

天翼云认证 高级解决方案架构师

重点知识手册



目 录

一、 架构设计基础	3
二、 云上架构设计	7
三、 云上安全架构设计	21
四、 云上运维架构	24
五、 容灾备份架构设计	27
六、 上云迁移方案	32
七、 通用解决方案	39
八、 国资云行业解决方案（选修）	54
九、 教育行业解决方案	57
十、 高速公路行业解决方案（选修）	61
十一、 汽车行业解决方案（选修）	64
十二、 医疗行业解决方案	67
十三、 政务行业解决方案	71
十四、 智慧城市解决方案	73
十五、 工业行业解决方案（选修）	76
十六、 商业需求调研与分析	77

一、架构设计基础

必备掌握知识点：

1. 传统 IT 架构演进过程

IT 架构是指导 IT 投资和设计决策的 IT 框架，是建立企业信息系统的综合蓝图。IT 架构通常分为数据架构、应用架构和技术架构三部分。此外，随着数据安全的问题日益受到重视，许多企业的 IT 架构也将安全架构置于重要的位置上。

- (1) 单体引用：通常服务器操作系统使用 Linux，应用程序使用 PHP 开发，然后部署在 Apache 上，数据库使用 MySQL，汇集各种免费开源软件以及一台廉价服务器就可以开始系统的发展之路了；
- (2) 应用与数据库分离：数据量增加，单台服务器性能以及存储空间不足，需要将应用和数据分离，并发处理能力和数据存储空间得到了很大改善；此时应用程序、数据库、文件分别部署在独立的资源上；
- (3) 使用缓存以改善性能：系统访问特点遵循二八定律，即 80% 的业务访问集中在 20% 的数据上。缓存分为本地缓存和远程分布式缓存，本地缓存访问速度更快但缓存数据量有限，同时存在与应用程序争用内存的情况；
- (4) 应用服务器集群：使用集群是系统解决高并发、海量数据问题的常用手段。通过向集群中追加资源，提升系统的并发处理能力，使得服务器的负载压力不再成为整个系统的瓶颈；
- (5) 数据库读写分离：读写分离就是在主服务器上修改，数据会同步到从服务器，从服务器只能提供读取数据，不能写入，实现备份的同时也实现了数据库性能的优化，以及提升了服务器安全；
- (6) 反向代理和 CDN 加速：为了应付复杂的网络环境和不同地区用户的访问，通过 CDN 和反向代理加快用户访问的速度，同时减轻后端服务器的负载压力。CDN 与反向代理的基本原理都是缓存；
- (7) 分布式文件系统和分布式数据库：随着系统的不断运行，数据量开始大幅增长，这个时候发现分库后查询仍然会有些慢，于是按照分库的思想开始做分表的工作。数据库采用分布式数据库，文件系统采用分布式文件系统。任何强大的单一服务器都满足不了大型系统持续增长的业务需求，数据库读写分离随着业务的发展最终也无法满足需求，需要使用分布式数据库及分布式文件系统来支撑。分布式数据库是系统数据库拆分的最后方法，只有在单表数据规模非常庞大的时候才使用，更常用的数据库拆分手段是业务分库，将不同的业务数据库部署在不同的物理服务器上。它的应用场景基本是电商、金融、零售、O2O 等领域，应用广泛；
- (8) 使用非关系型数据库：随着业务越来越复杂，对数据存储和检索的需求也越来越复杂，系统需要采用一些非关系型数据库如 NoSQL 和分数据库查询技术如搜索引擎来解决相关问题。应用服务器通过统一数据访问模块访问各种数据，减轻应用程序管理诸多数据源的麻烦；

2. 传统 IT 架构遇到的挑战

- (1) 挑战一：不是没有系统，而是遗留系统太多；

- (2) 挑战二：信息爆炸，数据异构，难以整合；
- (3) 挑战三：企业需要电子商务支持，但技术异构，难以协同；
- (4) 挑战四：业务变化快，僵化的 IT 基础设施难以迅速响应。

3. 云上 IT 架构演进过程

云上架构是一种全新的技术架构，将 IT 资源（包括服务器、存储、网络等）有效整合，形成统一资源池，以服务的方式对外提供云服务。

- (1) 单台云服务器：可以使用云上的云服务器（ECS）作为业务承载的工具，结合系统内核参数调优，web 应用的性能参数调优，数据库调优，保证基本上能稳定运行；
- (2) 应用与数据库分离（2 台 ECS 或者 1 台 ECS+1 台 RDS）：我们可以直接使用云上的 RDS 数据库资源，利用其丰富的数据结构可以完成不同业务类型的业务场景开发，更加节省成本；
- (3) 使用负载均衡构建集群：该架构中我们会提到一个集群的概念，即在云上部署一组有相同应用的 ECS，ECS 的数量能够不断扩充；
- (4) 动静分离（使用对象存储）：静态缓存+文件存储：通过将动态请求和静态请求的访问分离，有效解决服务器的 CPU、内存、磁盘 IO，以及带宽的压力；
- (5) 缓存数据库：通过数据库缓存，有效减少数据库访问压力，进一步提升性能；
- (6) 数据库读写分离（RDS）：在数据层，结合数据库缓存，当数据库压力还不是很大的时候，我们可以通过读写分离的方式，进一步切分及降低数据库的压力；
- (7) 分库分表（分布式关系型数据库）：将不同的应用按照功能的不同分别存放到不同的数据库中。此时，我们可以有数据的垂直拆分和水平拆分两种选择；
- (8) 当某个业务的数据量或者更新量到达了单个数据库的瓶颈时，此时需要进行数据库的水平拆分；
- (9) NoSQL 数据库（使用 NoSQL 和搜索引擎）：引入之后能够大大提高查询速度，但是也会带来大量的维护工作，我们需要自己实现索引的构建过程，设计全量增加的构建方式来应对非实时与实时的查询需求；
- (10) 中间件：即在消息的传输过程中保存消息的容器。用于连接可能出现不同语言开发的子模块和部署在不同平台的子系统；
- (11) 大数据服务：大数据服务是通过底层可伸缩的大数据平台和上层各种大数据应用，支撑机构或个人对海量、异构、快速变化的数据进行采集、传输、存储、处理（包括计算、分析、可视化等）、交换、销毁等覆盖数据生命周期相关活动的各种数据服务。

4. 使用云上资源之后的架构优势

- (1) 随需提供，按需购买，即简化信息资源的获取，提高信息服务质量。
- (2) 降低成本，即降低 IT 总投资成本，降低运维服务成本，延长 IT 设备资产的寿命。

(3) 提高效率，即提高系统运行效率、资源效能、以及运维管理效率。

(4) 提高可靠性，即提高数据存储的可靠性和系统运行的可靠性，实现计算的安全稳定。

5. 传统架构的定义和概念

(1) 框架通常指是为了实现某个业界标准或完成特定基本任务的软件组件规范，也指为了实现某个软件组件规范所要求的具有基础功能的软件产品。

(2) ISO/IEC 42010:2007 将架构定义为：一个系统的基础组织，体现在系统组件、组件之间及组件与环境之间的相互关系，以及对系统设计和演进进行治理的原则中。

(3) TOGAF 中的“架构”有两种含义：一个系统的正式描述，或指导系统实施的组件层级详细过程；组件结构、组件之间相互关系，以及对这些组件的设计和随时间演进的治理原则和指南。

(4) 架构师定义：一般指企业架构师，是企业软件的总设计师。负责设计系统整体架构，从需求到设计的每个细节都要考虑到，使设计的项目尽量效率高，开发容易，维护方便，升级简单。他不从事具体的软件程序编写工作，但他必须对开发技术非常了解，并且需要有良好的组织管理能力。

6. 云计算架构的概念

(1) 云计算架构主要指的是云计算所需的组件和子组件，这些组件包括前端（客户端、移动端）、后端（服务端、服务器、存储）、基于云的交付和网络。通俗的讲，云架构=企业架构+SOA 架构+云技术。

(2) 云计算架构师：需要交付包含前端、后端、网络和基于云计算的解决方案，需要将项目的技术需求转换为最终产品的体系结构和设计理念，专门为复杂问题提供可行性方案。反过来，倾听市场和客户需求，善于沟通并能看到问题的本质，能够抽象成产品和技术的要求，结合技术发展的趋势，懂得取舍，起到技术和业务的桥梁作用。

7. 云计算解决方案架构的概念

(1) 云计算解决方案架构，我们可以通俗的理解为将线下的解决方案架构搬迁到云上进行。而云计算解决方案架构设计则是利用云计算解决方案架构师丰富的知识累积与实践经验，从纷乱复杂的问题中，应用科学的解决方案分析方法，进行定量和确有论据的定性分析，找出企业要解决问题的核心原因，提炼能被实施的解决方案与设计架构，进而指导方案实施的过程。

(2) 天翼云解决方案架构师的岗位职责：能评估一个组织所需要的技能，以便在天翼云上实现和部署应用程序可以提出一些建议；需要非常熟悉天翼云云平台以及各种各样的产品体系；需要对开源的方案和其他云厂家的解决方案有一定的了解。

8. 架构设计的意义

架构设计源于客户需求；节省成本，提高效率；架构设计服务于整个开发过程。

9. 云原生架构的概念以及它的发展历程

(1) 云原生是一种构建和运行应用程序的方法，是一套技术体系和方法论。云原生（CloudNative）是一

个组合词，即 Cloud+Native。Cloud 表示应用程序位于云中，而不是传统的数据中心；Native 表示应用程序从设计之初即考虑到云的环境，原生为云而设计，在云上以最佳姿势运行，充分利用和发挥云平台的弹性以及分布式优势。

(2) 发展历程:

- ① 2013 年 Matt Stine 提出云原生架构的几个特征：12 因素、微服务、自服务敏捷架构、基于 API 协作、抗脆弱性；
- ② 到了 2017 年，Matt Stine 在接受采访时又改了口风，将云原生架构的特征重新归纳为：模块化、可观察、可部署、可测试、可替换、可处理 6 种特质。Pivotal 最新官网将云原生概括为 4 个要点：DevOps+持续交付+微服务+容器
- ③ 到了 2018 年，云原生计算基金会（CNCF）又更新了云原生的定义，即容器化封装+自动化管理+面向微服务+服务网格（Service Mesh）+声明式 API。

10. 云原生架构的典型技术特征

采用轻量级的容器；设计为松散耦合的微服务；通过 API 进行交互写作；使用最佳语言和框架开发；通过 DevOps 流程进行管理。

11. 云原生架构特点（与传统架构相比）

- (1) 开发模式：云原生是以应用为中心的开发模式，烦琐的软件安装通过自动化的模式来完成，保证了软件环境一致性，减少了系统依赖的风险，同时开发人员只要聚集在应用上，其他由基础设施服务一键完成，大大提高了软件的生产效率；
- (2) 交付模式：传统模式的发布流程是中断、有隔离的，并不流畅。云原生模式中，从开发到测试再到上线及监控反馈，整个过程可以不断反馈和螺旋上升；
- (3) 架构设计模式：传统的架构设计更多关注功能需求的满足，由于架构变化不易实现，所以更倾向于保持架构的稳定性。云应用架构设计意味着更快的迭代速度、持续可用的服务、弹性扩容及一些非功能需求，包括追求产品创新时间的技术挑战、以用户体验为中心的挑战和移动互联网时代的突发性挑战。

12. 云架构设计原则

- (1) 高性能：通俗的可以理解为网页秒开、高清视频——即要确保系统能够高效、快速地响应用户的请求。
 - ① 在浏览器端，可以通过浏览器缓存、使用页面压缩、合理布局页面等手段改善性能；
 - ② 使用 CDN，将网站静态内容分发至离用户最近的网络服务机房，使用户通过最短访问路径获取数据；
 - ③ 应用服务器端，可以使用服务器本地缓存和分布式缓存，通过缓存在内存中的热点数据处理用户请求，加快请求响应速度；

- ④ 在网站有很多高并发用户的情况下，可以将多台应用服务器组成一个集群共同对外服务，提高整体处理能力；
- ⑤ 在代码层面，我们可以通过使用多线程、改善内存管理等手段优化性能；
- ⑥ 使用 NoSQL 数据库优化数据模型。

(2) 可用性：通俗理解就是系统运行的连续性，尽量避免出现业务中断。

- ① 衡量指标：网站可用性的指标就是网站的总可用时间（除去故障时间）。
- ② 在设计方面：对于应用服务器而言，将多台应用服务器通过负载均衡设备组成一个集群共同对外提供服务，任何一个宕机，只需把请求切换到其他服务器上面就可实现应用的高可用；对于存储服务器而言，需要的数据存储进行互相备份，这样，当服务器宕机时，将数据访问转移到可用的服务器上，并进行数据恢复，以保证继续有服务器宕机时数据依旧能用。

(3) 弹性：所谓弹性就是架构能够根据系统的需求进行弹性的伸缩。

(4) 在设计方面：对于应用服务器集群，可以通过使用合适的负载均衡设备向集群中不断加入服务器；对于缓存服务器集群，我们需要注意的是改进缓存路由算法保证缓存数据的可访问性；在数据库方面，因此可考虑在集群伸缩方案之外通过路由分区将部署有多个数据库的服务器组成一个集群。

(5) 可靠性：可理解为系统在规定的时间内及规定的环境下完成规定功能的能力，也就是系统无故障运行的概率。可靠性的衡量指标：平均无故障时间（MTTF）、平均故障修复时间（MTTR）

(6) 安全：主要涉及业务范围是企业数据资产、用户数据与隐私等——即如何能够保证云上系统的安全，以防止被黑客攻击。

- ① 衡量安全的标准：主要可以考虑使用加密传输、防 DDoS/CC 攻击、流量限制等手段进行安全设置。
- ② 在设计方面：设计安全性；设备安全性；云端安全；网络中的数据安全。

(7) 可管理性：可管理性虽然不是最主要的设计原则，但也是架构设计中必不可少的。搭建的架构如果能够方便后续的管理，会帮助我们节省很多的管理成本。

二、云上架构设计

必备掌握知识点：

1. 传统 IT 基础架构与云上基础架构

IT 基础设施主要包含：网络、计算、存储这三方面的内容。

(1) 对于两种架构而言，资源方面的不同点在于：

- ① 线下资源：网络设备里面包含，互联网接入层的设备、核心层的设备、汇聚层的设备、接入层的设备。
- ② 云上资源：云上的 IT 基础架构主要的资源如图中所示：网络层有 VPC，计算有云服务器等，存储有对象存储等。

- ③ 安全组是一个逻辑上的划分，这个分组由同一个地域内具有相同安全保护需求并相互信任的云主机组成。安全组用来实现安全组内和组间虚拟机的访问控制，加强虚拟机的安全保护。安全组创建后，用户可以在安全组中定义各种访问规则，当虚拟机加入该安全组后，即受到这些访问规则的保护。安全组默认出方向放行，并且组内云主机可相互访问。
 - ④ 子网是属于 VPC 的资源，一个 VPC 内的子网可以进行通信，不同 VPC 的子网不能进行通信。
 - I. 子网创建好后，网段不能进行修改。
 - II. 子网的网段要在 VPC 的网段内部，VPC 提供三段私网网段，10.0.0.0/8~24、172.16.0.0/12~24 和 192.168.0.0/16~24，所以子网的网段也会在这些范围内。
 - ⑤ 公有云提供弹性公网 IP（EIP）、NAT 网关、弹性负载均衡（ELB）等方式连接公网。
 - ⑥ EIP 提供独立的公网 IP 资源，包括公网 IP 地址与公网出口带宽服务。可以与弹性云服务器、裸金属服务器、虚拟 IP、弹性负载均衡、NAT 网关等资源灵活地绑定及解绑。拥有多种灵活的计费方式，可以满足各种业务场景的需要。
 - ⑦ ELB 将访问流量自动分发到多台弹性云服务器，扩展应用系统对外的服务能力，实现更高水平的应用容错。为负载均衡器配置需要监听的端口信息以及弹性云服务器，通过监听器来检查后端弹性云服务器的运行状态，确保将请求发送到正常的弹性云服务器上，提高系统可用性。
 - ⑧ NAT 网关能够为 VPC 内的弹性云服务器提供 SNAT 和 DNAT 功能，通过灵活简易的配置，即可轻松构建 VPC 的公网出入口。
 - ⑨ 两个同一区域内的 VPC 之间使用私有 IP 地址进行内网通信时，需要使用到对等连接服务。
- (2) 对比这两种类型的基础架构，并不能直观看到两者的差异。最主要的区别就在于服务器与存储。
- ① 服务器方面：将传统服务器与云服务器从产品性能、可靠性、安全、价格进行对比。
 - ② 存储方面：本地存储一向以可靠性高、稳定性好，功能丰富而著称，但与此同时，本地存储也暴露出横向扩展性差、价格昂贵、数据连通困难等不足，容易形成数据孤岛，导致数据中心管理和维护成本居高不下；云上存储即分布式存储主要是以软件定义存储为主。云存储提高了存储效率，通过分布式技术解决了存储空间的浪费，可以自动重新分配数据。

2. 云上基础架构解析

- (1) 云服务器优势：可用性强、稳定性强、安全性强、可扩展性强。
- (2) 云负载均衡特点：支持多协议、转发灵活、会话保持、配合弹性伸缩。
- (3) 关系型数据库：即开即用、稳定可靠、可弹性伸缩。
- (4) 对象存储：容量无限大、数据安全可靠、使用方便。

3. 基础架构设计案例

案例是一个典型的 3 层 web 应用系统，包括 web 层、应用层、数据层。系统状态保存在数据库中。

在弹性负载均衡器 (ELB) 后运行多个弹性云主机 (ECS) 实例可以提供系统的可用性和可伸缩性, ELB 通过弹性 IP 接入 Internet。数据备份: 可将数据逻辑备份保存在对象存储产品中; 数据层: 使用关系类数据库, 建议直接使用天翼云 RDS 服务。

- (1) 对 CPU、内存、硬盘空间无特殊要求。
- (2) 对成本比较敏感。
- (3) 对安全性、可靠性要求高。
- (4) 对网络带宽有一定的要求。

4. 天翼云高性能架构设计

云上高性能架构升级云上虚拟化硬件配置、优化云上高性能架构、就近部署。

5. 升级云上虚拟化硬件配置

主要从云主机、物理机服务、GPU 云主机三方面进行产品选型。GPU 加速云主机能够提供优秀的浮点计算能力, 从容应对高实时、高并发的海量计算场景。特别适合于深度学习、科学计算、CAE、3D 动画渲染、CAD 等应用。GPU 加速型云主机分为图形加速基础型 (G1、G2、G5) 和计算加速型 (P1、P2V)。GPU 适用于虚拟化环境下运行的图形渲染、工程制图等应用场景。物理机可以为用户提供资源独享、安全可靠的云上物理机服务器。

6. 云上高性能架构优化

- (1) 云上架构可扩展性。这里主要考虑负载均衡和消息队列的使用。这里我们会了解到天翼云分布式消息服务, 它是一项基于分布式集群技术的消息中间件服务, 具有高可靠、高并发、低时延、海量消息堆积的能力特点。
- (2) 缓存: 这里关注的主要是数据层高性能设计。在数据层高性能设计环节, 主要就是数据库和存储的产品设计。数据库方面可以统称为结构化数据, 存储主要就是非结构化数据。我们需要了解关系型数据库、分布式缓存服务、天翼云的文档数据库服务。非结构化数据主要从云硬盘、共享云硬盘、对象存储、弹性文件存储来进行产品选型, 进行架构设计。

7. 高性能架构的就近部署

CDN (CT - CDN, Content Delivery Network), 即内容分发网络, 是中国电信依托分布于全国的网络节点搭建的一层虚拟网络。它将源站内容分发至最接近用户的节点, 使用户可就近获取所需内容, 解决因跨运营商访问、跨地域访问、服务器带宽及性能带来的访问延迟问题, 提高用户访问的响应速度和成功率。天翼云 CDN 的相关产品与服务主要有下载加速、静态加速、视频直播加速、视频点播加速。静态加速 (Static Content Delivery, SCD), 又名静态内容分发网络。网站的图标、图片、文字、动画、脚本等组成了网站的静态内容, 其文件类型包括但不限于 JPG、GIF、CSS、JS、HTML 和 PDF 等。静态内容传递了网站的核心价值。通过天翼云静态内容加速, 可极大减少网站的响应时间, 显著提升

网页用户体验。

8. 天翼云高性能架构设计案例

前端用户请求通过 CDN 服务响应，CDN 主要用来做服务加速，对于可以满足的响应直接使用 CDN 解决，无法满足的请求转发给后端 ELB。

9. 弹性架构概念

弹性架构即随着业务的变化能够进行灵活的、自动的弹性伸缩的一种架构。它包括基础设施层的弹性、应用层的弹性、数据层的弹性等。

(1) 优点：弹性、按需计算，充分优化企业的计算资源。

(2) 缺点：应用要从架构层做到可横向扩展化改造，依赖的底层配套比较多，对技术水平、实力、应用规模要求都较高。

10. 弹性架构设计原则

(1) IT 基础设施层弹性设计：主要讲的是应用服务器集群的弹性设计。这个设计中，我们了解到请求分发装置负载均衡服务器。HTTP 重定向负载均衡；DNS 域名解析负载均衡；反向代理负载均衡；IP 负载均衡；数据链路层负载均衡。DNS 根据 A 记录和负载均衡算法可以计算得到一个 IP 地址。

(2) 应用层的弹性设计：通常是由 PHP、Java、Python 等写的逻辑代码构成的，需要依赖后台数据库和缓存层面的东西。最核心的就是，应用层不要有状态，将状态分散到缓存层还有数据层。

(3) 存储层的弹性设计：这里主要是有缓存的弹性和数据层的弹性两方面。

① 缓存弹性：以 Memcache 分布式缓存集群的访问模型；分布式缓存的一致性 Hash 算法。

② 数据层的弹性：关系数据库集群的弹性设计和 NoSQL 数据的弹性设计。

(4) 弹性架构的设计模式：水平扩展（增加更多的系统成员）和垂直扩展（增加单个系统成员的负荷）。

11. 传统弹性架构解决方案

主要从脚本、配置、监控系统、自动化部署工具角度来设计。遇到的问题有配置管理操作复杂、脚本稳定性不高、自动化程度不高、学习成本高等问题。

(1) 展示层为用户交互，接受和呈现信息：弹性伸缩监控；应用成本分析展示；虚拟计费（待定）。

(2) 逻辑层为运维自动化的核心：弹性伸缩系统；自动化部署；计算资源分配。

(3) 资源层为计算、存储、网络、CDN 等基础设施资源。

12. 天翼云弹性架构设计

(1) 基础设施层的弹性设计：

① 公有云 IaaS，它通常通过互联网为企业提供虚拟化的计算资源。

② 天翼云 EIP 支持与云主机、物理机、NAT 网关、负载均衡等实例灵活地绑定与解绑，支持带宽灵活调整，应对各种业务变化；天翼云 NAT 网关能够为虚拟私有云（Virtual Private Cloud，

VPC) 内的计算实例提供网络地址转换服务, 多个弹性云主机可以共享使用弹性 IP 访问 Internet 或使多个弹性云主机提供互联网服务。

I. 同一个 NAT 网关下的多条规则可以复用同一个弹性 IP, 不同网关下的规则必须使用不同的弹性 IP。

II. 弹性 IP 的功能

➤灵活绑定: 支持弹性 IP 灵活地绑定和解绑, 用户可以使用弹性 IP 快速解绑故障实例, 绑定到正常实例上, 保证业务可用性。

➤网络适配: 可以根据自身业务需求灵活调整网络带宽。

➤独立管理: 可以独立管理弹性 IP 生命周期。

➤功能叠加: IPv6 功能叠加在 IPv4 弹性 IP 功能上实现, 用户只需考虑 IPv6 与 IPv4 的对应关系即可, 无需考虑 IPv6 与后端云主机等的绑定关系, 绑定关系仍由 IPv4 弹性 IP 实现。

