京东云

# 京东云安全
# 白皮书

2018/9

扫码关注下载PDF

京东云安全

## · 版权声明 ·



## · 商标声明 ·



## · 法律声明 ·

# 目录

# 01

# 京东云简介

2018 / 9

京东云（JD Cloud）是京东集团旗下的全平台云计算综合服务提供商，拥有全球领先的云计算技术和丰富的云计算解决方案经验。为用户提供从 IaaS、 PaaS 到 SaaS 的全栈式服务（Full Stack），从 IDC 业务、云计算业务到综合业务的全频道服务（Full Spectrum），以及包含公有云、私有云、混合云、专有云在内的全场景服务（Full Services）。同时，京东云依托京东集团在云计算、大数据、物联网和移动互联网应用等多方面的长期业务实践和技术积淀，形成了从基础平台搭建、业务咨询规划，到业务平台建设及运营等全产业链的云生态格局，为用户提供一站式全方位的云计算解决方案。

下页（P5- 图 1）为京东云目前基于多年业务实践形成的云计算整体架构：

2017 年云服务调查报告结果显示，用户选择云服务的最重要指标为安全稳定。京东云以用户为核心，整合京东专业的安全团队，为用户提供全方位的安全防护措施，保障用户的业务安全及稳定，让用户放心上云。京东多年的安全技术和经验效力于提供合规、安全、稳定的云计算服务，全面保障云平台安全运营能力，通过构建安全生态让用户轻松体验京东云安全能力。



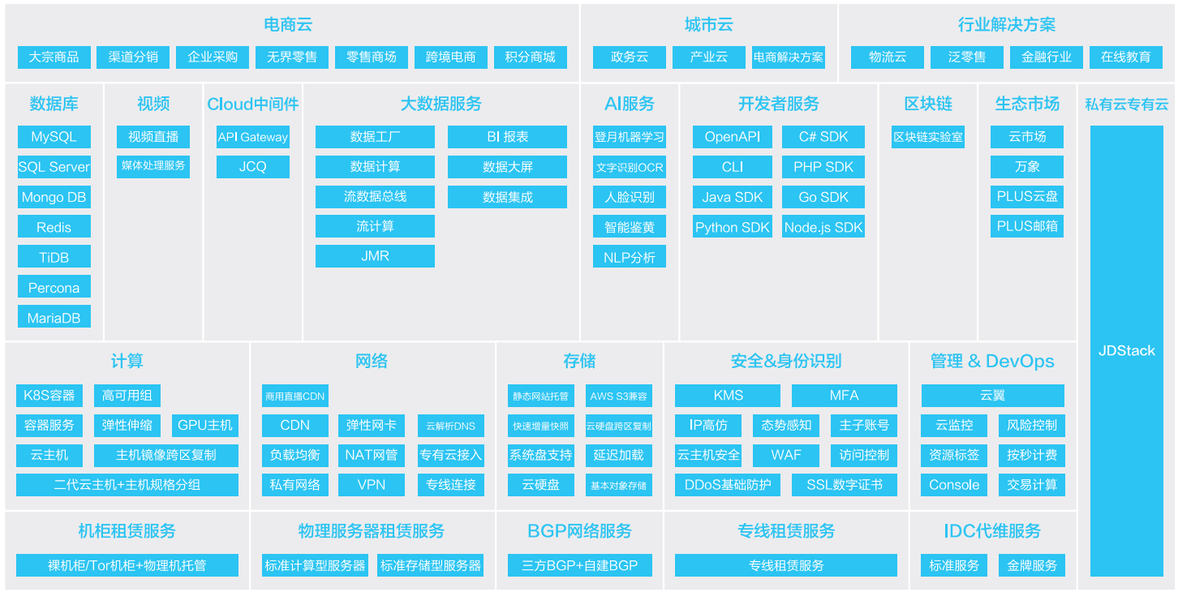


图 1 京东云产品与服务架构

# 02

# 安全责任共担

2018 / 9

安全性与合规性是京东云和用户共同的责任。京东云负责云平台自身的安全，用户负责云平台上的业务安全。

<table>
<tr><td rowspan="4">用户</td><td colspan="3">用户数据</td><td rowspan="2">用户数据安全</td><td rowspan="4">身份管理与资源访问控制</td></tr>
<tr><td>客户端数据加密&完整性验证</td><td>服务器端加密（文件系统/数据）</td><td>网络传输保护（加密/完整性/身份验证）</td></tr>
<tr><td colspan="3">平台，应用程序，身份和访问管理</td><td rowspan="2">用户平台及应用安全</td></tr>
<tr><td colspan="3">操作系统，网络，防火墙配置</td></tr>
<tr><td rowspan="4">京东云</td><td colspan="4">云主机，容器，云硬盘，云数据库，云存储，云安全<br>云操作系统</td><td rowspan="2">云平台及应用安全</td><td rowspan="4">身份管理与资源访问控制</td></tr>
<tr><td>计算</td><td>存储</td><td>数据库</td><td>网络</td></tr>
<tr><td colspan="4">京东云基础设施</td><td rowspan="2">基础设施安全</td></tr>
<tr><td>地域（Region）</td><td>区域（AZ）</td><td colspan="2">边缘站点</td></tr>
</table>

图 2 京东云安全责任共担模型



## 2.1 京东云安全责任

京东云负责基础设施、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。

## 2.2 云用户安全责任

云用户基于京东云提供的服务构建云端应用系统，并运用京东云安全的云产品和安全服务以及安全生态第三方安全产品保护自己的业务系统。云用户负责对在云平台上使用的网络、系统、应用、管理、数据、安全等服务的定制配置、自行部署及运维运营。云用户负责安全的使用云平台，确保业务的安全设计、数据保护、认证加密等必要的安全措施和功能实现，管理好账号密码和人员授权，安全的开发应用、运营业务。

# 03

# 基础架构安全

2018 / 9

京东云从数据中心自身的安全容灾，到设备的选型和测试、产品和平台的研发设计、数据和网络的访问及控制，经过了严格设计和全面测试，最终为用户提供安全、可靠、稳定易用的云服务。此外，还提供广泛的可配置安全选项以及对这些选项进行控制的功能，方便用户自定义安全措施来满足组织部署的独特要求，而满足 IT 控制策略并遵守外部法规。作为云计算服务提供商，京东云着力为每一个用户提供安全、稳定、持续、可靠的物理基础设施。

## 3.1 安全合规和隐私

京东云一直致力于完善云安全体系、建设安全合规能力、依据行业安全最佳实践和各种 IT 安全标准设计，不断完善自身的管理与机制，并通过了一系列的标准认证、第三方安全评估和审计，务求更好的向用户展提供合规、安全、稳定的云计算服务。

### 3.1.1 安全合规

京东云主要认证、测评、资质：

- ISO9001：ISO 质量管理体系认证
- ISO27001：ISO 信息安全管理体系认证
- 中国信息通信研究院“可信云服务认证”
- 中国公安部“信息安全等级保护三级”
- 工业和信息化部“ITSS 云计算服务能力标准符合性证书”





### 3.1.2 隐私保护

京东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。

用户完全拥有并可以全权控制自己的数据，包括数据的产生、收集和使用。京东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。未经用户许可，京东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。

为了更好地为用户提供安全、可信的云产品和云服务，京东云将在用户进行账号注册、管理、或实名认证等过程中适当收集用户的个人信息或企业信息，并严格按照《隐私政策》进行收集、使用、存储和分享用户的相关信息。同时，京东云的信任中心提供了全面的合规信息，希望可以帮助用户更好地理解京东云在合规方面的各种实践。

## 3.2 基础设施安全

京东云全球基础设施包括机房、网络、硬件和支持这些资源的软件。京东云全球基础设施是根据安全最佳实践以及各种安全合规性标准进行设计和管理的。数据中心的广泛地理覆盖范围使得京东云非常靠近用户，以降低网络延迟并实现异地冗余的备份和故障转移。为用户提供高可用、安全、可信的云计算基础设施。

