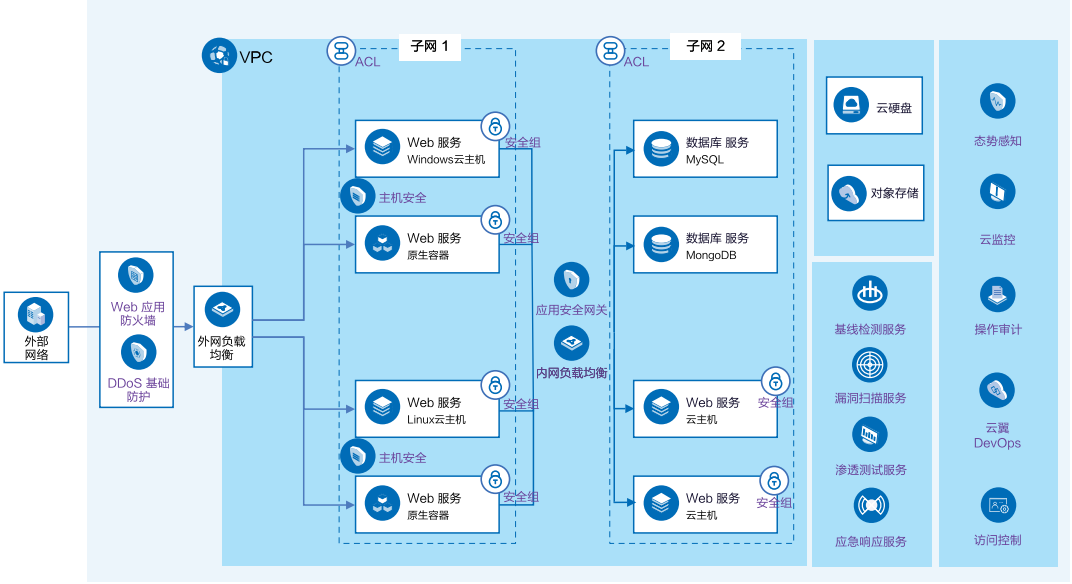


图 4 专有云安全产品部署示意图

4.2 云平台安全

4.2.1 物理安全

京东智联云执行严格的 IDC 标准、服务器准入标准以及运维标准，以保证云计算整个基础框架的高可用性、数据的可靠性以及云主机的高可用性，提供不低于 99.9% 的服务可用性。保证基础架构及环境高可用特性，比如供电系统、空调系统、火灾检测防护系统、动力系统等具备的灾备和冗余能力。京东智联云专有云的数据中心机房配置了多级的安全保护措施，运维运营团队严格执行访问控制、安保措施、监控审计、应急响应等措施，以确保专有云数据中心机房的物理和环境安全。

· 电力保障

数据中心机房的电源系统为充分冗余且可维护，保障业务 7*24 小时持续运行，使用电力供应采用来自多变电站的双路市电供电， 当市电供电中断后柴油发电机及 UPS 能正常接管电力， 并且在机房供电线路上配置了稳压器和过压防护设备。

· 温湿度控制

通过精密空调、集中加湿器自动调节， 数据中心机房温湿度保持在设备运行所允许的范围内，使服务器及设备元器件处于良好的运行状态。

· 防静电

数据中心机房内部安装防静电地板，机柜、线槽等均安装接地线，用以防御静电给电器设备带来的损害。

· 消防能力

数据中心机房安装了自动火灾探测及扑救设备，实现自动报警并及时灭火。

· 监控管理

数据中心机房安装配备 CCTV 系统、门禁系统、环境与设备集中监控系统，监测冷通道内温湿度、配电柜开关状态、机柜电流、UPS 运行状态、冷冻水空调系统运行状态、漏水和漏油监控报警系统，并执行严格日常维护保障系统机房巡检要求，安全隐患能被及时发现并修复。

· 访问控制

专有云数据中心机房具备访问控制，制定了机房管理制度策略和访问控制策略。例如，根据数据中心人员类别和访问权限，建立完整的人员访问控制安全矩阵。对于携带设备进出机房，对物理设备的操作等，均需具备相应的访问控制策略。

4.2.2 网络安全

专有云提供成熟的网络安全架构及多层防护的安全方案，对生产网络与非生产网络、业务网络和管理网络、虚拟网络和物理网络进行了安全隔离和严格的访问控制。

· 网络高可用

采用冗余技术手段保证主要物理网络设备、虚拟网络设备的业务处理能力满足业务高峰期的需求。关键网络设备均采用冗余部署。

通过边界处的安全设备（防火墙 / 入侵检测 /DDoS 防护），配合云平台自身的流量调度的能力，为用户或租户提供实时安全流量清洗防护。

按照业务需求合理配置通信网络中核心、汇聚等各层交换设备的处理能力。

· 网络安全隔离

业务网络、物理网络、管理网络间通过网络访问控制策略实现三网逻辑隔离。

通过访问控制技术，限制外部通信网络直接访问内部通信网络，并限制由虚拟机非法访问内部通信网络。

内部通信网络采用 VLAN 协议对用户数据包做隧道封装， 保证内部通信网络实现二层隔离，虚拟机接收不到目的地址不是自己的非广播报文。

虚拟机接入虚拟网络时，可通过安全组或主机防火墙产品设置访问控制策略，隔离由虚拟机向外发起的异常协议访问，保证其发出的数据包源地址为其真实地址。

4.2.3 系统安全

4.2.3.1 服务器系统安全

专有云物理服务器信息安全措施主要包括：访问控制、入侵检测、恶意病毒防范、漏洞扫描、安全加固等方面进行安全设计和控制，为用户信息系统运行提供一个安全的环境。

· 系统加固

专有云物理服务器系统进行安全加固，实现文件强制访问控制、注册表强制访问控制、进程强制访问控制、服务强制访问控制、三权分立的管理、管理员登录的强身份认证、文件完整性监测等功能。

对服务器系统管理员的账号和密码进行管理，同时对物理服务器端口进行安全策略设置。

及时打上补丁避免漏洞被蓄意攻击利用。

对于一段时间内完全不会用到的服务器，完全关闭；对于期间要使用的服务器，关闭不需要的服务。

· 安全防护

配置防火墙，通过适当的安全策略配置以达到最好的防护效果。

部署主机入侵检测（HIDS）模块，进行异常进程检测、异常端口检测、异常行为检测。

· 日志和备份

为防止不能预料的系统故障或用户不小心的非法操作，对系统进行安全备份。

通过运行系统日志程序，系统记录下所有用户使用系统的情形，包括最近登录时间、使用的账号、进行的活动等。

4.2.3.2 虚拟化系统安全

专有云虚拟化资源层通过 CPU 隔离、内存隔离、I/O 隔离、网络隔离等技术手段实现虚拟主机操作系统与访客虚拟机操作系统之间的隔离，并通过 Hypervisor 让虚拟主机操作系统与访客虚拟机操作系统使用不同的权限运行，来保证云平台系统资源的安全。基于硬件虚拟化技术的虚拟机管理，将多个计算节点的虚拟机在系统层面进行隔离，租户不能访问相互之间未授权的系统资源。

· CPU 隔离

基于硬件虚拟化的 CPU 隔离主要是指虚拟化平台与虚拟机之间的隔离，虚拟机内部的权限分配和虚拟机与虚拟机之间的隔离。在专有云平台使用的虚拟化环境中，将用户实例作为独立的虚拟机运行，并且通过使用物理处理器权限级别强制执行隔离，确保用户虚拟机无法通过未授权的方式访问物理主机和其他用户虚拟机的系统资源。

· 内存隔离

虚拟化平台负责为虚拟机提供内存资源，保证每个虚拟机只能访问到其自身的内存。虚拟化平台管理虚拟机内存

与真实物理内存之间的映射关系，保证虚拟机内存与物理内存之间形成一一映射关系。

· I/O 隔离

虚拟化平台为每个虚拟机提供独立的虚拟 I/O 设备，避免多个虚拟机共享设备造成的信息泄露。每个虚拟磁盘对应虚拟化平台上的一个镜像文件或逻辑卷，保证虚拟机只能访问分配给它的物理磁盘空间，从而实现不同虚拟机硬盘空间的安全隔离。

· 网络隔离

私有网络为用户划分一片隔离安全的私有空间，私有网络间独立隔离，将云主机部署在不同私有网络下即可实现虚拟网络隔离。

4.2.4 应用安全

4.2.4.1 云产品 SDL

专有云所有提供服务的云产品，在开发过程中严格遵循产品的安全开发生命周期 (Security Development Lifecycle，简称 SDL) 安全开发流程。京东智联云的安全开发基于业界安全开发的最佳实践， 并针对其中的环节做了优化。在产品开发各个阶段中消除信息安全和隐私问题， 确保所有的云产品在其生命周期内均能获得足够的安全管控与评估。

