合众数字化资产管理系统在京东云上的最佳实践

· 法律声明 ·

本文档仅供用户相关技术信息指引，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，京东云不承担任何法律责任。

由于产品版本升级、调整或其他康因，本文档内容有可能变更。京东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。

目录

1 摘要 4
2 在京东云上运行合众数字化资产管理系统的好处 5
3 京东云基础介绍 5
3.1 地域与可用区 5
3.2 云主机 6
3.3 云数据库 RDS 6
3.4 网络负载均衡 6
3.5 云硬盘 7
3.6 云镜像 7
3.7 私有网络 7
3.8 资源编排 7
3.9 对象存储服务 7
4 合众数字化资产管理系统介绍 8
5 合众数字化资产管理系统在京东云上的最佳实践 8
5.1 网络最佳实践 9
5.2 可用性最佳实践 9
5.3 可扩展性最佳实践 10
5.4 安全性最佳实践 10
5.5 灾难恢复最佳实践 11
5.5.1 京东云上的跨地域灾难恢复 11
5.5.2 将本地或其他云上部署的应用恢复到京东云 12
6 京东云安全模型 13
6.1 责任共担模型 13
6.2 访问控制 14
6.3 监控与日志 14
6.4 网络安全 14
6.5 数据加密 15
7 结论 15
8 文档作者 15
9 参考 15

1 摘要

本文档覆盖了合众数字化资产管理系统部署到京东云所涉及的各个方面。希望能帮助企业利用京东云的各种云服务和特性运行好合众数字化资产管理系统。

2 在京东云上运行合众数字化资产管理系统的好处

1. 不再需要容量规划。传统的 IT 环境下，上线业务需要对未来的业务容量进行细致的规划，事实上仍然没法准确估计。会造成如下结果，如果估计的过高，实际业务容量达不到购买的设备容量，会造成资源的浪费；如果估计的少了，严重影响业务运行。将应用部署到京东云上后，初始可以配置很小的容量，随着业务发展，快速扩展资源容量满足业务需求。
2. 充分利用云的弹性。在本地部署的环境下，你必须为应用准备硬件、软件、网络监控等等资源，为了应对硬件的失败，还必须保证软件、硬件有必要的冗余。如果应用部署到京东云上，可以利用负载均衡服务、高可用组、多可用区等服务能力构建一个可用性高、易扩展的应用。
3. 灾难恢复。传统的灾难恢复方案，如两地三中心方案，为了较低的 RTO 和 RPO，需要部署大量的冗余设备，产生很多沉没成本。受益于京东云的按需付费等特性，以及我们在后文中所述的灾备方案，客户能够以一个相对较低的成本获得灾难恢复的能力，保证业务的连续性。
4. 缩短应用的上线周期。在传统的应用上线模型中，新上线业务或业务增加，都要扩容，如增加服务器、硬盘、内存等等，扩容的周期是非常长的，里面任何一个环节都会造成上线周期增长，不利于业务快速应对市场的响应。
5. 高可用性。高可用是关键业务的重要指标。在京东云的可用区范围内，云主机具有 99.95% 的可靠性，通过将业务云主机分布到多个可用区，能够实现更高的 SLA。业务的关键数据通过远程同步或异步复制技术自动将数据同步到备主机实例。这些自动化技术让京东云上的应用成就了更高的可用性。
6. 京东云可以促进低成本快速创新。当客户有些新的想法需要实践时，传统的环境下，资源按照计划供应的，从新的想法到上线可能需要数月时间，如果在京东云上进行创新实验测试，可以在几分钟内构件好创新所需的基础环境，快速测试，快速验证闭环。而且云上的资源是按使用量计费，相对传统硬件环境的成本极低。