### 3.2.1 京东云基础设施

- 遍布全球的顶级数据中心


图 3 京东云全球数据中心

· 中国大陆地域及可用区

| 地域名称 | | 可用区名称 | 所在城市 |
|---|---|---|---|
| 中国大陆地区 | 华北-北京 cn-north-1 | 可用区A cn-north-1a | 北京 |
| | | 可用区B cn-north-1b | 北京 |
| | 华东-宿迁 cn-east-1 | 可用区A cn-east-1a | 宿迁 |
| | 华东-上海 cn-east-2 | 可用区A cn-east-2a | 上海 |
| | | 可用区B cn-east-2b | 上海 |
| | 华南-广州 cn-south-1 | 可用区A cn-south-1a | 广州 |

表 1 中国大陆地域及可用区

### 3.2.2 基础设施安全

京东云执行更严格的 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 99.95% 的服务可用性。

京东云实现了 Region 区域级、AZ 可用区级、FD 故障域级容灾能力，在此基础上全线产品进一步实现了不同维度的高可用架构和稳定服务品质。

· 多地域可用区云数据中心

华北机房、华东机房、华南机房、海外机房拥有电信、联通、移动、BGP 多线接入高容量带宽动力监控系统、环境监控系统、消防监控系统、安保监控系统、网络监控系统。

· 高可用的基础设施

用户提供全球部署多地域多可用区的云数据中心，采用多线 BGP 网络提高网络接入体验，京东云分布式云操作系统为所有云产品提供高可用基础架构和多副本数据冗余。

· 持续不间断服务

全球领先的热升级技术使得产品升级、漏洞修复不影响用户业务。高度自动化的安全运维，为用户实时分析与计算，并自主响应安全策略。以确保云平台提供不间断的服务。

· 多副本冗余

京东云使用分布式存储，文件被分割成许多数据片段分散存储在不同的设备上，并且每个数据片段存储多个副本。分布式存储不但提高了数据的可靠性，也提高了数据的安全性。



## 3.3 物理与环境安全

### 3.3.1 机房物理安全

京东云制定了完善的物理和环境安全防护策略、规程和措施，满足 GB 50174《电子信息机房设计规范》A 类和 TIA 942《数据中心机房通信基础设施标准》中的 T3+ 标准。包含本章以下物理与环境安全控制要求。京东云在数据中心里包含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、例行监控审计、应急响应等措施，以确保京东云数据中心的物理和环境安全。

· 机房选址

京东云全球各数据中心均按照相关国际标准和当地安全要求进行选址、建设或租赁。

· 电力保障

数据中心的电源系统为充分冗余且可维护，保障京东云业务 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

数据中心安装了自动火灾探测及扑救设备，以减少风险。火灾探测系统利用所有数据中心环境中的烟雾探测传感器、机械和电气基础设施空间、冷藏室及发电设备室。这些区域受到湿式、双重联锁预动式或气体式喷洒系统的保护。

· 监控管理

数据中心安装配备 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。

### 3.3.2 人员访问管理

京东云制定完善的《机房出入管理制度》，从制度策略，到流程管理，并配合严格的监察审计，建立了一套全方位的安全管理体系，通过持续改进来保证云计算数据中心的物理和环境安全。

京东云各数据中心按不同级别的区域安全要求制订了严格的制度，包门禁系统、人员车辆权限及检查站，配备了 7*24 小时无盲点的视频监控告警系统并配备安保人员。

根据数据中心人员类别和访问权限，建立了完整的人员访问控制安全矩阵。明确规定公司人员出入审批管理，第三方人员出入审批管理，数据中心机房出入要求，实现对数据中心的各类人员的访问、操作等行为的有效管控。基于访问员工岗位和角色，授予员工有限的资源访问权限并遵循最小权限和职责分离原则。

所有外部人员（访客、供应商技术人员、测试人员、代维人员等）在数据中心机房等受限区域进行操作时进入机房必须由机房经理确认后方可进入机房，做好机房出入的登记，并由内部员工全程陪同，对整个过程负监护责任。

## 3.4 网络安全

京东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。京东云提供可靠的网络基础结构以支持应用程序和服务连接需求，包括 Internet 与云平台之间、云平台中的资源之间、本地资源与托管的资源之间可能存在网络连接或访问。

### 3.4.1 安全架构

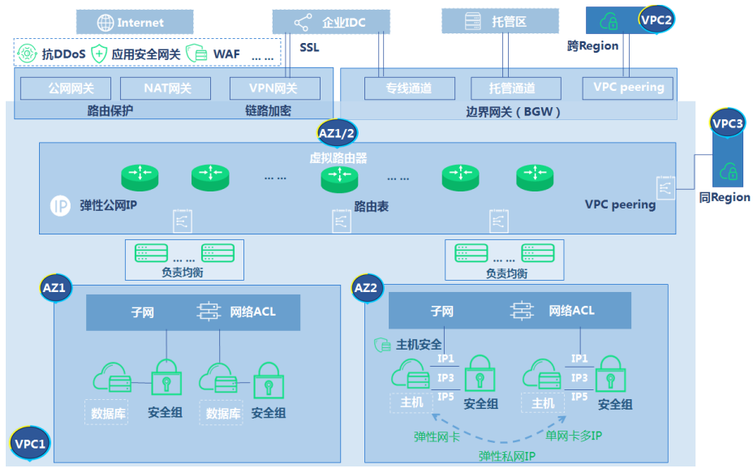


图 4 网络安全架构





在 Internet 与云平台服务、资源组之间的边界区域提供可靠的安全组件，可防止不受信任的网络访问内部网络资源。包括抗拒绝服务 (DDoS) 、应用安全网关、Web 应用防火墙 、以及 VPN 设备，同时实施防火墙策略、访问控制列表 (ACL) 或特定路由等安全策略。

在云平台网络资源提供了各种安全工具和功能创建相应的安全服务。京东云私有网络支持用户在京东云上构建逻辑隔离的网络环境，在这里用户可以自主规划网络部署，包括网络范围、子网网段、路由策略等，并通过安全组和网络 ACL 等实现多级安全防护。

### 3.4.2 边界网络安全

边界网络是在 Internet 与云平台虚拟网络之间网络区域。对于来自 Internet 的入站流量，DDoS 防护可防御针对京东云的大规模攻击，应用安全网关，Web 应用防火墙对云平台网站或 APP 服务进行安全防护。用户定义的公共 IP 地址，可以根据这些路由保护确定哪些流量可以通过云服务进入云平台虚拟网络。VPN 网关提供基于 Internet 的数据加密传输服务。

在 Internet 流量进入虚拟网络之前，云平台本身将实施两层安全性：

· 边界防护

DDoS 防护提供高效的防护能力，保证云平台网络的稳定。详情请见“4.8.1DDoS 防护”章节。

Web 应用防火墙避免网站服务器被恶意入侵，保障业务的核心数据安全。应用安全网关对云平台网站或 APP 服务进行可视化安全分析和应用层安全防护。详情请见“4.8.4 Web 应用防火墙，4.8.5 应用安全网关”章节。

· 路由保护

通过路由及策略、弹性公网 IP 、应用程序网关以及其他云平台功能启用，以便将路由到用户资源的公共 IP 地址呈现给 Internet，使用网络地址转换 (NAT) 将流量路由到云平台虚拟网络上的内部地址和端口，云服务或资源组就可以公开公共 Internet IP 地址和端口。此路径是外部流量进入虚拟网络的主要方式，可以对公共 IP 地址进行配置，确定可以传入哪种流量，如何在虚拟网络上转换该流量以及要将它路由到何处。