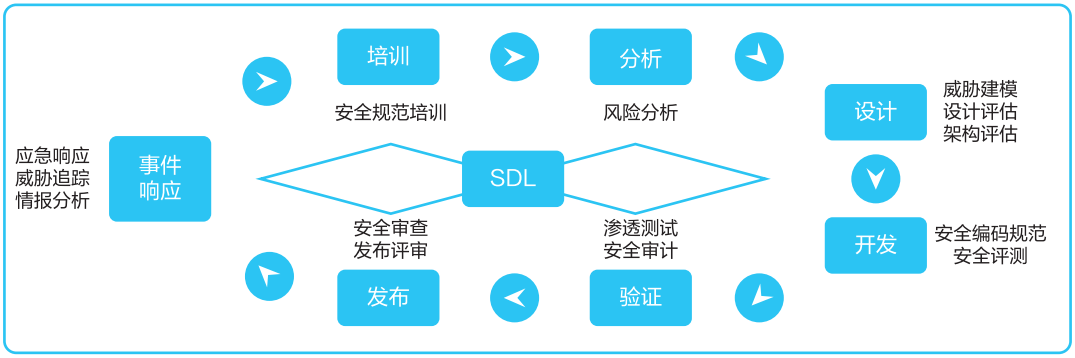


图 5 云产品 SDL 安全开发流程

如上图所示，整个云产品安全生命周期分为七个阶段：培训阶段、分析阶段、设计阶段、开发阶段、验证阶段、发布阶段、事件响应阶段。

· **培训阶段：**开发团队的所有成员都接受相应的安全培训，了解相关的安全知识，培训对象包括开发人员、测试人员、项目经理、产品经理等。

· **分析阶段：**在项目确立之前，提前与项目经理或者产品负责人进行沟通，确定安全的要求和属于产品范围的安全基线，确认项目计划和里程碑。

· 设计阶段：安全团队进行威胁建模，评估现有的需求和设计架构，沟通设计中的安全问题及应对方式。

· 开发阶段：项目组严格遵守安全编码规范或指南，最大限度减少编码时出现的安全漏洞。项目组使用安全团队提供的安全评测工具，确保开发编码的安全性。

· 验证阶段：安全团队提供对产品的人工渗透测试工作和白盒代码审计工作，并修复其漏洞。

· 发布阶段：产品上线前，需经过安全复核并且得到安全审批许可后，产品才能通过标准发布系统部署到生产环境。

· 事件响应：受 SDL 要求约束的每个软件在发布时都必须包含事件响应计划。

4.2.4.2 Web 应用防火墙

专有云平台采用 Web 应用防火墙对平台应用安全进行安全防御，Web 应用防火墙是对网站或 APP 服务进行安全和合规性保护的应用安全防护产品；通过恶意特征提取和大数据行为分析识别恶意流量并处理，针对应用的 OWASP TOP 10 攻击进行防护，保护云平台网站应用安全。详细内容请查看“6.3 Web 应用防火墙”。

4.2.5 数据安全

京东智联云遵循数据安全生命周期管理的业界先进标准，采取管理和技术两方面的手段进行全面数据安全体系建设。数据安全管理遵循“责任明确、授权合理、流程规范、技管结合”的工作方针。围绕事前防范、事中保护和事后追溯三个阶段， 为用户数据打造一个安全可靠的底层平台。

· 事前防范

· 静态数据加密

专有云提供各种加密功能，便于用户选择满足自己需求的最佳解决方案。帮助用户保持对密钥的控制，以便云应用程序和服务用于加密数据，使用云磁盘加密来加密虚拟机，存储服务加密可以加密用户存储帐户中的所有数据。

· 数据隔离

对云端数据的隔离是通过私有网络（VPC）实施的，此私有网络空间由用户完全掌控，它将不同租户间的网络深度隔离，保证了不同租户间的数据不会被越权获取。

应用硬件虚拟化技术在虚拟层为云服务器等资源提供完整的租户间虚拟资源隔离能力，用户只能访问其已购买的云计算资源，有效实现多用户之间的数据隔离。

基于数据库存储对用户数据进行隔离存储，即与用户业务数据及专有云平台自身数据等不同类别的数据相隔离，并等同享受数据库存储数据的安全保障措施。

· 存储加密

云硬盘加密对存储在云硬盘上的数据进行加密，从而保障云硬盘中静态数据的安全性和数据在云主机实例和云硬盘间传输的安全性。

保护存储在对象存储服务（OSS：Object Storage Service）数据中心的磁盘上数据，用户可以对存储空间设置默认加密，从而对其中默认加密生效期间存储的对象进行服务器端加密。在使用服务器端加密时，OSS 将对象保存到其数据中心的磁盘上之前对其进行加密，并在下载对象时对其进行解密。

数据库 RDS 支持使用透明数据加密（TDE）来加密运行 Microsoft SQL Server 的数据库实例中存储的数据。TDE 会在数据写入存储前自动加密这些数据，并在从存储中读取时自动解密这些数据。数据库文件的加密在页级别执行，已加密数据库中的页在写入磁盘之前会进行加密，在读入内存时会进行解密。

· 存储备份

京东智联云的存储容灾服务为弹性云服务器、云硬盘和专属存储等服务提供容灾能力，通过存储复制、数据冗余和缓存加速等多项技术，为用户存储数据提供可跨区域复制功能并实时同步到指定区域，实现数据异地容灾。

数据备份服务拥有完善的数据备份机制，支持自动备份和手动备份，每个实例默认每天自动备份一次，也可以根据业务情况随时创建备份，备份文件以三副本的形式保存在京东智联云对象存储中，无需担心数据丢失。

· 传输加密

云产品控制台上的通信都受到了 HTTPS 安全协议的加密保护。使用行业标准传输层安全性的 SSL/TLS 加密在用户与云、云平台系统和数据中心之间的内部通信，保护传入或传出组件的数据，以及在内部传输的数据。

· 事中保护

为了确保用户在使用云服务的过程中，用户数据受到实时的保护，并及时发现潜在的数据安全事件，在云平台的各个层面精心部署了全面的安全防护，并将京东智联云自身的事中保护能力转化为用户能够感知和应用的云安全产品，以帮助云用户快速高效地部署云端安全防护。详细内容请查看“6 专有云安全产品服务”。

· 事后追溯

· 运维数据安全

为保障专有云平台的平稳运行，建立了一套严格的、细粒度的权限管理机制，要求运维管理人员始终坚持“与用户数据有关的操作需获得用户授权，不进行有损用户数据的操作”的基本原则。对于与用户数据安全直接相关的虚拟机迁移、数据搬迁、业务扩容关键运维操作，制定了明确操作规范，规范化要求运维人员。

· 安全响应与审计

专有云提供数据安全应急预案并支持 7*24 小时的全天候安全运维响应，通过安全审计机制进行监控、审计、分析，对运维过程中的可疑操作进行问题排查与追溯。

4.2.6 安全管理服务

4.2.6.1 云翼 DevOps

专有云提供集中化运维管理平台（云翼 DevOps），基于自身自动化运维能力，针对专有云构建的一套 DevOps

产品。云翼一站式解决业务生命周期内服务管理闭环，为用户提供全链路的部署、监控、容器、服务管理等解决方案，解决专有云平台自身的应用运维、服务管理、代码管理、持续发布、集成测试、服务监控、日志管理等各类管理维护问题。详细内容请查看“5.5.4 平台运维”。

4.2.6.2 访问控制

访问控制（Identity and Access Management，简称 IAM）是专有云提供的一项用户身份管理与资源访问控制服务。用户可以通过使用 IAM 创建、管理子用户，并控制这些子用户访问专有云资源的操作权限。详细内容请查看“5.5.2 访问控制”。

4.2.6.3 安全审计

安全审计机制对专有云平台进行监控、审计、分析，及时发现异常数据流向及操作行为，一旦出现可能导致数据外泄、受损的恶意行为时，审计机制可以第一时间发出威胁告警。生产环境的运维操作通过堡垒机进行，后台运维操作记录均有统一的日志记录，并进行自动化安全审计。同时操作记录实时传输到集中日志平台，通过违规事项审计规则，主动发现异常或违规行为。

4.2.7 安全运营服务

针对专有云平台，依托安全产品服务和安全运营标准，专有云提供安全评估、安全监测、安全响应、安全巡检等安全运营服务。

· 安全评估

对云平台的系统进行安全评估，发现云平台中存在的网络安全、主机安全、应用安全隐患，并针对发现的安全隐患进行加固。对云平台运行过程中发现的安全漏洞（口令问题、配置问题等）进行修复。

· 安全监测

安全运营机制可以及时获知并解决外部安全威胁及内部安全漏洞，云平台利用安全自动监测系统，搭配威胁情报、反欺诈功能以及态势感知分析模型，有效阻止黑客入侵、恶意攻击等问题，并在第一时间处理相关安全事件，保证云平台的安全稳定及用户数据业务安全。

· 安全响应

在云平台及服务日常运行过程中，进行主动的风险管控，利用安全专家团队及云平台及服务自愈恢复能力，在紧急情况进行存储、应用等不同级别的数据与业务恢复。京东智联云配置了 7*24 的安全事件响应专家团队，执行应急预案及恢复流程，安全漏洞通告并进行风险整改，帮助用户快速解决安全问题并降低对业务的影响。

· 安全巡检

保障专有云平台的安全稳定运行，掌握云平台服务状态，除了对物理资源进行巡检外，还按计划对云平台组件、云服务状态、资源统计、平台警报、操作日志、产品版本等进行巡检。检查内容包括物理资源、计算资源、存储资源、网络资源、高级云服务、云监控、日志审计等，并对产生的安全风险进行处理。

4.3 云用户（租户）安全

4.3.1 网络安全

4.3.1.1 流量接入与防护

京东智联云 Network fast 1 ADC（以下简称 NF1）流量接入与防护平台为专有云提供强大的业务处理性能、安全能力、稳定性，针对高并发、高流量、高动态的用户接入场景。

NF1 可提供基于 DPDK 技术的高性能网络负载均衡功能。NF1 提供私有化部署的 DDoS 防护功能，支持 Syn flood，Ack flood，UDP flood，ICMP flood 等攻击防护。

NF1 提供丰富的数据监控维度，提供多维度分析报表，支持业务报表。在安全方面可对攻击行为、来源，进行统计，实现安全可视化。详细内容请查看“5.8 专有云 NF1”。

4.3.1.2 私有网络

私有网络 (Virtual Private Cloud，简称 VPC)，帮助用户构建一个隔离的网络环境， 此私有网络空间由用户完全掌控，支持自定义网段划分、路由策略等。详细内容请查看“5.2.1 私有网络”。

4.3.2 系统安全

· 安全防护

提供完善的安全组及 DDoS 防护等服务，增强网络防御能力，为主机提供全面防护。使用安全组完成单台或多台云主机的网络访问控制，实现用户间网络 100% 隔离。实时监控主机安全风险，精准防御黑客入侵行为，保障用户数据安全。