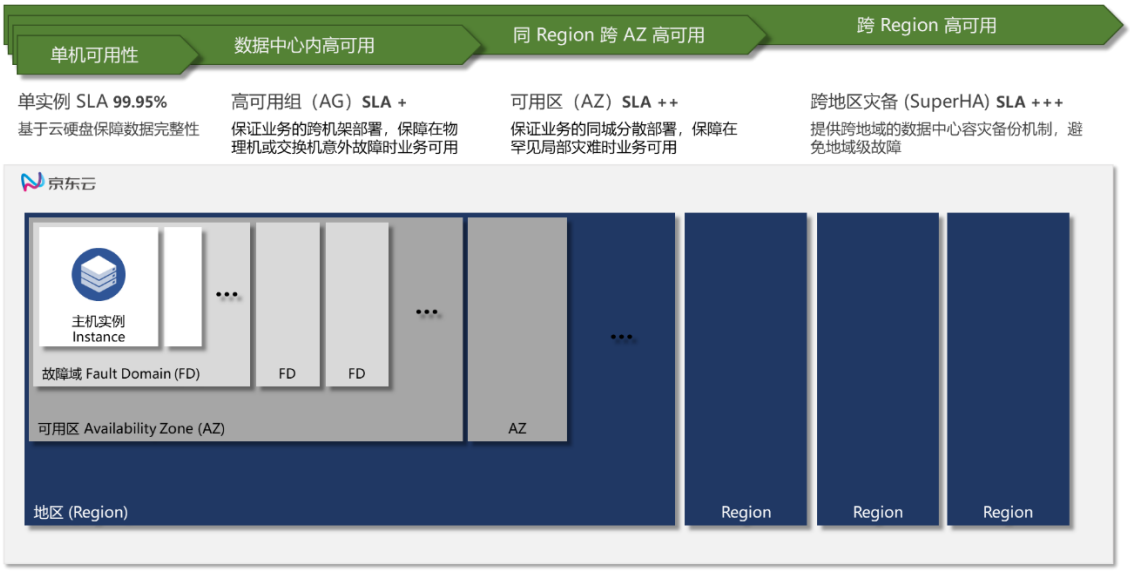
3 京东云基础介绍

京东云是京东旗下的云计算综合服务提供商，拥有全球领先的云计算技术和完整的服务平台。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方面的长期业务实践和技术积淀，致力于打造社会化的云服务平台，向全社会提供安全、专业、稳定、便捷的专业云服务。

3.1 地域与可用区

京东云云主机机房分布在全球多个位置，这些位置称为地域。每个地域（region）都是一个独立的地理地域，每个地域都是完全独立的。

京东云支持您在不同地域部署云业务，同时为了避免单地域部署可能带来的单点风险，建议在部署方案设计阶段考虑多地域多可用区部署。可用区（Availability Zone）是电力及网络之间互相独立的物理区域，相同可用区内的实例之间较之同地域不同可用区内实例之间的网络延时更小。同地域内不同可用区之间提供内网互通环境，可用区之间可做到故障隔离。
高可用组(AG)是京东云提供的业务高可用部署解决方案，是计算资源逻辑集合。提供了组内单元在数据中心内横跨多个故障域（Fault Domain，简称 FD)均衡部署的机制，示例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实例，您的业务仍为可用状态。故障域间故障隔离，最大程度规避了局部故障对高可用应用整体的影响。



3.2 云主机

云主机（Virtual Machines,VM）是京东云提供的一种基础计算服务单元，提供处理能力可弹性伸缩的计算服务。京东云提供超大内存云主机，独享 1464GB DDR4 内存，满足对数据交换速度和内存容量有极高要求的大型业务部署场景。支持官方镜像，客户私有镜像/共享镜像，和云市场第三方镜像等丰富镜像来源。

3.3 云数据库 RDS

云数据库 RDS 是京东云基于全球广受欢迎的 MySQL, Percona, MariaDB, SQL Server, PostgreSQL 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 RDS 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，彻底解决数据库运维的烦恼。

3.4 网络负载均衡

网络负载均衡（Network Load Balancer，简称 NLB）是京东云自主研发、专注四层业务服务的负载均衡产品，支持过亿并发连接和每秒百万级新建连接的高性能、低延时、会话保持等能力。