· 其他安全防护

> 防火墙：对传入请求实施防火墙规则或访问控制策略。

> 威胁检测和预防：检测并缓解来自 Internet 的恶意攻击。

> 审核和日志记录：维护详细记录供审核和分析。

> 反向代理：将传入请求重定向到相应的后端服务器。 此重定向涉及到将前端设备（通常是

防火墙）上的目标地址映射并转换成后端服务器地址。

> VPN 设备：充当跨界 VPN 网关，用于在本地网络上的用户与虚拟网络之间进行跨界 VPN 连接。

### 3.4.3 虚拟网络安全

虚拟网络是构建于物理云平台网络结构之上的逻辑构造。每个虚拟网络与其他所有虚拟网络相互隔离，这可帮助确保其他云平台客户无法访问部署中的流量。虚拟网络隔离可确保与其他所有网络完全隔离，而且流量只能流经用户配置的路径和方法。可以使用安全组、路由转发和网络虚拟设备来创建安全边界，以保护受保护网络中的应用程序部署。

· 流量隔离

私有网络是云平台上的流量隔离边界。 一个私有网络中的不同虚拟机 (VM) 无法直接通信，即使是由同一个用户所创建。 针对虚拟网络的入站流量，隔离可确保用户 VM 与通信在虚拟网络中保持私密性。

· 多层拓扑

虚拟网络允许用户通过分配子网并为工作负荷的不同元素或“层”指定独立地址空间，来划分多层拓扑。这些逻辑分组和拓扑可让用户根据工作负荷类型来定义不同的访问策略，以及控制各层之间的流量。

· 跨域连接

用户可以在虚拟网络和多个本地站点或京东云中的其他虚拟网络之间创建跨域连接。 客户可以使用 VNet 对等互连、VPN 网关、第三方网络虚拟设备或专线通道来构造连接。

· 安全组

用户根据所需的粒度（网络接口、单个 VM 或虚拟子网）创建规则 (ACL)。通过跨域连接或直接 Internet 通信来允许或拒绝虚拟网络内的工作负荷，以控制访问。

· 自定义路由和 IP 转发

允许用户定义虚拟网络中不同层之间的通信路径。用户可以部署防火墙、IDS/IPS 和其他虚拟设备，并通过这些安全设备来路由网络流量，以实施安全边界策略、审核和检查。

· 其他网络虚拟安全设备

云市场和 VM 映像库中提供了防火墙、负载均衡器和 IDS/IPS、堡垒机等安全设备。 用户可将这些设备部署到其虚拟私有网络，特别是安全边界（包括外围网络子网），以实现多层安全网络环境。

## 3.5 数据安全

京东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。在身份认证、权限管理、访问控制、数据加密、数据隔离、传输安全、存储安全、数据销毁等方面，保证用户对其数据的隐私权、所有权和控制权不受侵犯，为用户提供最切实有效的数据保护。

· 身份认证和访问控制

京东云提供的一项用户身份管理与资源访问控制服务（IAM）。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云资源的权限。详情请见“4.6.2 访问控制”章节。

· 静态数据保护

用户负责确保按标准加密云平台中存储的数据。云平台提供各种加密功能，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。 提供各种数据存储解决方案，以满足不同需求，包括文件、磁盘和表存储等。

· 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。详情请见“4.2.1 私有网络”章节。

· 传输中数据保护

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。

· 数据冗余

出现网络攻击或者数据中心遭到物理损坏时，可确保数据受到保护。数据可在选定的地理区域中进行复制以实现冗余，但不会传输到此区域以外。用户可以使用多个选项来复制数据，包括指定副本数量，以及复制数据中心的数量和位置。

· 数据销毁

在用户提出请求和合同终止时，京东云会执行完全数据删除。当用户删除数据或离开京东云时，将根据行业标准实践对所有退役的磁性存储设备进行消磁和物理销毁。当某个存储设备已达到其使用寿命的最后时期时， 京东云程序中包括的退役流程可防止用户数据暴露给未授权的个人。





# 04

# 云产品服务安全

2018 / 9

京东云为用户提供 IaaS、PaaS 和 SaaS 多类的云产品服务，涉及计算、网络、存储、数据库、大数据分析、应用、管理和安全等方面，为用户安全赋能、便捷上云提供保障。下面对各云服务做基本技术及安全性介绍， 具体内容可登录京东云官网 www.jdcloud.com 查询。

## 4.1 计算服务

### 4.1.1 云主机

云主机是京东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。京东云提供了多层次的云主机安全防护和保障。

#### 4.1.1.1 用户隔离

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。此外，可通过 VPN 或专线等服务将用户本地服务器与京东云主机连通，实现对现有网络部署的扩展。

#### 4.1.1.2高可用组

高可用组是京东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。

· 数据高可靠

京东云主机承诺 99.95% 的服务可用性和不低于 99.9999999% 的数据可靠性。网络架构稳定，云硬盘多副本容灾，同时提供数据及镜像的快照功能，支持整机备份。

· 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。

· 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。

#### 4.1.1.3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。

#### 4.1.1.4安全防护

· 丰富的安全组件

京东云为云主机提供一体化安全服务，包括主机安全、免费的 DDoS 基础服务、付费的 DDoS 高防、入侵检测及漏洞扫描等。

· 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 秘钥

京东云允许使用密钥加密解密基 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 客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。

#### 4.1.1.5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。

· 批量部署软件环境

对已经部署好环境的云主机自定义制作镜像，然后基于此镜像批量创建云主机，主机创建之后，拥有和之前云主机一致的软件环境，以此可以达到批量部署软件环境的目的。

· 服务器运行环境备份

对一台云主机制作镜像， 如果该云主机在后续使用过程中软件环境被损坏无法正常运行，则可以使用该镜像恢复受损的云主机。

### 4.1.2 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 技术实现不同租户实现完全隔离。

· 可靠存储

可扩展云硬盘及快照。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，将容器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。此外，可通过 VPN 或专线等服务将用户本地服务器与京东云容器连通，实现对现有网络部署的扩展。

· 弹性公网 IP

弹性公网 IP 与京东云账户关联，用户可以将其余同地域下的任意容器关联，实现容器的外网访问，同时可根据网络实际使用情况调整带宽带宽、更改绑定容器。

· 安全组

安全组是一种分布式、有状态的虚拟防火墙， 具备检测和过滤容器进出的数据包的功能。使用安全组可以完成单台或多台容器的网络访问控制，包括容器之间的东西向流量以及容器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。

· 安全镜像

支持 Docker 标准镜像，可选择 Docker Hub 下载镜像或从私有镜像仓库下载镜像。可以保存第三方镜像仓库认证信息。

· 监控管理



多维度监控，实时掌握实例运行状态，提供 CPU 使用率、内存使用率、系统盘读写流量、网络进出流量，可针对不同监控参数设置报警功能，实时预警，方便用户快速感知业务高峰及时调整实例规格。

· 日志查看

提供容器标准日志查询功能，日志最大容量为 10M。

### 4.1.3 云硬盘

云硬盘是京东云为云主机提供的低时延、持久性、高可靠的数据块级存储。云硬盘内的数据以多重实时副本的方式存储，避免因组件故障导致数据不可用，同时为用户提供高可用数据存储服务。云硬盘容量可弹性扩展，用户可以在几分钟内以低廉的价格扩充数据存储空间，并实现数据的持久化存储。

· 高性能

单盘最大提供 20000 随机 IOPS，100MB/s 吞吐量，帮助用户轻松应对业务侧高吞吐量的数据访问需求。

· 可靠性

基于数据多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。

· 易扩展

用户可以自由配置云硬盘存储容量，单磁盘容量范围为 20-3000GB，支持按需扩容。

## 4.2 网络服务

### 4.2.1 私有网络

京东云私有网络 (Virtual Private Cloud，简称 VPC)，是用户在京东公有云上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 整体架构如下：