➤共用带宽: IPv6 与 IPv4 共用 IPv4 的带宽, 无需额外申请 IPv6 带宽。

III. 每个 VPC 支持的 NAT 网关数为 1。

IV. 用户不能在 VPC 下手动添加默认路由。

V. VPC 内的每个子网只能添加一条 SNAT 规则。

VI. SNAT 和 DNAT 不能共用同一个弹性 IP。

VII. DNAT 规则不支持将弹性 IP 绑定到虚拟 IP。

VIII. 当云主机同时配置弹性 IP 服务和 NAT 网关服务时, 数据均通过弹性 IP 转发。

IX. NAT 网关的规格会影响 SNAT 功能的最大连接数和每秒新建连接数, 数据吞吐量由弹性 IP 的带宽决定。

X. 在系统并发数由小到大逐渐增大的过程中, 系统的吞吐量一般是先逐渐增大, 达到一个极限后, 随着并发数的增加反而下降, 达到系统崩溃点后, 资源耗尽, 此时的吞吐量为 0。

XI. SNAT 规则中添加的自定义网段, 对于虚拟私有云的配置, 必须是虚拟私有云子网网段的子集, 不能相等。

XII. SNAT 规则中添加的自定义网段, 对于云专线的配置, 必须是云专线侧网段, 且不能与虚拟私有云侧的网段冲突。

XIII. 路由表允许用户添加自定义路由, 使 VPC 内其他云主机通过绑定弹性 IP 的云主机访问 Internet 网络。

(2) 应用层的弹性设计: 从弹性云主机、天翼云负载均衡服务、天翼云弹性伸缩服务来进行考虑设计。

① 负载均衡类型: 天翼云提供公网负载均衡。

② 会话保持: 用户可针对负载均衡服务监听器开启会话保持功能, 针对 7 层 (HTTP 协议) 服务,

负载均衡系统是基于 cookie 的会话保持；针对 4 层（TCP 协议）服务，负载均衡系统是基于 IP 地址的会话保持。

- ③ 获取用户真实 IP：针对 7 层（HTTP 协议）服务，负载均衡支持通过 Http Header: X-Forwarded-For 获取来访者真实 IP；针对 4 层（TCP 协议）服务，支持通过配置 TOA 插件获取用户真实 IP。
 - ④ 转发策略：用户设置负载均衡监听器转发策略时，可选择轮询、最小连接数和源地址三种模式的转发规则。
 - ⑤ 健康检查：支持用户自定义健康检查方式和频率，负载均衡根据预设的健康检查规则定时检查后端云主机是否正常运行，一旦检测到云主机为非健康状态，则不会将访问流量分派到这些非健康云主机实例。
 - ⑥ 天翼云弹性云主机具备快速开通的优势，无论是一台还是百台，均可实现分钟级开通使用。
 - ⑦ 当购买的天翼云弹性云主机的 CPU 和内存不能满足要求时，可以通过规格变更进行处理。
- (3) 数据层的弹性设计：从结构化数据和非结构化数据来进行考虑。结构化数据：数据库层面来考虑，数据库 RDS、分布式关系型数据库、分布式缓存进行选择设计。非结构化数据从云硬盘、对象存储来进行考虑设计选型。注意（云硬盘主要是进行块存储。天翼云云硬盘是一种基于分布式架构的、可弹性扩展的数据块级存储设备。可为云主机提供系统盘和数据盘，满足文件系统、数据库或者其他应用等的存储）。

13. 天翼云弹性架构综合案例

天翼云混合云解决方案：依托中国电信云与网的优势，以及丰富的项目经验，为客户提供包含云专线，云网关，私有云，混合云等完整的解决方案。满足客户不同的上云选择，帮助企业实现数字化转型或其他业务战略。该架构具备的特点有：统一管理，统一服务；云网协同，弹性部署；运维管理，统一平台；无缝互联，灾备保障。

14. 高可用架构概念

- (1) 系统运行中遇到的问题：资源不可用，包括网络和服务器出故障，网络出故障表明节点连接不上；资源不足，在高并发的情况下，节点无法正常工作，对外表现为响应超时；节点的功能有问题，这个主要体现在我们开发的代码上，比如它的内部业务逻辑有问题，或者是接口不兼容导致客户端调用出了问题。
- (2) 可用性概念：可用性=平均故障间隔/(平均故障间隔.+平均修复时间)，也就是我们常说的多少个 9，99.9%，99.99%，即可用性层次级别。

15. 高可用架构架构设计原则

- (1) 接入层设计原则：接入层主要是流量入口，经过简单。设计时应该注意：制定相关的《域名规范

管理说明》，例如根据产品重要等级，制定使用高防 IP 的策略；搭建我们 API 网关，方便 API 日常管理，包括版本管理，升级，回滚。同时提高调试工具，方便开发人员，QA 调试和测试。更重要的是 API 网关起到限流防刷（CC 攻击）作用，保护后端服务。

(2) 应用层设计原则：可以水平扩展；无状态设计；回滚设计；灰度设计。

(3) 服务层设计原则：服务分级管理。这里涉及各级服务的部署原则、各级服务上线发布原则、各级服务监控原则。

(4) 数据层设计原则：统一数据视图；数据、应用分离；数据异构；数据读写分离；用 mysql 数据；合理使用缓存。连接关系型数据库实例。以 Linux 系统为例，执行如下命令。

```
mysql -h <hostName> -P <port> -u <userName> -p --ssl-ca=<caName>
```

参数	说明
<hostName>	目标实例的弹性公网 IP。
<port>	目标实例的数据库端口。
<userName>	用户名，即关系型数据库账号（默认管理员账号为 root）。
<caName>	相应的 SSL 证书文件名，该文件需放在执行该命令的路径下。

16. 高可用架构传统解决方案

高可用架构具体可分为计算高可用和存储高可用。

(1) 计算高可用架构：

- ① 方法：通过增加更多的服务器来达到计算高可用。
- ② 计算高可用架构分为主备、主从、对称集群、非对称集群。主备又分为冷备和温备。前面需要人工更换，集群则会自动更换。

(2) 存储高可用架构

- ① 存储高可用架构本质：通过将数据复制到多个存储设备；通过数据冗余的方式来实现高可用。
- ② 常见的存储高可用有主备、主从、双主，集群（数据集中集群和数据分散集群），分区。

17. 天翼云高可用架构设计

(1) 基础设施层高可用架构设计：天翼云云基础设施围绕区域（Region）和可用区（“AZ”）构建。每个地域完全独立，但同一个地域内的可用区之间使用低时延链路相连。基于天翼云产品搭建的高可用架构可支持多区域多可用区使用。我们用区域和可用区来描述数据中心的位置，您可以在特定的区域、可用区创建资源。

- ① 区域（Region）指物理的数据中心。每个区域完全独立，这样可以实现最大程度的容错能力和稳定性。资源创建成功后不能更换区域。

- ② 可用区 (AZ, Availability Zone) 是同一区域内，电力和网络互相隔离的物理区域，一个可用区不受其他可用区故障的影响。一个区域内可以有多个可用区，不同可用区之间物理隔离，但内网互通，既保障了可用区的独立性，又提供了低价、低时延的网络连接。
- ③ 下图阐明了区域和可用区之间的关系。



(2) 应用层高可用设计：应用层主要处理的是业务逻辑。它有一个显著的特点就是应用的无状态性。

在应用层设计中，我们需要解决的问题是：应用服务器宕机、应用服务 bug。

- ① 天翼云单台弹性云主机的可用性可达到 99.95%；并且弹性云主机可在不同可用区中部署（可用区之间通过内网连接）。
- ② 天翼云的弹性负载均衡，服务器本身有冗余设计，不会出现单点故障。并且会自动剔除不健康云主机，保证在健康主机上进行负载，实现业务可用性。
- ③ 天翼云弹性负载均衡支持 TCP、UDP 协议的四层负载均衡和 HTTP 协议的七层负载均衡（HTTP 协议、HTTPS 协议）。
- ④ 天翼云的弹性伸缩服务可以支持非负载均衡场景和负载均衡场景下的弹性伸缩服务，自动替换不健康实例。可自动增加或者减少云主机，操作灵活，从而保障业务灵活可用，避免损失。它可以实现伸缩组管理、伸缩策略管理、伸缩配置管理功能。

伸缩组配置：

- I. 最大/最小实例数：伸缩策略条件满足时，根据最大实例数和最小实例数自动调整需要添加或移除的云主机数量。例如，按照伸缩规则要求，需要将云主机数量增加到 10 台，但最大实例数是 8，则系统会按照 8 台云主机数量进行弹性伸缩活动。
- II. 期望实例数：默认的云主机数量，伸缩组创建时，自动创建的云主机数量。创建后可以手工修改该值，修改该值就会触发一次弹性伸缩活动。
- III. 冷却时间：冷却时间是指冷却伸缩活动的时间，在每次触发伸缩活动之后，系统开始计算冷却时间。伸缩组在冷却时间内，会拒绝由告警策略触发的伸缩活动。其他类型的伸缩策略（如定时策略和周期策略等）触发的伸缩活动不受限制，但会重新开始计算冷却时间。

说明：如果伸缩活动是伸缩策略触发的，以伸缩策略的冷却时间为准；如果是手工修改期望实例数量或者其他方式引起的伸缩活动，则以伸缩组的冷却时间为准。

IV. 健康检查方式：伸缩组的健康检查方式，默认是“云主机健康检查”方式。伸缩组使用弹性负载均衡器时，会增加“弹性负载均衡健康检查”方式。

V. 实例移除策略：实例优先被移除的策略。当满足条件时，会触发实例移除活动，包括如下四种方式：

- 根据较早创建的配置较早创建的实例：根据“较早创建的配置”较早创建的“实例”优先被移除伸缩组。
- 根据较早创建的配置较晚创建的实例：根据“较早创建的配置”较晚创建的“实例”优先被移除伸缩组。
- 较早创建的实例：创建时间较早的实例优先被移除伸缩组。
- 较晚创建的实例：创建时间较晚的实例优先被移除伸缩组。

VI. 弹性伸缩服务可以单独使用，也可以同弹性负载均衡（ELB），云监控（CES）一起使用。其中，云监控服务为免费服务，系统默认开通；负载均衡服务在有需求时可以部署，例如，有分布式集群需求的场景下，可以使用 ELB。

VII. 天翼云弹性负载均衡 CT-ELB 中，如需要使用 80、8080、443、8443 备案端口，请提前进行备案。4 个备案端口默认是关闭状态，备案完成后将开放。

(3) 数据层高可用设计。在实际的选择天翼云产品时，我们可以从结构化数据高可用和非结构化数据高可用来考虑设计。

① 结构化数据高可用我们可以通过关系型数据库和分布式缓存数据库来实现。

I. RDS 具有完善的性能监控体系和多重安全防护措施，并提供了专业的数据库管理平台，让用户能够在云中轻松的进行设置和扩展关系型数据库。

II. 分布式关系型数据库（简称 DRDS），是一款分布式关系型数据库。它兼容 MySQL 协议，采用存储计算分离架构的模式，使得存储层、计算层可以无限扩展，从而拥有了海量数据高并发访问能力。

III. RDS 的可用性集中在：

- 双机热备：RDS 采用热备架构，故障系统 1 分钟自动切换。
- 数据备份：支持自动备份和手动备份，并支持通过备份数据恢复实例。用户可以设置自动备份的周期，还可以根据自身业务特点随时发起备份，选择备份周期、修改备份策略。
- 数据恢复：支持按备份集和指定时间点的恢复。在大多数场景下，用户可以将 35 天内任意一个时间点的数据恢复到 RDS 临时实例或克隆实例上，数据验证无误后即可将数据迁

回 RDS 主实例，完成数据回溯。

IV. 分布式缓存：天翼云分布式缓存数据库-DCS 提供单机和主备两种缓存实例类型，支持自动容灾切换、在线扩容、数据备份、实例监控等数据库服务。它的可用性体现在：双机热备、数据持久化。

② 非结构化数据高可用可以通过云硬盘、对象存储、弹性文件服务来实现。

I. 云硬盘采用分布式存储，每份数据在后台保存多份副本，多副本数据实时同步，不会因存储掉电、故障导致用户数据丢失，保证数据安全可靠。数据存储的持久性可达 99.99995%。

II. 云硬盘的存储系统采用三副本机制来保证数据的可靠性，即针对某份数据，默认将数据分为 1 MB 大小的数据块，每一个数据块被复制为 3 个副本，然后按照一定的分布式存储算法将这些副本保存在集群中的不同节点上。

III. 云硬盘三副本技术的主要特点如下：存储系统自动确保 3 个数据副本分布在不同服务器的不同物理磁盘上，单个硬件设备的故障不会影响业务。存储系统确保 3 个数据副本之间的数据强一致性。天翼云硬盘不支持减容操作。如果当前磁盘使用的是 MBR 格式，并且磁盘的分区数量已经达到上限，则此时需要替换原有分区，替换原有分区不会删除原有分区的数据，但是需要先卸载原有分区，会影响线上业务运行。如果当前磁盘使用的是 MBR 格式，并且扩容后磁盘容量已经超过 2 TB，则 MBR 格式无法对超过 2 TB 的部分进行分区。此时若将 MBR 分区方式换为 GPT，更换磁盘分区方式时会清除磁盘的原有数据，请先对数据进行备份。

IV. 对象存储服务设计可用性不低于 99.9%；数据设计持久性可高达 99.9999999999%；对象存储服务规模可大规模在线扩展，不影响对外服务；支持多副本和纠删码冗余。

➤ 命名规范：对象容器（Bucket）的命名规范是：

- ✧ Bucket 名称必须全局唯一；
- ✧ Bucket 名称长度介于 3 到 63 字节之间；
- ✧ Bucket 名称只能由小写字母、数字、短横线（-）和点（.）组成；
- ✧ Bucket 名称可以由一个或者多个小节组成，小节之间用点（.）隔开，各个小节需要：
 - ✓ 必须以小写字母或者数字开始；
 - ✓ 必须以小写字母或者数字结束。
- ✧ Bucket 名称不能是 IP 地址形式（如 192.162.0.1）；
- ✧ Bucket 名称不能是一组或多组“数字.数字”的组合；
- ✧ Bucket 名称中不能包含双点（..）、横线点（-.）和点横线（.-）；
- ✧ 不允许使用非法敏感字符，例如暴恐涉政相关信息等。

➤ 访问权限

中国电信天翼云对象存储系统提供 Bucket 级别的权限控制, Bucket 目前有 3 种访问权限: public (公有), private (私有), public-read (只读)。各自的含义如下:

- ✧ 公有: 任何人(包括匿名访问)都可以对该容器(Bucket)中的对象(Object)进行 Put, Get 和 Delete 操作。这些操作可能会造成 Bucket 所有者数据的增加或者丢失, 且所有这些操作产生的费用由该 Bucket 的所有者承担, 所以请慎用该权限。
- ✧ 私有: 只有该 Bucket 的所有者可以对该 Bucket 内的对象进行读写操作(包括 Put、Delete 和 Get Object); 其他人无法访问该 Bucket 内的对象。
- ✧ 只读: 只有该 Bucket 的所有者可以对该 Bucket 内的对象进行写操作(包括 Put 和 Delete Object); 任何人(包括匿名访问)可以对该 Bucket 中的对象进行读操作(Get Object)。

V. 弹性文件服务具备高可用性和持久性, 为海量数据、高带宽应用提供有力支持。

18. 天翼云高可用案例介绍

分布式消息服务解决方案: 基于天翼云提供完整的电商云解决方案, 提供资源的弹性伸缩能力、全方位的云安全服务、分布式云中间件、微服务应用平台等, 帮助企业快速搭建安全可靠的电商云平台, 从容应对促销、秒杀场景; 大数据服务能力帮助客户进行精准营销和用户运营。

19. 高性能架构衡量指标

从技术人员的视角, 我们可以从响应时间、吞吐量、并发量、性能计算器来了解。

- (1) 响应时间: 指应用执行一个操作需要的时间, 包括从发出请求开始到收到最后响应数据所需要的时间。它直观的反映了系统的“快慢”;
- (2) 并发数: 指系统能够同时处理请求的数目, 这个数字直接反映了系统的负载特性。
- (3) 吞吐量: 指单位时间内系统处理的请求数量, 体现系统的整体处理能力;
- (4) 性能计算器: 它是描述服务器或者操作系统性能的一些数据指标。包含系统负载、对象与线程数、内存使用、CPU 使用、磁盘与网络 IO 等。

20. 高性能架构的设计原则

高性能架构的设计主要集中在两个方面: 设计时尽量提升单服务器的性能, 将单服务器的性能发挥到极致; 如果单服务器无法支撑性能, 考虑服务器集群方案。

(1) 计算高性能:

- ① 单服务器高性能: 它设计的关键之一就是服务器采取的网络编程模型;
- ② 集群高性能: 它的本质很简单, 通过增加更多的服务器来提升系统整体的计算能力。我们可以选择水平扩展的方式——也就是增加机器, 以扩大计算能力。

(2) 存储高性能: 存储高性能主要解决存储层读写性能低的问题, 常见的方式有: 读写分离、数据分

片、添加缓存。

- ① 读写分离：该方式适合读多写少的场景，通过增加机器水平扩展，使得读性能同步提高。该架构往往采用主从架构，主机写，从机读，但是主从同步需要时间，特别是在网络状况差的情况下，耗时能到分钟级别。这时如果主、从数据往往不一致，会导致数据延迟；
- ② 数据分片：当单机无法存储全部数据时，需要对数据进行分片存储。但是如何设计分片却是个问题；
- ③ 添加缓存：缓存主要是为了弥补存储系统在复杂业务场景下的不足，数据落地存储一般在 SSD 或者硬盘中，其吞吐量大但是延迟高，而缓存一般以内存为载体，速度高但是容量低。可以将热数据放在缓存中，这样数据请求时，不必访问低速的最终存储，转而访问高速的缓存，这样可以减少响应耗时。

21. 高性能架构的传统解决方案

主要从升级硬件配置、优化架构、就近部署来考虑。

- (1) 硬件配置是实现高性能服务的先决条件，在硬件配置方面经常需要使用的高性能方案。服务器性能主要从 CPU、内存和磁盘三个方面来考虑；在网络方面，只有在保证带宽的情况才能实现高性能服务。
- (2) 优化架构：主要是从可扩展和缓存两个方面来考虑。分布式缓存-缓存的本质是通过 key-value 形式的 Hash 表来提升读写速度；在可扩展性方面，我们了解低耦合的系统更容易扩展，低耦合的模块更容易复用，一个低耦合的系统设计也会让开发过程和维护变得更加轻松和容易管理。在这里，我们主要是考虑是服务分层。
- (3) 就近部署，这里我们会提到异地多活数据中心和 CDN 加速。异地多活数据中心：异地多活指分布在异地的多个站点同时对外提供服务的业务场景。异地多活与传统的灾备设计的主要区别在于“多活”，即所有站点都是同时在对外提供服务的；CDN 加速将网站的内容缓存在网络边缘（离用户接近网络最近的地方），然后在用户访问网站内容的时候，通过调度系统将用户的请求路由或者引导到离用户接入网络最近或者访问效果最佳的缓存服务器上，由该缓存服务器为用户提供内容服务。

22. 传统解决方案存在的问题

在高性能架构的基础设施层，如果业务扩大，可以采取横向扩展或者纵向扩展的方式；如果线下搭建高性能架构，需要很成熟的技术作为支撑，并且需要投入较高的资金成本。

23. 传统架构的痛点

系统紧耦合，效率低，难扩展；”烟囱式“结构，容易形成资源和信息孤岛；流程化系统饼图，效率低；套装系统软件，响应慢；多类型前端、后端难以打通；面对突发的海量业务，无法高效处理消息。

24. 分层解耦架构的概念

这里需要了解松耦合、紧耦合、解耦的相关概念。

(1) 松耦合系统通常是基于消息的系统，此时客户端和远程服务并不知道对方是如何实现的。客户端和服务之间的通讯由消息的架构支配，只要消息符合协商的架构，则客户端或服务的实现就可以根据需要进行更改。松耦合架构的优点：

- ① 多任务并行处理能力获得极大提升；
- ② 实现负载自适应机制；
- ③ 基本杜绝了对 Server 服务端的网络攻击行为，由于代理服务器的隔绝和筛查作用，同时结合其它安全管理手段，当外部攻击代理服务器时就会被识别和过滤掉，这样就保护了后面的服务器不受影响；
- ④ 异步操作减少了网络资源消耗和操作关联；
- ⑤ 提高了系统的可维护性。

(2) 紧耦合是模块或者系统之间关系太紧密，存在相互调用。紧耦合架构优点：架构简单、设计简单、开发周期短、能够快速的发展、投入、部署、应用。

(3) 解耦合的字面意思就是解除耦合，将系统之前的耦合关系解除，形成相对独立的模块。但是在软件工程中，做到完全解耦是不太可能的，因此，降低耦合度即可以理解为解耦。解耦合架构的优势：

- ① 模块化，缩小故障范围；
- ② 降低变更成本；
- ③ 开发人员写作更简单；
- ④ 易于扩展。

25. 分层解耦架构常见方案

支撑分层解耦架构的解决方案常见的有中间件，微服务。

(1) 中间件在操作系统、网络和数据库之上，应用软件的底层，它的作用是为处于自己上层的应用软件提供运行与开发的环境，帮助用户灵活、高效地开发和集成复杂的应用软件。消息中间件的使用：即将同步转为异步，通过异步来实现解耦。我们可以先将消息发送给消息中间件，只要消息中间件是高可用性的没有宕机，整个接口集成过程就是 OK 的，而消息中间件再以异步方式分发消息给目标系统，同时支持重试

(2) 微服务：如果微服务已经实施完成并出现了大量紧耦合的情况，那么我们就需要在后期考虑对微服务架构进行重构。

26. 消息队列能解决的问题

系统耦合性；处理性能低；扩展难度大。

27. 消息中间件的作用

消息中间件实现了发布者和订阅者在时间、空间和流程三个方面的解耦。

28. 分布式消息服务

分布式消息服务（Distributed Message Service，简称 DMS）是一项基于高可用分布式集群技术的消息中间件服务，提供了可靠且可扩展的托管消息队列，用于收发消息和存储消息。使用 DMS，您可以创建消息队列，将消息队列作为一个传输消息的中转站，存储应用程序不同组件间传递的消息，从而做到在应用程序的不同组件之间传输消息时，不要求各个组件同时处于可用状态。它可以加快系统的响应速度、降低耦合性、实现数据缓存。

29. 分布式消息服务的优势

主要从性能、灵活性、可靠性、集成这四个方面来考虑。

- (1) 性能方面：支持亿级消息堆积，在消息堆积下不影响队列性能，单队列最高至 10 万 TPS，并可通过队列数扩展提升整系统并发能力；
- (2) 灵活性：队列处理能力按需自动扩展，及时方便完成系统扩展，消息投递时间可至毫秒级，保证消息及时性；
- (3) 可靠性：支持数据同步落盘与多副本冗余，数据可靠性高达 99.99999999%，采用集群化部署，保障服务可用性高达 99.95%；
- (4) 集成：支持多种队列类型（普通、有序、Kafka）以及多协议（HTTP RESTful、TCP、Kafka）接入，轻松完成和其他系统的集成。

30. 分布式消息服务场景：

- (1) 分布式系统异步通信：在单体应用中，各服务耦合度紧，单个服务出现问题会导致系统对用户请求响应慢，可以进行系统解耦拆分，并用消息队列作为系统间的异步通信通道，提升整个系统的响应速度。
- (2) 削峰填谷：在电子商务系统或大型网站中，系统上下游处理能力存在差异，当处理能力高的系统上游突发请求超过系统下游处理能力时，系统对外呈现的服务能力为 0。此时可以通过队列服务堆积请求消息，对请求消息实现削峰填谷，错峰处理，避免下游因突发流量崩溃。
- (3) 分布式消息服务 RabbitMQ 的应用场景：应用解耦：以电商秒杀、抢购等流量短时间内暴增场景为例，传统做法如果库存系统发生故障，订单系统获取不到数据，订单失败。这种情况下，订单系统和库存系统两个子系统高耦合，分布式消息即可顺畅支撑应用系统解耦。
- (4) 分布式消息服务 Kafka 应用场景：日志收集：Kafka 能够做到流计算处理，如股市走向分析、气象数据测控、网站用户行为分析等，这些领域中数据产生快、实时性强、数据量大，很难统一采集并入库存储后再做处理。而 Kafka Stream 以及 Storm/Spark 等流计算引擎，可根据业务需求对数据进行计算分析，最终把结果保存或者分发给所需组件。