3.5 云硬盘

云硬盘是京东云为云主机提供的低时延、高持久性、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，同时为您提供高可用的数据存储服务。云硬盘容量可弹性扩展，您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。云硬盘可以挂载到云硬盘所在数据中心的任何运行中的云主机上，云硬盘通常适合于需要频繁更新的数据（如文件系统、日志、数据库等），具有高可用、高可靠、高性能的特点。

3.6 云镜像

云镜像是实例运行环境的模板，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实例，也可以根据需求从任意多个不同的镜像启动实例。

3.7 私有网络

京东云私有网络(Virtual Private Cloud，简称 VPC)，是您在京东公有云上自定义的逻辑隔离的网络空间，与您在数据中心搭建的传统网络类似，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。另外，您可以通过 VPN\专线接入，打通您的 IDC 内网和京东云网络，实现应用的混合云部署，以及将应用平滑地迁移至云上。

3.8 资源编排

资源编排是一项简化云计算资源管理和运维的服务。用户通过模板描述多个京东云资源的配置信息和依赖关系，通过模板创建资源栈，自动完成所有资源的创建和配置，以实现资源的统一管理和自动化运维等目的。 服务本身免费，仅收取所使用资源的费用：如云主机、公网 IP、云数据库实例等。

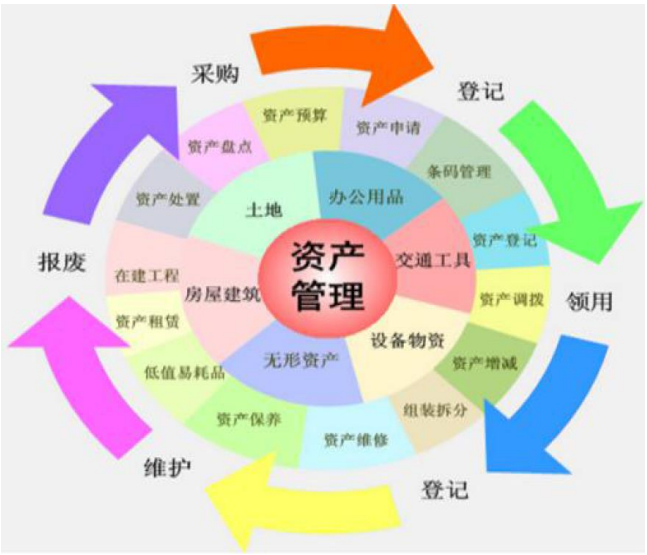
3.9 对象存储服务

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。京东云对象存储提供包括文件上传、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，都能够为您提供完整的存储方案。

4 合众数字化资产管理系统介绍

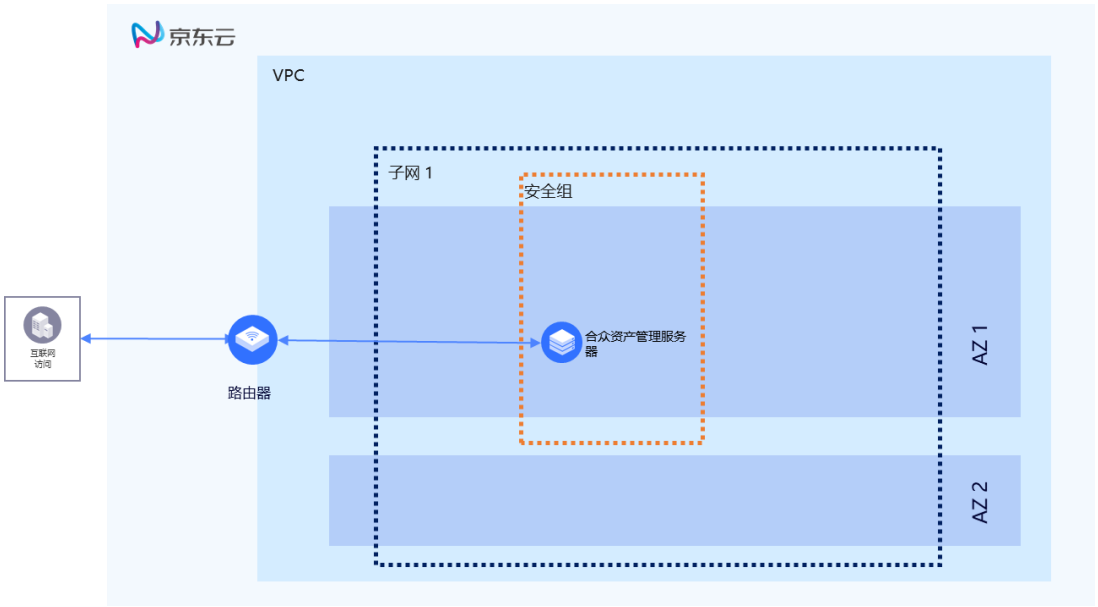
合众资产管理，汇聚数千家不同领域企业的资产管理成功实践，推出新一代的“云+端”资产管理解决方案。线上结合线下的方式为您提供资产的全生命周期管理，让我们为您的资产贴上专属的条码，通过微信和 PDA 扫一扫即可获知资产的相关信息,资产归属问题迎刃而解。全员手持扫描枪或者手机即可对资产进行量盘点，盘点数据实时传递。