· 安全隔离

用户实例隔离基于硬件虚拟化技术的虚拟机管理， 在系统层面将多个虚拟机进行隔离。同时，在虚拟化管理层提供了存储隔离和网络层隔离。

· 安全镜像

云主机提供多种镜像功能，包括公共基础镜像、自定义镜像以及镜像市场镜像，可以基于镜像启动任意数量云主机，也可以根据需求从任意多个不同的镜像启动云主机。可用于数据备份，便于用户快速实现灾难恢复。

· 安全管理

主机安全产品通过在云主机上部署轻量级 Agent 实时感知主机安全风险，有效防御恶意攻击行为。运维管理员登录京东智联云控制台即可实时了解云主机安全状况，根据业务需求对主机做不同级别的安全加固优化，降低主机被入侵风险有效保障云主机业务安全性和连续性。

4.3.3 应用安全

4.3.3.1 代码安全

京东智联云所有为用户提供服务的云产品，在开发过程中严格遵循产品的安全开发生命周期 (SDL) 安全开发流程，在各开发节点严格审核和评估代码的安全性。同时，建议企业用户对其上线的应用进行黑白盒代码安全检测，排除存在的安全漏洞，增加业务的安全强壮性。

4.3.3.2 应用安全网关

应用安全网关（VPC-WAF）部署在 VPC 网络边界或内部，是对云租户网站或 APP 服务进行可视化安全分析和应用层威胁防护的产品。通过提供 WAF、用户访问审计、业务安全可视和合规性检查等功能。详细内容请查看“6.2 应用安全网关”。

4.3.4 数据安全

为保障用户安全的处理数据，专有云对数据全生命周期的数据生产、数据存储、数据传输、数据访问、数据使用、数据销毁各阶段应用不同安全措施。

· 数据生产

数据生产是用户产生新的内容，或对已有内容的替换、更新或修改。针对这一阶段，京东智联云建议用户首先做好数据分类，并进行风险分析，再根据风险分析结果，明确防护数据的存储位置、存储服务和安全防护措施，在数据全生命周期的起始阶段就做好数据的区分与隔离。

· 数据存储

数据存储是将数据提交到某种存储库中，通常在数据生产时发生。对于专有云存储的敏感及重要数据，建议用户使用加密措施进行防护，降低数据泄露的风险。京东智联云通过安全策略及工具让用户拥有和控制自己的数据，确定内容的存储位置、保护动态和静态内容，并为用户管理对云服务和资源的访问权限。京东智联云提供密钥管理服务 KMS（Key Management Service，简称 KMS），帮助用户管理及备份其加密密钥，提供云上密钥创建、禁用、轮换、删除等全生命周期管理。

· 数据传输

京东智联云对于数据的交换、转移和分享提供标准的传输加密协议，满足云平台以及系统间传输敏感数据的需求。支持 HTTPS 安全数据加密传输，并使用传输层安全性 (TLS) 协议，在云服务和用户之间传输数据时提供保护。

· 数据访问

数据访问是指用户对云端数据的访问。建议用户对数据的访问和传输进行严格的管控及安全防护。为保证数据的合法访问，京东智联云提供身份鉴别、授权管理、权限鉴别三合一的用户业务访问控制。

· 数据使用

数据使用过程中，对其中的敏感数据进行数据脱敏、水印等处理可以确保数据合规使用，并规避信息泄露和法律法规遵从风险。针对用户敏感数据，采用适当的脱敏算法进行处理，防止敏感数据被滥用和泄露，实现敏感隐私数据的可靠保护。用户上传文件到对象存储后，京东智联云提供丰富的数据处理服务，可以在云端实现图片的缩放、裁剪、水印、鉴黄、格式转化和样式管理，同时提供数据安全性、透明性、可溯源性。

· 数据销毁

在用户提出请求和合同终止时，京东智联云会严格遵循数据销毁标准与用户之间的协议约定，执行用户注销和数据删除。

京东智联云账户注销后，用户个人信息会在京东智联云系统中去除，使其保持不可被检索、访问的状态，或对其进行匿名化处理。根据相关法律规定，相关交易记录须在京东智联云后台保存一定时间。用户在操作之前，将自行备份京东智联云账户相关的所有信息和数据。

当用户删除数据或离开京东智联云时，京东智联云会对指定的数据及其所有副本进行全面的清除，包括删除用户与数据之间的索引关系，并将内存、块存储等存储空间进行清零操作。

4.3.5 安全管理服务

4.3.5.1 态势感知

态势感知是为用户提供的大数据安全分析产品。对多维度海量安全和业务数据进行快速、自动化的关联分析，通过图形化、可视化的技术将威胁和异常的总体安全态势呈现给用户。详细内容请查看“6.4 态势感知”。

4.3.5.2 云监控

云监控（CloudMonitor）对用户的京东智联云资源进行监控和报警的服务，展现各项监控指标情况并对指标设置报警。通过监控，用户可了解在专有云的资源使用情况、性能和运行情况，通过报警，用户可以及时作出反应，保障应用程序的稳定运行。详细内容请查看“5.5.1 云监控”。

4.3.5.3 操作审计

操作审计（Audit Trail），用户可通过操作审计保存的所有操作记录，实现精确追踪、还原用户行为审计。详细内容请查看“5.5.3 操作审计”。

4.3.6 安全运营服务

针对租户使用专有云平台的资源和管理策略进行安全运营的工作，包括基线检测、漏洞扫描、渗透测试、应急响应等服务，持续保障用户业务的持续、安全地运行。详细内容请查看“6.7 安全服务”。

5 专有云云产品安全

5.1 计算

5.1.1 云主机

云主机是京东智联云提供的一种云计算基础服务单元，提供处理能力可弹性伸缩的计算服务。包含 CPU、内存、操作系统、磁盘、网络、安全等全部所需资源，每种资源都提供多种规格，以满足不同业务的个性化需求。京东智联云提供了多层次的云主机安全防护和保障。

5.1.1.1 安全隔离

用户实例隔离基于硬件虚拟化技术的虚拟机管理， 在系统层面将多个虚拟机进行隔离。同时，在虚拟化管理层提供了存储隔离和网络层隔离。

· 虚拟机隔离

通过对服务器物理资源的抽象，将 CPU、内存、I/O 等物理资源转化为一组统一管理、可灵活调度、可动态分配的逻辑资源，并基于这些逻辑资源，在单个物理服务器上构建多个同时运行、相互隔离的虚拟机执行环境。

· 存储隔离

基于虚拟机的计算与存储分离， 实现计算和存储的自主扩展，使提供多租户和隔离变得简单。在虚拟化层，保证虚拟机只能访问分配给它的物理磁盘空间，从而实现不同虚拟机硬盘空间的安全隔离。

· 网络隔离

私有网络为用户划分一片隔离安全的私有空间，私有网络间独立隔离，将云主机部署在不同私有网络下即可实现网络隔离。用户完全掌控网络管理，支持自主划分子网、配备公网 IP 等。

5.1.1.2 安全及监控

· 安全防护

京东智联云为云主机提供一体化安全服务，包括主机安全、入侵检测及漏洞扫描等。用户间网络 100% 隔离，实时监控主机安全风险，精准防御黑客入侵行为，保障用户数据安全。提供完善的安全组及 DDoS 防护等服务，增强网络防御能力，为主机提供全面防护。

· 安全组

安全组是一种分布式、有状态的虚拟防火墙，具备检测和过滤云主机进出的数据包的功能。使用安全组可以完成单台或多台云主机的网络访问控制，包括云主机之间的东西向流量以及云主机与公网通信的南北向流量。通过使用安全组功能，可以实现云主机之间的网络安全隔离。

· SSH 密钥

京东智联云允许使用密钥加密解密基于 Linux 系统的主机登录信息，进一步提升云主机的安全。SSH 密钥登录是

指使用密钥技术对登录信息进行加密解密，用户需要创建一对唯一匹配密钥对：“公钥”和“私钥”。公钥需存储在京东智联云上，用于对数据进行加密，公钥是公开的，可以按需将其配置到目标服务器上自己的相应帐号中。私钥需用户存储，私钥只能对与之匹配的公钥所加密的数据进行解密，SSH 用户端使用私钥向服务器证明自己的身份。

· 漏洞修复

实时监控主机安全风险，对于操作系统官方发布漏洞及高危漏洞，京东智联云会第一时间通知用户，并提供漏洞修复方案，保障用户业务不受影响。

· 资源监控

基于多维度监控云主机，方便用户实时掌握云主机资源使用情况、性能及运行状态。 支持针对不同监控指标自定义报警规则，通过短信、邮件等方式发送报警通知，满足不同用户场景下需求，保障应用程序的持续稳定运行。

5.1.1.3 安全镜像

镜像是云主机运行环境的模板，包含操作系统和预装的软件以及相关配置。可以基于镜像启动任意数量云主机，也可以根据需求从任意多个不同的镜像启动云主机。京东智联云提供京东智联云提供官方公共基础镜像、基于自有云主机创建的自定义镜像以及镜像市场镜像。镜像集成了已知的高危漏洞补丁，如发现新的高危安全漏洞及时更新镜像并提供给用户，防止主机上线之后即处于高风险状态。

5.1.2 原生容器

原生容器是基于京东在容器技术方面的深厚积淀的创新型容器产品。充分融合了容器和虚拟机的优点，无需管理虚拟机或集群，为用户打造安全、易用的容器服务，灵活计费方式，有效降低用户的投入成本。

· 安全隔离

采用独立内核技术，基于虚拟机的隔离性，避免容器间共享内核的安全隐患; 基于 SDN 技术实现不同租户完全隔离。

· 可靠存储

云硬盘为原生容器实例和原生容器 Pod 提供低时延、高可靠的持久化存储。云硬盘有高效云盘、SSD 云盘两类云硬盘供用户选择。支持按需设置云硬盘的容量并随时扩展以满足业务快速增长。通过对云硬盘数据制作快照可进一步满足数据备份、批量部署、快速恢复等需求场景。