31. 天翼云微服务平台快速搭建微服务架构

- (1) 天翼云微服务云应用平台（ServiceStage，CT-SS）是面向企业级开发一站式 DevOps 平台服务，支持基于微服务的应用开发、治理、部署及运维监控的全生命周期管理，并提供大规模容器集群管理等平台能力，帮助用户快速构建云分布式应用。
- (2) 平台优势：开放-微服务框架；治理-保障高可靠；管理-全生命周期；灵活-弹性伸缩。
- (3) 构建分布式系统：分布式应用相对于传统单进程应用新增或加强了很多技术点，例如服务发现，负载均衡，熔断容错，限流降级，调用追踪，日志聚合等，把这些通用能力全部打包到一个 SDK 里，开发人员只需几个简单的注解即可把上述所有通用能力导入到其开发的业务微服务里，对业务逻辑完全无侵入性。

32. 天翼云服务分层解耦架构案例

工业电商云解决方案-基于天翼云提供完整的电商云解决方案，提供资源的弹性伸缩能力、全方位的云安全、分布式云中间件、微服务应用平台等，帮助企业快速搭建安全可靠的电商云平台，从容应对促销、秒杀场景；大数据服务能力帮助客户进行精准营销和用户运营。它的优势体现在支持快速弹性伸缩、全面安全防护、数据安全及实现大数据服务。

三、云上安全架构设计

必备掌握知识点：

1. 七类网络安全事件

包括：《国家网络安全事件应急预案》规定，网络安全事件是指由于人为原因、软硬件缺陷或故障、自然灾害等，对网络和信息系统或者其中的数据造成危害，可分为有害程序事件、网络攻击事件、信息破坏事件、信息内容安全事件、设备设施故障、灾害性事件和其他事件。

2. 网络安全事件的分级

依据损失程度，分为 4 级：特别重大、重大、较大、一般。

3. 中国第一部《网络安全法》

我国第一部《网络安全法》于 2020 年 6 月 1 日起正式实施。

4. 等保概念

等保是指对网络和信息系统按照重要性等级分级别保护的一种工作。安全保护等级越高，安全保护能力就越强。根据信息系统在国家安全、经济建设、社会生活中的重要程度，以及信息系统遭到破坏后对国家安全、社会秩序、公共利益，以及公民、法人和其他组织的合法权益的危害程度等因素，将信息系统安全等级由低到高分五个等级。

5. 传统安防方案

包括：硬件防火墙、硬件 WAF、硬件 Anti-DDoS。

6. 新型安防方案

包括下一代防火墙、态势感知

7. 安全责任共担模型

不同组织承担实施、运维和管理不同的责任。因此安全责任由不同的组织分担，所有的参与的组织都包含其中。这个体现安全责任的模型被称为共享责任模型。

8. 云服务提供商 CSP 的安全责任包括：

- (1) 承担全部基础设施的安全；
- (2) 网络安全，承担网络隔离、安全服务白名单、外部 DDoS 泛洪攻击、扫描的防护；
- (3) 主机安全，承担虚拟化层的安全加固、系统镜像库、租户根访问权限。

9. 云租户 CSC 安全责任包括：

- (1) 承担虚拟机内应用的安全；
- (2) 网络安全，承担网络威胁检测、安全监控；
- (3) 主机安全，承担访问控制管理、补丁管理、配置加固、安全监控、日志分析。

10. 天翼云通用场景安全服务解决方案，以云平台数据安全为核心，主要覆盖网络、系统（主机）、应用、数据、运维等基础领域。

11. Anti-DDoS 流量清洗（CT-AntiDDoS，Anti-DDoS）通过专业的 DDoS 防护设备来为用户互联网应用提供精细化的抵御 DDOS 攻击能力，如 UDP Flood 攻击、SYN Flood 攻击和 CC 攻击等。用户可以业务模型配置流量参数阈值，可以监控攻防状态，实时保证业务安全运行。拒绝服务攻击（Denial of Service Attack，缩写：DoS）亦称洪水攻击，是一种网络攻击手法，其目的在于使目标电脑的网络或系统资源耗尽，使服务暂时中断或停止，导致合法用户不能够访问正常网络服务的行为。当黑客使用网络上两个或以上被攻陷的电脑作为攻击机器向特定的目标发动“拒绝服务”式攻击时，称为分布式拒绝服务攻击。天翼云 Anti-DDoS 流量清洗功能提供查看安全报告能力，其查看区间为一周。

12. SSL VPN 统一业务安全接入平台，帮助用户在任何时间、任何地点、使用任何主流终端，安全、快速地接入业务系统。它以 SSL/IPSec 二合一 VPN 安全网关为基础，融合远程应用发布（EasyConnect）等多种移动终端的安全接入方式，通过构建一套平台，即可满足移动办公、分支互联、协同办公、应用虚拟化等多种需求。

13. 服务器安全卫士

通过对主机信息和行为进行持续监控和分析，快速精准地发现安全威胁和入侵事件，并提供灵活高效的问题解决能力，将自适应安全理念真正落地，为用户提供下一代安全检测和响应能力。

14. 服务器安全卫士产品

规格分为三种：基础版、企业版、旗舰版。应用风险的功能是只有旗舰版才支持的功能。

15. Web 应用防火墙（CT-WAF, Web Application Firewall）

一款专业为网站提供安全防护的服务。通过多维度防御策略，为网站拦截 SQL 注入、XSS 跨站、命令&代码注入、敏感文件访问、恶意爬虫等 Web 类型的攻击，保障您的业务安全稳定运行。

16. 天翼云数据库安全为天翼云用户提供数据脱敏、数据库审计、敏感数据发现和数据库攻击防护等功能，是一体化数据库安全解决方案，利用反向代理技术，部署在数据库的前端，为数据库提供实时安全保护和合规性的数据库安全防护服务。

17. 数据加密服务基于国家密码局认证的硬件加密机提供可独占、高性能、安全合规的加密域计算资源，将用户线下加密设备能力转移到云上，为用户提供云上数据加密服务，可处理加解密、签名、验签、产生密钥和密钥安全存储等操作。

18. 日志审计（CT-LA Log Audit）通过主被动结合的方式，实时不间断地采集用户网络中各种不同厂商的安全设备、网络设备、主机、操作系统、以及各种应用系统产生的海量日志信息，并将这些信息汇集到审计中心，进行集中化存储（可根据日志规模大小进行分布式存储，支持水平弹性扩展和数据高可靠性存储）、索引、备份、全文检索、实时搜索、审计、告警、响应，并出具丰富的报表报告，获悉全网的整体安全运行态势，实现全生命周期的日志管理。

19. 态势感知为用户提供统一的威胁检测和风险处置平台。态势感知能够帮助用户检测云上资产遭受到的各种典型安全风险，还原攻击历史，感知攻击现状，预测攻击态势。

20. 天翼云态势感知服务高级版的独有功能包括：权威情报数据、权威安全预警、攻击源警告和恶意网站告警。

21. 云堡垒机是一款针对云主机、云数据库、网络设备等的运维权限、运维行为进行管理和审计的服务。主要解决云上 IT 运维过程中操作系统账号复用、数据泄露、运维权限混乱、运维过程不透明等难题。云服务器配置决定云堡垒机的并发性能，并发会话数指运维端和云服务器的运维连接数；并发会话数取决于云服务器的硬件配置，可以通过提高硬件配置来提高并发会话数。

22. 云上安全架构设计原则为：

（1）没有绝对的安全，根据业务实际需要与预算进行合理设计。

（2）安全是一项系统工程，适用木桶原则：任何一项安全短板都会降低整体的安全性。因此在安全设计规划阶段需要系统性地对网络、主机、应用、数据和运维各方面的安全风险进行规划防范。

（3）规划的思路我们可以从各方面面临的安全威胁入手，进而得到需要落地的防护技术。

23. 天翼云整体安全架构由网络安全、主机安全、数据安全、应用安全和运维安全服务组成。天翼云提供一站式云安全解决方案，不仅保障物理、环境安全和虚拟化安全，同时可解决基础设施、应用和数据相关的全方位安全控制与防护。

24. 天翼云等保合规服务流程包括以下四个环节：

- (1) 定级备案：主要对信息系统的重要程度进行定级，并与公安机关进行系统备案；
- (2) 差距分析：根据等级保护体系的标准与规范，进行合规性与风险分析；
- (3) 安全整改：提出贴合信息系统实际情况的安全整改与加固设计方案；
- (4) 等保测评：对信息系统进行测评，并出具等级保护测评报告。

25. 天翼云 5S 安全体系包括系统 (System)、保密 (Secrecy)、持久 (Sustainability)、标准 (Standard) 和服务 (Service) 五部分内容。

四、云上运维架构

必备掌握知识点：

1. 传统运维工具——Cacti、Nagios、Ganglia、Zabbix、Centreon。
2. 管理控制台是网页形式的，您可以使用直观的界面进行相应的操作。而如果您需要将云平台上的服务集成到第三方系统，用于二次开发，可以选择 API 的方式来进行云资源的运维和管理。
3. 天翼云管理控制台是统一查看和管理天翼云产品及服务的平台。管理控制台面向天翼云用户，通过图形化界面、Cloud shell 命令行工具等进行配置操作。核心功能主要包括但不限于：
 - (1) 管理云账号和基础安全设置。
 - (2) 获取在天翼云消费的所有账单信息，管理发票、合同等财资业务。
 - (3) 全面使用和管控天翼云产品。
 - (4) 订阅第三方合作伙伴提供的应用。
 - (5) 通过工单方式获得服务支持等等。
4. API，英文全称 Application Programming Interface，翻译为“应用程序编程接口”。是一些预先定义的函数，目的是提供应用程序与开发人员基于某软件或硬件得以访问一组例程的能力，而又无需访问源码，或理解内部工作机制的细节。
5. 云 API 产品优势：
 - (1) 云 API 提供多语言 SDK，方便开发者访问 API。
 - (2) 简单配置即可快速提供 API，少量的代码即可轻松使用 API。
 - (3) 私有加密协议，传输内容更精简，使用更安全。
 - (4) 完善的监控报警功能让您无忧管理 API。
6. 在监控的通用架构中，首先，监控系统在监控对象中进行数据采集，比如在 ECS 云主机或者 RDS 云数据库中进行数据的采集。然后，采集到的各类指标进行各种处理后会进行监控数据的存储。最后数据会应用到两个重要的用途——监控告警和监控展示。
7. 云监控服务面向云主机、云硬盘、RDS 等产品提供监控服务，实现性能指标监控、自动告警、历史信息查询等功能。借助云监控服务，用户可以更详细地了解云资源的使用情况，方便用户及时调整。云监

控目前支持的指标如下所示：

- (1) 弹性云主机 9 个指标：CPU 使用率、磁盘读速率、磁盘读操作速率、磁盘使用率、磁盘写速率、磁盘写操作速率、内存使用率、带内网络流入速率和带内网络流出速率。
- (2) 云硬盘 4 个指标：卷读速率、卷写速率、卷读请求速率、卷写请求速率。
- (3) 弹性伸缩组 1 个指标：实例数。
- (4) 负载均衡 10 个指标：并发连接数、活跃连接数、非活跃连接数、新建连接数、流入数据包数、流出数据包数、网络流入速率、网络流出速率、异常主机数、正常主机数。
- (5) 虚拟私有云 2 个指标：上行带宽、下行带宽。
- (6) 关系型数据库 40 个指标：CPU 使用率、内存使用率、IOPS、网络输入吞吐量、网络输出吞吐量、数据库总连接数、当前活跃连接数、QPS、TPS、缓冲池利用率、缓冲池命中率、缓冲池脏块率、InnoDB 读取吞吐量、InnoDB 写入吞吐量、InnoDB 文件读取频率、InnoDB 文件写入频率、InnoDB 日志写请求频率、InnoDB 日志物理写频率、InnoDB 日志 fsync() 写频率、临时表数量、Key Buffer 利用率、Key Buffer 写命中率、Key Buffer 读命中率、MyISAM 硬盘写入频率、MyISAM 硬盘读取频率、MyISAM 缓冲池写入频率、MyISAM 缓冲池读取频率、Delete 语句执行频率、Insert 语句执行频率、Insert_Selection 语句执行频率、Replace 语句执行频率、Replace_Selection 语句执行频率、Selection 语句执行频率、Select 语句执行频率、Update 语句执行频率、行删除速率、行插入速率、行读取速率、行更新速率、硬盘利用率。
8. 云监控的主要功能：监控概览、云主机监控、云服务监控、数据可视化、支持查看和导出监控数据、支持告警管理。其中，云主机监控功能主要是指基础监控和操作系统监控。
9. 云监控内部组件大体上可以划分为 Console 模块、API 模块、消息队列模块、告警处理模块、数据聚合模块和数据库模块。一个典型的业务流程：被监控的云服务（比如弹性云主机）将指标数据上报到云监控，用户通过 console 模块添加告警规则，告警规则通过 API 模块处理后，一方面将规则入库，一方面通过消息队列模块下发告警规则到告警处理模块。告警处理模块按照设置的规则从聚合模块取数据，判断处理告警状态后触发告警或通知。
10. 天翼云云审计服务是天翼云安全解决方案中专业的日志审计服务，提供对各种云资源操作记录的收集、存储和查询功能，可用于支撑安全分析、合规审计、资源跟踪和问题定位等常见应用场景。
11. 云审计的功能：
 - (1) 记录审计日志：支持记录用户通过管理控制台或 API 接口发起的操作，以及各服务内部自触发的操作。
 - (2) 审计日志查询：支持在管理控制台对 7 天内操作记录按照事件来源、资源类型、事件名称、资源名称/ID、事件级别和时间范围等多个维度进行组合查询。

(3) 审计日志转储：支持将审计日志周期性的转储至对象存储服务（Object Storage Service，简称 OSS）下的 OSS 桶，转储时会按照服务维度压缩审计日志为事件文件。

12. 立体化运维：天翼云提供应用运维管理和应用性能管理结合的立体化运维解决方案，为大型分布式应用保驾护航。

13. 运维的发展

(1) 手工管理阶段。通过人工，对机房动力环境，以及服务器、数据库、存储介质、网络等生产设备进行管理。

(2) 工具批量操作阶段。借助一些软件工具，比如 Shell 脚本、厂家网管界面等，进行管理。

(3) 平台管理阶段。通过综合网管界面、专业运维平台厂家等进行运维管理。

(4) 系统自调度阶段。这是针对云服务的运行方式采取的一种自动化运维的方式。

除此之外，当前还衍生出了运维+开发（DevOps）和人工智能+运维（AI+Ops）的方向，也会是未来的发展趋势。

14. 云运维的难点

(1) 多厂家：存在不同厂家互联互通的壁垒。

(2) 多层级：云架构包含多个层级，涉及各类软硬件，接口类型也多。

(3) 多指标：不同类型软硬件的指标不同，而且既有国际标准指标项，也有各自厂家或行业自定义的指标。

15. 自动化运维逻辑架构，自下而上分别为：

(1) 管控平台。

(2) 系统平台：数据平台、容器管理平台、操作平台、配置平台。

(3) 集成平台：主要提供各类接口。

(4) 网管平台：包括标准运维、监控系统、故障自愈、运维日志等。

16. 天翼云云监控服务应用场景

(1) 查看运行状态，设置监控项和告警规则。场景优势包括：实时可视化监控、重点指标集中呈现、个性化定制告警服务。搭配使用的云产品有：云主机、云硬盘、弹性 IP、裸金属、弹性伸缩、负载均衡等。

(2) 异常场景及时处理。场景优势包括：及时发送告警信息，灵活设置告警规则。搭配使用的云产品有：云主机、云硬盘、弹性 IP、裸金属、弹性伸缩、负载均衡等。

17. 其他自动化运维工具，由底层向上分为：

(1) 初始化工具，用于操作系统的安装，或云上虚拟机，如：Kickstart、Cobbler、Docker

(2) 配置管理工具，用于系统配置，如：Cfengine、Puppet

(3) 命令和控制工具，用于提供应用服务，如：Fabric、SaltStack、Ansible

(4) 平台工具，如：云厂家网管平台

五、容灾备份架构设计

必备掌握知识点：

1. 灾难的定义：从一个计算机系统的角度来讲，一切引起系统非正常停机的事件都可以称为灾难。针对系统的灾难大致可以分成以下三个类型：
 - (1) 自然灾害，包括地震、火灾、洪水、雷电等，这种灾难破坏性大，影响面广。
 - (2) 设备故障，包括主机的 CPU、硬盘等损坏，电源中断以及网络故障等，这类灾难影响范围比较小，破坏性小。
 - (3) 数据中心故障，包括电源故障、人为蓄意破坏等等，都可能影响 IT 系统业务连续性。
2. 容灾就是在灾难发生时，在保证生产系统的数据尽量少丢失的情况下，保持生存系统的业务不间断地运行。容灾系统是指在相隔较远的异地，建立两套或多套功能相同的 IT 系统，互相之间可以进行健康状态监视和功能切换，当一处系统因意外(如火灾、地震等)停止工作时，整个应用系统可以切换到另一处，使得该系统功能可以继续正常工作。
3. RPO: (Recovery Point Objective, 恢复点目标) 是指业务系统所允许的在灾难过程中的最大数据丢失量，用来衡量容灾系统的数据冗余备份能力。RPO: 以数据为出发点，衡量能够容忍的数据丢失量。
4. RTO: (Recovery Time Objective, 恢复时间目标) 是指信息系统从灾难状态恢复到可运行状态所需的时间，用来衡量容灾系统的业务恢复能力。RTO: 以应用为出发点，衡量能够容忍的应用系统恢复时间。
5. 镜像是在两个或多个磁盘或磁盘子系统上产生同一个数据的镜像视图的存储过程。远程镜像技术是在主数据中心和备援中心之间的数据备份时用到。同步远程镜像也叫同步复制技术，是指通过远程镜像软件，将本地数据以完全同步的方式复制到异地，每一本地的 I/O 事务均需等待远程复制的完成确认信息，方予以释放。异步远程镜像也称异步复制技术，保证在更新远程存储视图前完成向本地存储系统的基本操作，而由本地存储系统提供给请求镜像主机的 I/O 操作完成确认信息。远程的数据复制是以后台同步的方式进行的，这使本地系统性能受到的影响很小，传输距离长(可达 1000 公里以上)，对网络带宽要求小。
6. 快照是通过软件对要备份的磁盘子系统的数据快速扫描，建立一个要备份数据的快照逻辑单元号 LUN 和快照 cache。快照是通过内存作为缓冲区(快照 cache)，由快照软件提供系统磁盘存储的即时数据映像，它存在缓冲区调度的问题。
7. 基于 IPSAN 的远程数据容灾备份技术：利用基于 IP 的 SAN 的互连协议，将主数据中心 SAN 中的信息通过现有的 TCP/IP 网络，远程复制到备援中心 SAN 中。

8. 数据容灾，是指建立一个异地的数据系统，该系统是本地关键应用数据的一个可用复制。应用容灾，是在数据容灾的基础上，在异地建立一套完整的与本地生产系统相当的备份应用系统（可以是互为备份）。业务级容灾是全业务的灾备，除了必要的 IT 相关技术，还要求具备全部的基础设施。
9. 备份指将文件系统或数据库系统中的数据加以复制，一旦发生灾难或错误操作时，得以方便而及时地恢复系统的有效数据和正常运作。
10. 根据备份的时间及读写可用性可以将备份分为冷备、热备和温备，冷备：备份点平时不启动（甚至可以在主节点首次故障时才进行部署），当主节点故障时，需要先恢复备份点的数据，再启动备份组件。热备：备份点提前部署好。备份组件启动但不处理数据或请求。数据几乎实时镜像到备份点，主备系统有一致的数据。温备：备份点提前部署好，但备份组件平时不启动。当主节点故障时，启动备份节点上的备份组件。
11. 根据备份的内容可以将备份分为全量备份、增量备份以及差异备份，全量备份就是指对某一个时间点上的所有数据或应用进行的一个完全拷贝。增量备份是指在一次全备份或上一次增量备份后，以后每次的备份只需备份与前一次相比增加和者被修改的文件。差异备份：是指在一次全备份后到进行差异备份的这段时间内，对那些增加或者修改文件的备份。
12. Host-Base 备份方式，基于主机的备份系统是最简单的一种数据保护方案，在大多数情况下，这种备份大多是采用服务器上自带的磁带机或备份硬盘，而备份操作往往也是通过手工操作的方式进行的。
13. LAN-Base 备份方式，LAN-Based 备份结构，是小型办公环境最常使用的备份结构。在该系统中数据的传输是以局域网络为基础的，首先预先配置一台服务器作为备份管理服务器，它负责整个系统的备份操作。磁带库则接在这台备份服务器上，当需要备份数据时，备份服务器把数据通过网络传输到磁带库中，完成数据的备份。
14. LAN-free 有多种实施方式。通常用户都需要为每台服务器配备光纤通道适配器，适配器负责把这些服务器连接到与一台或多台磁带机相连的 SAN 上。同时，还需要为服务器配备特定的管理软件，通过它，系统能够把块格式的数据从服务器内存、经 SAN 传输到磁带机或磁带库中。还有一种常用的 LAN-free 实施办法，在这种结构中，主备份服务器上的管理软件可以启动其他服务器的数据备份操作。块格式的数据从磁盘阵列通过 SAN 传输到临时存储数据的备份服务器的内存中，之后再经 SAN 传输到磁带机或磁带库中。
15. Server-free 也有几种实施方式。通常情况下，备份数据通过名为数据移动器的设备从磁盘阵列传输到磁带库上。另一种实施方法就是利用网络数据管理协议 (NDMP)。NDMP 把命令从服务器传输到备份应用中，而与 NDMP 兼容的备份软件会开始实际的数据传输工作，且数据的传输并不通过服务器内存。
16. 容灾不等于备份，容灾是为了在遭遇灾害时能保证信息系统能正常运行，帮助企业实现业务连续性的目标，而备份是为了应对灾难来临时造成的数据丢失问题。

17. 容灾和备份的联系：容灾备份产品的最终目标是帮助企业应对灾害，备份是容灾的基石。容灾不能代替备份。
18. 容灾和备份的区别：
 - (1) 容灾主要针对火灾、地震等重大自然灾害，因此生产站点和容灾站点之间必须保证一定的安全距离；而备份主要针对人为误操作、病毒感染、逻辑错误等因素，用于业务系统的数据恢复，数据备份一般是在同一数据中心进行。
 - (2) 容灾系统不仅保护数据，更重要的目的在于保证业务的连续性；而数据备份系统只保护不同时间点版本数据的可恢复。一般首次备份为全量备份，所需的备份时间会比较长，而后续增量备份则在较短时间内就可完成。
 - (3) 容灾保证数据的完整性；备份则只能恢复出备份时间点以前的数据。容灾是在线过程；备份是离线过程。
 - (4) 容灾系统中，两地的数据是实时一致的；备份的数据则具有一定的时效性。故障情况下，容灾系统的切换时间是几秒钟甚至几分钟；而备份系统的恢复时间可能几小时到几十小时。
19. 基于天翼云平台的容灾解决方案有以下亮点：
 - (1) 多数据中心：天翼云在全球分布有多个数据中心，用户可根据需求部署跨地域、跨可用区的天翼云产品，完成容灾架构设计。
 - (2) 稳定：每个区域及产品比较稳定，天翼云关键部件（ELB、ECS、Redis、RDS 等）经多轮迭代具备比较完善的灾备能力，可以实现更细粒度的控制，可以通过更多已经产品化的功能模块实现容灾。
 - (3) 弹性：用户可根据业务需求横向、纵向扩缩容，按需购买使用的服务。
20. ELB 灾备设计：集群部署，多可用区部署，健康检查
21. ECS 灾备设计：快照备份、快照回滚、镜像备份、镜像恢复。如果云硬盘的数据发生错误或者损坏，可以回滚快照数据至创建该快照的云硬盘，从而恢复数据。注意：只支持回滚快照数据至源云硬盘，不支持快照回滚到其它云硬盘。
22. 2200S 灾备设计：多副本保存、数据高可用性，跨地域容灾。
23. 数据库容灾——RDS 同城容灾：通过购买主备实例实现，主备实例采用一主一备的双机热备架构，故障系统 1 分钟自动切换。主节点故障时，主备节点秒级完成切换，整个切换过程对应用透明；备节点故障时，RDS 会自动新建备节点以保障高可用。
24. 数据库容灾——RDS 异地容灾/自建数据库容灾：数据库复制服务（DRS）+OOS 跨区域复制实现主实例和异地灾备实例之间的同步。
25. 应用容灾——同城容灾通用架构：
 - (1) 在同一地域下选择购买云产品。建议在 VPC 网络环境下，选择同一可用区或者同地域不同可用区