通过现代的 4G 技术和二维码技术结合。通过简单的场景化体验，来感受：从资产申购——资产入库——资产申领——资产转换——资产盘点——资产维修维护保养——资产价值的全生命周期管理。



5 合众数字化资产管理系统在京东云上的最佳实践

下图是一个合众数字化资产管理系统在京东云上的部署案例，此部署案例中，合众数字化资产管理系统部署采用单服务器部署模式，也可将数据库分离部署，有助于提升应用的可用性。



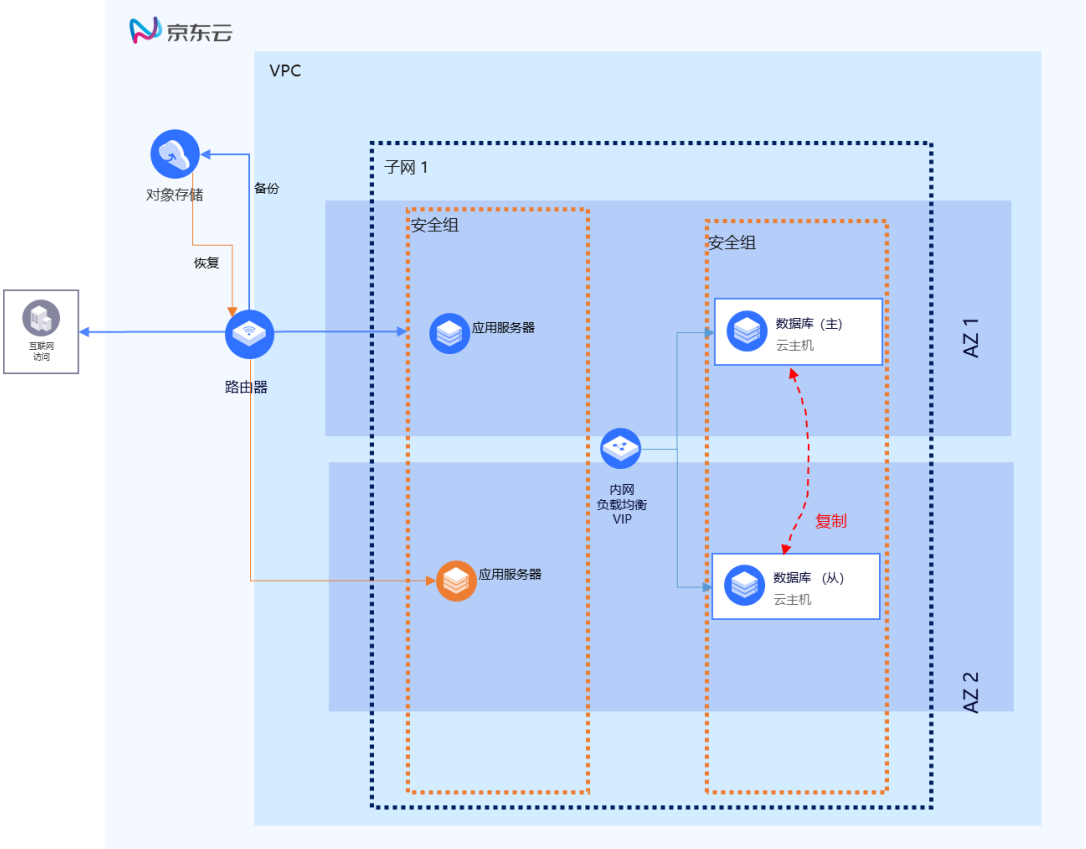
5.1 网络最佳实践

- 私有网络 VPC 设计。
  VPC 是云上的私有网络，为客户的应用提供一个独立的隔离的私有网络环境。客户在京东云上部署合众数字化资产管理系统时，需要规划一个独立的私有网络。与其他客户进行网络隔离。
- 子网设计。
  对于合众数字化资产管理系统的部署，可以建立 1 个子网，用于合众数字化资产管理系统的单台部署。
- 弹性 IP 设计。弹性 IP 可以让客户的应用实例和广域网联通，供客户远程访问应用。应用部署到京东云上时，需要为应用申请一个弹性 IP。
- 安全组设计。安全组用于云主机实例的安全防护。为了安全起见，安全组应只允许必需的端口访问通过。安全组开发的端口需查询应用的端口矩阵。

5.2 可用性最佳实践

京东云的多可用区特性具备故障隔离的功能，结合多可用区机制、镜像机制及数据库的高可用性机制可以实现应用的高可用。