· 网络隔离

私有网络为用户划分一片隔离安全的私有空间，私有网络间独立隔离，将原生容器实例和原生容器 Pod 部署在不同私有网络下即可实现网络隔离。可通过 VPN 或专线等服务将用户本地服务器与京东智联云原生容器实例或原生容器 Pod 连通，实现对现有网络部署的扩展。

· 安全组

安全组是一种分布式、有状态的虚拟防火墙，具备检测和过滤进出原生容器实例和原生容器 Pod 的数据包的功能。使用安全组可以完成单个或多组资源的网络访问控制，包括资源之间的东西向流量以及资源与公网通信的南北向流量。通过使用安全组功能，可以实现容器之间的网络安全隔离。

· 监控管理

提供多维度监控，方便用户实时掌握容器资源使用情况、性能及运行状态。支持针对不同监控指标自定义报警规则，通过短信、邮件等方式发送报警通知，满足不同用户场景下需求，保障应用程序的持续稳定运行。

5.1.3 Kubernetes 集群

Kubernetes 集群服务采用管理节点全托管的方式，为用户提供简单易用、高可靠、功能强大的容器管理服务。

· 可靠性

同地域下，集群的管理、工作节点可跨可用区部署，支持单集群至少运行三台云主机作为管理节点，同时基于京东智联云高可用组隔离故障域，进一步增强了可靠性。

· 可用性

基于京东智联云 SDN 网络，提供 CNI 网络插件，依托京东智联云私有网络的高可用及可靠性，轻松适应不同规模生产环境的网络需求；提供 CSI 存储插件，集成京东智联云云硬盘，提供安全可靠的持久化存储；集成京东智联云负载均衡服务，提供安全、可靠的网络访问。

5.1.4 容器镜像仓库

容器镜像仓库是全托管的容器镜像存储、分发平台，提供安全、可靠的镜像服务，与京东智联云原生容器、Kubernetes 集群服务无缝集成，为基于容器的应用提供一站式部署服务。

· 安全可靠

冗余、高可用的架构，99.999999999% 数据持久性，支持全链路数据加密，保障数据安全。具有有效期的授权令牌，可用于注册表和镜像仓库的管理。

5.1.5 云硬盘

云硬盘是京东智联云为云主机提供的低时延、持久性、高可用块存储。云硬盘的数据以三副本方式存储，避免因组件故障导致数据不可用，同时提供高可靠数据存储服务。云硬盘容量可弹性扩展，同时支持快照和自定义镜像功能。

· 可靠性

基于数据三重实时副本保证数据可靠性高达 99.9999999%，为用户提供安全可靠的数据存储服务。支持云硬盘加密，支持快照数据备份。

· 云硬盘快照

云硬盘快照是某一时间点上某一块云硬盘的数据备份，作为云硬盘的数据备份，以应对误操作、攻击或病毒等导致的数据丢失的风险。

· 云硬盘加密

云硬盘加密功能基于京东智联云 KMS 系统，对云硬盘加密，为用户提供了一种简单的安全的加密手段，能够对新创建的云硬盘进行加密处理。用户无需构建、维护和保护自己的密钥管理基础设施，也无需更改任何已有的应用程序，无需做额外的加解密操作，云硬盘加密功能对于用户的业务是透明的。

5.1.6 高可用组

高可用组是京东智联云提供的云主机逻辑集合，高可用组内的云主机分散部署在相互隔离的物理资源上，当出现硬件故障或定时维护时只会影响部分云主机，用户的业务仍为可用状态。

· 业务高可用

高可用组支持跨可用区，当用户选择在高可用组内部署云主机时，京东智联云将保证用户的云主机分散在多可用区的不同的物理故障域上，故障域之间相互隔离，当一个故障域内发生硬件故障或定时维护时仅影响部署在该故障域上云主机，其他故障域上云主机仍为可用，保障用户业务正常运行。

· 资源监控

基于多维度监控高可用组内云主机，可视化图表展示，方便用户实时掌握云主机资源使用情况及运行状态。 自动上报 CPU 利用率、内存利用率及磁盘读写吞吐量等监控数据，支持用户使用不同统计方法监测资源，如平均值、最大值等。

· 自动化运维

无需人工实时干预，动态调整云主机数量，高可用组支持根据用户预设的告警 / 定时策略动态新增和删除云主机，轻松应对业务负载波动，保障业务波峰时服务能力，节约业务波谷时业务成本。

5.1.7 弹性伸缩

弹性伸缩（Auto Scaling）是根据用户的业务需求和伸缩策略，自动调整资源规模的服务。可以通过设置定时任务、监控告警策略确保用户拥有适量的资源来保证业务平稳健康的运行。在业务高峰期，自动增加云主机实例的数量，以保证业务性能不受影响；当业务需求较低时，则会减少云主机实例数量，以节省成本。

· 报警伸缩

基于云主机监控性能指标（如 CPU、内存利用率、网络进出流量等）情况调整业务的部署，可以自定义告警触发策略。当业务负载使得指标达到阈值时，根据设定的策略自动增加或减少云主机实例，从而灵活应对业务负载变化，提高资源利用率。

· 定时伸缩

可以设置定时任务，对用户的资源扩 / 缩活动进行提前规划。用户可以配置周期性任务，定时地自动增加或减少云主机实例，从而灵活应对业务负载变化，提高资源利用率。当周期性需求有所波动时，可同时配置告警伸缩模式以应付不可预期的变化。

· 自动加入负载均衡

通过告警、定时策略增加的云主机实例，会直接关联已有负载均衡，分担业务流量，提高服务可用性。

5.1.8 GPU 云主机

基于 GPU 的高效计算服务，适用于人工智能、图像处理等多领域场景。 实时高速，提供卓越的并行计算及浮点计算能力，快速构建异构计算应用。

不同用户之间资源全面隔离，保障用户的数据安全。同时，GPU 云主机与云安全无缝对接，享有普通云主机同等的云安全服务。通过安全组和网络 ACL 实现 VPC 内多级安全防护。详细内容请查看“5.1.1 云主机”。

5.2 网络

5.2.1 私有网络

京东智联云私有网络(VPC),是用户在京东智联云自定义的逻辑隔离的网络空间，此私有网络空间由用户完全掌控，支持自定义网段划分、路由策略等。用户可以在 VPC 内创建和管理多种云产品，如云主机、负载均衡等，同时可配置网络内的资源连接 Internet。

私有网络 VPC 是用户网络在京东智联云上的表现形式，包含了一系列的网络及安全功能，与其他的 VPC 逻辑隔离。在实例级别实现安全组一级防护，在子网级别实现网络 ACL 二级防护，在 VPC 间实现网络 100% 安全隔离，达到访问控制的目的。

· 自定义网络

京东智联云提供安全隔离的私有网络，不同 VPC 之间完全隔离，且用户可自定义 VPC 网段范围，自主配置 VPC 内的子网、路由表、ACL 等。

· 子网路由策略

京东智联云提供可灵活配置的路由策略，可实现基于子网的路由策略编辑，精确控制进出子网的网络流量。路由表是一系列路由规则的集合，用于控制私有网络中子网的流量流出方向。京东智联云共有两种类型的路由表：默认路由表和自定义路由表。随私有网络创建时自动创建的路由表为默认路由表，用户主动创建的路由表为自定义路由表。

· ACL

网络访问控制列表（Access Control List，简称 ACL）是一个子网级别无状态的可选安全层，用于控制进出子网的数据流，可以精确到协议和端口粒度，可用作防火墙来控制进出一个或多个子网的流量。

ACL 实现在虚拟路由器 VRouter 上，VRouter 本身并未对用户暴露，用户可以通过 ACL 配置子网级别东西向和南北向的访问控制。具有相同网络流量控制的子网可以关联同一个网络 ACL，通过设置出站和入站允许规则，对进出子网的流量进行精确控制。

· 安全组

安全组是一种分布式、有状态的包过滤功能的虚拟防火墙，可实现对云主机和容器的网络访问控制，从而控制一台或多台云主机和容器的访问流量。创建云主机和容器时，可以关联相应的安全组，将同一地域内具有相同网络安全隔离需求的云主机和容器加到同一个安全组内。通过配置安全组策略对云主机和容器的出入流量进行安全过滤。

新建安全组默认对所有出口 / 入口流量执行 All drop 规则，出口包含一条缺省配置允许所有流量。用户可以随时添加或删除安全组的规则，新规则会自动应用于与该安全组相关联的所有云主机和容器。

· NAT 网关

同一 VPC 内的多台云主机同时有访问 Internet 的需求且公网 IP 资源不足时，可通过创建 NAT 网关解决此问题。京东智联云支持自建 NAT 网关，实现 SNAT 功能。京东智联云私有网络的 NAT 网关提供 IP 的安全转换，帮助与用户隐藏私有网络内主机的公网 IP 以避免暴露其网络部署。

5.2.2 专线服务

专线服务 (Direct Connection) 是京东智联云提供的一款高速、安全、稳定的网络接入服务。

· 网络高可用性

多条物理链路支持做 ECMP，满足用户的高可用网络质量需求允许在用户的 IDC 和京东智联云专线接入点间创建多条物理链路，实现流量的负载均衡，保障专线服务的高可用性。

· 多用户多业务隔离

物理链路支持多用户、多业务共用，用户间及业务间相互隔离、互不影响。可将已接入公有云的物理链路共享给其他用户使用，用于实现物理链路的充分使用，同时物理链路上可以运行多种不同的业务。

· 安全可靠

物理链路由接入的用户独享，无数据泄露风险，安全性高，满足游戏、金融、政府企业等对网络安全性要求高的用户需求。

5.2.3 VPN

VPN 网关提供基于 Internet 的数据加密传输服务，可实现不同 VPC 的网络互连，打通企业 IDC 和京东智联云内网，实现混合云部署。使用带有 VPN 功能的镜像，可创建 VPN 网关。