的云产品。

(2) 在前端购买 ELB，提供负载功能，当后端 ECS 资源使用紧张时可以直接横向扩展，对业务无影响。

(3) 建议 ECS 服务器至少两台，避免单点故障。

(4) 数据库业务尽量不要和应用服务部署在同一台 ECS 上，防止不同服务之间资源抢占，同时方便日常管理和后期扩容。数据库服务器推荐直接购买 RDS 产品，数据安全有保障，同时也不需要花太多精力去运维管理。

26. 应用容灾——同城容灾推荐架构：

(1) 在同城不同可用区之间对原有应用架构做一套完整的备份，ELB、ECS、RDS 等均在两个机房同时部署。

(2) 前端部署 DNS 解析，如果某个可用区出现像 IDC 机房断电或者火灾等机房级故障时，可以通过前端切换 DNS 来及时恢复业务。

(3) 非机房级故障（某个机房的单产品故障，如其中一个机房的 ECS 服务器损坏），故障切换保障由单产品的灾备设计保障。

27. 天翼云同城容灾架构优势：

(1) 可用区之间高速、低延时互联，快速复制数据。

(2) 可用区之间配置网络一体化环境，方便发布、部署、配置变更等工作。

(3) 负载均衡（ELB）支持多可用区实例，产品化实现容灾及切换。用户设置负载均衡监听器转发策略时，可选择轮询、最小连接数和源地址三种模式的转发规则。

(4) ELB 可直接同时挂载多个可用区的 ECS，实现负载均衡及容灾切换。

(5) 数据库支持多可用区实例，产品化实现灾备切换。

28. 应用容灾——异地容灾架构设计：

(1) 在不同地域、不同可用区中均对原有应用架构做一套完整的备份。

(2) 不同地域之间可以采用天翼云的高速通道进行私网通信，保障数据库之间的数据实时同步，将数据传输延迟降到最低。

(3) 故障发生时可以通过前端 DNS 实现快速切换，及时恢复业务。这种容灾架构方式既可以解决单机房故障也可以应对像地震等灾难性故障。

(4) 业务系统和容灾系统产生的配置信息、日志、快照和备份文件等，通过 OOS 跨区复制，完成主实例和容灾实例之间的数据同步。

29. 天翼云异地容灾架构优势：

(1) 云 DNS 提供智能解析、方便流量分配或容灾切换。

(2) 提供 VPC 之间的高速通道，提供统一发布、部署、配置变更功能。

- (3) 产品化提供 OOS 不同区域之间的数据复制。
- (4) 通过数据库复制服务（DRS）提供不同区域之间的数据同步。
- 30. 天翼云混合云自助式容灾服务提供准应用级热备容灾服务，支持物理隔离或逻辑隔离模式的容灾中心，提供“自服务”的数据传输计划、容灾演练、切换、恢复服务。
- 31. 数据备份顾名思义，就是将数据以某种方式加以保留，以便在系统遭受破坏或其他特定情况下，重新加以利用的一个过程。数据备份的根本目的，是重新利用，这也就是说，备份工作的核心是恢复，一个无法恢复的备份，对任何系统来说都是毫无意义的。
- 32. 基于天翼云平台构建的备份解决方案具备以下优势：
 - (1) 依托于天翼云的“无限”扩展能力为用户提供按需调用的数据备份资源。
 - (2) 利用多点分布的云资源池满足用户异地备份的需求。
 - (3) 通过数据中心内部的高速网络传输数据提供高性能的传输。
- 33. 云主机备份：
 - (1) 通过存储一致性快照技术，将云服务器包含的多个云硬盘的数据，以及云服务器的配置规格信息（CPU、内存、网卡等配置）备份到对象存储。
 - (2) 支持周期性自动备份。
 - (3) 支持恢复原云服务器，和使用备份数据创建镜像，发放新云服务器。
- 34. 云硬盘备份：
 - (1) 通过存储快照技术，将云硬盘数据备份到对象存储。
 - (2) 支持周期性自动备份。
 - (3) 支持恢复原云硬盘，和使用备份数据创建新云硬盘。
- 35. 永久增量备份：
 - (1) 首次备份为全量备份，备份硬盘已用的数据块；后续备份为增量备份，备份全量备份之后变化的数据块。
 - (2) 每个备份点都是一个虚拟的全备，多次备份间有依赖关系的数据块以指针索引的方式引用。
 - (3) 删除某个备份数据（手工删除或者自动过期）时，仅删除它没有被其他备份数据所依赖的数据块。
- 36. 崩溃一致性备份：基于多个云硬盘的一致性快照技术，实现云服务器的崩溃一致性备份（云服务器内的多个云硬盘的备份为同一时间点创建的；但备份前未冻结应用和文件系统，不备份内存数据）。
- 37. 应用一致性备份：需要先冻结应用，保证备份期间正在运行的应用程序能完成所有操作（如数据库事务）并将缓存中的数据刷新到磁盘中。
- 38. 当企业业务已经部署在天翼云云服务器、云硬盘、SFS 服务上时，建议采用云备份解决方案，使用云硬盘备份和云主机备份。

39. 当企业希望将应用通过混合云的方式，将数据、应用备份在天翼云上时，建议使用混合云备份解决方案，通过天翼云备份搭建混合云备份架构，具有以下优势：
- (1) 快速部署，云化交付
 - (2) 安全可靠，异地保护
 - (3) 按需投入，灵活购置，便于管理，运维简单。
40. 天翼云为招商局提供专属云、专用物理机、虚拟私有云、STN 云专线、云托管、系统迁移、云小机等服务，规划双活网络方案，设计云平台灾备中心的 VPC 和各种网络流向。
41. 在借助天翼云平台资源+云专线等资源能力，招商局实现了应用级双活灾备中心的建设，两个中心负载分担业务流量，打造分钟级灾备应急能力，确保招商局综合管控系统可持续、稳定、安全的运行。
42. 为了提升银行的整体效率南京银行依托天翼云云专线将省内 14 个数据节点汇总到的数据中心实现与总部数据互联互通，并通过天翼云提供的存储网关汇聚，以增量备份的形式，配合通用互联网文件系统、网络文件系统、文件传输协议和小型计算机系统接口等多种协议接口，将数据存储到天翼云的对象存储平台南京节点。并以三副本的形式备份电信对象存储平台常州、南通 2 个节点。确保南京银行 1 份数据在南京、常州、南通 3 地各保存 1 份。

六、上云迁移方案

必备掌握知识点：

1. 迁移背景：经过数十年的发展，云计算的应用服务范围日益扩大，影响力也持续增强。随着云计算经历了两大发展阶段，即云计算 1.0 时代与 2.0 时代，企业进行云迁移迫在眉睫。如果说 1.0 时代，云计算企业大量涌现，市场“觉醒”，那么 2.0 时代，大型云服务提供商则聚焦于更完整的产品解决方案、更好的生态建设加速全球化。计算时代的技术变革使得传统平台不再满足企业业务需求，上云成为传统企业转型与数字变革的唯一解决方案。
2. 上云迁移策略：上云迁移策略的主要目标是为应用程序和数据顺利运行提供一个良好的场所。从长远来看，借助云迁移，企业将能够获得这三个好处：节约成本、提高性能和获得充足的安全性。
 - (1) Re-Host 重新托管，也称为“直接迁移”：即对应用程序运行环境不做改变的情况下迁移上云。
 - (2) Re-Platform 更换平台，也称为“修补后迁移”：在迁移上云时，在不改变使用核心架构的基础上，对应用程序做些简单的云优化。
 - (3) Re-Purchase 重新购置，也称为“放弃后购买”：指放弃使用原先的产品，改为采购新的替代产品。
 - (4) Re-factor 重构/重新构建：改变应用的架构和开发模式，进行云原生的应用服务体现，例如单体应用向微服务架构改造。
 - (5) Retire 停用：确定不再使用当前的基础设施，表明这部分系统或应用已经没有使用价值且还在持续消费资源，应该进行必要的归档备份后停用。

(6) Retain 保留：在部分应用或者业务未做好上云准备，或是更为适合本地部署时，保留现状，不强
行进行迁移上云操作。

3. 迁移流程：一般的迁移流程我们会按照评估分析-规划设计-验证实施-优化验收来进行。

(1) 评估分析：收集现网业务应用信息，盘点本地资源，梳理业务流程及依存关系，计划从何处开始向
云上迁移。

① 信息收集：收集业务信息和技术信息。

② 关键性分析。

③ 评估各种费用还有成本。

(2) 规划分析：结合业务目标和愿景，规划采用何种类型的迁移策略来满足业务计划的目标，稳定产品
组合和迁移方式，制定全面的业务上云计划。

① 流程规划

② 解决方案设计

③ 方案验证

(3) 验证实施：天翼云提供灵活且功能强大的迁移工具，结合强大的行业迁移经验及认证合作伙伴计划，
以更高效、更稳健的方式进行迁移，确保其对业务的影响降到最低。

① 环境部署

② 迁移实施

(4) 优化验收：应用在云上运行之，不断将运行模式采用优秀实践转变，持续监控并优化配置提升安全
性、改善性能和可靠性，实现 ROI 达到业务预期。

① 优化

② 验证和评估

4. 上云迁移遇到的挑战

(1) 安全问题：选择好的云计算服务商是很重要的。

(2) 成本管理：企业将业务迁移到云平台的成本可能很高，具体取决于企业必须迁移的数据量，因为迁
移所需的带宽成本等因素必须在其考虑范围内。

(3) 合规性问题：每个企业都应确保所考虑的云计算提供商可以提供与其行业相关的合规性法规兼容的
服务。

(4) 保持可接受的性能：当企业迁移到云平台中时，其业务运营取决于所选云计算平台的性能。

(5) 管理更复杂的环境。

5. 服务器迁移模式介绍

(1) P2P：将物理机服务器上的操作系统及其上的应用程序和数据迁移到另外一台物理服务器；

- (2) P2V: 将物理服务器上的操作系统及其上的应用程序和数据迁移到云平台管理的云服务器中;
- (3) V2V: 从其他云平台或传统虚拟化平台的虚拟主机迁移到天翼云的云虚拟主机, 比如 Vmware 迁移到天翼云, AWS 迁移到天翼云等;
- (4) V2P: 将云平台的云虚拟主机迁移到其他物理服务器上。

6. 服务器迁移方式介绍

(1) 镜像迁移: 镜像迁移是指通过把源主机上的操作系统和应用程序及数据“镜像”到一个虚拟磁盘文件并上传到天翼云镜像中心, 成为上传用户的自定义镜像后通过此镜像启动一个和源主机一模一样的云主机实例, 来达到应用上云迁移的目的。

- ① 冷迁移: 通过工具直接镜像被迁移服务器主机, 但其无法保证数据一致性。
- ② 热迁移: 通过镜像迁移工具部署在被迁移服务主机或远程连接的方式迁移, 迁移过程可以保持数据实时同步。

(2) 手工重新打包部署: 这种方式和物理主机部署方式一致, 需要自己手动重新部署一套完整的。这种方式通用性比较强, 但是效果较低, 操作较为复杂, 需要的人工干预较多, 也有一定的局限性。

7. 天翼云服务器迁移工具介绍: 服务器迁移工具是天翼云为上云用户量身打造的零停机的无缝 P2V/V2V 在线迁移工具。无需中断生产业务, 通过实时复制技术帮用户实现 X86 物理机或虚拟机迁移到天翼云, 帮助企业快速上云。天翼云服务器迁移工具支持系统盘、数据盘, 只要是块设备, 都支持迁移。支持 I SCSI/FC 和 LVM、动态盘、多路径盘等多种磁盘。

(1) 产品功能:

- ① 复制技术: 基于磁盘块级的数据复制, 无需卷改造; 采用 IP 网络的异步传输, 无距离的限制; 限制使用主机的资源, 对主机影响小。
- ② 平台应用方面: 支持异构硬件平台; 支持 Windows/Linux 下的各种应用, 包括自我开发的; 支持异构存储, 可自由选择合适的存储。
- ③ P2V/V2V 迁移: 支持从物理服务器迁移至虚拟服务器; 支持从虚拟机迁移至虚拟机。

(2) 产品优势

- ① 经济高效: 低成本高效率
- ② 操作简单: 可视化界面
- ③ 无缝迁移: 在线不停机
- ④ 兼容性好: P2V V2V

(3) 应用场景: 服务器迁移适用于多种场景, 可以很好的为政府、企业客户以最小化的成本投入实现最大价值, 最有保证力度的迁移解决方案。主要的场景有: 快速上云; 业务迁移; 机房搬迁; 信息化建设。

(4) 上云迁移步骤：服务器迁移操作需要完成安装控制端、购买 License、完成授权、源端安装客户端、配置目的端、迁移。

8. 数据库迁移模式

(1) 在线迁移：在线数据迁移，是指将正在提供线上服务的数据，从一个地方迁移到另一个地方，整个迁移过程中要求不停机，服务不受影响。

(2) 离线迁移：即业务可以忍受长时间停机从而将全部数据一次性整体迁移；或者业务对数据的访问具有明显的热点，并且技术上可以将冷数据与热数据剥离，这样就可以将冷数据下线并迁移到目标端。

(3) 在线迁移与离线迁移的区别在于迁移过程中是否需要停机。

(4) 全量迁移：即搬迁当前库中所有的历史数据（该过程会搬掉库中大部分数据）。

(5) 增量迁移：即记录全量迁移开始的时间，搬迁全量迁移过程中变更了的数据。由于迁移过程中业务服务一直运行，因此全量迁移完成前，也要将全量时间点后的数据追回来。

9. 数据库自带迁移工具

(1) MySQL: Mysqldump 命令是将数据库中的数据备份成一个文本文件。表的结构和表中的数据将存储在生成的文本文件中。

(2) 在创建天翼云关系数据库 MySQL 实例时，不需要配置存储空间。

(3) Oracle: RMAN (Recovery Manager) — 备份与恢复管理器，它提供了一个备份资料库保存备份的详细信息，可以给出针对备份的各种报表，并且整合了相关的操作命令和 SQL*Plus 命令为 RMAN 命令，跨平台的 RMAN 命令既支持交互式调用，也支持脚本式调用，其目的是保护备份并且最大限度地降低备份和恢复操作中发生人为错误的可能性。

(4) RMAN: 可以用来备份和还原数据库文件、归档日志和控制文件。它也可以用来执行完全或不完全的数据库恢复。注意：

① RMAN 不能用于备份初始化参数文件（备份控制文件时一齐备份）和口令文件。

② RMAN 启动数据库上的 Oracle 服务器进程来进行备份或还原。备份、还原、恢复是由这些进程驱动的。

③ RMAN 可以由 OEM 的 Backup Manager GUI 来控制。

(5) SQL Server: SSMS (SQL Server Management Studio)：它是一个集成环境，用于访问、配置、管理和开发 SQL Server 的所有组件。

10. 天翼云数据库复制服务介绍：数据库复制 (CT-DRS, Data Replication Service) 是为上云用户提供的一种易用、稳定、高效、用于数据库在线迁移的云服务，可解决多场景下数据库之间数据流通问题，满足数据传输业务需求，同时减少数据传输成本。实时迁移是指在数据库复制服务器能够同时连通源数据库和目标数据库的情况下，只需要配置迁移的源、目标数据库实例及迁移对象即可完成整个数据

迁移过程，再通过多项指标和数据的对比分析，帮助确定合适的业务割接时机，实现最小化业务中断的数据库迁移。实时迁移支持多种网络迁移方式，如：公网网络、VPC 网络、VPN 网络和专线网络。通过多种网络链路，可快速实现跨云平台数据库迁移、云下数据库迁移上云或云上跨区域数据库迁移等多种业务场景迁移。由于安全原因，数据库的 IP 地址有时不能暴露在公网上，但是选择专线网络进行数据库迁移，成本又高。这种情况下，您可以选用数据库复制服务提供的备份迁移，通过将源数据库的数据导出成备份文件，并上传至对象存储服务，然后恢复到目标数据库。备份迁移可以帮助您在云服务不触碰源数据库的情况下，实现数据迁移。天翼云数据库复制服务中的实时同步功能不会应用于云下数据库迁移上云的场景。

(1) 产品功能：

- ① 在线迁移：数据库在线平滑迁移；
- ② 迁移能力：多种数据库迁移类型；
- ③ 多网络：多种网络场景下数据库迁移；
- ④ 直观可控：多种辅助功能保障迁移可管可控。

(2) 产品优势：

- ① 便捷：操作便捷：操作便捷、简单，仅需按照提示步骤就能搭建完成数据库迁移任务，启动并管理迁移任务，同时支持全量、增量在线迁移。
- ② 高效：周期短：仅需分钟级就能搭建完成数据库在线迁移任务，让整个环境高效快速。
- ③ 无缝：平滑：通过服务化，免去人力成本，硬件成本，极具性价比。支持数据库不停机迁移，最小化迁移过程引起的业务中断时间。
- ④ 直观：直观可控：提供丰富数据辅助功能，迁移监控，数据一致性对比等多项特性，迁移过程的进度及对比可见，提升迁移任务成功率。

(3) 应用场景：

- ① 数据库迁移上云场景：在云上创建数据库后，将面临云下数据库迁移上云的场景，通过在线迁移，有效地将业务系统中断时间和业务影响最小化，实现数据库平滑迁移上云。
- ② 跨云平台数据库迁移：数据库复制服务支持将其他云平台上的数据库的数据在线迁移至本云数据库，无需手动导入导出数据，方便您快速实现迁移过程中业务和数据库不停机，业务中断时间最小化的数据库迁移。
- ③ 云上灾备中心场景：数据库复制可支持本地 IDC 作为业务中心，天翼云作为灾备中心的数据同步。可轻松为本地 IDC 机房实现容灾，而无需预先投入巨额基础设施。建议搭配关系型数据库 MySQL，云专线，虚拟专用网络 VPN 使用。

11. 非结构化数据迁移模式：传统的 NAS 存储存在的问题有如下：

- (1) 性能瓶颈，NAS 机头的瓶颈始终有限，扩容柜能持续扩容，NAS 机头却不行；
- (2) NAS 底层文件系统的限制，最常见的就是但目录下文件数量超过限制了，同时文件数量增大到一定量级，读写效率明显降低；
- (3) 备份问题，也是受限于机头和备份方式，再就是 NAS 文件系统的访问机制，整体效率特别低。

12. 迁移难点

- (1) 用户的存储容量很大，能达到 TB~PB 级别，这样对于迁移来讲也是很大的挑战。
- (2) 规模：同样，您需要一个能够处理数十亿个文件、PB 量级数据的解决方案。
- (3) 延迟感知：规模很重要，但规模的扩大不能建立在网络响应时间延长的基础上。
- (4) 云端适配：如今，在云端存储数据的成本非常低，但是将数据从云端迁出、迁入是非常麻烦的。

13. 天翼云对象存储迁移方式

- (1) 迁移背景：由于非结构化数据不断涌现，会造成种类与数量众多的同时，将非对象存储上的数据迁移到 OOS，这里的数据源可能来自本地或第三方云存储；OOS 之间的数据迁移，此场景是指将 OOS 源桶数据迁移到 OOS 目标桶。
- (2) 迁移方式：一种是云专线迁移；一种是使用天翼云 OOS 数据迁移工具进行迁移。云专线迁移方式为企业上云提供优质的网络传输服务，解决现有业务系统平滑迁移的能力。
- (3) 适用场景：用户将迁移工具部署在本地服务器或云主机上，将其它云存储的数据迁移到对象存储或者进行对象存储各资源池间数据迁移。目前其他云存储支持从阿里云迁移数据至对象存储。
- (4) 对象存储数据迁移工具有以下特点：
 - ① 支持断点续传。迁移过程中，如果出现中断，重新启动工具后，可以继续执行迁移工作。
 - ② 支持流量控制。迁移过程中，可以动态调整从源云存储资源池下载对象时产生的下行流量。
 - ③ 支持迁移指定前缀的文件。
 - ④ 支持对象并行下载和上传。
- (5) 迁移步骤：迁移准备—安装迁移工具—修改配置文件—执行迁移—断点续传—日志。

14. 上云迁移案例项目背景

- (1) 客户背景：本次客户是一家基于工业互联网与物联网，专注高等教育阶段相关教学实训硬件/软件开发、数据平台及教学资源搭建的科技企业。
- (2) 客户为积极响应国家数字化建设，同时也为了促进自身企业的发展，在多方选择之下，决定将自己的主要业务系统“智能编程平台”从自己的数据中心迁移至天翼云。

15. 迁移原则

- (1) 上云先后顺序
 - ① 先简单、后复杂的应用；

- ② 先普通、后重要的应用；
- ③ 先空闲、后繁忙的应用；
- ④ 先应用系统、后数据库；
- ⑤ 结合应用系统的从属关系和与数据库的关联关系等因素，优先迁移非核心业务和紧急上线业务；
- ⑥ 对于业务复杂度高和核心业务需要进行深入调研，细化方案，演练成熟后进行迁移。

(2)分阶段、逐步迁移原则：迁移工作涉及面广，如应用系统、数据库、不同的数据中心网络，涉及的人员有应用开发厂家、IT 维护部门、业务部门和最终用户，各方人员对系统的熟悉程度、配合度对项目的顺利推进，都具有至关重要的作用。

(3)先迁移，后优化原则：避免两个过程互相交叉缠绕，在迁移出现问题时，影响故障定位，无法明晰分工职责，拖延排障时间，最终影响整个项目工期。

(4)数据安全性：迁移过程中需要保证原有数据的安全性，避免因数据迁移造成原有数据的丢失、损坏；同时，通过使用专用线路，或者建立虚拟专用网，以及对迁移过程传输数据的加密，保证迁移前后数据的一致性和过程中数据不被窃取。迁移过后，对关键数据进行一次全备份。

(5)业务连续性：由于业务系统的运行要求不同，对业务连续性的要求也不同。对于关键的连续性要求较高的业务应尽量减少因迁移而造成的停机时间，保证其业务的连续性。

16. 迁移流程



17. 整体迁移过程

(1)调研分析：业务系统信息调研是上云方案设计的基础工作，调研结果也是上云方案设计的主要信息输入。在业务系统信息调研阶段，需获取客户现网数据中心详细信息，如网络拓扑结构，服务器、存储设备类型及负载性能数据，业务系统逻辑架构、业务关联关系及运行环境等；同时，为了保障迁移工作的顺利推进，客户数据迁移需要提前评估所需网络带宽并完成内部网络架构调整，及与天翼云平台的网络连通性测试。

(2)规划设计：分为应用服务器迁移和数据库服务器迁移两种，在应用服务器中有两种方式，一种是

采用服务器迁移工具进行迁移，一种是手动一比一还原复制迁移。数据库迁移建议采用数据库复制技术。

- (3) 测试验证：测试验证必须在迁移实施之前，同比比例缩小的进行 PoC 验证，也叫概念性验证，在选用服务器上运行真实数据的运行，对承载用户量和运行时间进行实际测算，尤其是一些大型应用复杂系统，可以将系统架构进行划分，对功能模块小范围的进行验证和测试。
- (4) 迁移实施：在迁移的过程中需要注意文档的输出、随时记录问题、停机时间窗口提前通知和声明、由专业的开发和运维人员进行迁移实施。
- (5) 监控优化：系统迁移成功后会由客户方专业人员进行对系统业务的监控，天翼云专业运维人员进行云平台，云服务器稳定性的监控。

七、通用解决方案

必备掌握知识点：

1. 天翼云安全服务可以划分为五大模块：网络安全、主机安全、应用安全、数据安全和业务安全。

(1) 网络安全。涉及的重点产品包括：

- ① Anti-DDoS 流量清洗：通过专业的 DDoS 防护设备为用户互联网应用提供精细化的抵御 DDOS 攻击能力，如 UDP Flood 攻击、SYN Flood 攻击和 CC 攻击等。支持提供四层到七层的攻击防护，包括 CC、SYN flood、UDP flood 等所有 DDoS 攻击方式。支持查看安全报告的功能，查看区间为一周，支持查询前四周统计数据，包括防护流量、攻击次数、攻击 top10 排名。
- ② DDos 高防 IP：针对互联网服务器在遭受大流量的攻击后导致服务不可用的情况下，推出的付费增值服务。用户可以通过配置高防 IP，将攻击流量引流到高防 IP，确保源站的稳定可靠。采用替身防御模式，接入防护后，业务 IP 返回的是天翼云高防节点 IP，源 IP 将不再暴露，彻底阻断针对源 IP 的攻击，确保源 IP 安全。
- ③ SSL VPN：统一业务安全接入平台，帮助用户在任何时间、任何地点、使用任何主流终端，安全、快速地接入业务系统，可满足移动办公、分支互联、协同办公、应用虚拟化、APP 安全加固业务需求。
- ④ 域名无忧：为天翼云用户自助实现域名监测、域名告警、域名刷新，通过对电信所有省份的 DNS 服务器的检测，及时发现域名是否被污染，并且提供按次刷新的服务，清除 DNS 服务器缓存，还原原始 DNS 解析记录。
- ⑤ 云解析：使用自主研发的 DNS 专用设备，具备完善的网络架构，支持 IPv6 和下一代互联网技术。
- ⑥ 微隔离防火墙：面向云化数据中心的跨平台统一安全管理软件，能够对数据中心的内部流量进行全面精细的可视化分析和高细粒度的安全策略管理；能够帮助用户快速便捷地实现环境隔离、域间隔离以及端到端隔离。与云下一代防火墙互补，实现纵深防御。