- 数据库主从高可用部署。将部署数据库的云主机分布到不同的 AZ，并将其安装的数据库配置成主从模式。数据库前端部署负载均衡，实现数据库访问的负载均衡及高可用。
- 将应用服务器创建镜像。将应用服务器创建镜像，镜像保存到 region 的对象存储中，当可用区出现问题时，可在别的可用区将应用服务器基于镜像恢复，保证应用的继续可用。



5.3 可扩展性最佳实践

合众数字化资产管理系统软件本支持单机部署、应用服务器与数据库分离部署等多种部署方案，

- 应用和数据库分离部署。为了安全性及扩展性考虑，可以将应用服务器和数据库服务器分离部署，数据库采用主从式、一主多从式等多种部署方案，提升应用性能。
- 纵向扩展。为了满足性能的要求，可以提升服务器的规格，让应用的业务处理能力更强，用户体检更好。例如开始可以选择 2C4G 的 c.n2.large 的规格类型，随着业务的快速发展可将规格类型变为 4C8G 的 c.n2.xlarge。关于京东云主机规格的类型可以参考京东云主机帮助文档。

5.4 安全性最佳实践

将合众数字化资产管理系统部署到京东云上，安全性主要从云平台的管理和应用相关的云资源 2 个维度考虑。

- 云平台管理安全实践。
  1. 账户安全。日常操作京东云不使用根账户，根账户要启用多因素认证，保证账户登录安全。日常的京东云操作要使用子账户。不要将账户的用户名和密码明文保存等等。
  2. AK/SK 安全。如果没有 API 对接需求，不需要启用 AK/SK 机制。
  3. 访问控制安全。要设置访问权限设置，要为子账户设置合理的访问权限。