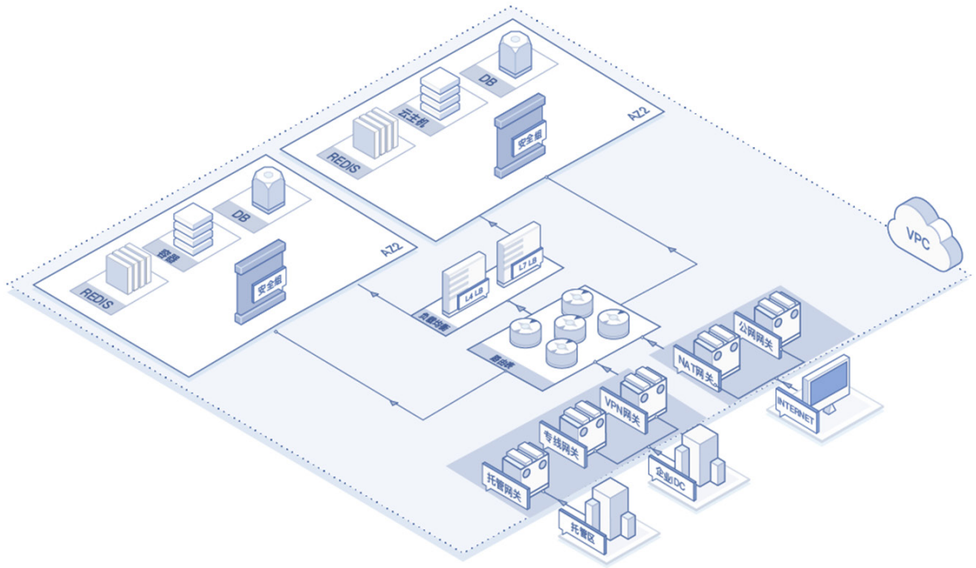


图 5 私有网络逻辑架构图

私有网络 VPC 是用户网络在京东云上的表现形式，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。

#### 4.2.1.1 自定义网络

京东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。

#### 4.2.1.2 子网路由策略

京东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。

#### 4.2.1.3 ACL

网络访问控制列表（Access Control List，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。

#### 4.2.1.4 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。可以在每个区域每个私有网络下创建 50 个安全组，每个安全组双向最多可添加 100 条规则，以满足用户对网络安全隔离的需求。

#### 4.2.1.5 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。

#### 4.2.1.6 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。京东云支持自建 NAT 网关，实现 SNAT 功能。京东云私有网络的 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。

#### 4.2.1.7 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。

### 4.2.2 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。



## 4.3 存储与 CDN 服务

### 4.3.1 对象存储服务 OSS

京东云对象存储（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。提供简单方便的 RESTful 接口与方便易用的 SDK。提供包括文件上传、存储、下载、分发、在线处理在内的全系列产品，从几字节到数 TB 的数据，提供完整的存储方案。

· 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

OSS 针对 Bucket 提供防盗链配置功能，为了减少用户存储于 OSS 的数据被其他人盗链而产生额外费用，OSS 支持设置基于 HTTP header 中表头字段 Referer 的防盗链方法。可通过控制台设置 Referer 字段的白名单，以约束访问来源。

· 跨域访问

跨源资源共享 CORS（Cross-Origin Resource Sharing ） 定义了在一个域中加载的用户端 Web 应用程序与另一个域中的资源交互的方式。这种机制让 Web 应用服务器能支持跨站访问控制，使跨站数据传输更加安全，减轻跨域 HTTP 请求的风险。OSS 提供 HTML5 协议中的跨域资源共享 CORS 设置，帮助用户实现跨域访问。

### 4.3.2 内容分发网络 CDN

京东云 CDN（Content Delivery Network），基于京东优质网络基础设施和智能云计算技术，向用户提供低成本、高性能、可扩展的互联网内容分发服务。利用广泛的节点覆盖和先进的云调度、云存储技术，将海量内容更快、更可靠地投递给互联网终端用户，降低网站运营成本，提升用户互联网应用体验。京东云 CDN 的前身是服务于京东商城的自建 CDN 平台，历经多年 618 和 11.11 等大促业务活动考验，京东云 600+ 节点广泛覆盖于全国各区域和运营商，精选全网优质基础设施，边缘节点覆盖全网、全地域，真正实现就近接流、就近推流。


图 6 京东云内容分发网络节点示意图

CDN 在访问控制、安全协议与网络攻击防护方面实现了以下功能：

· Referer 防盗链

防盗链功能基于 HTTP 协议支持的 Referer 机制，通过 Referer 跟踪来源，对来源进行识别和判断，用户可以通过配置访问的 Referer 黑白名单来对访问者身份进行识别和过滤，从而限制 CDN 资源被访问的情况。

· URL 鉴权

URL 鉴权功能是通过京东云 CDN 加速节点与用户资源站点配合实现的一种更为安全可靠的源站资源防盗方法。由 CDN 用户站点提供给用户加密 URL（包含权限验证信息），用户使用加密后的 URL 向加速节点发起请求，加速节点对加密 URL 中的权限信息进行验证以判断请求的合法性，对合法请求给予正常响应，拒绝非法请求，从而有效保护 CDN 用户站点资源。

· IP 黑名单

当用户域名受到攻击或暴力访问时， IP 黑名单可以对来源 IP 做访问限制，拒绝其访问。

· 安全防护

提供 HTTPS 加密内容分发，及强大的抗 DDoS 攻击、CC 防护等安全防护能力。

· 安全审计

日志下载：支持对过去 30 天指定域名或全部域名访问日志的查询和下载，日志打包的时间周期可以是小时粒度或是天粒度。

访客分析：可分析指定时间范围内，访问量的地域分布，以及各地域的流量、访问量、流量占比、平均下载速度、首包响应时间、命中率等信息。

热点分析：支持对热点域名的流量、访问量及带宽查询分析。

## 4.4 云数据库与缓存服务

### 4.4.1 云数据库 MySQL

云数据库 MySQL 是京东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。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。

· 高可用性

默认支持主从热备架构，故障自动转移，提供持续性的数据库访问，拥有完善的数据自动备份机制，每个实例默认每天自动备份一次，同时可根据业务情况手动创建备份，无需担心数据丢失。

· 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。

· 实例容灾

京东云为全球多个地域提供云计算服务，每个地域（Region）都包含多个可用区（AZ）。云数据库 MySQL 默认提供主从高可用架构，支持选择主从副本部署在同一可用区或不同可用区，支持可以承受机架级别的故障的可用区部署和可以承受机房级别的故障多可用区部署。

· 访问控制

设置 IP 白名单控制哪些 IP 地址能够访问 MySQL 数据库，管理员需提前对每个进入数据库的权限进行配置（读写或只读）。云数据库 MySQL 的域名访问地址，只允许内网访问。

### 4.4.2 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。

· 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。

· 主备高可用，故障自动切换

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。

· 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。

· 安全审计

基于 SQL Server 原生审计，可靠性高，审计无遗漏。审计结果为二进制格式，无法篡改。

· 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。

### 4.4.3 云数据库 MongoDB

云数据库 MongoDB 是京东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，提供三节点副本集的高可用架构，支持容灾切换，故障迁移自动完成，确保业务可用性。



· 安全特性

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。支持用户自定义 IP 白名单，从访问源进行安全控制。

· 实例容灾

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。

· 备份恢复

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。

### 4.4.4 云数据库 Percona

云数据库 Percona 是京东云基于开源的 Percona 5.7 版本构建的稳定可靠的数据库服务。数据库 Percona 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。

· 高可靠性

拥有完善的数据自动备份机制，每个实例默认每天自动备份一次，同时可根据业务情况手动创建备份，无需担心数据丢失。

· 高可用性

默认支持主从热备架构，故障自动转移，提供持续性的数据库访问，数据库自动备份和手动备份等功能有效提升数据库可用性。

· 安全模式

默认的云数据库 Percona 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。

### 4.4.5 分布式数据库 TiDB

京东云联合 PingCAP 基于国内开源 NewSQL 数据 TiDB 打造的一款同时支持 OLTP 和 OLAP 两种场景的分布式云数据库产品，实现了自动的水平伸缩，强一致性的分布式事务，部署简单，在线异步表结构变更不影响业务，同时兼容 MySQL 协议，使迁移使用成本降到极低。