(2) 主机安全，涉及的重点产品包括：

- ① 终端杀毒：面向政企用户，以大数据技术为支撑、以可靠服务为保障，能够精确检测已知病毒木马、未知恶意代码，有效防御 APT 攻击，为政企事业单位提供终端病毒、漏洞管控能力。
- ② 云下一代防火墙：专门为云计算环境设计的虚拟化网络安全产品，以虚拟主机形态，提供高性价比的云安全部署方案，为客户提供了下一代防火墙、高可用性（HA）、入侵防御（IPS）、病毒过滤（AV）、服务质量保证（QoS）、云沙箱、僵尸网络 C&C 防护、IP 信誉等丰富功能。
- ③ 服务器安全卫士：专注于服务端主机的安全防护，通过对主机信息和行为进行持续监控和分析，快速精准地发现安全威胁和入侵事件，包括资产清点、风险发现、入侵检测、合规基线四大功能的智能集成和协同联动。
- ④ 漏洞扫描：通过对网络主机的扫描及时发现安全漏洞，客观评估系统风险等级。
- ⑤ 登录保护：采用双因素认证技术，为云主机的操作系统提供安全认证的产品。
- ⑥ 云堡垒机：一款针对云主机、云数据库、网络设备等的运维权限、运维行为进行管理和审计的工具。主要解决云上 IT 运维过程中操作系统账号复用、数据泄露、运维权限混乱、运维过程不透明等难题。云堡垒机对整个运维过程（事前预防、事中控制和事后审计）进行全程参与。

(3) 应用安全，涉及的重点产品包括：

- ① Web 应用防火墙：基于云安全大数据实现，对客户网站提供一整套的 4-7 层应用安全防护方案，核心能力包括各类 WEB 应用安全防护、CC 攻击防护、0day 漏洞和未知威胁防护、BOT 行为管理和业务安全可视化分析等，能有效阻拦网站系统被篡改、被挂马、漏洞攻击，恶意扫描等黑客行为，充分保障用户网站安全。
- ② 网页防篡改：针对网站篡改攻击的一款防护产品，通过文件底层驱动技术对 Web 站点目录提供全方位的保护，为防止黑客、病毒等对目录中的网页、电子文档、图片、数据库等任何类型的文件进行非法篡改和破坏提供解决方案。
- ③ 日志审计：通过主被动结合的方式，实时不间断地采集用户网络中各种不同厂商的安全设备、网络设备、主机、操作系统、以及各种应用系统产生的海量日志信息，并将这些信息汇集到审计中心，进行集中化存储（可根据日志规模大小进行分布式存储，支持水平弹性扩展和数据高可靠性存储）、索引、备份、全文检索、实时搜索、审计、告警、响应，并出具丰富的报表报告，获悉全网的整体安全运行态势，实现全生命周期的日志管理。
- ④ 渗透测试：通过模拟恶意黑客的攻击方法，来评估计算机网络系统安全的一种评估方法。
- ⑤ 网站安全监测：依托全球部署的分布式监测集群，对目标系统提供 7*24 小时安全监测服务，通过对网站可用性、安全事件、OWASP Top 10 Web 漏洞以及 DNS 监测，协助客户及时发现目标系

统风险，并解决安全隐患，为网站安全保驾护航。

(4) 数据安全，涉及的重点产品包括：

- ① 数据加密：基于国家密码局认证的硬件加密机，提供可独占、高性能、安全合规的加密域计算资源，将用户线下加密设备能力转移到云上，为用户提供的云上数据加密的服务，可处理加解密、签名、验签、产生密钥和密钥安全存储等操作。
- ② 数据库安全：提供旁路模式数据库安全审计服务功能，通过实时记录用户访问数据库行为，形成细粒度的审计报告，对风险行为和攻击行为进行实时告警。

(5) 业务安全，涉及的重点产品包括：

- ① 等保咨询：为每一位有网络安全合规需求的用户提供快捷、一站式、专家式等保咨询相关安全服务。
- ② 态势感知：为用户提供统一的威胁检测和风险处置平台。能够帮助用户检测云上资产遭受到的各种典型安全风险，还原攻击历史，感知攻击现状，预测攻击态势，为用户提供强大的事前、事中、事后安全管理能力，通过资产管理、脆弱性评估、威胁检测等手段完成用户网络的安全检查、风险评估、可视化呈现。
- ③ 内容安全：专业为客户提供站点主动扫描检测和用户内容检测上传的服务。可提供指定域名深度扫描服务，以及用户内容检测上传 Agent 或 API 接口服务。

2. 天翼云安全服务典型应用场景：大型央企、金融场景、网站安全场景。

(1) 大型央企：对内需要做总部系统安全，在分支机构做本地安全，对外实现不同终端设备安全访问。

解决方案/涉及产品：DDoS 高防 IP、微隔离防火墙、云解析、服务器安全卫士、云堡垒机、漏洞扫描。拓展策略：提供一站式云安全解决方案，不仅保障物理、环境安全和虚拟化安全，同时可解决基础设施、应用和数据相关的全方位安全控制与防护，减轻用户的运行责任。

(2) 金融场景：为最终的用户提供稳定、极速的行情和交易。解决方案/涉及产品：Web 应用防火墙、微

隔离防火墙、云解析、DDoS 高防 IP、云下一代防火墙等领域天翼云产品。拓展策略：金融机构通常已经有一定规模的安全防护系统，可从重新爆发的网络威胁入手，提供模块化的单项解决方案。

(3) 网站安全场景：客户在 IT 技术领域有一定积累，但在 CT 领域缺乏完备的技术支撑能力。解决方案/

涉及产品：数据安全、数据库安全、云审计、容器安全服务、网站安全监测、云下一代防火墙等领域天翼云产品。拓展策略：云网融合 2.0 服务于互联网企业转型、智慧城市的数据安全防护领域、智慧园区的综合安防系统支撑、数据安全的存储调优应用。

3. 灾备总体分类

(1) 同构主备，1:1 建设，主用设备工作，备用设备空载处空闲状态。只有当主用失效或故障时，备用系统才投入工作成为临时的“主用”。这种建设方式成本很高，适用于非常看重切换后的运行平稳

性、连续性的客户。

(2) 异构主备，主用是一套完整的主系统，备用采用一个简版的系统或异结构系统，或者第三方提供租用服务。这种方式所服务的业务通常是可以暂时中断一会儿也没有太大关系的业务，比如企业邮箱，OA 系统。

(3) 同构双活，相同结构的主、备两套系统同时工作，服务客户业务。主要针对一些主系统中中断时间内可能造成重大损失的场景，比如电商活动、实时支付场景。而多数据中心的建设需要投入大量资金，其项目周期往往很长，涉及的范围也比较大。从技术上来说，要实现真正意义上的双活，就要求网络接入层、应用层、储存层和数据层都要双活。

(4) 异构双活，应用非常少，只有设备厂家的解决方案中存在，但不是真正意义上的异构双活，实现难度非常大。就现阶段来看，大多数客户的多数据中心建设还达不到完全的双活要求，主流的建设目标是实现应用层双活。

4. 目前客户建设多数据中心的模型可以归纳为：单纯的数据容灾、构建业务连续性、提升业务服务能力。

(1) 单纯的数据容灾：正常情况下只有主数据中心投入运行，备数据中心处于待命状态。发生灾难时，灾备数据中心可以短时间内恢复业务并投入运行，减轻灾难带来的损失。

(2) 构建业务连续性：两个数据中心（同城/异地）的应用都处于活动状态，都有业务对外提供服务且互为备份。但出于技术成熟度、成本等因素考虑，数据库采用主备方式部署，数据库读写操作都在主中心进行，灾备中心进行数据同步。

(3) 提升业务服务能力：多个数据中心同时对外提供服务且互为备份，各中心的数据库可同时处理应用的读写请求，网络、存储、应用和数据库全部实现多活。各数据中心独立运营，用户流量可被智能调度，形成灵活、弹性和可扩展的面向服务的业务架构。

5. 银行双活总体解决方案

(1) 总行数据中心整体上分为主中心和灾备中心，二者的网络架构、业务系统和服务能力都基本相同，同时对外提供服务，形成双活数据中心。

(2) 数据中心内部划分为互联网业务区、核心生产业务区、数据库区、业务测试区，出于成本考虑，灾备数据中心不设业务测试区。

(3) 主备数据中心和各一级分行之间通过专线互联，利用动态路由协议组建企业内部专网。

6. 网银业务设计场景

(1) 结构布局：把网银业务从逻辑上分为接入侧和服务侧：接入侧包括出口链路、全局负载设备；服务侧包括 WEB 服务单元、APP 服务单元和 DB 服务单元。

① WEB 服务单元包含 SSL 卸载设备、WAF 防火墙、负载均衡和服务器。

② APP 服务单元包含防火墙、负载均衡和服务器。

- ③ DB 服务单元包含防火墙、负载均衡、数据库审计和数据库。
- ④ WEB 服务单元和 APP 服务单元在 2 个数据中心同时提供服务，实现应用双活。

(2) 实现方式

① 流量调度

- I. 数据中心层面：推荐使用两层逻辑算法的智能 DNS 调度策略。
- II. 服务单元层面：WEB、APP 和 DB 服务单元都配备了本地负载均衡器，用户访问流量到达数据中心内部后，由服务单元的负载设备根据预设策略分发给各服务器，可根据用户需求灵活选择轮询、优先级、最小连接等算法。

② 业务连续性

- I. 数据中心层面：通过 DC Cookie 保证用户接入同一数据中心。
- II. 服务单元层面：WEB 服务单元的负载建议通过 cookie 会话保持（插入、改写和被动）保证业务连续性；APP 服务单元的负载可通过 cookie 或源 IP 会话保持保证业务连续性；DB 服务单元一般不需要会话保持。

③ 健康状态检查

- I. 服务单元层面：通过内置的应用级健康监视器对服务器进行主动探测，提供 HTTP、HTTPS、RADIUS、FTP 等常用模板。
- II. 数据中心层面：全局负载与服务侧的各区域负载均衡联动；全局负载设备会探测出口各链路健康状态，结合服务侧整体服务能力和设备自身负荷情况，综合判断该数据中心的健康状态（正常、繁忙、故障）。

④ 故障切换

- I. 服务单元层面：服务单元内部某服务器繁忙或故障时，将用户请求调度到其他正常服务器。
- II. 数据中心层面：
 - 数据中心的 WEB 或 APP 服务器全部繁忙或全部故障时，用户接入链路不切换，通过专线将数据转发至正常数据中心对应服务单元。
 - 主数据中心的数据库服务器全部故障时，用户接入链路不切换，通过专线将直接激活备数据中心的数据库，实现数据库一键切换。
 - 数据中心的所有链路同时故障时，全局负载设备将用户流量平滑牵引至正常数据中心。单链路故障时，可根据用户需求切换至本中心其他链路或其他中心同 ISP 链路。

7. 从迁移方向来分，上云迁移类型可以归纳为两大类：从 IDC 机房迁移到天翼云、从其它云迁移到天翼云。

8. 上云迁移两种方式：平迁和云化。

(1) 平迁

- ① 改变的是底层设备、云平台、云产品类型。
- ② 不变的是系统架构、用户业务流程、应用软件。

(2) 云化

- ① 改变的是底层设备、系统架构、应用软件、云平台、云产品类型。
- ② 不变的是用户业务流程。

9. 场景一：从客户 IDC 机房向天翼云的迁移

客户本地的数据中心，把文件系统、存储系统，迁移到天翼云的私有云 VPC 中，通过虚拟机、缓存、数据库、容器、中间件、NFS 解决相应的问题。在具体的操作中：

- (1) 客户原来在 IDC 机房中使用的 F5 或 A10，可以用天翼云上自带的负载均衡来实现。
- (2) 客户原来使用的 Nginx 功能，可以通过天翼云的负载均衡来实现。
- (3) 客户原来使用磁盘阵列的存储方式，可以用 NAS 的方式来实现。
- (4) 原 IDC 机房当中用的 MySQL 数据库，在天翼云上可以用关系型数据库 RDS 来实现。
- (5) 原系统上用的 Hadoop 软件架构，在天翼云上可以用 MR 系统来实现。
- (6) 原批量设备远程操控时使用的跳板机，在天翼云上可以用云堡垒机来实现。

10. 场景二：从其他云向天翼云的 VPC 迁移

- (1) 客户原来的 5F\A10 的负载均衡，可以用天翼云的负载均衡实现。
- (2) Nginx 分布式、正反向代理，也可以用天翼云的负载均衡实现。
- (3) 盘阵存储，可以用 NAS 实现。
- (4) MySQL 关系型数据库管理，可用天翼云 RDS 实现。
- (5) Hadoop 分布式处理的软件架构，可用天翼云的 MR 来实现。
- (6) ELK 海量日志管理服务，可以用天翼云的日志服务来实现。
- (7) 其他厂家的 K8S 容器化应用管理程序，可以用天翼云的 K8S 容器管理服务来实现。
- (8) 跳板机运维，可以用天翼云的堡垒机实现。
- (9) SVN 开放源代码版本控制系统，可以用天翼云开发软件系统来替换。
- (10) 原来平台的 SOA，可以采用天翼云的云治理服务来实现。
- (11) 使用天翼云专用的传输工具来完成数据的传递。

11. 混合云能解决的业务问题：

- (1) 建设成本高：自建机房硬件配置要求高、建设周期长、成本不可控、基础设施建设不完备；
- (2) 运营成本高：计算、网络、存储等多厂商多形态设备，中小企业普遍存在专业技术人员能力不足、运维难度高的难题；

(3) 不可持续性：单纯的私有云模式，无法快速匹配不断变化的业务需求，产品及服务种类匮乏；且无法利用新技术助力企业业务创新；

(4) 多平台管理成本高：多平台管理技术要求高，熟悉各个平台功能逻辑需要大量精力，难以聚焦业务。

12. 天翼云混合云解决方案的应用场景有：

(1) 混合云管理：统一管理私有云、公有云以及其他第三方云平台等各类云资源。能够帮助企业提高多云 IT 资源环境下的管理能力、运维效率以及优化企业 IT 运营成本，从而提升企业 IT 的能力、效率与价值，帮助企业实现数字化转型。

(2) 智能运维：利用混合云实现业务的智能扩容到公有云，使用公有云分担业务负载，达到降低投资、简化运维、节约成本的目的。多维度资源监控、统计，实现对业务健康度的分析。

(3) 业务按需部署：考虑到安全合规方面的要求，结合公有云和私有云各自的特点，通过标准化服务目录，屏蔽底层不同资源平台的差异性，以标准化的方式呈现云主机、云数据库、云存储等资源，业务和数据按需部署在公有云和私有云平台上。

(4) 备份和容灾：为客户提供多云以及跨云的容灾备份能力，利用从控制面和数据面打通混合云实现数据和业务的灾备，满足企业业务部署、数据保护和管理的综合策略，提高关键数据安全可靠性从而有效保障企业业务连续性。

13. 天翼云混合云解决方案的重点产品有：弹性云主机+负载均衡 ELB+云备份+云存储网关+虚拟私有云 VPC+VPN 连接+云专线 CDA 等。

14. 高并发场景常见的衡量单位：

(1) QPS 或者 TPS。QPS 是指每秒钟之内响应的请求数量；TPS 是指每秒当中处理的事件的数量。

(2) 吞吐量。指单位时间之内处理的请求的总数量。

(3) 响应时间。指系统对单一的某一个请求，做出响应的平均时间。

注意，QPS 并不等于并发数。并发是指某个时刻有多少访问同时到来，而 QPS 是指每秒钟响应的请求数量。他们的换算公式为：并发数=QPS x 耗时。

15. 高并发场景常见的解决方式

(1) 增加机器：增加机器数量，涉及到 db 主从、读写分离、负载均衡等技术。原理是分流，把以前集中的压力分散开来。该方案见效快，灵活。

(2) 增加单机性能：单机性能增加的程度，取决于机器配置，也取决于服务到底有多复杂。常见的提升单机性能的方法，比如：增加不常变化数据的缓存，开启 php 的 opcache，优化代码（如：n+1 问题、多重嵌套循环、深层递归等），db 表优化等等。

16. 典型场景-秒杀场景

(1) 场景需求

- ① 吸引用户关注：大幅推广。
- ② 典型的读多写少：瞬时售空。
- ③ 秒杀流程一定要短：定时上架，瞬时并发高。

(2) 解决方案/涉及产品

- ① 云主机、负载均衡、CDN、全站加速、分布式缓存服务。
- ② 关系型数据库 MySQL 版、关系数据库 SQL Server 版、关系数据库 PostgreSQL。

(3) 拓展策略：弹性扩容，用户数据自主化，网络加速。

17. 典型场景-招生场景

(1) 场景需求

- ① 在开放系统时间段内，第一天第一小时或者最后一天的最后一小时，访问量峰值很高。
- ② 既不能因访问量在短时间内过大造成主机退服，又要对客户订单进行有效响应。

(2) 解决方案/涉及产品

- ① 云主机、负载均衡、CDN、全站加速、分布式缓存服务。
- ② 关系型数据库 MySQL 版、关系数据库 SQL Server 版、关系数据库 PostgreSQL。

(3) 拓展策略：弹性扩容，用户数据自主化，网络加速。

18. 高可用性指标

(1) 高可用性是指系统具有较高的无故障运行能力。

(2) 可用性 = 正常运行时间 / 系统总运行时间，一般使用几个 9 来描述系统的可用性。

可用性	年故障时间	日故障时间
90% (1个9)	36.5天	2.4小时
99% (2个9)	3.65天	14.4分钟
99.9% (3个9)	8小时	1.44分钟
99.99% (4个9)	52分钟	8.6秒
99.999% (5个9)	5分钟	0.86秒

(3) 对于高并发系统来说，最基本的要求是：保证 3 个 9 或者 4 个 9。

19. 应用场景-电商场景

(1) 场景需求

- ① 痛点：客户访问量随机变化，在某特定时刻客户访问量、下单量、评论量陡增，造成系统过载而崩溃，无法服务。
- ② 需求：有较强的 IT 维护能力，要求分钟级或秒级故障恢复，有较大的业务并发量，需要负载均衡。

(2) 解决方案/涉及产品：负载均衡，弹性伸缩，VPC，云主机，云存储，防火墙，双运维系统，入侵防御。

(3) 拓展策略：毫秒级恢复能力，数据双备份。

20. 应用场景-政务场景

(1) 场景需求

① 痛点：客户访问量随机变化，在某特定时刻客户访问量、上报表格量瞬时激增，造成系统过载而崩溃，无法服务。另外在访问安全性、内容审核、网络安全、网页防篡改等方面也有特别要求。

② 需求：有较强的 IT 维护能力，要求分钟级或秒级故障恢复，有较大的业务并发量，需要负载均衡。

(2) 解决方案/涉及产品：负载均衡，弹性伸缩，云专线，云主机，云存储，防火墙，DDos 防护，网页防篡改，防木马，堡垒机，态势感知，CDN。

(3) 拓展策略：安全防护从外到内，快速应用响应，多重保护备份。

21. 高性能计算（High Performance Computing, HPC）是利用并行处理和互联技术将多个计算节点连接起来，提供高效、可靠、快速运行的计算平台，可以提供比普通台式计算机或工作站更高的性能，以解决科学、工程或商业中复杂的问题。

22. 天翼云 HPC 解决方案的主要应用场景包括：

(1) 图形 CAD 工作站：适用于机械/工业设计/制图能力/建筑信息模型/三维建模渲染，该场景对网络资源和存储资源的需求适中。

(2) 松耦合高性能计算：适用于金融风险评估/遥感与测绘/分子动力学场景，该场景对网络资源和存储资源的需求适中。

(3) 紧耦合高性能计算：适用于电磁仿真/流体动力学（CAE）/汽车碰撞模拟/AI 训练，该场景需要高网络 IO，对存储资源的需求适中。

(4) 数据密集型高性能计算：适用于气象预报/基因测序/图形渲染/深度学习/能源勘探/计算金融，该场景需要高网络 IO 和高存储 IO。

23. 天翼云 HPC 解决方案的重点产品有：物理机+GPU 云主机+对象存储 OOS+云安全+云监控 CES+云专线 CDA。

24. 高性能计算（High Performance Computing, HPC）是一个计算机集群系统，提供一种性能卓越、稳定、安全、便捷的计算服务，它通过各种互联技术将多个计算机系统连接在一起，利用所有被连接系统的综合计算能力来处理大型计算问题，所以又通常被称为高性能计算集群。

25. 并行计算、超级计算和高性能计算对比

(1) 并行计算，指同时使用多种计算资源解决问题的过程，把问题分解成若干个部分，利用多个处理器来协同求解，各部分均由一个独立的处理机来并行计算。主要目的是快速解决大型且复杂的计

算问题。

(2) 超级计算：是用计算机去研究、设计产品及支持复杂的决策，除了最领先的计算硬件系统外，还包括软件系统和测试工具、解决复杂计算的算法等。计算速度是超级计算追求的第一目标，最快的速度，最大的存储，最庞大的体积，最昂贵的价格。

(3) 高性能计算：是传统超高速计算机和多个 CPU 组成的并行计算机，不过一般来讲，HPC 几乎等同于超级计算。高性能计算典型地通过计算机建模、模拟和分析，用于解决高级问题并进行研究活动。

26. HPC vs 云计算

(1) 高性能计算在完成一个任务时，需要多台服务器共同安装一套操作系统，组成集群，然后多个集群内部组网后形成一个整体，再进行计算。

(2) 云计算在完成一个任务时，把任务分成若干份，交给多台服务器，同时计算。它的计算任务是可以拆分的。

27. HPC 主要应用于卫星测绘、气象科学、能源勘测、航空航天、生命科学、基础科学研究、汽车电子、动漫渲染等行业。这八大行业应用场景可归结为三类 HPC 高性能计算模式：松耦合高性能计算、紧耦合高性能计算和数据密集型高性能计算。

28. HPC 典型架构，从下到上依次分为：基础设施层、HPC 基础层、管理调度层、行业应用层。

(1) 基础设施层：在 HPC 场景服务器的数量多、功耗大，建议选择 PUE 低的数据中心，从而降低了运营成本。

(2) HPC 基础层：根据应用场景选择计算、存储、网络。

(3) 管理调度层：在底层基础设备、系统搭好的基础上，涉及到集群管理、作业调度、消息传递、各种运算库、编译器等等。

(4) 行业应用层：是偏向于行业的各种业务所需要使用的应用，能源勘探、CAD 仿真，基因测序、气象预测等等。

HPC 集群算力提供商主要关注的是在 L2 层，即计算、网络、存储怎么去设计满足低成本高算力的要求，从而具备更强的市场竞争力。

29. 应用场景示例-高校

(1) 需求痛点：本地资源限制，计算处理能力受限；实战应用方面，需要海量数据存储；高校专业需求日趋复杂，在保证性能的同时，需要更加智能、高效与灵活升级的部署模式。

(2) 拓展策略：联合集约运营建设；打造首个方案，快速复制。

30. 应用场景示例-气象

(1) 应用场景：现代气象观测系统所获取的气象信息是大量的，要求高速度地分析处理。许多现代气象观测系统，都配备了超算中心，及时分析处理观测资料和实时给出结果。

(2) 拓展策略：商机摸排；掌握需求；攻坚突破。

31. 以太网交换机 VS IB 网络交换机

	以太网交换机	IB网络交换机
端口速率	10M, 100M 1000M=GE 10000M=10GE	100GE 200GE 400GE
距离	两点之间 400米--5公里 多点级联 至全球	两点之间 400-5公里 多点级联 最大10公里
连接设备类型	PC, 以太网交换机, 路由器	服务器 存储设备 IB网络设备
价格	较低 起步200	较高 地歩 上万
稳定型	差	高