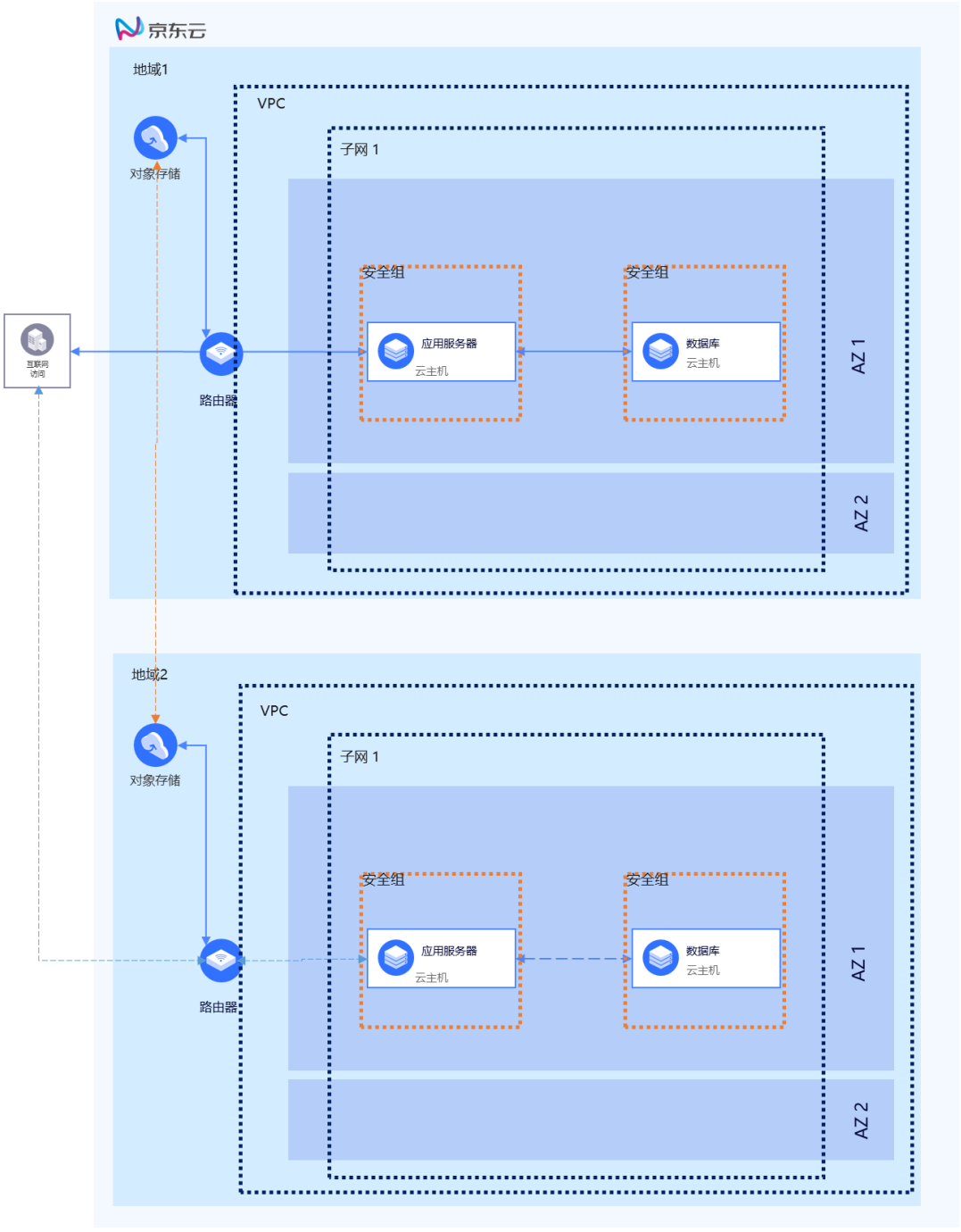
- 应用资源配置最佳实践
  1. 网络安全。可按照应用所需的最小端口矩阵，开放安全组、NACL 端口，合理的规划设置子网。网络相关的最佳实践可参考京东云私有网络操作指南。
  2. 主机安全。要为应用所在的主机安装杀毒软件，防止主机中毒。
  3. 应用安全。要及时为应用所需的中间件更新补丁，防止应用本身的安全漏洞。详情请参考京东云机安全文档。

5.5 灾难恢复最佳实践

5.5.1 京东云上的跨地域灾难恢复

尽管单个地域利用多可用区实现的高可用对大部分的应用已经足够了，但是一些客户可能仍想考虑多个地域的灾难恢复方案，这主要取决于业务的需求。跨地域的灾难恢复如下图所示，可以通过如下步骤实现：