· 服务高可用性

TiDB 使用多副本进行数据存储，并依赖业界最先进的 Raft 多数派选举算法确保数据 100% 强一致性和高可用。主副本故障时自动切换，无需人工介入，自动保障业务的连续性。

· 访问控制

设置 IP 白名单控制那些 IP 地址能够访问 TiDB 数据库。每个账号只能读写、只读自己的数据库。

### 4.4.6 缓存 Redis

Redis 是京东云提供的基于 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。

· 高可用性

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。

· 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。

· 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。

## 4.5 大数据分析服务

### 4.5.1 数据计算服务

京东云数据计算服务（Data Computing Service，简称：DCS）是一个全托管、低使用成本的云上数据仓库服务。数据计算服务提供开箱即用的数据管理、灵活弹性的计算资源、开放的数据





接口、细粒度的权限体系，帮助用户快速构建企业级数据分析平台，并持续聚焦在释放数据价值的工作。能够快速的解决海量数据计算问题，有效降低企业成本，并保障数据安全。

· 权限管理

系统通过 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。

### 4.5.2 JMR

JMR(JingDong MapReduce) 是一个管托集群平台，可以在京东云上运行大数据框架（如 Apache Hadoop 和 Apache Spark）或运行这些框架相关的开源项目（如 Apache Hive 和 Apache Pig），您可便捷地使用 MapReduce，Hive，Spark，Presto 等服务低成本开展大规模分布式数据计算服务和海量数据分析。

JMR 的应用场景非常广泛，可应用于数据仓库、日志分析、ETL 处理、临时性处理分析、即席查询分析、流式实时计算、数据对外服务等多个场景，从而为用户提供全面、实用、便捷的服务，能够有效解决企业数据来源和类型较为复杂、工作负载差异较大等问题。

· 深度整合

与京东云其他产品如云存储、云监控，大数据分析平台等深度整合，作为 JMR 产品中 Hadoop/Spark 计算引擎的输入源或者输出目的地。

· 安全可靠

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；集群自带高可用方案并提供集群监控管理功能。

· 全方位监控

集群主要指标：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。

集群节点指标：监控集群中的每个节点的网络状态，硬盘状态等。

集群服务进程：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。

## 4.6 管理与监控服务

### 4.6.1 云监控服务

云监控（CloudMonitor）是对用户的京东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。云监控服务能够监控云主机、云数据库 Redis 和负载均衡等各种京东云服务资源。借助云监控服务，方便用户了解在京东云上的资源使用情况、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。

### 4.6.2 访问控制

访问控制（Identity and Access Management， IAM）是京东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。



#### 4.6.2.1 用户身份管理

· 子用户管理

主账户，也叫根账户，是京东云资源归属、计费的主体，在用户注册、激活京东云时由系统创建。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。

#### 4.6.2.2 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。

#### 4.6.2.3 安全身份凭证

京东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 - MFA）

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。

### 4.6.3 DevOps

京东云 DevOps，是在京东多年技术积累的基础上，针对公有云的场景和特性，构建的一套 DevOps 产品。通过统一操作平台，打破开发和运维团队之间的障碍，提高应用的编译、上线、部署效率。可统一收集应用实例的日志，能够快速查询和检索，帮助快速定位问题，助力企业快速实现 DevOps，支撑企业业务快速稳定发展。

· 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。这也就意味着用户不用再为一两台服务器的宕机，而经历一个不眠之夜。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

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。

## 4.7 内容安全服务

内容安全基于业界领先的深度学习技术，使用海量的样本数据，能够高覆盖、准确识别各类图片，提供图片、视频，文字等多媒体的内容风险智能识别服务，可根据用户需求对产品进行优化，整合京东云其他产品，如人脸识别 , 图片鉴黄，BI 报表，用户画像等。帮助用户降低色情、暴恐、涉政等违规风险，提供准确、全面的业务安全保障。

· 智能鉴黄

智能鉴黄基于先进的深度学习和计算机视觉算法，提供精准高效的色情图片鉴别服务。可以应用于儿童安全上网、直播色情画面审核等业务场景，减少企业审核人力成本、降低违规风险。

· 文字识别 OCR 服务

文字识别 OCR 服务，能够准确获取指定图片中的文字内容，通过与涉嫌违禁相关的关键词的对比分析，能够快速图片中是否有夸大宣传、政治敏感、色情文字能内容，从而帮助管理人员进行内容审核和管控。

· 人脸识别

人脸识别是基于人的脸部特征信息进行身份识别的一种生物识别技术。应用在人脸验证（Face Verification）、人脸身份判断（Face Identification）场景，对比两张人脸图像判定相似度。

· NLP（自然语言处理）分析服务

NLP 能够将文本中特定类型的事物名称或符号识别出来，方便文本搜索与文本数据挖掘。有效识别色情、暴恐涉政、广告、辱骂等文本垃圾。

## 4.8 安全产品服务

### 4.8.1 DDoS 防护

#### 4.8.1.1DDoS 基础防护

京东云免费为用户提供最高 2Gb 的默认 DDoS 基础防护能力，在用户成功申请公网 IP 后防护为用户自动开启基础服务，根据实际业务需求，可以灵活设置清洗触发值，调整防护策略。在攻击流量超过清洗触发值后，公网 IP 将触发黑洞状态。抵御 SYN Flood、ICMP Flood 等各种大流量攻击。

#### 4.8.1.2 IP 高防

IP 高防，是依托京东云安全团队雄厚的技术力量，在京东商城多年攻击防护的实战经验上，推出的一款抗 DDoS 攻击的安全增值服务。旨在用户遭受大流量的 DDoS 攻击的情况下，保护用户服务器的安全。

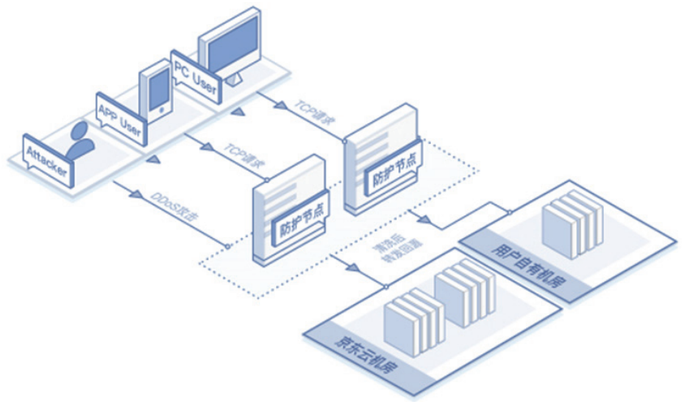


图 7 DDoS 防护示意图

根据不同用户的互联网业务需求，可提供以下 DDoS 防御能力：

· 源站隐藏

开启 IP 高防服务后，IP 高防的 IP 地址，将代理用户对源站的访问，使用户源站不再直接暴露在外，从而有效保护源站的安全。

· 防护多种类型的 DDoS 攻击

支持电信、联通、移动、BGP 等多条线路，机房集群高达 1000G+ 的清洗能力，单线支持 400G 超大防护带宽。能从容应对 SYN Flood、ACK Flood、ICMP Flood 等各种类型大流量 DDoS 攻击和 CC 防护。

· 快速接入，弹性防护

只需用户在 DNS 服务商处， 将待保护的域名在 CNAME 解析到京东云 IP 高防服务上，即可完成接入。

开启弹性防护后，当用户受到的攻击超过购买套餐的峰值时，用户的业务仍可继续得到京东云的防护。使用弹性防护功能，用户无需再担心因为攻击超过套餐峰值导致服务中断的问题。

· 全业务支持

非网站类 + 网站类场景全面覆盖，支持 TCP/UDP/HTTP/HTTPS 协议，覆盖金融、电商、政府、移动 APP 等各种业务场景。

### 4.8.2 主机安全

主机安全是京东云基于京东云安全在电商防御和安全大数据分析方面的积累，推出的云主机安全管理产品，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，提供包括高危漏洞检测、异地登录提醒、Webshell 查杀和暴力防破解在内主机防御和检测功能，保障公有云主机安全。