(1) InfiniBand 即“无限带宽”技术，通常缩写为 IB，是一个用于高性能计算的计算机网络通信标准。

它最重要的一个特点就是高带宽、低延迟，应用于计算机与计算机之间的数据互连，也用作服务器与存储系统之间的直接或交换互连，以及存储系统之间的互连。

(2) IB 网络采用了 mellenox 的 IB 网卡（目前最新带宽已经达到 400Gb/s，入门级是 100Gb/s），通过专用 IB 交换机和控制器软件 UFM 实现网络通信和管理。

(3) 在应用场景方面，以太网可以实现全球通信的互联，IB 则没有那么大的通信距离和范围，最远理论距离 10 公里。

32. 紧耦合高性能计算方案框架：天翼云采用 Intel 第三代 CPU+IB 网络+高性能存储的方案，满足紧耦合高性能计算对网络、IO、算力的要求。

(1) 基础设施层，包括计算、存储、网络，IP 网络（主要用于管理信令传递），IB 网络（真正承载客户主要流量），安全产品等。

(2) 系统软件服务层，提供操作系统、调度器、并行环境等。

(3) 应用层，是紧耦合 HPC 在各类领域的应用。

33. 紧耦合高性能计算场景-计算实现方案

(1) 新一代 Intel CPU

- ① 沿用继承客户先前经验, 迁移风险降到最小。
- ② 提高效能，进一步降低总拥有成本 TCO。
- ③ 更高的单核性能，更大的内存带宽和容量，比上代提升 50%。
- ④ IO 能力带宽和吞吐量进一步拓展 48 通道的 PCIe 3.0。

(2) 内存：为 HPC 场景专门定制的物理内存条插法。

(3) 服务器

- ① BIOS 选项调优, 精准适配客户业务软件需求。
- ② RAID1 SSD 系统盘配置，提供数据高可靠性。

(4) 操作系统调优：移除冗余无关进程、绑核，进一步降低系统损耗。

(5) 业务系统调优

① 细致分析软件负载特点，根据负载特点做全栈调优。

② IO 密集型数据调优。

③ CPU 密集型计算调优。

34. 紧耦合高性能计算场景-存储实现方案

存储方案采用并行文件系统：选择高性能的全闪型存储硬件，为用户提供超高 IO 吞吐，支持多协议文件存储的能力，结合定制化开发，满足用户的多种数据存储和调用的需求。该方案的优点：

(1) 面向混合负载-性能更高：一套存储同时支持高带宽&高 IOPS，32GB/s 带宽&40 万 IOPS/U，性能密度业界领先。

(2) 超高密设计-成本更优：24 盘位/2U 高密大容量硬件，冷热数据智能分级，平衡数据价值与成本。

(3) 多协议互通-效率更佳：POSIX/NFS/CIFS/HDFS/S3 无损互通，数据零拷贝，面向 HPDA、AI 演进。

35. 紧耦合高性能计算场景-网络实现方案

网络方案采用 IB 网络：计算节点之间、计算节点与存储之间互联均采用 100G 的 IB 网络，它具有极高的吞吐量和极低的延迟，极大提升数据交互的效率。该方案的优势：

(1) 高带宽：IB 网卡最高带宽已达到 EDR(100Gbps)和 HDR(200Gbps)，同时 IB 交换机无阻塞交换，提供超高网络带宽。

(2) 低时延：IB 交换机转发时延在 100 纳秒级，可提供端到端小于 1 微秒的最低转发时延。

(3) 零丢包：RDMA 技术保证端到端不丢包，消除传统 TCP/IP 网络中重传包带来的性能降低。

(4) 高度适配性：IB Verbs 接口对于 HPC 中大量采用的 Open MPI/Intel MPI 等通信原语进行了优化，提升传输效率。

(5) 高度安全性：IB 协议原生与 IP 不兼容，独立组网，提升了业务计算中数据的安全性。

36. 紧耦合计算的特点：对于各计算节点间彼此工作的协调、计算的同步以及信息的高速传输有很强的依赖性。

37. 松耦合高性能计算方案框架

(1) 部署模式：可根据安全、采购模式等需求，选择公有云或私有云部署，专线与企业数据中心互联。

(2) 任务调度管理：可选择商用调度器，或云上调度器。

(3) 计算：以基于 CPU 的计算任务为主，计算实时性要求低，可选用更高性价比 CPU。

(4) 存储：基于以太网的 NAS 文件存储，提供 NFS 服务，海量文件存储为主，读写性能中等。

(5) 网络：以 10GE-25GE 以太网网络为主，可选双网口提高可靠性，整体网络带宽收敛比根据实际业务需求确定。

38. 裸金属服务器是一款兼具虚拟机弹性和物理机性能的计算类服务，为用户以及相关企业提供专属的云

上物理服务器，为核心数据库、关键应用系统、高性能计算、大数据等业务提供卓越的计算性能以及数据安全。用户可灵活申请，按需使用。与物理服务器相比，裸金属服务器没有实体硬盘，性能可达到物理服务器的 90%-95%，性价比比较高。

39. 松耦合场景-计算实现

- (1) 考虑性能：选择代数新、主频高、有版本迭代的 CPU 型号。
- (2) 考虑适配：应用软件环境调优，对 CPU 和内存比有比例要求（如 1:20）。
- (3) 考虑负载：满足适配比例后，内存条数必须是某双数的倍数（如 2、4 或 8），因为内存通道双数效率最高，坚决不允许出现诸如 15 或 17 之类的单数内存条数。
- (4) 考虑扩展：目前计算以 CPU 为主，后续 GPU 有全部取代或部分取代 CPU 的趋势，因此考虑预留 GPU 卡槽，现阶段可能会引起功耗的提升和成本的增加，但综合考虑设备整生命周期的成本，仍具备商务竞争的优势。
- (5) 考虑冗余：因为计算节点依赖程度低，且高性能计算数据结果都十分重要，计算网络和存储网络两平面位于不同网卡，并做主备。

40. 松耦合场景-存储实现

存储节点具备高性能、易扩容和管理的特点，满足海量小文件的频繁读写操作，管理简单、使用便捷。存储读写机头成本一期计入，扩容仅加硬盘，利润空间后期体现。备份本地、异地同时进行，源端删重，减少存储和带宽负荷及成本。

- (1) 超大容量：需支持数 10+PB 容量，上百亿个文件的存储。
- (2) 容量和性能按需线性扩展：性能线性增长、容量按需增长。
- (3) 管理简单：向导式管理、开箱即用。使用者普遍是业务设计研发人员，对 IT 设备不了解。

41. 松耦合场景-网络实现

由于计算节点之间对于彼此信息的相互依赖程度较低，网络性能要求也相对较低，一般以太网即满足性能要求，客户预算充足的情况下，可以用 RoCE 或 IB 网络替代升级。

- (1) 在松耦合场景中，计算节点之间对于彼此信息的相互依赖程度较低，网络性能要求相对较低。
- (2) 数据安全性要求高，计算网络和存储网络分离，双网双平面，并做主备冗余。
- (3) 网络性能一般没有过高要求，考虑性价比和投资回报，以太网可满足场景需求。客户预算充足的前提下，可以考虑用 RoCE 或 IB 网络替代。

42. 松耦合计算的特点：在松耦合场景中，计算节点之间对于彼此信息的相互依赖程度较低，网络性能要求相对较低。一般金融风险评估、遥感与测绘、分子动力学等业务属于松耦合场景。

43. 数据治理—三数两用

- (1) “三数”指的是：“有数”、“治数”和“用数”。
- (2) “两用”指的是“可用”和“好用”。

44. IT 需求建设难点，对应传统 IT 需求建设流程四大环节，可以概括为“四慢”与“四难”。

- (1) 在申请、部署硬件环境阶段：硬件扩容慢（大于 30 天），性能扩容难。
- (2) 在申请、部署软件系统阶段：系统软件准备周期慢（大于 30 天），组件多、使用难。
- (3) 在业务需求上线阶段：需求开发测试慢；创新和复用难。
- (4) 在系统运维阶段：RTO 大于 2 小时，人工运维故障快速定位难。

45. 根据工信部印发的《推动企业上云实施指南（2018-2020 年）》，云服务类型包含以下几种：

- (1) 基础设施类，包括：计算资源服务、存储资源服务、网络资源服务、安全防护服务。
- (2) 平台系统类，包括：数据库服务、大数据分析服务、中间件平台服务、物联网平台服务、软件开发平台服务、人工智能平台服务。
- (3) 业务应用服务，包括：协同办公服务、经营管理应用服务、运营管理服务、研发设计服务、生产控制服务、智能应用服务。

46. 按部署模式的不同，客户业务需求上云可以选择的上云方式：

- (1) 公有云：具有规模化、运维可靠、弹性强的特点，适合门户网站、电商、游戏、视频行业。
- (2) 私有云：具有自主可控、数据私密性好的特点，适合金融、医疗、安防行业。
- (3) 混合云：具有规模化、运维可靠、弹性强的特点，适合金融、医疗、政务行业。
- (4) 专属云：比公有云更好的隔离性，比私有云更好的灵活性，适合有特定需求的行业。

47. 中国电信 IT 上云的五步十流程

- (1) 第一步，系统上云分析。主要包括梳理上云系统清单和上云需求驱动力分析两个流程。具体为梳理全量上云系统清单，从业务需求驱动、局部性能不足、底线思维限制、维护能力不足、安全隐患驱动、数据孤岛、能力封闭等分析上云需求和上云驱动力。
- (2) 第二步，确定上云模式。上云模式关系到应用进行上云改造的程度与成本投入，为应用挑选正确的上云模式对企业上云至关重要。需要应用分析系统原有架构，判断是否依赖应用厂商，从而确定上云标准和模式。
- (3) 第三步，技术选型与架构设计。主要包括技术选型和架构设计两个流程。
- (4) 第四步，上云实施与部署。主要包括架构部署、应用改造和数据迁移/割接三个流程。
- (5) 第五步，上云交付与运维。主要包括上云交付和上云运维两个流程。

48. AI 市场前景

- (1) 政策支持：“十四五”规划《纲要》“上云用数赋智”行动指出：“上云”重点是推行普惠性云服务支持政策，“用数”重点是更深层次推进大数据融合应用，“赋智”重点是支持企业智能化改造。

(2) 技术趋势

- ① 以人工智能等数字化技术赋能为本质特征的第四次工业革命蓬勃发展。

② 2020 年我国数字经济增加值突破 40 万亿大关，相比 2019 年增长 12%。

49. 天翼云 AI 中台的组成

- (1) 第一层是云原生底座，通过虚拟化来解决算力的问题，同时包括了算力任务管理、弹性伸缩、分离部署和灵活调度。
- (2) 第二层是数据中台，包括了数据服务、数据交换、数据资产管理、数据标准管理和数据质量稽核等功能。
- (3) 第三层是 AI 中台。AI 中台，又包含了三大平台：数据标注平台、算法开发平台和能力开放平台。
- (4) 第四层是业务中台，包括三维城市构建器、3D 数字资产生产线和场景化算法与 MVP。这些是实现数字孪生的基础型模块。

50. 能力开放平台简介

- (1) 能力开放平台是具备虚拟化异构算力和弹性扩缩容能力的在线推理平台，能帮助用户解决模型部署复杂、资源浪费、手工扩展资源效率低下的问题。可以实现模型一键部署和 API 发布。平台对外提供 CV，NLP，智能语音相关原子能力接口。
- (2) 应用场景：内容审核、人脸比对、AI 应用开发。
- (3) 目标客户：有智能化转型需求的企业客户、AI 业务部门和有相关 AI 能力需求的组织。

51. 能力开放平台 2.0 架构包括：天翼云算力层、天翼云存储层、PaaS 能力层和 SaaS 能力层。其中，在算力层，CPU 主要用于进行控制型计算，GPU，适用于大量的图片、视频类文件，而 TPU，主要面向 AI 的一些算法程序。另外 ASIC 芯片，是为专门目的而设计的集成电路。

52. 能力开放平台 2.0 相较于 1.0 进行的性能优化：

(1) 平台架构升级

- ① 基于微服务的新架构，提升 SLA。
- ② 升级监控与报警系统，上线业务指标采集新框架，实现细粒度监控指标感知。

(2) 提供私有化版本，一站式交付。

(3) 全面提升用户体验

- ① 全面提升网关性能 QPS（QPS 即每秒查询率，是对一个特定的查询服务器在规定时间内所处理流量多少的衡量标准。）。
- ② 全新界面交互体验。
- ③ 引入更多原子能力。

53. 为满足不同客户的需求，能力开放平台的私有化版本又分为两种版本：标准版和增强版。

(1) 标准版：支持人脸识别、内容审核以及 OCR 识别功能。

(2) 增强版：可以为用户提供 7 大类，全部 32 项 AI 算法接口。除了标准版的功能外，还可以基于场景进行智能图像识别，比如安全穿戴、电子围栏、吸烟识别、打架识别等；可以进行文本情感分析，

比如积极、消极、中立等，可以智能理解语义；可以进行文本纠错，自动检查并提示错别字情况，降低因疏忽导致的错误表述。

八、国资云行业解决方案（选修）

必备掌握知识点：

1. 国资云的定义：由国企建设和运营、专门服务于国有企业的云平台。旨在保障国有资产数据安全和推进国有企业数字化转型，可提供国资监管、国企管理和数字化运营等服务，覆盖包括 IaaS、PaaS、DataS 及 SaaS 内在的综合云服务。
2. 国资云内涵：对各级地方国资委而言，有利于国企探索国有企业改革及管理模式快速创新，保障国有企业网络和数据安全，实现国企快速转型。对于国企而言，国资云的建设将有效弥补国企 IT 基础设施不完善及人员能力不足等问题。
3. 国资信息化发展“三步曲”：
 - (1) 1.0 阶段，报告式监管。由企业登录国资委的系统，进行相关数据填报。在这个阶段，企业不需要建立专用的数据信息资源池和平台网站，而是将数据直接填报到国资委的系统平台上。
 - (2) 2.0 阶段，穿透式监管。通过对运营管理的某些环节嵌入式采集数据，对企业进行监管，减少人工交互。
 - (3) 3.0 阶段，数智国资。国有企业业务应用上云，进行流程优化，赋能决策。在 3.0 阶段，国资云的雏形开始显现。
4. 国资云四大特点
 - (1) 优化监管：国资云会进一步强化国有企业数据监管。
 - (2) 保障安全：国资云具备更强的安全保障能力。
 - (3) 加强集约：国资云可以满足国企央企 IT 集约化的需求。
 - (4) 释放价值：国资云可以充分释放国有企业数据价值。
5. 国务院及国资委高频政策发文，央企上云空间巨大，以优化监管效率为核心，聚焦国资监管、综合办公、经营管理和生产运营四大应用场景优先落地。
6. 国企上云痛点：
 - (1) 国资监管应用和平台建设不系统。
 - (2) 国有企业数据孤岛多，壁垒深。
 - (3) 国有企业数字化技术发展不均衡。
 - (4) 国有企业数据安全保障较薄弱。
7. 天翼云在国资云建设和上云过程中的定位与作用
 - (1) 数字化赋能者：基于中国电信自身 IT 和业务上云用数赋智实践沉淀，对外输出央企/国企全业务场景数字化整体方案与实施能力，助力国资国企数字化转型。

(2) 云网资源提供者：基于电信优质网络资源（5G、OTN、CN2-DCI、5G+光纤网络和云边端分布式云架构）提供 IaaS+PaaS+AI/大数据的一体化全栈云网资源服务，实现“云+网+应用”的统一管控，助力国资云建设和优化升级。

8. 国资云场景化方案总体架构，概括为“1+4+6 模式”：1 底座、4 大场景、6 引擎

(1) 1 底座：天翼国资云平台。具备国产虚拟化能力、IaaS 产品能力、PaaS 产品能力和信创能力。

(2) 4 大场景包括：国资监管场景、综合办公场景、经营管理场景、生产运营场景。

(3) 6 引擎包括：迁移、等保、数据安全、灾备高可用、信创、交付运维。

9. 国资云建设总体布局构想：打造“三层云池两专网，三种形态一朵云”国资云整体布局。

(1) 对国资云的理解

- ① 国资体系包括部委、省市县四级国资委系统和央企、地方国有企业。
- ② 国资云以云计算核心技术研发为基础，构建国资基础公有云统领、行业云和企业私有云共生的混合云架构，牵引国企数字化转型。
- ③ 一朵国资云包括三种云平台形态，彼此互联互通：
 - I. 国资委牵头投资、设立、运营的综合性的国资公有云平台。
 - II. 国企自行建设的私有云平台。
 - III. 针对特定行业用户共用的行业云平台，如金融团体云、能源行业云。

(2) 建设布局：参照国资委《加强中央企业云计算应用的指导意见》1+N+M 布局，全国国资云建设需要做好总体规划和顶层设计，并分级分类因地制宜，按需建设：

- ① 按照国资系统垂直管理特点，全国国资云整体划分为中央部委、省/直辖市，地级市三级建设，上下互通。
- ② 每级国资云包括公私专三种资源池建设方式，彼此横向互通。

要结合当地主导产业和国企行业分布特点，灵活确定建设方案，例如省市层级 1 朵国资公有云是刚需，必须建；N 朵省级国资行业云则是按需建设；地级市层级 M 朵国企私有云也是按需建设。

10. 国资云参考架构

(1) 国资云分为三层体系：

- ① 国资云私有云。为某一个国有企业设计一个私有云，这个体系中，采用天翼云统一云底座，X 86 的场景，或者信创的环境。
- ② 国资行业云。以 DevOps 平台作为一条基线，针对辖区内各个国资企业所在行业，行业当中有多个企业或者多个子分支，比如汽车行业、电力行业、石化制造、医药等。
- ③ 国资公有云。同样以 DevOps 这个平台为基线，下面采用了天翼云的基础底座，上面装一个国资监管平台，用来对下面的行业和企业做监管。

11. 典型场景-国资监管

(1) 解决方案架构：通过搭建多形态的国资监管系统，构成 1+N+M 的整体体系，打造数据互通，能力共享的国资监管平台；各形态国资监管系统采用统一的数据采集平台及交换平台，确保数据格式的统一，实现数据的高效交互。

(2) 方案优势：数据互通、能力标准化、决策科学、安全可靠、应用智能化、容灾高可用。

12. 典型场景-综合办公

(1) 解决方案架构

① 天翼云：提供了全栈式信创底座，涵盖了 IaaS、PaaS、网络、安全的相关能力；提供了天翼云电脑、云终端。

② 信创已适配 SaaS 应用：WPS 云文档、WPS 文档中台、金山协作、时代易信邮件系统、蓝信移动办公。

(2) 方案优势：安全可控、业务集中、场景丰富、定制性强。

13. 典型场景-经营管理

(1) 采购系统面临的挑战：信息渠道单一、管理成本高、采购流程复杂、过程不透明。

(2) 解决方案架构

① 天翼云：提供了全栈式信创底座，涵盖了 IaaS、PaaS、网络、安全的相关能力。

② 合作伙伴：构建 SaaS 层的采购云：以连接、协同、共享、创新为核心理念，立足需方构建涵盖采购寻源（招标/谈判/询价）、合同中心、采购协同、云采超市、废旧拍卖、可视与分析、供应商关系管理等多个模块的社会化网络交易平台。

(3) 方案优势：采购云化；多渠道采购，保障采购安全；高效协同，提升企业效率；全流程管控，降低内部风险。

14. 典型场景-生产运营

(1) 现状及挑战

① 应用烟囱式建设，企业业务得不到沉淀和持续发展。

② 运维监控点多、数据分散建设、故障处理挑战大。

③ 筒仓模式应用交付，难以适应数字化转型。

④ 能力封闭、低效，不开放，无法构筑生态圈。

⑤ 数据中心业务目前“三多”现状急需破局。

⑥ 缺乏去“0”技术储备与工具。

(2) 解决方案架构：针对不同类型的业务对于实时性、可靠性、成本的要求，可部署于标准公有云，专属云，混合云等多种形态，为企业提供安全防护能力、高可用能力及主机/数据库层面的伸缩能

力。可满足国产化/XC 需求的同时，实现数据的互通。

- ① 标准公有云：低成本、灵活扩展，主要适配企业需通过互联网提供服务的 CRM、SRM、OA 等应用部署。
- ② 专属云：在公有云平台中提供计算、计算+存储资源专享模式，进一步提升性能及可靠性，主要适配企业 ERP。
- ③ 混合云：私有云或专属云（网络隔离）承载对时延有严格要求的核心生产系统，如 MES、DCS 等，需与公有云/专属云上的系统打通或进行灾备。

(3)方案优势：平滑迁移、安全可靠、容备高可用、属地服务。

15. 国资云市场拓展建议

以天翼云“1+N+M”资源池能力为底座，引入合作伙伴联动，围绕四大场景为切入，提供“一揽子交钥匙”服务。其中，“1”是指针对国资综合性公有云平台。“N”是指针对国资行业特色云平台。“M”是指针对国有企业丰富多彩的私有云。充分发挥中国电信属地化服务优势，“一市一策，以点带面”形式，优先部分 IT 系统上云，逐步拉动上云增量。

九、教育行业解决方案

必备掌握知识点：

1. 传统在线教育面临的挑战有

- (1)信息孤岛：教学资源分散、共享困难；IT 资源利用率低，普遍在 5%-20%之间；资源使用效果和效益评估困难。
- (2)繁重运维：终端故障现场维护，时间长，效率低；不同的 IT 系统以及资源分布在不同的部门，出现问题，协调工作量大。
- (3)缺乏敏捷：学校系统多而分散，使用不便；服务器、存储等采购、交付、上线周期长；且随着业务发展，无法做到弹性伸缩，以及无法提前预留资源；用户分布不同，城区的网络质量较好，偏远地区的网络状况不好。

2. 天翼云教育云解决方案的架构特点是：

- (1)实现空中课堂管理功能，包括上课点名、桌面监控、课程统计、锁屏等功能；
- (2)可支持点播、录播、直播等多种教学模式，结合云端实现音视频互动、数据交互、文字消息互动等多种方式，提升教学效率；
- (3)应用、系统、数据库等不同级别的安全和灾备措施，保障数据安全高可用，便于教育数据长期储存；
- (4)音视频快速解码，降低数据的读取时间、支持播放器秒开，支持多个音视频并行转码，提升大流量高并发的数据操作能力。

3. 天翼云教育云解决方案的重点产品有：弹性云主机+关系数据库 RDS+云转码+CDN+安全整体解决方案。

4. 天翼云在线教育解决方案中使用的云产品有 ECS 弹性云主机、关系数据库 RDS 主从配置，在 Web 接入的时候使用了 CDN 和解析服务等，然后在 ECS 的 Web 层使用了 OOS 和云转码服务，最后安全方面使用了一整套云上安全解决方案，包括 Anti-DDoS、漏洞扫描、Web 应用防火墙、服务器安全卫士等等。
5. 高校上云政策：《高等学校数字校园建设规范（试行）》
 - (1) 总体目标：充分利用信息技术特别是智能技术，实现高等学校在信息化条件下育人方式的创新性探索、网络安全的体系化建设、信息资源的智能化联通、校园环境的数字化改造、用户信息素养的适应性发展以及核心业务的数字化转型。
 - (2) 建设内容包括：信息素养、基础设施、信息资源、应用服务、网络安全、保障体系。
6. 高校上云行业市场现状：
 - (1) 多数院校信息化采购两种方式并存：
 - ① 各院系自主采购。以双一流或一本院校为主，各院系、部门间存在较大差异，二级学院拥有较多自主采购权。
 - ② 信息化部门集中采购。以二三本和文科类为主，校长或副校长级来掌握预算、支出的支配权，信息化部门统筹管理。
 - (2) 高校信息化决策特点
 - ① 自主性强：自有信息化建设部门，负责建设和管理部门。
 - ② 人员素质高：信息化负责人多为信息化领域专家，且具备科研能力。
 - ③ 管理集中度低：各院系、科研项目有自主决策能力，信息化部门偏向于引导和服务，信息化需求较多部门设有信息科或信息化专员。
7. 需求方向：云需求主要集中在信息中心和二级院系，包括：基础网络、环境设施、计算设施、基础平台和应用服务。
8. 高校上云特点
 - (1) 信息中心/二级院系自建+采购服务。
 - (2) 通过校内多机房/分校区机房实现灾备。
 - (3) 90%以上高校自建机房，校均服务器 50+台。
 - (4) 高性能计算（HPC）需求明显。
 - (5) 人工运维成本高、管理复杂。
 - (6) 关键信息系统等保三，安全风险隐患多。
 - (7) 临时性系统上线带来的算力溢出情况增加。
 - (8) 二级院系需求分散，弹性大，管理难。
9. 高校上云项目复杂度（由低到高）