· 提供加密数据传输通道

京东智联云 VPN 使用 IPSEC、IKE、预共享密钥方式对数据进行加密，基于公网提供安全可靠的通信隧道。

· 灵活的组网方式，支持多隧道共享网关

支持 VPN 网关下组建多条隧道（需不同的对端网关），提供相对灵活的组网方式，应对不同业务场景需求。

· 隧道连通性检测，自动修复隧道功能

VPN 默认提供隧道连通性自动检测，定时检测隧道的连通状况，一旦发现隧道连接断开自动重新连接保证隧道可用性。

5.2.4 弹性网卡

弹性网卡是一种虚拟网络接口，用户可以在云主机上绑定弹性网卡以使云主机接入不同网络。弹性网卡可以在构建业务流量分离、多业务承载以及网络高可用等应用场景时提供支持。 京东智联云提供地域级属性弹性网卡，弹性网卡可以绑定私有网络内任意一台云主机。单台云主机可以绑定多块弹性网卡，绑定数量需依据云主机规格而定。

· 路由控制

云主机可挂载多块分属不同子网的弹性网卡，每个子网可分别设置访问控制策略与路由转发策略，实现业务与网络隔离。

· 业务安全

云主机挂载多块弹性网卡，特定业务可由特定弹性网卡承载流量，不同弹性网卡可分别绑定安全组，应用不同安全策略，实现对业务流量的精确管控。

· 容错可靠

提供无可用区属性弹性网卡，支持弹性网卡在不同可用区云主机间动态迁移，实现可用区级的高可用方案，缩短故障时间，提升系统可靠性。

5.2.5 负载均衡

负载均衡可将大并发流量分发到多台云主机，调整资源利用情况，消除由于单台云主机故障对系统的影响，提高系统可用性、扩展系统服务能力。

· 高可用性

京东智联云负载均衡通过自动冗余机制提供高可用服务，创建负载均衡实例后会自动提供双活的负载均衡服务，保证服务的高可用性。

· 自动健康检查，保证可用性

负载均衡服务会检查云服务器池中云主机的健康状态，自动隔离、挂载后端提供服务的云主机，消除服务器单点

故障，保障业务正常运行。

· 弹性公网 IP 绑定，内网保护

负载均衡可配置在内网环境，通过绑定公网 IP 提供对外服务，因此可隐藏内部网络结构，增强系统安全性；并且因内网部署，可通过设置防火墙等构建更加安全的防护体系。

· 防 DDoS 攻击

提供基于公网 IP 的抗 DDoS 攻击能力，提升服务的安全性能。

5.3 存储

5.3.1 对象存储

京东智联云对象存储（Object Storage Service，简称 OSS）是利用京东在分布式存储领域多年的深厚技术积累，为用户提供安全、稳定、海量、便捷的对象存储服务。

· 稳定可靠

使用京东自行研发的存储和 CDN 技术，规模自动扩展，不影响对外服务，数据自动多重冗余备份并可通过智能调度实现自动故障恢复，保证稳定、高可用的服务。

· 异地容灾

根据业务热点就近选择存储地区，减少资源获取延迟。同时，多地存储可以帮助用户实现异地容灾。

· 访问控制

OSS 提供权限控制 Bucket Policy，在创建存储空间的时候选择相应的权限控制，也可以在创建之后，在权限设置中修改 Bucket Policy。

· 防盗链机制

支持多种防盗链设置，保障用户不受资源盗用的困扰。通过设置 Bucket 的防盗链黑白名单，在外部请求存储空间资源时，判断 HTTP 请求 header 的 referer 是否在黑白名单中，从而禁止或允许外部请求，可以用来防止资源盗用及被盗用后产生的额外流量费用。

5.3.2 云文件服务

云文件服务（Cloud File Service）是一种高可靠、可扩展、可共享访问的全托管分布式文件系统。

· 服务持久可靠

云文件服务采用分布式架构，三副本设计。用户所有文件和目录均以三副本方式分散于不同的故障域存储，防止单点故障引起的数据不可访问或数据丢失。具备高可用性和高持久性。

· 访问权限管理

提供网络及文件数据级别的权限管理。云文件服务的挂载点置于用户 VPC 内，所有对文件存储的访问均受到用户 VPC 的网络安全隔离控制保护；支持用户通过标准的 POSIX 权限控制对文件数据的读写访问控制。

5.4 云数据库与缓存

5.4.1 云数据库 MySQL

云数据库 MySQL 是京东智联云基于全球广受欢迎的 MySQL 数据库提供的稳定可靠的云数据库服务。相比传统数据库，云数据库 MySQL 易于部署、管理和扩展，默认支持主从热备架构，提供数据备份、故障恢复、监控等全套解决方案。

· 高易用性

快速部署：选择规格后下单，几分钟内即可创建高可用的 MySQL 实例。具备完善的监控、告警功能，可立即投入使用，立即创造价值。

运维便捷：提供数据库实例各项指标的实时监控及自动告警功能，随时随地了解实例动态；降低用户数据库运维成本和服务器网络运维成本。

· 高扩展性

弹性扩展：可按需升级实例的内存、磁盘空间大小，提升业务处理能力，升级过程不影响业务正常访问和使用，实现快速、平滑扩容，满足业务快速发展需要。

只读实例: 支持只读实例，横向扩展数据库读取能力，每个只读实例拥有独立的链接地址，可由应用端控制压力分配。帮助用户轻松实现读写分离架构，应对业务海量请求压力。

· 高可靠性

全量备份：每天在用户指定的时间自动全量备份 MySQL 数据库并保留 7 天；此外支持即时的手动备份。

增量备份：云数据库 MySQL 会自动备份过去 7 天的数据库增量部分，以实现基于任意时间点的回滚。

数据恢复：支持一键恢复备份数据至当前实例；此外基于增量备份，支持根据七天内任意时间点的数据创建新的数据库实例。

· 高安全性

安全模式: 默认的云数据库 MySQL 实例采用的是标准模式，支持切换到高安全模式，具备一定的 SQL 拦截能力，同时也提供了 SQL 审计功能。

5.4.2 云数据库 SQL Server

云数据库SQL Server是基于微软的SQL Server 打造的适合云端的数据库产品，具有: 服务高可用，数据高可靠，功能丰富，高效稳定，运维省心等种种优点，是最适合政府、企业及电商的商业级云数据库。

· 主备高可用

提供基于 SQL Server 镜像的一主一备高可用架构，主实例数据实时同步到备实例；发生故障时，系统可自动感知并进行主备切换；切换可在数十秒内完成，切换过程中数据零丢失，应用几乎无感知。

· 自动备份

系统可根据用户定义的时间段，每天自动备份，在线备份最长可保持 2 年，满足企业或政府合规要求；提供备份下载功能，可以将备份下载保存到其他介质；同时提供实例级和数据库级的手工备份和恢复功能，满足用户各种不同的需求。

· 数据库审计

基于 SQL Server 原生审计，可靠性高；可自定义审计策略，满足不同业务场景需求；审计结果为二进制格式，无法篡改。

· 身份认证

云数据库 SQL Server 仅支持私有网络，只提供内网连接，公网不可访问。使用云数据库 SQL Server 时需要有云主机。SQL 身份验证，使用用户名和密码。

· 访问控制

设置 IP 白名单控制哪些 IP 地址能够访问 SQL Server 数据库。 每个账号只能读写、只读自己的数据库。

· 数据加密

SQL Server 提供内置的加密函数，可以进行数据加密。京东智联云对云数据库 SQL Server 提供安全可靠的安全加密方式，防止数据库数据泄露、拖库等危害。

· 安全防护机制

宿主机位于防火墙保护之下，只开放必需的端口，且安装有各种系统补丁，能够抵御各种恶意攻击，保障数据库安全。

SQL Server 实例运行在逻辑隔离的私有网络（VPC）中，避免了数据库直接暴露在公网上，可规避绝大部分攻击。

通过安全组、ACL 规则可定义和强化安全策略，进一步加强数据库的安全性。

· 多维度监控，自定义告警

从各个维度提供系统级和数据库实例级的监控，监控指标丰富。可根据监控指标自定义告警规则，并通过短信，Email 等方式进行通知。

5.4.3 云数据库 MongoDB

云数据库 MongoDB 是京东智联云基于全球广受欢迎的 MongoDB 提供的高性能 NoSQL 数据库服务，完全兼容 MongoDB 协议，默认提供三节点副本集的高可用架构，支持自动容灾切换，确保业务可用性，并支持在线扩容、备份恢复等功能，降低管理维护成本。

· 高安全性

VPC 私有网络: 实例部署在用户自定义的 VPC 私有拟网络内，在 TCP 层直接进行网络隔离保护，确保数据安全性。

IP 白名单：支持用户自定义 IP 白名单，从访问源进行安全控制。

· 高可用性

三节点副本集：自动搭建三节点副本集，三个数据节点位于不同的物理服务器上，自动同步数据。

自动容灾: 默认 Primary 和 Secondary 节点提供服务，当 Primay 节点出现故障，系统自动选举新的 Primary 节点。Secondary 节点不可用时，由备用节点接管服务，多重保障服务可用性。

同城容灾：支持多可用区部署方式，主从节点与隐藏节点分布在不同的可用区，可以承受机房级别的故障。

· 高可靠性

自动备份：每天自动全量备份数据并保留 7 天，备份文件以三副本的方式存放在云存储。

手动备份：支持即时手动创建备份，备份数据长期保存。

备份恢复：支持一键恢复备份数据至当前实例；此外支持根据备份创建新的云数据库 MongoBD 实例。

· 高易用性

快速部署：通过控制台，几分钟内即可创建出功能完善的云数据库 MongoDB 实例，可快速投入使用创造价值。

弹性扩容：支持扩容缩容，可根据业务情况按需升级或降级实例配置，提高资源利用率，降低使用成本。

监控与报警：提供丰富的监控信息，并支持设置多项自动报警规则，随时随地掌握服务运行状态。

5.4.4 云缓存 Redis

云缓存 Redis 是京东智联云提供的基于 Redis 协议的在线缓存服务，支持主从版、集群版的多种规格供用户选择。可满足多种业务场景对可用性、可靠性和高读写性能的要求，支持双机热备，提供自动容灾切换、实例监控等服务，以降低业务风险，确保业务的连续性。