· 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。

· 异常登录提醒

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。

· 防暴力破解

有效阻断暴力破解行为，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、端口等方式获取尝试暴力破解的 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。

· 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 提供漏洞修复建议需手动完成漏洞修复。

· Webshell 检测

京东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。

### 4.8.3 态势感知

云态势感知（Cloud Situation Awareness）是一种基于公有云计算环境的、在用户充分授权的情况下，收集各个安全组件的海量数据，通过大数据关联分析和机器学习技术，从全局视角提升对安全威胁的发现识别、理解分析、响应处置，最终提供用户安全决策能力。

云态势感知具有以下功能：

· 安全能力

提供安全事件闭环处理工作流，探测应用层攻击、暴力破解、系统弱口令等 25 种安全威胁并且提供详细证据和安全建议，提供免费的上百种威胁模型。

· 数据接入能力

提供云基础防护 DDoS 检测数据，网络入侵检测引擎数据，主机入侵检测引擎数据。

· 大数据分析能力

提供海量重复事件聚合能力以及定向攻击关联分析。

· 威胁概览

提供用户业务安全状态量化指标，提供以攻击者视角的单一攻击事件、定向攻击事件，以防御者视角的安全引擎开启覆盖率、弱点事件指标与变化。同时提供 Top10 被攻击资产，Top10 威胁分类 。

· 单一攻击事件分析

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，以及事件处理状态更细。同时提供具体事件详情和修复建议。

· 定向攻击事件分析

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。

· 弱点事件

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。

· 云上网络和主机资产关联

提供云上网络和主机资产关联，提供基于内外网 IP 查询，以及网络检测引擎开放和关闭功能。

### 4.8.4 Web 应用防火墙

Web 应用防火墙 (Web Application Firewall, 简称 WAF) 是京东云推出的专业的安全防护服务。可以防御 SQL 注入、XSS 跨站脚本、常见 Web 服务器插件漏洞、木马上传等 OWASP 常见攻击，抵御恶意 CC 攻击 , 避免网站资产数据泄露，保障网站的安全与可用性。

京东云 WAF 服务多地域部署。每个 WAF 接入节点采用 BGP 多线接入，智能选择最优路径，毫秒级响应延迟。能根据源站地址列表智能选择访问体验最优的 WAF 接入节点。站点无须安装任何硬软件，只需修改 DNS 记录，即可对网站开启防护。并且支持配置 WAF 为旁路观察模式，对于攻击请求只记录日志不阻断，便于用户观察 WAF 在实际业务中的工作情况。

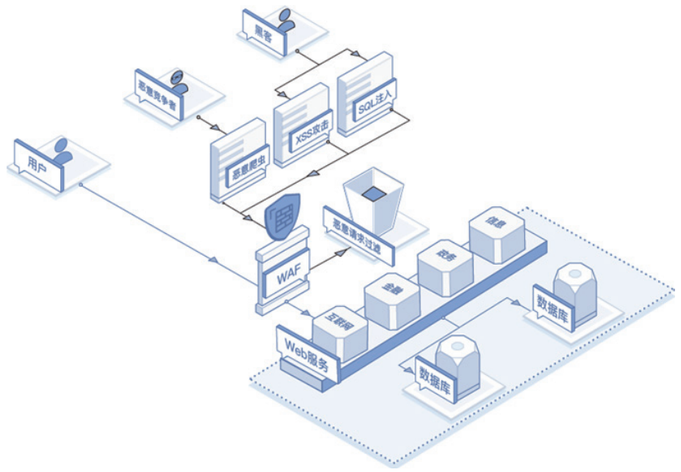


图 8 Web 应用防火墙安全防护示意图

WAF 主要功能：

· 网站隐身

通过域名 DNS 牵引流量，不对攻击者暴露源站地址，从而有效保护源站的安全。

· 常见 Web 应用攻击防护

防御 OWASP TOP 10 常见威胁攻击，包括但不限于：SQL 注入、XSS 跨站、Webshell 上传、后门隔离保护、命令注入、非法 HTTP 协议请求、常见 Web 服务器漏洞攻击、核心文件非授权访问、路径穿越、扫描防护等。

· CC 攻击防御

对单一源 IP 的访问频率进行控制、重定向跳转验证、人机识别。通过建立威胁情报与可信访问分析模型、快速识别恶意流量。

· 精准访问控制

支持 IP、URL、Referer 等 HTTP 常见字段的条件组合，轻松依据需求，设置精准访问控制策略，

识别可信与恶意流量。

· 0day 补丁定期及时更新

及时更新最新漏洞补丁，第一时间全球同步下发最新补丁，对网站进行安全防护。

### 4.8.5 应用安全网关

应用安全网关（VPC-WAF）是基于京东云高性能负载均衡集群的 Web 应用安全防护产品，通过提供 WAF 功能、业务安全可视、BOT 行为管理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 Web 或 APP 业务因攻击导致的异常或合规性问题。

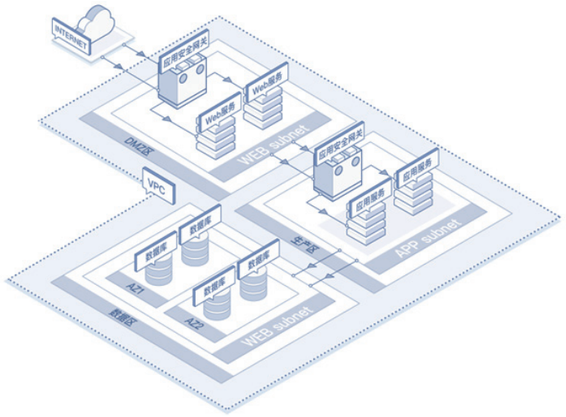


图 9 应用安全网关防护示意图

应用安全网关主要功能：

· Web 应用防火墙

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

京东云应用安全网关提供多种 CC 防护模式，通过 Cookie 验证、验证码挑战等更多种挑战验证算法，能够有效的防护 CC 攻击行为。通过自定义 CC 规则，能够对特定 URI 或页面进行 CC 精细化防护，满足大型 Web 站点特定页面的应用层 DOS 防护需求。

· 精准访问控制策略



支持自定义检测：支持灵活的检测对象定义，包括任意 HTTP 协议字段与 HTTP BODY 字段，支持各种检测运算。

支持条件组合检测：支持多个检测条件的逻辑组合，以支持复杂规则的定义。

支持防护规则自定义：提供全面覆盖复杂应用交互场景的自定义规则，能作用于具体的防护对象之上，大大提高了规则的有效性和精准度。

· BOT 管理

对搜索引擎爬虫行为，进行友好和恶意判断，对恶意的机器行为进行甄别和处置，有效提供网站运行的稳定性。通过对 HTTP 协议分析和大数据建模，对暴力破解、拖库、撞库等机器人行为进行分析和和处理，保障网站业务安全。

> 预定定义 BOT 行为管理： 支持爬虫防护、暴力破解防护等功能，有效保障网站业务安全。

> 自定义 BOT 管理策略： 用户可以根据 Web 站点的业务特性，添加自定义 BOT 规则，选择访问频次和动作类型，对特定的关键字或者 URI 进行机器人行为判断，提供业务防护准确性和有效率。

· Web 站点合规性

京东云应用安全网关提供通过提供网页防篡改、敏感信息防泄漏、协议合规性检查等功能，提供 Web 站点合规性检查和防护。

· 业务安全可视化

> 攻击分类报表：攻击类型分布一目了然，针对攻击类型分类，制定安全加固策略。

> 攻击趋势图：查看攻击趋势图，了解黑客对业务的关注程度。

> CC 攻击防护趋势：CC 攻击趋势统计，实时查看防护效果和统计。

> 访问控制趋势 : 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。

· 便捷管理

> RESTfulAPI 支持：提供全套 RESTfulAPI 接口，可实现页面自定义。

> 无 DNS 修改：无需修改 DNS 实现业务防护和监控，和负载均衡一起实现证书自主管理和 SSL 卸载功能。

### 4.8.6 SSL 数字证书

京东云 SSL 证书（JD SSL Certificates）提供证书上传、下载、管理等功能，在云上可签发 Symantec、GlobalSign、GeoTrust 证书，为网站、移动应用提供完善的 HTTPS 解决方案，提