- (1) 公有云+云专线
- (2) 全栈混合云+云专线
- (3) 全栈混合云+云专线+公有云
- (4) 全栈混合云+云专线+公有云+云灾备
- (5) 全栈混合云+云专线+公有云+云灾备+大数据/AI
- (6) 全栈混合云+云专线+公有云+云灾备+大数据/AI+应用系统

10. 高校上云可归纳为三大板块，包括 10 个主要场景。教学科研板块：包括电教室教学、在线课堂、VR 实训、ICT 实训场景。信息服务板块：包括应用加速+IPv6 的改造、5G 实验室、科研系统场景。校区管理板块：包括平安校园、智慧校园、5G+智慧校园场景。

11. 电教室教学场景

(1) 场景需求/痛点

- ① IT 资源利用率低，普遍在 5%-20%之间。
- ② 教室、阅览室、微机室、多媒体教室等多种场景并存，缺乏统一规划。
- ③ 多场景给 IT 维护带来巨大工作量，OS、APP、硬件维护，且故障恢复时间长。

(2) 解决方案/涉及产品

- ① 云电脑将电教室的 Windows 桌面搬到云端，采用统一镜像分发给学生机，重启后恢复标准化环境，应用云端部署，免维护。
- ② ISV 提供第三方电子教室软件，教师机可对学生做同屏广播，完全控制学生机，可实时分组教学，分组考试，分组讨论等多种场景化教学方案。

(3)拓展策略：以“降低运维压力、缩短采购周期、降低一次性采购成本、软硬解耦、数据安全”等优势进行切入。

12. 在线课堂场景

(1)场景需求/痛点

- ① 需求：教师居家通过网络开展多方音视频直播教学，将线上教学过程中录制的视频及教师的课程视频资源存储到点播平台，学生在家中通过终端访问平台观看学习。
- ② 痛点：业务高并发、对带宽要求高、多种接入终端类型工具，终端类别多样、课件播放时出现的卡顿、不稳定。

(2)解决方案/涉及产品

- ① 建设校级集约化平台，高效利用云网资源。
- ② 视频直播、云点播、CDN、对象存储、在线课堂软件、摄像头。

(3)拓展策略：面向高校信息中心，紧抓疫情不停学需求，以公有云+应用平台/私有云扩容+应用平台

满足系统快速上线需求。

13. 5G 实验室场景

(1) 场景需求

- ① 用户端模块。
- ② 工业、医疗等专业学习需要 5G 实景环境。

(2) 解决方案/涉及产品

- ① 5G 虚拟仿真实训系统为针对院校设计的 B/S 架构的在线 5G 教学系统，支持云端部署与本地部署多样化的部署方式，适用于不同场景的学习使用需求。
- ② 通过云化部署可以使学生将实验任务带出课堂，也可以实现多元化的教学场景应用。

(3) 拓展策略

- ① 骨干讲师→系主任→二级学院院长→主管教学副校长→校长
- ② 与定制网结合，拓展 5G 定制网项目

14. VR 实训场景

(1) 场景需求

- ① 需求：结合 VR/AR 技术，打造出高度仿真、沉浸式、可交互的虚拟学习场景。
- ② 痛点：高成本、高风险等教学和实训难以实现场景教学；传统 VR 时延高、用户体验差。

(2) 解决方案/涉及产品

- ① 采用云端部署渲染平台，云端将画面和声音等经过编码压缩成视频流后，通过 5G 传输到用户的终端设备，实现 VR 业务内容上云、渲染上云，满足渲染业务的低时延需求。
- ② 涉及产品：GPU 云主机、渲染平台、5G、VR 终端。

(3) 拓展策略：面向高职院校院系，聚焦研发设计、辅助维修等虚拟实训场景。

15. 应用加速+IPv6 改造场景

(1) 场景需求/痛点

- ① 面临 HW（护网行动）建设关键时期，需加强校园网站安全防护。
- ② 应用打开缓慢，校园应用登录缓慢、课程视频及科研文库无法加载、访问师生等待白屏时间长等。
- ③ 源站 IPv6 改造，支持双栈，天窗问题。

(2) 解决方案/涉及产品：安全加速（SCDN），兼具内容加速与全方位安全防护。

(3) 拓展策略

- ① 快速切入存量客户：操作简单，成本低，不受源站影响，通过先迁移 CDN 达成合作关系，再进一步迁移计算存储等迁移成本较高的产品。

- ② 以 IPv6 改造切入：创新性改造，方案/成本均优于传统双栈解决方案。

16. 平安校园场景

(1) 场景需求/痛点

- ① 缺乏智能安防系统，无法统一管控，传统校园安防依赖人防+视频监控，缺乏事中联动预警、事后取证，无法事前研判预警。
- ② 访客、考勤等流程机制比较低效、存在很多漏洞，亟需优化。

(2) 解决方案/涉及产品

- ① 合作伙伴提供平安校园应用系统如访客管理系统、考勤系统、视频监控系统等。
- ② 天翼云提供 IaaS 及视频直播、视频点播、诸葛 AI 等。

- (3) 拓展策略：摸排客户安全漏洞，政策引导，切入视频监控联网、防控体系建设场景，与云、AI、物联网等方案融合。

17. 智慧校园场景

(1) 场景需求

- ① 通过新建信息系统助力智慧校园建设。
- ② 业务增长/老旧替代带来云平台扩容需求。

- (2) 解决方案/涉及产品：天翼云全栈混合云、天翼诸葛 AI 平台。

(3) 拓展策略

- ① 统谈统签：天翼私有云方案 100% 递交客户，叠加 IT PaaS 能力，联合集成体系单位/省内合作伙伴发挥集成优势提供“云+网+应用”整体解决方案。
- ② 分包单签：引导客户拆分云平台分包，聚焦云基础设施建设。

十、高速公路行业解决方案（选修）

必备掌握知识点：

1. 高速公路相关部门需求

(1) 交通部

- ① 增强对地方的监管。
- ② 能指挥调度以应对全国性突发事件。
- ③ 能提出行业标准并实现各省评比。

(2) 交通厅

- ① 数据统一规范。
- ② 系统上云整合。
- ③ 大数据分析应用。

(3) 高速公路管理局

- ① 通过全省高速路网系统整合，提升行业监管能力。
- ② 需要投入小、业主协调工作少的云方案。

(4) 公路局

- ① 可靠的网络资源。
- ② 经济的云服务。
- ③ 实用的养护系统。

(5) 交警

- ① 交警系统整合上云。
- ② 视频联合分析，提高案件侦查能力。

(6) 交投企业

- ① 自动化填报，减轻特殊车辆登记工作。
- ② 多视频联合分析、降低偷逃等稽查类工作难度。
- ③ ETC 推广、车牌付应用，解决现金管理问题。
- ④ 掌握路段过车车牌信息，辅助收费清分对账。

(7) 公路使用者

- ① 不堵车。
- ② 智能服务。
- ③ 快速收费。
- ④ 高速通行。

(8) 生态伙伴

- ① 拓宽客户面。
- ② 提升综合解决方案能力。
- ③ 创新应用。
- ④ 与运营商合作共赢。

2. 天翼云高速公路信息化解决方案整体架构图

(1)接入终端：传感器、监控设备、智能终端。

(2)网络层：CN2、4G\5G、PON、NB-IOT、IPRAN、OTN、WIFI。

(3)平台层：基础云平台、大数据、AI、视频服务、数据挖掘、数字孪生、AI 使能、数据使能、应用使能。

(4)应用层：高速公路建设、高速公路运营、高速公路养护、高速公路管理。

(5) 运维服务体系

(6) 安全保障体系

3. 施工建设场景

(1) 场景需求：包括环境隐患监测、预警分析、人员管理以及项目管理信息的实时查询。

(2) 解决方案/涉及产品

- ① 现场采集数据的即刻上传 需要无线网络。
- ② 视频录像云端保存，多地访问。
- ③ 物料进场。
- ④ 电子围栏。

(3) 拓展策略

- ① 可以采用 CPE 热点。
- ② 上传的视频，可以在云端、在天翼云上进行云存储。
- ③ 现场的一些 OA 的管理系统，可以放在云主机上进行运行。

4. 路政管理场景

(1) 场景需求

- ① 路政管理：管理路政巡查、路政治超。
- ② 交通安全：全路段感知、道路信息统揽、应急指挥、事件告警。

(2) 解决方案/涉及产品

- ① 日常违法点视频捕获
- ② 流动监督视频点
- ③ 沿途巡检点打卡
- ④ 关键路口传感器
- ⑤ 行业专网终端
- ⑥ 数据分析预警

(3) 拓展策略：以上解决方案的实现，需要云主机，以及关键路口的传感器，以及连接的有线专网。

5. 路桥养护场景

(1) 场景需求

- ① 养护流程管理：路面数据采集、病害分类分析。
- ② 养护质量管理：路面等级评估、移动巡检路线规划。
- ③ 养护任务分布：决策辅助、资源调配。

(2) 解决方案/涉及产品：通过对 BIM 与 GIS、物联网、无线终端技术、大数据等进行有机融合，实现了

桥梁结构感知实时化、在线预警及时性、结构评估有效性、巡养流程规范化、技术状况评估自动化、病害分析智能化等。大型桥梁和桥梁群的监测养护需求，提供桥梁健康监测、桥梁巡检养护和桥梁群综合管理的服务。

(3) 拓展策略

- ① NB-IOT
- ② 5G 专网
- ③ 云主机
- ④ 云存储
- ⑤ 检测平台软件系统

6. ETC 收费场景

(1) 场景需求

- ① 内部数据运营：多业务系统协同。
- ② 高速运营服务：出行服务、车路协同、联网服务、服务区客流分析。

(2) 解决方案/涉及产品：天翼云为高速公路打造的数字孪生系统，通过大数据、5G、云计算等技术，完成收费广场信息、车流信息、ETC 收费信息的实时映射仿真展示，并实现 ETC 收费、精准引导、应收不漏、收费异常提醒等功能，从多个角度赋能高速公路的智慧交通建设。

(3) 拓展策略

- ① 5G 切片专网
- ② 云主机
- ③ 弹性伸缩
- ④ 负载均衡

十一、汽车行业解决方案（选修）

必备掌握知识点：

1. 政策背景：国家重大政策措施推进汽车行业“新四化”升级转型。其中，“新四化”指的是：电动化、网联化、智能化、共享化。
2. 汽车行业数字化转型重点：汽车研发设计数字化、汽车生产方式数字化、汽车营销方式数字化、汽车用户服务数字化。
3. 汽车行业数字化市场全景地图
 - (1) 研发：协同研发、CAX 计算机辅助设计、PDM 产品数据管理、智能排产。
 - (2) 生产：PLM 产品生命周期管理、MES 制造执行系统、工业机器人。
 - (3) 物流仓储：TMS 物理管理系统、WMS 仓库管理系统。

- (4) 营销：数字化营销、智慧门店。
- (5) 移动出行与服务：智能座舱、智网门店。
- (6) 智能驾驶：辅助驾驶。
- (7) IT：云基础设施、数据中台、AI 中台、IOT 平台、BI 商业智能、RPA 机器人流程自动化。
- (8) 采购：采购数字化。
- (9) 财务：财务数字化。
- (10) HR：HR 数字化。

4. 汽车行业云总体架构

- (1) 接入终端：工业设备、控制与感知设备、智能终端。
- (2) 网络层：CN2、4G\5G、PON、NB-IOT、IPRAN、OTN、V2X。
- (3) 平台层：基础云平台、大数据、AI、视频服务、研发服务、生产服务、车联网服务、自动驾驶开发服务。
- (4) 应用层：汽车研发、汽车制造、汽车供应链、汽车营销、汽车大数据、汽车安全、车联网、自动驾驶。

5. 研发场景

(1) 困难&挑战

- ① 国内汽车行业竞争加剧，亟需加速汽车产品研发效率，提升新车盈利能力。
- ② 持续性增长的成本是制约车企发展的瓶颈，尤其是高性能计算的投入巨大。
- ③ 本地资源池不能迅速满足各研发部门对 HPC 波动性需求。
- ④ 多部门协同设计、需要数据共享以及标准的、统一的业务流程管理。

(2) 场景需求/用户痛点

- ① 数据可靠性低：企业数据信息存放本地，发生故障数据丢失。
- ② 运维管理复杂：分布地域广，难以集中管理，桌面标准化难度大。
- ③ 灵活性差：移动办公兴起，希望不受时差和地域限制办公。

(3) 解决方案/涉及产品

- ① 前处理：采用各种 CAD 工具，建立几何模型，划分计算网络。
- ② 仿真计算：指定荷载和边界条件，提交给 HPC 进行计算。
- ③ 后处理：显示计算结果，评估产品性能，以及结果数据管理。
- ④ 提供一定数量的办公&软件研发桌面（云电脑）、负载 GPU 云电脑满足不同场景需求。
- ⑤ 天翼云电脑私有架构部署，分为计算资源、存储资源、网络资源，接入内部网络，防火墙逻辑隔离。

(4) 方案优势

- ① 强化安全：数据与终端分离，外设可控，桌面水印。
- ② 集中管理：统一业务管理台，快速批量创建桌面，实现桌面标准化。
- ③ 灵活部署：设备解耦，不与瘦终端、服务器厂家绑定。

6. 5G+生产场景

汽车生产制造环节系统众多。基于系统不同特性，天翼云提供“公私专混”多种云服务模式进行承载，助力企业实现精益化生产经营管理。

(1) 解决方案/涉及产品

- ① 标准公有云：低成本、灵活扩展，主要适配企业需通过互联网提供服务的 CRM、SRM、OA 等应用部署。
- ② 专属云：在公有云平台中提供计算、计算+存储资源专享模式，进一步提升性能及可靠性，主要适配企业 ERP。
- ③ 混合云：私有云或专属云（网络隔离）承载对时延有严格要求的核心生产系统，如 MES、DCS 等，需与公有云/专属云上的系统打通或进行灾备。
- ④ 5G+分布式边缘云 MEC：保障数据不出园区，灵活部署，满足大带宽、低时延高可靠连接，实现汽车生产制造过程中工件表面缺陷检测等功能，增强过程管理和质量控制。

(2) 方案优势

- ① 安全可靠：通过 5S 安全体系确保生产管理系统的长期安全稳定运行。
- ② 网络保障：5G 高带宽作为备份云专线，低时延、高可靠。
- ③ 业务中立：为客户处理和理解数据，但不会使用技术手段获取客户的数据进行商业变现。

7. 天翼云角色定位

天翼云是汽车行业数字化转型的“数字化赋能者+云网资源提供者+行业使能者”。

- (1) 基于云边端架构，提供 IaaS+PaaS+AI/大数据的全栈服务，为车企构建全业务场景数字化“平台底座”，打造支撑业务增长的“黑土地”。
- (2) 基于电信优质网络资源提供全场景差异化云网服务，实现“云+网+应用”的统一管控，助力车企云化升级。
- (3) 天翼云 4.0 提供分布式云服务，包括：计算、存储、网络、ABC 全栈服务（A 是 AI、B 是大数据、C 是云计算）、高性能计算服务、视频服务、安全服务、运营运维服务。

8. 车联网场景

(1) 场景需求

- ① 无线网络远距离连接。

② 低时延、高吞吐率。

③ 数据互传共享。

(2) 解决方案/涉及产品

① 车联网平台作为智能网联汽车云底座，支撑 TSP 平台、新能源汽车监控平台（NEV）、出行服务平台等，实现车辆物理资产安全、可靠、高效地联接到云端转换成数字资产使能车企数字化转型。

② 4G、5G 无线专网。

③ 车联网平台，包括：接入平台、基础服务、应用服务。

④ 外接系统接口。

(3) 方案优势

① 使用 5G 切片专网传输。

② 天翼云行业云底座发挥基础层支撑作用。

③ 支持容器应用。

④ 外接系统接口丰富。

9. 自动驾驶场景

自动驾驶是一个系统工程，包括信息采集、信息预处理，数据分析，算法选择，决策模型，运行监测，数据验证等多个环节。

(1) 场景需求/痛点：海量数据处理难；数据标注成本高；仿真测试效率低；软件研发周期长。

(2) 解决方案/涉及产品：基于天翼云底座运行的自动驾驶开发云提供多种组合能力。

① GPU 云主机

② HPC

③ 云间高速

④ 4G/5G 网络

⑤ 弹性伸缩

⑥ 负载均衡

⑦ 分布式缓存

⑧ 微服务云平台

⑨ 漏洞扫描

(3) 方案优势：海量存储能力；一站式 AI 开发平台；自动化数据标注；仿真测试平台。

十二、医疗行业解决方案

必备掌握知识点：

1. 远程医疗的业务挑战有：

- (1) 医疗孤岛现象：行业内目前存在各类基于不同软件、硬件系统为底层的远程医疗系统，由于软件及硬件的品牌、构架方式存在较大区别，往往都为独立自用的系统，相互之间无法进行对接，成为一个个孤岛，封闭使用。
- (2) 会诊效果较差：目前多数的远程会诊系统，采用纯软件方式构架或者使用基于 PC 个人应用的硬件后台进行系统支撑，存在较普遍的视音频效果差、会诊效率低、使用体验一般的情况。
- (3) 会诊应用场景简单：较多的会诊系统建设整体简单、对于会诊中所需的各类辅助资料无法进行全部高质量的远程提供，导致只能实现简单的问诊类远程会诊场景。
- (4) 缺乏有效的运营手段和运营：目前多数医院的远程会诊系统建设完成后，存在形式大于内容的情况，无法真正地实现运营级别的远程会诊应用，且缺乏专业的运营后台维护和保障体系。

2. 天翼云远程医疗解决方案的应用场景有：综合远程会诊中心平台、综合远程会诊中心、专科/MDT 会诊室、医生/专家个人会诊室。

3. 天翼云远程医疗解决方案的架构特点有：

- (1) 部署灵活：远程会诊的整体平台具备很强的灵活性选择，既可虚拟化部署，也可以硬件部署，更支持云端部署。
- (2) 体验优异：各类会诊应用场景都具备体验优异的对应解决方案，其中综合会诊中心更是将会诊中的各类会诊服务体验提升到极致，具备沉浸式会诊的效果。
- (3) 专业定制：可根据不同类型用户的会诊需求及应用场景进行从会诊场景到后台软件开发对接的定制服务。
- (4) 互联互通：整体系统具备良好的兼容互通能力，并且可配合定制服务解除医疗孤岛的现象，实现和其他系统的对接。

4. “十四五规划”明确了“十四五”时期卫生健康标准化工作指导思想、基本原则和发展目标。提出到 2025 年，基本建成有力支撑健康中国建设、具有中国特色的卫生健康标准体系。紧密结合《健康中国“2030”规划纲要》和当前卫生健康重点工作，注重发挥标准的规范、引领、支撑、保障、联通作用。重点领域包括：

- (1) 开展医联体建设试点。
- (2) 推进县域医共体建设。
- (3) 基层重点任务。
- (4) 加强县域医疗共同体建设。

5. 行业市场

(1) 四大市场重点攻坚：

- ① 县域基层医疗：扩大重点领域优势，面向全民健康平台、县域医共体平台等有基础、有局部优势的行业数字化平台，全面挖掘。
- ② 公共卫生：成为公共卫生领域领先的信息化服务商，攻坚省、市级公共卫生应急指挥、多点触发传染病监测预警等重点平台。
- ③ 智慧医院：打造标杆提升影响，精选 10 个左右全国头部三甲医院的新建院区以及新建的大型三甲医院的信息化项目，打造智慧医院标杆。
- ④ 5G 健康医疗：5G 专网规模突破，以 5G+云做透、5G+急救场景，扩大 5G+远程诊断、智能疾控、医院管理试点项目规模。

6. 医联体 VS 医共体

(1) 医联体：松散结构，人力/财务各自独立，以三甲医院为核心，联合若干城市二级医院、康复医院、护理院、社区卫生服务中心。该领域潜在天翼云产品需求包括：专用物理机、弹性云主机、负载均衡、弹性伸缩、对象存储、数据库审计、容灾灾备、云防火墙、漏洞扫描、云视讯等。

(2) 医共体：统一结构，人力/财务统一，以县医院为核心，县医院为龙头，乡镇医院为枢纽，村卫生室为基础。该领域潜在天翼云产品需求包括：云电脑、云存储、弹性云主机、云安全卫士、云专线等。

7. 医院信息化建设的层次，由下往上依次为：全量全要素的数据连接、数据服务的实时、数据服务的按需、数据服务自助化、业务的可视化。

8. 智慧医院技术架构

(1) 基础层

- ① 医院信息系统云平台：云主机、云存储、云电脑、容器、微服务、大数据、AI。
- ② 医院智能网络：医疗行业专网、云专线/互联网专线、5G 定制网/物联网。
- ③ 云安全：安全管理中心、安全计算环境、安全区域边界、安全通信网络。
- ④ 云灾备：数据备份、应用容灾、数据库容灾。

(2) 数据层

- ① 数据对接
- ② 服务总线
- ③ 数据中心
- ④ 服务组件

(3) 应用层

- ① 统一门户
- ② 智慧服务
- ③ 智慧医疗

- ④ 智慧管理
- ⑤ 公众服务

9. 医院信息化场景

(1) 场景需求

- ① 计算，通过多部服务器组成的系统进行处理和分析这些小程序，得到结果并返回给用户。
- ② 存储，一种网上在线存储的模式，即把数据存放在通常由第三方托管的多台虚拟服务器，而非专属的服务器上。
- ③ 通信，网络可以支持云，也可以完全基于云。在支持云的网络中，网络位于本地，但用于管理它的部分或全部资源位于云中。
- ④ 负载均衡，可以将来自多个公网地址的访问流量分发到后台云服务器上，自动检测后端主机端口并剔除不可用的主机，提高业务可用性，并提高资源利用率。
- ⑤ 安全，是“云计算”技术的重要分支，已经在反病毒领域当中获得了广泛应用。

(2) 解决方案/涉及产品：天翼云电脑，天翼云盘，人脸对比，可视化大屏开发工具，云主机，智能组网，天翼云会议，MySQL 数据库，云专线，天翼云办公。

(3) 拓展策略：新一代医院数据中心将是以私有云为主、以多云结合为特征的医疗云数据中心。

10. 互联网医院场景

(1) 场景需求

- ① 前端，即网站前台部分，运行在 PC 端、移动端等浏览器上展现给用户浏览的网页。
- ② 后端，服务包括结构化的数据存储、用户和权限管理、文件存储、云参数、云代码、推送、支付、实时通信等。
- ③ 支付，指通过互联网作为载体进行资金的转移，利用银行所支持的某种数字金融工具，发生在购买者和销售者之间的金融交换。
- ④ 医保，为了补偿劳动者因疾病风险造成的经济损失而建立的一项社会保险制度。
- ⑤ 商保，是指通过订立保险合同运营，以营利为目的的保险形式，由专门的保险企业经营。

(2) 解决方案/涉及产品：云主机，云网融合，天翼云数据库，5G 专网，智能组网，可视化大屏开发工具，云专线，CDN 加速，人脸对比。

(3) 拓展策略：坚持“一张网络、一个平台、一套机制”的建设理念，依托智慧医疗行业数字平台，加速形成“智慧+”的新型医疗体系。

11. 防疫平台场景

(1) 场景需求

- ① 客户端接入层完成数据采集的需求。

- ② 天翼云核心服务完成数据转换的需求。
- ③ 主备切换完成系统保护的需求。
- ④ 云专线/云专网完成专用传输通道的需求。

(2) 解决方案/涉及产品：CDN、WAF、GSLB，云主机、服务器集群、云存储、Redis 集群、云数据库。

(3) 拓展策略：面向省级、市级卫健委，防疫指挥部，建成地市级的防疫云平台。

12. 防疫云灾备场景

(1) 场景需求

- ① 公共场所进入。
- ② 街道/社区核酸点。
- ③ 飞机场、火车站出发与到达。

(2) 解决方案/涉及产品

- ① 主备方式：主备中心通过专线互通。当主数据中心出现故障，通过调整 DNS 解析 IP，将业务数据调整至备中心。
- ② 双活方式：主备中心通过裸光纤/波分互通，实现二层打通。当主中心出现故障，全局负载均衡将业务调整至备中心。业务双活架构要求主备数据中心之间距离不超过 100 公里。