· 高可用

双机热备，自动切换。当主节点发生故障后，从节点会被迅速提升为新的主节点，继续提供服务；服务数据持久化，实例跨可用区部署，保证数据的安全和业务的不间断运行。

· 可靠性

云缓存 Redis 将数据完全保存在内存中，保证了高效性，并且同时会在物理磁盘进行持久化，保证数据安全。

地域内增加的多可用区部署，保证数据的安全和业务的不间断运行，从而保证了用户业务的高可用。

· 访问控制

实例运行在私有网络（VPC）中，增强了安全性和隔离性。提供了子网、访问控制策略等限制访问的功能。

· 监控告警

为用户提供多种类型的监控，包括如使用量、连接数、QPS、Key 数量等多种监控，可视化数据监控展示。全链路监控预警，帮助用户提前预警提示风险、快速定位和解决问题。

5.5 管理

5.5.1 云监控

云监控（CloudMonitor）是对用户的云资源进行监控和报警的服务，展现各项监控指标情况并对指标设置报警，云监控会通过短信、邮件等方式发送报警通知，还提供当前报警状态和报警历史的查看。

· 资源监控

可以查看各资源的各项监控指标的情况。

· 站点监控

站点监控是一款针对互联网网络状况进行探测的监控类产品。用户可通过站点监控模拟真实用户访问请求，从而得到被监控地址的可用性和响应时间等性能数据。

· 报警设置

用户根据实际业务需求，灵活设置各资源监控指标的报警规则，当资源消耗达到用户的报警阈值后，京东智联云会迅速通过短信、邮件告知，方便用户及时处理。

· 报警模板

用户可以使用京东智联云平台提供的默认报警模板或自己创建的自定义报警模板，快速为云资源创建报警规则。

5.5.2 访问控制

访问控制（Identity and Access Management，简称 IAM）是京东智联云提供的一项用户身份管理与资源访问控制服务。用户可以通过 IAM 服务创建、管理子用户账号，并控制这些子用户访问京东智联云资源的权限。使用访问控制，用户可以向他人授权管理账户中的资源，而不必共享账户密码或访问密钥，按需为用户分配最小粒度的

操作权限，从而降低主账号的信息安全风险。

IAM 包含授权管理，身份鉴别，权限鉴别三个模块：

· 身份鉴别

当用户、应用、或资源发起对某个京东智联云账号下的资源访问时，准确识别发起方的身份。

· 授权管理

主账号分权操作，允许其他用户、应用、或资源在可控的权限范围内访问自己的资源、执行可控的操作。

· 权限鉴别

判定发起访问方是否有权限执行访问。

5.5.2.1 用户身份管理

· 子用户管理

主账户，也叫根账户，是京东智联云资源归属、计费的主体，在用户注册、激活京东智联云时由系统创建。主账户为其名下所有的资源付费，并拥有所有京东智联云服务和资源的全部权限。

子账户是由主账户创建的一种实体用户，有确定的身份 ID 和安全凭证。子账户不是独立的京东智联云账户，它归属于主账户，只能在主账号的空间下可见。子账户必须得到主账户的授权，才能登录控制台或使用 API 操作主账号授权的资源。

一个主账户可以通过 IAM 服务来创建一个或多个独立的子账户，为子账号设置、重置控制台登录密码。

· 用户组管理

也可以将多个子用户加入一个用户组，统一授权。一个子用户可以属于多个用户组，此时子用户权限为各组权限的合集。

5.5.2.2 授权策略管理

IAM 帮助定义用户或其他实体可在账户内执行的操作，通常称为授权。权限是通过策略授予的，在附加到身份或资源时，策略定义了它们的权限。在用户发出请求时，京东智联云将评估这些策略。策略中的权限确定是允许还是拒绝请求。主账号拥有其名下所有资源的全部操作权限。如果主账号未对子账号进行授权，子账号默认没有任何资源的访问权限。只有得到主账号的授权时，子账号才能通过控制台或 API 访问特定的资源。主账号授权子账号的方式，是为子账号（或其所在的群组）附加授权策略。子账号所拥有的资源访问权限，是子账号和其所在的群组附加的授权策略的合集。

· 权限粒度

支持对单个资源的读、改、删权限控制。

· 系统授权策略

系统提供各类资源的管理员和只读权限，可以直接进行分配。

· 自定义授权策略

便利化策略生成器：无需撰写 JSON，通过可视化方式选择要授权的操作和被操作的资源。策略编辑器：基于已有策略模板编辑 JSON，也可以直接生成 JSON，以实现授权需求。

5.5.2.3 安全身份凭证

京东智联云通过安全凭证来验证用户是否有权访问所请求的资源或服务， 安全凭证是用于证实用户真实身份的凭据，包括以下类型：

· 用户名和密码

密码是用户最初创建账户时指定的。用户在登录京东智联云控制台时，需要使用密码。同时，该密码也可以用于 API 方式访问京东智联云资源。IAM 支持用户的安全管理员设置登录策略，避免用户密码被暴力破解或者因为访问钓鱼页面等，导致账号信息泄露。

· 多因素验证

（Multi-Factor Authentication，简称 MFA），是一种简单有效的最佳安全实践，它能够在用户名和密码之外再额外增加一层安全保护，并且在京东智联云进行敏感操作时，进行身份验证防止误删。

虚拟 MFA 设备是一种基于软件，产生动态验证码的应用程序，它遵循基于时间的一次性密码（TOTP）标准（RFC 6238），可以将虚拟 MFA 设备安装在不同的移动设备上，如智能手机。启用 MFA 后，用户登录京东智联云时，系统将要求输入用户名和密码，然后要求输入来自其 MFA 设备的 6 位动态验证码，即使他人盗取用户的密码，也无法登陆用户的账号，双因素的安全认证将最大限度地保障用户的账户安全。

· 访问密钥（AccessKey）

为了保证云资源的使用安全，当以 API 调用相关资源和操作时，要求使用 Access Key 验证用户和应用程序的身份，以确保访问者具有相关权限。Access Key 包含它由 Access Key ID 和 Access Key Secret 构成。拥有用户的 Access Key 的任何人将与用户拥有相同的资源访问和操作权限，可以无限制的访问用户账户中的所有资源并进行相应的操作。用户可以创建、禁用或删除用户的 Access Key，同时也建议用户定期轮换 Access Key 以保证用户的账户和资源安全。

5.5.3 操作审计

操作审计（Audit Trail）是京东智联云提供的一项服务，用户可通过操作审计保存的所有操作记录，实现精确追踪、还原用户行为审计，对于安全分析，资源变更追查，合规审查有非常重要的作用。

· 实时可靠

用户能够及时了解操作事件情况，通过查看 Audit Trail 及时了解账号的操作行为，并将遇到的问题及时处理或反馈。

· 安全合规

通过实时有效的记录京东智联云账号内的所有操作行为，为问题、故障事件定位，确保在京东智联云上运行的业务安全合规。

· 操作记录

操作审计功能无需配置即可收集最近九十天的操作记录，并且在控制台操作审计页面可查看最近九十天的操作记录。

· 事件列表

用户可以通过控制台查看操作事件列表，并且支持从事件名称、产品类型、事件时间、操作账号等维度来查询操作事件。

· 记录详情

用户可以获取单个操作记录详情，包括访问密钥、地域、错误码、事件源、事件 ID、请求 ID、IP 地址。

5.5.4 平台运维

云翼 DevOps，是京东智联云结合自身自动化运维能力的基础上，针对专有云的场景和特性，提供的快速可靠的持续集成与持续交付服务产品。

· 服务容错

自动为宕机服务器上运行的容器 / 云主机重新迁移并生成新的实例，保障业务不掉线，高可靠运行。系统自动监控服务健康状态，动态调整集群，实时调度相关预案，实现故障自愈。

· 智能监控

全面覆盖了基础资源到业务逻辑的监控。拥有丰富的采集功能，支持基础监控，存活监控，性能监控和业务监控。通过监控用户可以全面了解资源的使用情况，性能和运行状态。通过异常检测和多维度数据分析可及时做出反应，缩短异常 MTTR，保障业务正常运行。

· 安全运维

云翼 DevOps 提供高可用、安全高效的镜像中心服务， 涵盖脚本执行、文件分发等基础操作，可以满足各种复杂运维场景一键式作业，实现真正的 Web 自动化运维。

5.5.5 管控平台

JDStack 管控平台，是 JDStack 专有云平台的核心组件，负责整个 JDStack 的部署搭建、资源管理和集群维护。负责机架、网络设备、服务器等底层硬件与上层操作系统、基础服务、平台应用的通信调度和交互操作。

JDStack 管控平台具一套完整的用户权限体系，保障专有云平台内资源被合法合理访问。全局展示服务器分布信息和监控状态，提供开关机、断网操作功能。监控中心负责监控 JDStack 所有服务器中日志文件和部分关键服务。

5.6 大数据与分析

大数据服务主要产品包括数据工厂，数据集成，数据计算服务，流计算，流数据总线，列式存储，数据大屏等产品。

· 安全隔离

各集群通过 VPC 网络隔离，自动配置防火墙管理网络访问，支持网络 ACL 和安全组的自动配置；集群部署在用户自定义的 VPC 私有网络内，在 TCP 层直接进行网络隔离保护，确保数据安全性。