升网站的可信度，有效防范劫持、篡改和监听等攻击行为，使业务安全保护和优良体验如影随形。同时，SSL 数字证书产品可为京东云和互联网用户提供丰富的证书品牌和证书类型，支持云上证书对生成、证书申请签发和续费， 还可以提供证书管理和详情查看，支持与京东云平台上其他产品业务进行绑定（如负载均衡、CDN），为京东云用户提供一站式证书安全存管和便捷使用的服务。

· 网站安全防护

实现网站 HTTPS 化，加密用户与网站间的交互访问，强化网站用户侧可信展示程度，有效防范会话劫持、恶意监听。

· 在线证书签发

可以在一个京东云平台购买不同品牌、不同类型和不同安全级别的数字证书，可以按照不同使用需求和习惯购买适合自己业务的数字证书。

· 在线证书管理

提供在数字证书管理功能， 用户可以在京东云平台查看所有证书的情况，包括证书类型、域名信息、证书颁发时间、证书到期时间等。

### 4.8.7 密钥管理服务（KMS）

密钥管理服务（Key Management Service，KMS）作为安全管理服务产品。借助密钥管理服务，用户可以安全、便捷的使用密钥，专注于业务需要的加解密功能场景及应用。

京东云 KMS 为用户提供的功能如下：

· 密钥管理与轮换

用户主密钥 CMK 管理，提供云上密钥的全生命周期管理，包括创建、禁用、轮换、删除等。

数据密钥，提供数据密钥 DEK 的生成、加密、解密，用于云上数据的加解密。

服务密钥，KMS 会为云上服务（如 OSS、EBS、RDS）的加密创建服务密钥。

· 数据加解密

KMS 提供小数据加解密与信封加解密两种使用方式。对于小于 4K 的数据，用户可以直接使用 CMK 对数据进行加解密，对于超过 4K 的数据，用户可以使用信封加密的方式对数据进行加解密。

KMS 已实现与云上多种产品集成，用户可以使用自己的 CMK 对云上产品的数据进行加密，即可实现云端数据的加密存储。

· 机密数据加密托管

机密数据托管，是一种私密数据加密管理服务，使用服务密钥对指定机密数据进行加密存储，



以标识 ID 代替明文数据进行访问应用程序、服务和 IT 资源所需的私密信息。借助该服务，用户可以在整个生命周期内，轮换、管理和检索数据库凭证、API 密钥和其他机密信息。用户和应用程序通过调用 API 来检索机密信息，从而无需对明文形式的敏感信息进行编码。

· 多用户与细颗粒度应用授权，弹性分配资源

基于京东云 IAM 系统角色授权，KMS 可以支持多用户的应用与身份鉴权。只有通过身份认证与应用操作鉴权，才可以对 KMS 存储的 CMK 进行操作。另外 KMS 对 CMK 进行了东西向隔离，每个用户只能访问与管理自己的 CMK，无法操作其他用户的 CMK，保证用户密钥的安全。

· 密钥 HSM 硬件模块保护

KMS 创建的密钥都会由服务端 HSM 硬件模块提供保护，并且由硬件产生真随机数，保障密钥的随机性。

· 支持 API 调用

KMS 提供丰富的 API 接口，用户可以根据自身需求进行调用，并且支持对 API 资源操作的鉴权，保障对资源操作的可靠与安全。

· 操作日志审计

对密钥的所有操作，都会产生日志并记录在服务端，用户可以对全部操作进行审计。

· 高可用性与容灾备份

KMS 通过完善的技术方案，保障服务的高可用性，并且拥有完善的容灾与备份措施，以保障密钥不会因为不可抗力而丢失。

# 05

# 运营管理安全

2018 / 9

## 5.1 流程管理

### 5.1.1 SDL 流程

京东云非常注重内部流程的安全性。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。京东云的安全开发基于业界安全开发的最佳实践，并专门针对其中的几个环节做了优化。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。

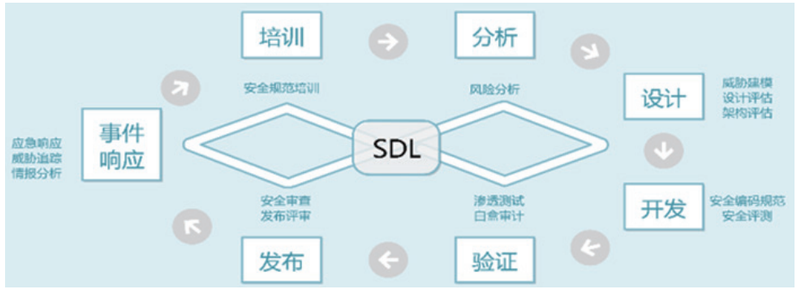


图 10 京东云安全开发流程示意图

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适当的安全培训，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 owner 进行沟通，确定安全的要求和需要做的事情，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，需经过产品安全部的最终审查后，产品才能发布到线上环境。安全团队发现存在安全需求落地执行不到位等情况时，将告知项目组产品的发布流程终止。

· 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。

### 5.1.2 运营运维流程

京东云运营管理团队的运维流程包括发布管理，变更管理，问题管理，和配置管理。发布管理是对产品服务上线前到上线后的准确流程。变更管理是针对生产环境中的变化，提出的有序流程。问题管理包括漏洞管理、事件处置流程和应急响应流程。配置管理则是对业务中所需的所有组件做配置的管理。

## 5.2 风险管理

京东云通过十多年互联网电商安全经验自主研发的云安全运营平台，通过多层次、多维度的实时监控和离线分析，为云用户提供体系化的安全服务，解决出现的各种突发性安全事件，以增强云用户业务系统的抗风险能力，防止系统发生重大安全事件。并根据漏洞提供有针对性的安全修复方案，尽最大可能确保云用户业务系统在上云后不发生安全入侵事件，系统能够安全可靠的运行和帮助云用户安全。

为保障数据中心基础设施及云平台的安全稳定运行， 由京东云安全团队负责云平台日常运行与维护，并提供云平台的技术支撑及远程维护工作。京东云安全运营机制可以及时获知最新网络安全、监管、攻防手段，会在第一时间处理相关安全事件，保证京东云平台的安全稳定及用户数据业务安全。

京东云安全运营服务体系主要分为两大板块：

· 基础安全运营服务：依托平台防护体系提供的基础安全运营服务，为用户提供更专注、更

可靠的基础安全运营服务。

· 增值安全运营服务：在基础安全运营服务之上建立高级、定制化的保障服务，为用户提供更为专注性的服务。包括用户上云安全保障服务、高级应急响应服务、安全培训服务、安全咨询等服务。

### 5.2.1 资产管理

京东云致力于为用户掌握和可视化展现全网网络的全部网络设备资产信息。资产维护包括资产的发现以及资产管理，资产发现提供了一套切实有效的资产探知系统，采用以大数据为基础的空间扫描技术，获取用户位于不同站点的所有资产信息。资产管理对所有资产信息集中管理， 提供统一的管理平台，为用户掌控、监察资产建立了完善而科学的资产维护体系。

### 5.2.2 权限管理

京东云团队为保障云平台的平稳运行，建立了一套严格的、细粒度的权限管理机制。结合自动化的运营管理机制，京东云提出了统一的云安全运维规范，所有对产品的运维操作都受到严密的权限控制和监控。

京东云要求权限管理分离到具体的运维操作，例如操作内容的平台化管理时，要求操作步骤按照操作规范，且经过 2 人以上评估通过后方可发起操作，并禁止在线上环境测试操作内容。京东云同样看重每位运营管理团队成员的权限管理，对于职责必须的权限，例如堡垒机管理审计权限，京东云要求运维人员的堡垒的管理审计权限必须每隔三个月重新申请一次。对于职责转变的情况，京东云将立刻撤销与该员工原职责相关的权限。