1. 将生产环境的应用服务器和数据库服务器备份到本地域对象存储空间。
2. 开启对象存储的跨地域复制功能，定期从生产环境所在的地域向灾难恢复地域同步数据。
3. 一旦生产环境发生灾难需要恢复业务时，在灾难恢复地域使用企业助手快速部署应用环境。
4. 将数据恢复到灾难恢复地域的应用中。
5. （可选）对于需要域名访问的应用，更改 DNS 即可的指向 IP 即可。

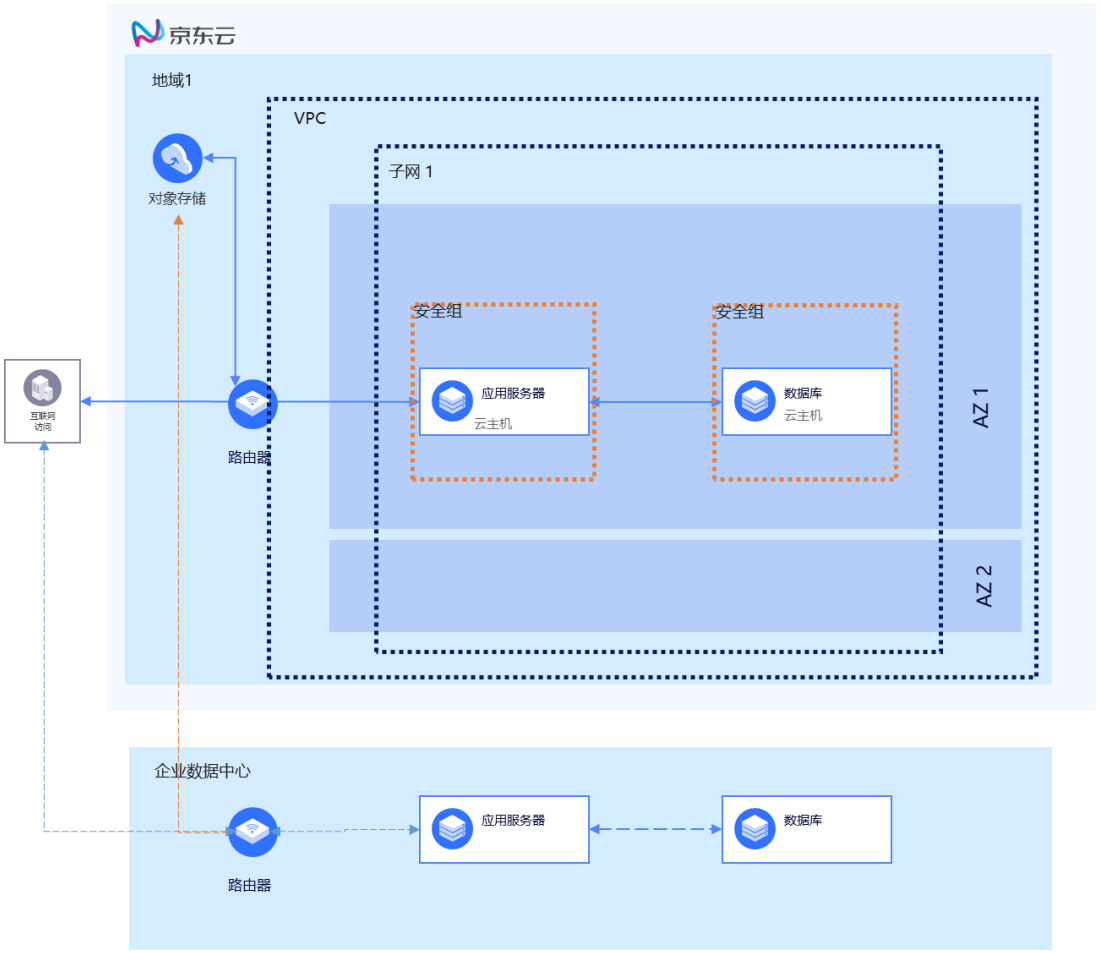


5.5.2 将本地或其他云上部署的应用恢复到京东云

客户也可以将京东云作为部署在本地或其他云的合众数字化资产管理系统生产环境的灾难恢复平台。这种场景里，生产环境仍然部署到客户的本地数据中心，而灾备恢复环境部署在京东云。如果生产环境出现故障，那么可以在京东云上恢复应用，并且提供服务。这个方案需要京东云企业助手的应用灾难恢复功能。如下图所示。