· 权限管理

系统通过访问控制（IAM）进行用户口令管理。使用多层次 ACL 数据访问授权机制，控制用户所能访问的数据内容及读写权限。对用户进行基于角色的访问控制，用户的角色决定了用户的权限等访问控制。对用户、群组和策略进行授权，限制数据被有限的用户所访问，使用权限方式管理用户对数据对象的访问。

· 传输安全

使用 HTTPS/TLS 进行数据传输，使用 X509 数字证书作为身份认证。对于 Web API 数据采集方式，通过应用层通过 HMAC-SHA1 算法实现数据验证。防止数据被非法访问、篡改、窃听、嗅探。

· 数据保护

对多用户的计算进行隔离，程序执行的安全沙箱，数据存储隔离，并提供加密选项。针对用户敏感数据，采用适当的脱敏算法进行处理，防止敏感数据被滥用和泄露。提供数据容灾热备功能，保护数据安全和提高数据的持续可用性。

· 安全监控

京东 JMR(JD MapReduce) 提供集群的可用性、性能监控，帮助用户发现问题、解决问题，同时满足用户对集群资源调整、释放等管理需求。监控集群中的每个节点的网络状态，硬盘状态等。根据用户集群中的相关组件进行监控。 监控服务节点是否正常运转。

5.7 互联网中间件

5.7.1 消息队列 JCQ

京东智联云消息队列（JD Cloud Message Queue，简称 JCQ）是京东智联云自主研发的分布式消息队列服务。产品能够提供消息发布订阅、消息查询和死信队列等一系列高可靠、高可用、高处理性能的消息云服务。

· 高可用

集群部署与主从自动切换技术，承诺服务可用性高达 99.95%。

· 高可靠

引入 Raft 算法实现数据高可靠性，同步写入，三副本数据备份，数据可靠性高达 99.999999%，并且默认消息持久化存储 3 天，支持重置消费位点消费 3 天之内任何时间点的消息。

· 安全防护

全面监控：提供多维度的资源运行状况和性能的监控、稳定性维护等功能，提前预警通知，降低日常维护工作量。

私有网络: 实例运行在私有网络（VPC）中，增强了安全性和隔离性。提供了子网、访问控制策略等限制访问的功能，抵御网络攻击，保护用户的业务隐私。

5.7.2 API 网关

API 网关（API Gateway），是 API 托管服务。提供 API 的全生命周期管理，包含发布、管理、运行、维护、下线等。用户可通过 API 网关实现自身系统集成和服务聚合，还能便捷安全地开放其业务功能和数据，并实现与开发者或合作伙伴的连接。

· 安全稳定

充分依托于京东智联云账户安全体系、支持 HTTPS 协议、同时集群可弹性扩容已支持超大并发，还提供了基本的防 DDoS/CC 等安全防护功能。

· 认证与限流

提供严格的认证服务。API 请求到达网关需要使用网关提供的密钥 AccessKey 和 SecretKey（简称 AK/SK），经过身份认证、绑定认证、后端签名才能到达后端服务，有效保护 API 的安全性。 提供有效的流控策略。用户可根据 API 的重要程度，配置单位时间内的 Access Key 流量限制、API 流量限制。

5.7.3 微服务平台

提供了注册中心、配置管理、调用链分析服务等功能的微服务框架，方便用户实施 Spring Cloud、Dubbo 等微服务应用。

· 高可用全托管

京东智联云微服务平台依托京东多可用区部署，服务跨可用区分布式部署。用户开通服务后，无需任何运维操作，即可享受跨机房的高可用性。

· 服务监控

数据监控和调用量监控相结合，用户可以方便地了解各服务各个维度的调用数据，以及服务之间的相互调用关系和调用状况。

5.8 专有云 NF1

京东智联云 Network fast 1 ADC（以下简称 NF1），不仅是一体化高性能负载均衡器，它提供强大的数据监控分析能力，集成企业级 WAF，降低成本同时减少网络部署复杂度。高可用、弹性扩展设计与 Cloud Native 亲和性适用于微服务架构。

· DDoS 防护

NF1 整体解决方案中，提供私有化部署的 DDoS 防护功能，支持 Syn flood，Ack flood，UDP flood，ICMP flood 等攻击防护。创新云端 IP 高防联动机制，正常状态离线分析，遭受攻击串联云端 TB 级防御能力，并提供安全专家团队 7*24 支持。

· Web 安全防护

NF1 可抵御 OWASP TOP 10 威胁，支持黑白名单、CC 安全防护、Web 自定义防护、限速、自定义页面、HTTP 流量管理、网站防篡改、恶意 IP 惩罚、防爬虫等安全防护能力，提供丰富的安全报表。

· 数据监控与日志分析

NF1 提供丰富的数据监控维度，包括实时流量、实时 QPS、状态码统计、协议占比统计、实时攻击行为、防御数量、请求来源统计，监控数据动态更新，更及时、更精准。NF1 提供多维度分析报表，支持业务报表，可对域名、VIP 等维度进行数据分析，并可快速分享到移动终端；安全方面可对攻击行为、来源，进行统计，实现安全可视化。

6 专有云安全产品服务

6.1 DDoS 基础防护

DDoS（Anti-DDoS Basic）基础防护，可为用户高效的抵御 DDoS 攻击。可根据业务需求设置清洗触发值，使常见的 DDoS 攻击将无法威胁到用户的业务，为用户的业务安全保驾护航。

· 自动防护

DDoS 基础防护基于先进的识别算法，帮助用户抵御 SYN Flood、ICMP Flood 等各种大流量攻击。使用 DDoS 基础防护服务后，SYN Flood、UDP Flood 等常见的大流量攻击将无法威胁到用户业务，同时支持 IPV4 和 IPV6 地址的防护。

· 防护快速

DDoS 基础防护会对所有流量进行实时检测，第一时间发现其中的攻击流量，秒级应对攻击，清洗迅速，保障业务的正常运行。

· 实时监控

实时监测并展示当前 DDoS 攻击数据，快速定位攻击来源，监控攻击状况，缩短黑洞时长，最快恢复业务。

6.2 应用安全网关

应用安全网关，是对网站或 APP 服务进行可视化安全分析和应用层威胁防护的产品。通过提供 WAF、用户访问审计、业务安全可视和合规性检查等功能，保障业务稳定可持续运行，提升用户体验，为网络服务提供者解决 HTTP/HTTPS 业务因攻击导致的异常或合规性问题。

· Web 安全防护

OWASP TOP 10 威胁防护：有效防御 SQL 注入、XSS 攻击、命令 / 代码执行、文件包含、木马上传、路径穿越、恶意扫描等 OWASP TOP 10 攻击。

0Day 漏洞防护：专业的攻防团队 7*24 小时跟进 0day 漏洞，分析漏洞原理，并制定安全防护策略，及时进行防护。

CC 攻击防护：支持全局模式和单 IP 防护模式，基于多种挑战验证算法进行 CC 攻击防护校验，防护应用层 DOS 功能。

· 业务安全可视化

五大安全分析报表：提供 Web 安全、CC 攻击、自定义访问控制规则、用户访问和运行监控五大安全分析报表，洞悉业务监控状态，安全防护状况和效果。

攻击趋势图概览：提供用户访问和攻击趋势图，了解黑客对业务的关注程度。

CC 攻击防护趋势概览：CC 攻击趋势统计，实时查看防护效果和统计。

用户访问趋势概览：对用户制定的访问控制规则进行统计分析，实时查询用户访问情况。

· 安全合规

精准的访问控制：用户可以对 HTTP 协议字段进行组合制定访问控制规则，确定优先级，提供多种定制方式和简单逻辑语法，满足个性化需求。

访问日志审计：记录所有用户对业务网站的访问日志，提供趋势分析，可以根据需要提供日志下载功能。

网页防篡改：采用强制静态缓存锁定和更新机制，对网站特定页面进行保护，即使源站相关网页被篡改，依然能够返回给用户缓存页面。

管理员操作审计：对所有管理员的操作提供审计日志，在进行安全合规排查可以根据需要提供。

· BOT 管理

反爬虫防护：对恶意爬虫进行识别和阻断，防止恶意内容抓取保护源站安全。

防暴力破解：自动识别注册或登录页面，采用多种挑战验证方式进行人机识别，保护用户账号安全。

自定义 BOT 策略：支持个性化业务安全防护定义，指定 URL 或特字段的频次和行为学习模式，针对分布式或者单 IP 模式的业务威胁进行防护。

6.3 Web 应用防火墙

Web 应用防火墙，是对网站或 APP 服务进行安全和合规性保护的应用安全防护产品；通过恶意特征提取和大数据行为分析识别恶意流量并处理，提高 Web 站点的安全性和可靠性，保护网站核心业务和数据安全。

· Web 攻击防护

OWASP TOP 10 威胁防护：有效防御 SQL 注入、XSS 攻击、命令 / 代码执行、文件包含、木马上传、路径穿越、恶意扫描等 OWASP TOP 10 攻击。专业的攻防团队 7*24 小时跟进 0day 漏洞，分析漏洞原理，并制定安全防护策略，及时进行防护。

· CC 攻击防护

智能防御策略：提供智能 CC 防护模式，通过 AI 分析行为特征，根据不同业务类型，服务器处理性能不同，生成定制化的 CC 防护规则。同时根据京东智联云全网大数据分析能力，共享攻击源情报数据，提高防护效率。