京东云为保障运维管理的安全质量，十分关注运营管理团队的安全意识培养。运营管理团队为每一位新加入的成员指派导师，导师均是行业内经验丰富的安全专家，导师对运维操作结果负责。京东云定期为运营管理团队做安全意识培训，定期进行运维操作规范更新及团队规范学习，使团队的安全意识和安全技术可持续的增长。

### 5.2.3 业务连续性管理

京东云十分关注用户的业务连续性，最大限度避免问题给用户的业务运行造成影响。京东云提供 DNS、负载均衡等网络服务；应用、数据库、缓存、云存储、云硬盘等均采用集群架构部署，保证各个应用层、数据层、网络层等多个层次均具备冗余和高可用能力，保障业务连续性。京东云针对不同场景，精心为用户设计了基础架构、信息架构和应用结构的不同业务解决方案，提供业务连续性和灾难恢复管理服务。

## 5.3 安全运营

### 5.3.1 安全情报

京东云建立了多层次立体的安全情报系统。结合内部的威胁情报分析系统，京东云将在互联网中关联分析网络攻击的特征，即时定位到网络攻击的源头。京东云的安全情报信息收集来自权威机构认证的外部威胁情报源，包含安全事件的信息、威胁事件的级别、IP 地址信誉等等。内部情报分析来自于京东的态势感知系统，可以收集到具体的操作日志和威胁特征等。

### 5.3.2 漏洞管理

京东云的漏洞管理包括漏洞感知、漏洞响应机制。京东云安全运营团队依托强健完备的漏洞管理平台，确保从基础设施、服务器，网络设备，操作系统，应用系统和云服务的自研和第三方漏洞在 SLA 时间内完成响应和修复，保障用户业务不受漏洞影响的风险。

京东云的漏洞感知系统利用安全扫描评估工具扫描公有云服务器及重要的网络设备，以对网络设备进行安全漏洞检测和分析，对识别出的能被入侵者利用来非法进入网络或者非法获取信息资产的漏洞，提醒管理员，及时完善安全策略，降低安全风险。

漏洞感知的流程中遵循以下原则：

· 规范性

安全扫描的实施由专业的安全扫描人员依照规范的操作流程进行，对操作过程和结果要提供规范的记录，并形成完整的服务记录、报告和成果。

· 可控性

安全扫描的工具、方法和过程要在双方认可的范围之内，保证双方对于服务过程的可控性。安全工程师要在双方认可的情况下提供服务支持。

· 最小影响

确保安全扫描工作对本项目范围内系统和网络正常运行的可能影响降低到最低限度，不会对网络的运行和业务的正常提供产生显著影响。

京东云的漏洞响应工单系统，直接接受漏洞感知系统的漏洞报警。应急响应团队初步确定入侵

路径、木马行为、是否影响数据、影响范围、感染用户（OA），危害级别、影响范围、漏洞利用场景，排查方案，并结合京东的相关应用场景，初步确定是否为安全事件，及事件等级（特大、重大、严重、一般），第一时间响应。

应急响应团队与业务方研发、业务运维和 IT 资源服务安全官和涉及人员共同参与讨论止损策略可行性、受影响环境规模、进一步确认风险、业务环境等。同时，应急响应团队针对该漏洞，结合外界信息和专业分析，确定修复方案。

### 5.3.3 安全响应

云安全事件是由于自然或者人为以及软硬件本身缺陷或故障的原因，对品牌、数据、用户、财务、业务、系统造成危害，或对社会造成负面影响的事件。一般特指因黑客入侵系统造成的安全事件。这些攻击行为包括但不仅限于植入病毒和后门、IDC 服务器多台机器感染木马、被挂 Webshell 等成功控制服务器行为。

京东云安全运营团队会从事件发现之前，对入侵的可能：隐患、漏洞、风险、盲点做整改并推进，减少安全事件的发生。一旦安全事件发生，安全运营团队第一时间发现该入侵情况，发现立即响应。安全运营团队评估事件的影响范围和危害程度，根据安全事件的影响范围和危害程度进行紧急处置，深入分析安全事件的根本原因；进一步调查处理事件涉及的业务和系统，降低事件影响和损失。针对存在问题和隐患的系统，进行安全修复及复测；帮助用户快速解决安全问题。

## 5.4 监控与审计

京东云要求对内部运营管理团队的运营操作实现全自动监控，监控范围覆盖内部、外部的关键服务组件，关键上下游服务组件等。监控对不同的服务组件设置了内存、磁盘、网卡等核心资源使用率等监控，设置更为严格的异常阈值线。及时告知运营团队通过错误统计结果，快速评估解决问题。监控的新增、删除、编辑需要有明确的流程，监控新增要明确监控等级、目标、监控接收人、异常处理预案，确保警报发生时的应急响应计划能第一时间进行。为了确定监控的有效性，京东云会定期触发测试报警进行监控有效性确认。

京东云自主研发一套基于服务树角色授权的线上机器认证登录系统，通过该系统对云平台所有的主机进行访问控制、操作历史记录等。运营管理团队人员通过该系统对服务器进行运维操作时，一旦出现高危命令，该系统能实时审计报警。统一日志审计系统将运营管理团队的所有后台运维操作记录加密存储，内部审计团队定期对运维操作记录进一步审核。

安全运维中应针对用户管理、系统认证、系统授权、系统登陆、数据获取 / 访问 / 修改等行为有完整的日志记录。记录内容包含如下必要信息：日志标签、时间、操作、用户 ID、用户名、用户组、IP 地址、访问方式，访问内容、访问结果。确保日志字段能够定位用户对组件访问时的具体操作。安全日志按照规定留存事件不少于 180 天。

## 5.5 服务支持

京东云的运营安全能力完备强大，可以提供全天候 7x24 小时专业技术支持服务，以及强大的解决方案支持能力，最大化满足用户需求。在标准服务的基础上，针对大型用户或特殊用户， 京东云能够确保提供一对一的专家服务，帮助用户更好地应用京东云提供的云产品。

京东云 365 天全方位为用户护航，为用户建立短信、邮件、站内信、公告等渠道推送通知、告警和安全事件等。

# 06

# 京东云安全生态

2018 / 9

云安全不是靠单一某个企业就能全部完成，云安全需要有云服务供应商、安全合作伙伴与用户的共同打造。希望通过构建云服务安全生态与云服务安全大数据共享平台来提升整个中国云计算安全服务能力，让的安全合作伙伴从单一安全产品功能和性能的比拼升级到云计算安全数据运营能力竞争，从业务角度洞悉安全问题，做到全面覆盖、合作共赢。

· 云安全生态构建

京东云为了保障云平台的安全，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，以及业界最优秀的第三方安全厂商打造完整的安全生态圈，实现云平台，网络，系统，数据和应用系统安全的全面覆盖。

· 大数据共享

京东云具有最佳的业务数据分析实践，结合信息安全行业特点，将为第三方安全合作伙伴打造云平台上的安全大数据分享平台， 包括安全运营数据的分享与安全大数据分析平台的共享，实现智能化的安全大数据分析和业务层面的用户安全态势分析。

· 预见无限可能，共建安全生态

京东云搭建公正、透明的渠道合作体系，在销售支持、技术支持、市场支持、商机支持、培训支持等方面，为合作伙伴提供全方面的业务支撑，并本着“不碰用户、不碰数据、不碰应用”的原则，与安全合作伙伴能力共享、资源共享、利润共享、生态共享，与合作伙伴展开深层次的合作，创造全新的“互联网 +”解决方案，培养行业基因，将积极联合全球安全伙伴打造一个开放、协作、共赢的云端安全生态圈。

京东云

预 见 无 限 可 能

关注社交平台：

京 东 云 微 信　京 东 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