1. 利用京东云企业助手将应用应用数据备份到企业在京东云账号下的对象存储中
2. 一旦企业数据中心发生故障，启动灾难恢复作业
3. 使用京东云企业助手在京东云上一键恢复应用
4. 将备份的数据恢复到应用应用中，应用恢复正常运行。

5. （可选）对于需要域名访问的应用，更改 DNS 即可的指向 IP 即可。



6 京东云安全模型

6.1 责任共担模型

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。

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。

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。

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。用户可以通过使用 IAM 创建、管理子用户，并控制这些子用户访问京东云资源的操作权限。使用访问控制，主账号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秘钥，按需为用户分配所需的最小权限，从而降低企业信息安全风险。

6.3 监控与日志

云监控（Monitoring）是对用户名下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。通过监控，方便客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，客户可以及时作出反应，保障应用程序的稳定运行。
日志服务（Log Service）是京东云提供的一站式日志服务平台。提供日志实时采集、日志存储，日志检索，智能分析等功能，协助用户通过日志解决业务运营，业务监控，日志分析等问题。

6.4 网络安全

在私有网络内，您可以使用 NACL 作为子网级别无状态的安全层，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。没有网络 ACL 的保护或者没有配置访问控制策略，会导致子网中的服务器所有网络端口更容易在互联网上遭受攻击甚至导致被入侵。网络 ACL 可用于对跨子网的东西向访问流量或者进出互联网的南北向访问流量进行过滤。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。

安全组是一种分布式、有状态的、包过滤虚拟防火墙。安全组用来控制一台或一组云主机、容器、负载均衡等实例出入访问流量，实现实例级的安全控制能力。

6.5 数据加密

云硬盘加密功能基于京东云 KMS 系统，对云硬盘加密，为您提供了一种简单的安全的加密手段，能够对您新创建的云硬盘进行加密处理。您无需构建、维护和保护自己的密钥管理基础设施，您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您的业务是透明的。产品功能包括：

- 支持云硬盘中的数据静态加密。
- 在云硬盘和云主机之间移动的所有数据加密。
- 从加密硬盘创建的所有快照自动加密。
- 从这些快照恢复的云硬盘自动加密。

7 结论

将合众数字化资产管理系统部署到京东云，企业可以有效减少 IT 费用，并且获得很多传统物理环境无法获得的好处，如高可用性、高扩展性和足够的弹性等等。下面是在京东云上部署合众数字化资产管理系统的几个优势，我们在文中都有所讨论。

1. 高可用性。获得 99.95%的单可用区的高可用性，如果在多可用区分布部署，可以获得更高的可用性。
2. 灵活性。基于京东云的弹性，支持横向或纵向的伸缩，按照业务需求容量更快的获取计算能力。
3. 较低的成本。与传统部署模式相比，京东云上部署应用将拥有成本（CPEX）转变为运营成本（OPEX），无需再承担设备的维护、供电、人工等等费用。

8 文档作者

高增，京东云解决方案架构师
王健永，天津合众唯一总经理

9 参考

合众数字化资产管理系统解决方案信息页
http://www.hz-union.com/index.asp
京东云云主机文档
https://docs.jdcloud.com/cn/virtual-machines/product-overview
京东云私有网络产品文档
https://docs.jdcloud.com/cn/virtual-private-cloud/product-overview
京东云可信中心
https://www.jdcloud.com/cn/service/trustedCenter
京东云对象存储产品文档

https://docs.jdcloud.com/cn/object-storage-service/product-overview
京东云网络负载均衡产品文档
https://docs.jdcloud.com/cn/network-load-balancer/product-overview