多种防御策略：支持限速模式，可以根据网站的业务处理能力或者访问源 IP 的 QPS 制定防御规则，对所有超过阈值的请求进行有效人机识别，对垃圾流量直接封禁处理。

自定义策略定制：可以根据需要，对特定的页面或者接口进行保护，可进行秒级、分钟级防御设置。

· 合规性保障

自定义防护规则：用户可以对 HTTP 协议字段进行组合，制定访问控制规则，支持地域、请求头、请求内容设置过滤条件，支持正则语法。

访问日志审计：记录所有用户访问日志，对访问源 TOPN 提供趋势分析，可以根据需要提供日志下载功能。

网页防篡改：采用强制静态缓存锁定和更新机制，对网站特定页面进行保护，即使源站相关网页被篡改，依然能够返回给用户缓存页面。

数据防泄漏：对 response 报文进行处理，对响应内容和响应进行识别和过滤，根据需要设置数据防泄漏规则，保护网站数据安全。

· HTTP 流量管理

支持 HTTP 流量管理：可以设置源 IP 或者特点接口访问速率，对超过速率的访问进行排队处理，减缓服务器压力。

请求头管理：可以根据业务需要对请求头和响应头进行处理，可进行请求头替换或者敏感信息隐藏设置。

· 安全可视化

四大安全分析报表：默认提供 Web 安全攻击报表、CC 攻击防护报表、用户访问统计报表和自定义规则命中报表，满足业务汇报和趋势分析需求。

全量日志处理：提供全量日志查询和下载功能，可以通过 OpenAPI 接口获取实时日志或离线日志信息。

实时数据统计：提供基于均值和峰值带宽统计信息，提供攻击带宽和正常占比，随时关注业务状况。提供多种组件，了解业务监控和核心指标变化情况。

6.4 态势感知

态势感知系统，是为用户提供的大数据安全分析产品。通过数据建模、行为学习、情报关联分析，全面洞悉安全全景、发现入侵和攻击威胁，帮助用户建设自己的安全监控和防御体系。对多维度海量安全和业务数据进行快速、自动化的关联分析，通过图形化、可视化的技术将威胁和异常的总体安全态势呈现给用户。

· 量化威胁指标

提供租户业务安全状态量化指标，以攻击者视角的告警事件、威胁事件，以防御者视角的引擎覆盖率、主机漏洞事件、网站漏洞事件指标与变化。同时提供安全事件 7/30 天发展趋势，以告警、威胁事件聚合统计的 Top10 风险资产，以告警分类、威胁模型聚合统计的 Top10 威胁形态 。

· 提供事件详情与修复建议

提供基于账号资产、详情时间段、攻击类型、等级和处理状态的查询，事件详情列表，以及事件处理状态。同时提供具体事件详情和修复建议。

· 威胁事件分析

提供基于账号资产、详情时间段、攻击类型、等级和处理状态的查询，事件详情列表，以及事件处理状态。同时提供具体事件详情和修复建议。

· 攻击链分析

提供基于账号资产、详情时间段、威胁模型、等级和处理状态的查询，事件详情列表，以及事件处理状态更细。同时提供具体事件详情。根据关联挖掘时长区分实时挖掘、离线挖掘。

· 弱点事件

主机漏洞：提供基于主机漏洞详情，以漏洞为统计维度向用户展示主机弱点。督促用户修复相关漏洞。

网站漏洞：结合白帽渗透测试实战经验，通过先进的爬虫，分布式技术对京东智联云提供全面网站威胁检测服务。帮助用户缩短云资产漏洞发现时间，及时修复漏洞，一定程度上缓解黑客入侵行动的进一步发生，同时避免遭受品牌形象和经济损失。

应急漏洞：当有紧急漏洞发生时，安全运营团队会提供应急漏洞验证 POC，帮助用户快速检查服务器的健康状态，缩短云资产漏洞发现时间，及时修复漏洞。

· 资产管理

提供云上网络和主机资产关联，提供基于内外网 IP、主机 ID 和主机名称账号资产查询。提供网络检测引擎开放和关闭功能。提供和资产相关告警、威胁、主机漏洞和网站漏洞数量。

· 事件报警

通过邮件、短信报警等功能，让用户快速获取威胁事件告警。

· 安全大屏

安全大屏，主要是帮助安全运营人员做安全运营决策，主要包含态势感知总览、网络安全态势 、主机安全态势等功能。

6.5 主机安全

主机安全，是为用户提供的云主机安全管理产品。采用轻量级安全防护进程实现主机风险实时监测、安全威胁及时预警，恶意入侵精准防护，有效提升主机安全防御能力，保障云主机业务安全。

· 防暴力破解

包括远程登录暴力破、数据库防暴力破解、FTP 防暴力破解，通过系统日志、网络数据包协议分析等方式获取暴力破解的 IP，并判断其是否满足防护规则。若满足规则，则进行拦截并上报云平台，可以告诉用户当前遭受的密

码破解事件和破解结果。

· 弱口令检测

系统内置弱口令字典，根据字典规则对账号口令进行检测，通过云平台展示存在弱口令风险，提醒用户修改，避免系统账号被破解。

· 登录异常提醒

根据系统设置规则自动识别异常登录行为并预警，用户可以设置常用登录地区，当出现登录地址为非常用登录地，则产生告警记录，上报到云平台提醒用户存在异地登录风险。

· 高危漏洞检测

定期检测系统高危漏洞上报云主机漏洞详情，产品提供 Windows 系统漏洞修复功能，Linux 提供漏洞修复建议，Linux 需要手动完成漏洞修复。防止主机因为高危漏洞导致系统性风险。

· Webshell 检测

京东智联云主机安全会对服务器上新创建的 Web 程序文件进行可疑风险判断，对有风险的 WebShell 文件进行预警，用户可以根据预警信息对 Webshell 文件进行处理。

· 升级维护

主机安全进程在运行过程中，出现异常情况下（主进程死锁、挂死、死循环、资源占用过高等情况），守护进程会对主机 Agent 进行监控，同时对异常进程进行重启和升级等保护操作，防止主机 Agent 异常对主机业务造成影响；云安全团队，会定期对主机安全 Agent 和主机漏洞进行安全更新和维护，保障主机安全，此过程无需用户参与。

6.6 密钥管理服务

密钥管理服务（Key Management Service，简称 KMS）是京东智联云为用户提供的一款安全管理类产品。KMS 使用硬件安全模块（HSM）来保护用户的密钥安全。用户可安全、可控、便捷的使用托管密钥。

· 密钥管理服务

用户密钥加密托管，KMS 提供加密密钥的集中化控制。用户可以使用京东智联云控制台、OpenAPI 等工具，轻松创建、管理、轮换用户的密钥。

机密数据加密托管，KMS 同时提供机密数据（Secrets）托管的服务，用户可以将敏感信息托管在 KMS 中来保障其安全性。

日志审计，用户存储在 KMS 中的密钥的每次使用都会记录在日志系统中，记录的信息包括用户、时间、日期和所用密钥的详细信息。

· 安全与可靠性

密钥托管安全可靠，KMS 旨在任何人均无法从服务中检索到用户的纯文本密钥，该服务使用了硬件安全模块（HSM）保护用户的密钥的机密性和完整性，用户的纯文本密钥不会以任何形式存储到任何存储中，且该密钥不会传输到 KMS 服务区域之外。

高可用与容灾备份，KMS 采用实时异地备份与离线异地备份保障密钥的安全与完整性，同时采用分布式系统来保障服务的高可用性。

6.7 安全服务

· 基线检测服务

在用户充分授权的情况下，对用户云上系统进行全面的安全基线检测，帮助用户掌握云上系统整体的安全脆弱性状况，并依据检测结果与用户业务模式特点，提供有针对性的安全修补建议，降低系统的安全威胁。

· 漏洞扫描服务

在用户充分授权的情况下，对用户指定的操作系统、Web 服务、数据库等提供全面的漏洞扫描服务，由京东智联云安全专家对扫描结果进行解读，并提供专业的漏洞扫描报告和修复指导建议，帮助用户有效地降低业务安全风险。

· 渗透测试服务

对现有系统不造成任何损害的前提下，以攻击者视角，模拟黑客入侵的技术手段对用户指定系统进行全面深入的攻击测试，发现系统中潜在的风险威胁，帮助用户降低因黑客入侵带来的经济损失。

· 应急响应服务

当用户遭遇网络攻击、木马病毒、数据窃取等黑客入侵事件时，京东智联云能够提供包括抑制止损、事件分析、系统加固、事件溯源等应急响应服务，帮助用户降低安全事件对自身造成的影响与损失。

7 结论

在数字化浪潮席卷而来的当下，京东智联云致力于为政府和企业提供一体化、专业化、现代化和生态化的专有云平台，在保障安全、可靠、敏捷、高效的同时，提升用户体验，推动客户数字化转型并与其共建数字化生态。

京东智联云专有云平台自主可控，安全有保障。网络安全方面，面对大流量攻击，其抗 DDoS 防护可迅速扩展安全防护能力，轻松解决用户面临大流量攻击本地防护能力不足问题，并结合可扩展的 Web 应用防火墙，多维度保护业务安全。数据安全方面，通过京东智联云自研对象存储产品，支持超大规模存储量，同时存储数据三副本备份。

京东智联云从端到端安全合规一体化、多层次资源一体化和开发运维一体化三方面综合打造一体化的专有云平台，最大程度降低基础架构运维压力，解除 IT 系统的后顾之忧，让技术和业务专家能够将精力聚焦于业务转型和创新。

稳定和安全是旅程而非终点，京东智联云将继续以“可信可靠、安全保障、生态赋能、用户信赖”为安全服务的宗旨，致力于成为推动全球数字化转型的赋能者，为合作伙伴和用户提供安全、稳定、高可用的基础设施，专业、全方位的产品和完善、可靠的服务。

8 参考文献

[1]《京东智联云安全白皮书》，2018 年；

[2]《京东智联云数据安全白皮书》， 2019 年；

[3]《京东智联云专有云思想指导力白皮书》，2018 年；

[4]《GB/T 35279–2017 信息安全技术 云计算安全参考架构》；

[5]《GB/T 31167–2014 信息安全技术 云计算服务安全指南》；

[6]《GB/T 31168–2014 信息安全技术 云计算服务安全能力要求》；

[7]《GB/T 22239–2019 信息安全技术 网络安全等级保护基本要求》。

京东智联云

关注社交平台：

京东智联云微信　京东智联云微博

如欲了解更多信息：

欢迎登陆：www.jdcloud.com

咨询热线：400-615-1212