(3) 拓展策略：对于已经建立了防疫平台的城市，推广给主系统做云灾备。

十三、政务行业解决方案

必备掌握知识点：

1. 安防视频监控市场规模快速增长，智能+运营将成为运营商差异化竞争的利器。

2. 行业需求

(1) 产业痛点

- ① 设备厂商平台捆绑，平台烟囱林立。
- ② 亿级三类点位接入难、数据可用性差。
- ③ 摄像头麻雀杆，缺统一规划。
- ④ AI 算法、应用割裂，方案杂乱。
- ⑤ 行业场景需求迭代更新快、对接缺标准。

(2) 目标定位：以视频为核心，利用视频监控、智能存储、AI 智能分析、视图大数据、云计算、物联网等新技术，打造视频监控产品体系，助力政府“社会治安立体防控体系建设”。基于电信原子能力，专门面向政法委、公安、基层政府以及平安中国建设要求的视频接入用户，提供视频监控点位建设、视频汇聚、实时预览、历史回放、远程控制调度、智能分析和场景化应用的智能视频大数据产品。

3. 天翼云视频监控技术架构

- (1) 终端层：国标 IPC、国标 NVR、1400 摄像头、物联网、非标摄像头、第三方平台。
- (2) 网络层：互联网、电信 4G/5G、公安专线、政务专线、SD-WAN、WLAN。
- (3) 云平台层：云主机、GPU 裸金属、块存储、对象存储、云专线、云安全。
- (4) 视频平台层：视频存储、视频分析、视图大数据。
- (5) 视频应用层：政法版、公安版、社会联防版、标准版。
- (6) 展示层：WEB 端、APP 端。

4. 监控点类型

“雪亮工程”是国务院提出的一项全国性安防工程。以县、乡、村三级综治中心为指挥平台。“雪亮工程”的一、二、三类点监控，区分如下：

- (1) 一类点：摄像机及设备直连视频专网，项目多为政法委牵头的相关部分直接招标、投资。其监控图像由当地公安派出所分控中心进行 24 小时实时监控。
- (2) 二类点：摄像机及设备通过电子政务外网或相应的系统专网连接，安装地址多为事业单位，如博物馆、政府机关办公楼、公立学校、金融、医疗、物流等，项目多为事业单位或系统统一招标。其监控图像由当地公安派出所分控中心进行实时监控或录像备查。
- (3) 三类点：多为社会资源，此类视频监控点位最多也最分散，通常为小区、民办学校、商场、酒店、超市等监控，入网方式为普通的互联网入网，投资方多为企业自建。此类视频监控点的监控图像以本地录像备查为主、实时监控为辅，有条件的地方可接入当地警务室、所属管理单位进行实时监控。

5. 天翼云政法公安视频云分为四个版本：标准版、社会联防版、公安版、政法版。

6. 标准版场景

- (1) 场景目标：主要面向有平安中国建设需求的社会面汇聚用户。
- (2) 解决方案/涉及产品：视频监控、视频回访、分屏浏览、视频回放、级联推送、地图查看、数据统计、摄像头列表、分权分域控制、播放控制。
- (3) 拓展策略：面向“雪亮工程”、“明厨亮灶”、“智慧门店”、“智慧园区”等业务场景，实现海量存储、AI 分析、点播加速等功能。

7. 社会联防版场景

- (1) 场景目标：为有平安中国建设需求的社会面用户提供社会联防视频应用，为社会和群众提供更多更好的服务。同时利用社会面资源，实现与公安政法机关视频图像共享平台联网对接。
- (2) 解决方案/涉及产品：实时监控、历史回看、语音对讲、十户联防、一键报警、综合布控、智能检测、入侵告警、人员出现提醒、客流统计等。
- (3) 拓展策略：在数据汇聚的基础上建设视频智能管理平台。通过优势资源互补，建立共同的价值网，为后续公安大数据平台研发提供宝贵经验。

- ① 补充视频盲区。
- ② 丰富治安防控系统能力。
- ③ 建设人像大数据综合技战应用。

8. 公安版场景

- (1) 场景目标：为基层公安提供社会面视频汇聚、监控能力。提供多种战法帮助公安实现小案快破。
- (2) 解决方案/涉及产品：国际级联、视图库级联、实时监控、历史回看、快速检索、综合布控、全息聚档、公安技战分析、时空碰撞分析、隐匿人员分析、同行人员分析等。
- (3) 拓展策略：提供高速、专用的网络连接，并支持数据同步存储、大数据分析。

9. 政法版场景

- (1) 场景目标：为基层政法委提供社会面视频汇聚、视频监控、视频分析、市域治理相关技战能力。服务综合社会治理。
- (2) 解决方案/涉及产品：国际级联、视图库级联、实时监控、历史回看、综合布线、全息聚档、快速检索、市域治理算法分析、首次入域分析、昼伏夜出分析、人车轨迹分析等。
- (3) 拓展策略：为治安管理、城市管理、应急指挥等提供视频基础能力。

10. 视频云业务架构

接入互联网的社会面二、三类视频及物联终端，进行 AI 解析及大数据分析，自成应用供用户使用；或者将视频流及分析的结构化信息发送至专网，与一类视频及用户的业务数据充分融合，更好地为用户的业务提供数据服务。

- (1) 公安信息网和公安视频网都是专网，只有视频码流进入和控制指令流出，没有视频码流流出和控制指令进入。
- (2) 这里的互联网是指终端摄像头向上连接的专线网络，也是内网与外网之间的互联网络。
- (3) 电子政务外网，包括市级视频平台、区委办局、综合公共安全视频图像信息交换共享平台。

11. 视频云部署模式

- (1) 订阅模式：社会面视频点位互联网接入，可实现跨市跨省的视频平台共享。
- (2) ICT 建设模式：一类、二类视频点位专网接入，还提供业务应用、视图大数据、AI 算法仓、视频存储、接入平台、专网现有视图云平台。

12. 视频云销售模式：套餐订阅的运营型、ICT 专网部署项目型。

十四、智慧城市解决方案

必备掌握知识点：

1. 政策背景

- (1) 主要政策发布

- ① 全国信标委组织编写的《城市大脑发展白皮书》
- ② 《国务院关于加强数字政府建设的指导意见》-国发〔2022〕14号

(2) 政策要求

- ① 智慧城市建设迈向城乡结合新阶段。
- ② 要大力提升县城公共设施和服务能力。
- ③ 智慧社区助力智慧城市建设走向精细化。

2. 当前智慧城市建设范围正在从早期的中心城市、地级城市为主，逐步向基层下沉。尤其在当前数字经济持续驱动国民经济发展的背景下，区县、镇街、社区的智慧化发展正在成为促进高质量发展、构建数字社会的基石。

3. 智慧城市发展重心已从项目建设转移到长效运营。

- (1) 智慧城市一期建设目标，通常是基础设施集约化。
- (2) 智慧城市二期建设目标，通常是民生服务智慧化，城市治理智能化。
- (3) 智慧城市三期建设目标，通常是产业经济数字化。

4. 智慧城市整体框架

智慧城市需要打造一个统一平台，设立城市数据中心，构建三张基础网络，通过分层建设，达到平台能力及应用的可成长、可扩充，创造面向未来的智慧城市系统框架。通常分为四层：

- (1) 感知层：电脑、手机、摄像头、传感器等终端。
- (2) 网络层：通信网、互联网、物联网。
- (3) 平台层：IT能力、CT能力、城市数据中心。
- (4) 应用层：应急智慧、数字城管、平安城市、政府热线、数字医疗、环境监控、智能交通、数字物流。

5. 当前智慧城市建设痛点：数据孤岛存在，难以发挥价值；数据智能化低，应用深度不够；重建设轻运营；前期追求共性，忽略区域特色。

6. 电信体系初步具备以天翼云为核心、全面承接城市大脑的业务能力。城市大脑能力构成如下：

- (1) 一套底座基础设施，包括：IDC基础设施、云平台底座、网络基础设施、云安全底座
- (2) 1个城市大脑智慧中枢，包括：数据中台、业务中台、技术中台、能力中台
- (3) N款特色智慧应用，包括：智慧政务、园区数字孪生、应急管理、乡村振兴
- (4) 1个运营指挥中心：数智驾驶舱

7. 城市治理场景

(1) 场景需求

- ① 城市生命线：保障城市管网、道路交通以及电力、通讯、燃气、热力、排水等生命线工程正常运行，提高抗风险能力。
- ② 数字政府：以“业务数据化、数据业务化”为着力点，构建政务新机制、新平台、新渠道，全

面提升政府的履职能力，形成用“数据决策、数据服务、数据创新”的现代化治理模式。

- ③ 智慧应急：强化灾害事件、安全生产等突发事件预警、派单受理、智能方案推送、督办处置、反馈评价等系统流程建设，力争实现“零延迟”响应。
- ④ 数字乡村：面向基层政府提供乡村治理管理服务，面向乡村百姓提供政策公开、在线办事、农技推广等乡村一体化服务，是数字政府向乡村的延伸。
- ⑤ 社会治理：市域社会治理将各种资源下沉到基层，实现统一指挥调度、基层社会治理、社会风险防控、基层政务服务等功能。

(2) 解决方案/涉及产品：FIRST 物联专网、云网融合、天翼云诸葛 AI 平台、人脸对比、5G 专网、智能组网、可视化开发工具、天翼云会议、NB-IOT、CDN 加速、天翼云办公。

(3) 拓展策略：坚持“一张网络、一个平台、一套机制”的建设理念，依托智慧城市行业数字平台，加速形成“智慧+”的新型城市治理体系，全面提升城市综合治理的运行感知、资源配置、异常预测和应急联动四大能力。

8. 民生服务场景

(1) 场景需求

- ① 智慧社区：指通过利用各种智能技术和方式，整合社区现有的各类服务资源，为社区群众提供政务、商务、娱乐、教育、医护及生活互助等多种便捷服务的模式。
- ② 智慧环保：“数字环保”概念的延伸和拓展，借助物联网技术，把感应器和装备嵌入到各种环境监控对象（物体）中。
- ③ 智慧医疗：打造健康档案区域医疗信息平台，利用最先进的物联网技术，实现患者与医务人员、医疗机构、医疗设备之间的互动，逐步达到信息化。
- ④ 智慧城管：通过新一代信息技术支撑实现全面透彻感知、宽带泛在互联、智能融合应用，推动以用户创新、开放创新、大众创新、协同创新为特征的以人为本的可持续创新。

(2) 解决方案/涉及产品：物联网卡、视频监控、服务器安全卫士、云等保评测、宽带共享、微服务引擎、DDOS 高防、天翼云全栈混合云、云专网、应用编排、云网助手。

(3) 拓展策略：以“惠民”为核心目标，深化推进与市民生活密切相关的公共服务信息化，建立符合居民习惯、方便快捷的公众服务体系。

9. 城市大脑建设思路

(1) 云网安底座：

- ① 云：天翼云底座，提供算力平台。
- ② 网：互联网、5G、物联网，和视频专网。通过物联网、工业互联网、移动互联网、区块链网络获取城市感知数据。

③ 安：天翼云安全体系，打造安全平台。

(2) 智慧中枢：融合了业务中台、数据中台、技术中台和能力中台，以及相应的运维服务。

(3) 分析处理：基于融合能力，对城市数据进行深加工，建立城市治理、风险防控等指标模型并提供数据应用开放能力。

(4) 决策服务：面向政府的大脑运行管理指挥中心和面向公众的大脑公共服务平台、面向城市产业经济服务平台。

10. 云网安底座场景

(1) 场景需求

① 云计算：指通过计算机网络(多指因特网)形成的计算能力极强的系统，可存储、集合相关资源并可按需配置，向用户提供个性化服务。

② 网络：包括核心网、数据网、传输网、接入网、承载网、交换网，可以按业务角度和传输角度这两个角度来划分。

③ 安全：防范对网络的攻击、侵入、干扰、破坏和非法使用以及意外事故，使网络处于稳定可靠运行的状态。

(2) 解决方案/涉及产品：天翼云电脑、智能专线、全站加速、DDoS 高防、弹性云主机、云网融合、智能边缘云、WEB 应用防火墙、GPU 云主机、CDN 加速、弹性 IP、网站安全检测。

(3) 拓展策略：以云网融合 2.0 的优势进行行业拓荒，可先在某行业做烟囱式发展。

11. 数据中台场景

(1) 场景需求

① 技术中台：数据治理、大数据分析、AI 算法服务。

② 数据中台：对数据执行采集、治理、汇聚、管理、分析等服务。

③ 业务中台：业务定制、公共支撑、物联网管护、数字孪生。

④ 能力开发中台：对数据进行管控、运营、输出、再加工。

(2) 解决方案/涉及产品：云硬盘、云主机备份、关系数据库 MySQL、对象存储、云存储网关、数据库复制、云服务备份、云空间、人脸识别。

(3) 拓展策略

① 补足客户原有系统平台的缺失功能。

② 在各平台之间做横向打通。

十五、工业行业解决方案（选修）

必备掌握知识点：

1. 工业云细分市场

(1) 基础设施市场：私有云、公有云、混合云。

(2) 解决方案市场：面向工业的云平台解决方案（平台型）、面向工业的云应用解决方案（应用型）。

2. 工业云服务商划分

① 制造企业：以满足自给自足需要的传统制造业企业为代表，比如航天科工、美的、海尔等。

② ICT 企业：以浪潮、华为、SAP 为代表，依托雄厚的云服务技术以及多年的云转型经验，助力制造业数字化转型。

③ 互联网企业：以阿里、腾讯为代表，在互联网和云计算上具有优势，可以依托其强大的云计算底层技术为相关的工业云平台企业、工业软件企业提供技术支撑。

3. 行业需求

(1) 终端层（人/设备）：在数字仓库、AGV、自动化生产线等领域，发挥天翼云数据采集优势。

(2) 接口层：在 HMI Barcode、生产设备 PLC、采集设备 SCADA\MDC\PLC 等领域，发挥天翼云数据转换优势。

(3) 平台层：在物联网支撑平台、数据支撑平台发挥天翼云数据聚合优势。

(4) 应用层：在生产设备调度管理、机床生产监控管理、设备健康管理、能源管理系统、三维动态模拟监控系统等领域发挥天翼云数据存储、数据调用、数据分类优势。

十六、商业需求调研与分析

必备掌握知识点：

1. 在进行市场调研时，常见调研资料来源有：

(1) 政务公开：国家统计局、中国人民银行、证监会官网、商务部官网等。

(2) 互联网资源：艾瑞网、中文互联网数据资讯网、36 氪、易观智库、Talkingdata 移动观象台等。

2. 市场调研的步骤及常用方法

(1) 界定问题：可以采用“黄金圈法则”。“黄金圈法则”是由营销专家西蒙·斯涅克提出的，其核心是：对事情从内而外进行提问，在思考或沟通的时候，按照由内圈向外圈，即 why—how—what 的特定结构来进行表述。

(2) 问题分层：可以采用“5W2H”法。“5W2H”是一种调查研究和思考问题的办法，又称“七问分析法”。

① Who：用户是谁？

② When：时间，从什么时候开始，什么时候结束？

③ Where：地点，在哪里实施？

④ What：做什么内容，执行？

⑤ Why：目的，为什么要做，原因？

⑥ How：如何做，实施，方法？

⑦ How much: 价格, 成本多少?

(3) 建立框架。

① 聚焦式: 围绕天翼云产品在用户侧的一些具体问题进行分析, 比如前面的界定问题和问题分层中的问题, 就是聚焦式分析。

② 发散式: 从产品向外延伸, 主要围绕外部环境和竞品的情况进行分析。

(4) 输出结论

① Word 形式的《市场调研报告》, 除封面、目录索引以外, 通常包括 5 大章节: 研究背景、市场情况、竞争对手情况、研究内容、研究方法。

② PPT 形式的《市场调研汇报》, 主要包含 5 个内容: 界定问题、调研对象、竞品营销方式、信息来源, 最后结论。

3. 天翼云产品面向的群体分为两种, 一种是某些特定用户群体, 另一种是单一用户:

(1) 特定用户群体: 需要识别个体标签、群体特征, 多为标准化产品, 调研时更重视用户习惯数据的采集。

(2) 单一用户: 需要识别用户特点、用户业务, 多为定制化产品, 调研时更重视用户的需求描述和本身业务的运行特征。

天翼云解决方案架构师所面对的客户, 通常是第二种, 为单一用户提供定制化的产品或解决方案。

4. 用户调研流程

(1) 明确调研目标: 明确业务规划、掌握业务细节、产出初步方案。

(2) 选取调研对象: 常见的调研对象包括高级管理者、基层管理者、运营人员、一线人员、客户。

(3) 确认调研方法: 深度访谈、调研问卷、轮岗实习、数据分析、行业研究。

(4) 执行调研计划: 时间计划、节奏安排。

(5) 总结归纳输出: 报告、汇报。

5. 三层调研模型

根据被调研者类型分为:

(1) 决策者: 围绕其关注的产品问题和期望, 探讨系统的目标与范围, 计划调研要点包括:

① 列举部分主要问题

② 提供相应案例的解决方案

③ 列举潜在问题

(2) 管理者: 围绕其关注的业务事件和管理方案, 探讨产品业务流程/工作流转过程, 计划调研要点包括:

① 列举相关业务事件列表

② 准备一些业务事件的关键点问题

③ 收集审批流程/权限的设定及业务部门边界

(3) 使用者：围绕其关注的业务活动和操作流程，获得业务操作过程经验，计划调研要点包括：

① 罗列相关业务活动

② 获取相关业务规则及数据字段信息

③ 获取相关业务节点和流转过程

6. 深度访谈：由调研人员与调研对象进行深度交流和互动，从而使最初的假设得到验证或排除，或从中寻找和挖掘到对解决问题有帮助和有价值信息的一种调研方式。深度访谈的主要特征是：调研的问题复杂，调研人员为专家，以开放式问题为主，互动性强。深度访谈时要注意以下几点：

(1) 准备好访谈大纲，并提前将访谈大纲发给被访者

(2) 从高级别人员开始访谈

(3) 提前研究访谈对象

(4) 访谈过程应循序渐进

(5) 形成书面记录

7. 用户访谈：用户访谈总结为八个技巧

(1) 通过预访谈修正大纲

(2) 寒暄和循序渐进

(3) 鼓励用户畅所欲言

(4) 不要使用用户不懂的术语

(5) 多询问曾经的真实经历

(6) 穿插现场操作，鼓励口述想法

(7) 不要问封闭式的问题

(8) 给用户荣誉感

其结果有利于下一步识别需求，以及用什么产品来对应解决。

8. 识别需求

(1) 目的：要“掘地三尺”找到需求的底层原因（真实原因）。

(2) 目标：要找到项目的使用者、管理者、投资者等项目干系人。

(3) 方法：既要从用户的表述中发现显性需求，又要通过访谈发现用户的隐性需求。

9. 四要素分析法：需求=用户+场景+目的+任务

10. 需求优先级：对用户量与发生频率评估打分，得分越高的需求，其重要性越高，越应该优先满足。

(1) 用户量大且发生频率高的需求得 4 分。

(2) 用户量大但发生频率低的需求得 3 分。

- (3) 用户量小但发生频率高的需求得 2 分。
- (4) 用户量小且发生频率低的需求得 1 分。
11. 一个 ICT 项目是否由云平台来做为支撑主体解决并实施，很多情况下，可以通过以下两点判断：
- (1) 是否有数据要放在共享服务器上，供更多的用户访问。
- (2) 是否有公共软件要放在共享服务器上，供更多的用户使用。
12. 产品架构图，应包含的模块包括：产品定位、产品业务、产品接口、用户端模块、基础模块等。
13. BRD 是商业需求文档；MRD 是市场需求文档；PRD 是产品需求文档。

项目	BRD	MRD	PRD
定义	Business Requirement Document 首字母缩写。 基于商业目标或价值所描述的产品需求内容报告，市场分析、销售策略、盈利预测，完成需要哪些资源，公司有没有能力完成。	Market Requirement Document 首字母缩写。 主要进行市场分析，目标客户分析、竞争对手分析，并给出主要需求。	Product Requirement Document 首字母缩写。 主要对功能进行分析，本次迭代有哪些功能，功能的目的，功能的交互界面，功能的逻辑实现。
对象	领导层、决策者、投资者	管理者	产品研发、运营工程师、UI 设计师、测试工程师
编写者	产品经理、产品市场经理、商业分析师	产品经理、产品运营、市场经理	产品经理
侧重点	项目背景、市场分析、团队能力、产品路线、财务计划、竞争对手分析等。	目标市场分析、目标用户分析、用户使用场景、用户分类、核心用户	详细功能说明、业务流程、业务规划、界面原型、数据需求（输入、输出、极限范围、数据格式）

14. PRD 通常包含以下内容：
- (1) 第一页，封面：整体文件的标题、文件状态。
- (2) 第二页，扉页：文件修订记录，版本号。
- (3) 第三页，目录：全书大纲。
- (4) 第 N 页，产品功能性需求：产品功能描述。
- (5) 第 N+1 页，产品架构图或产品组网图。
- (6) 第 N+m 页，软硬件环境：具体软硬件配置。
- (7) 第 N+p 页，产品升级维护需求：服务级别协议 SLA。
15. 产品规划后期工作

中标以后，需要让以后执行这个项目的各个部门，知道各自要完成哪些工作，这时，就要列出产品规划的这些内容，包括产品目标、业务目标、要做的模块、负责人等。

- (1) 产品目标：实现什么新的功能。
- (2) 业务目标：在项目周期内的完成时间点（段）、成本控制条件、客户关键需求点。
- (3) 要做的模块：所属哪个更大一级的功能模块。
- (4) 负责人：执行人是谁或部门。
16. 需求变更产生的原因

- (1) 需求范围没有圈定，就开始后续的细化工作。
 - (2) 没有指定需求的基线。
 - (3) 没有良好的结构适应变化。
17. 五级需求变更管理模型：一级需求(或变更)：紧急性需求（Urgent）；二级需求(或变更)：后续关键性需求（Necessary）；三级需求(或变更)：后续重要需求（Needed）；四级需求(或变更)：改良性需求（Better）；五级需求(或变更)：可选性需求（Maybe）。
18. 全生命周期的需求变更管理
- (1) 启动阶段变更预防
 - ① 基准文件定义的范围越清晰越好。
 - ② 需求分析要做好，文档清晰且要有客户签字。
 - ③ 合同范围超出，需要另外收费。
 - (2) 实施阶段变更
 - ① 需求一定与投入有关系
 - ② 要经过出资方的认可
 - ③ 小的需求变更也要经过正规流程
 - ④ 精确需求与范围定义并不会阻止需求的变更
 - ⑤ 注意沟通技巧
 - (3) 收尾阶段变更
19. 需求变更原则
- (1) 要建立需求基线。
 - (2) 制定简单有效的变更控制流程，并形成文档。
 - (3) 成立项目变更控制委员会 CCB，或者类似职能的组织，负责裁定接受哪些变更。
 - (4) 需求变更一定要先申请，再评估，最后经过与变更大小相当级别的评审确认。
 - (5) 需求变更后受影响的计划、产品、活动，都应进行相应的变更，以保持和更新的需求一致。
20. 解决方案三步曲
- (1) 初次交流的解决方案：向客户做品牌宣传、服务能力介绍、标杆项目呈现。
 - (2) 采购过程中的解决方案：与（1）一起都可称为《售前解决方案》，是在销售/售前阶段帮助客户解决具体业务问题的沟通工具。
 - (3) 决策汇报/述标会的解决方案：也可称为《技术解决方案》，对一个具体项目的规划设计，围绕具体的需求而展开，阐述技术、方法、产品和应用。
21. 售前解决方案设计
- 把客户需求的功能，与天翼云中对应的产品或服务进行组合，并交付给客户。具体制作该方案时，要

注意以下几点：

- (1) 交流目标：介绍天翼云产品及能力、客户业务系统、IT 现状，探索客户的概念。
- (2) 交流重点：探索客户的期望与需求、收集信息。
- (3) 材料风格：简洁、抛砖引玉。
- (4) 避免销售拜访秀。

22. 通用方案设计模型

实施难度由简到繁包括如下模型：

- (1) 通用方案 1：云主机（用天翼云主机替换原有物理机或虚拟机）。
- (2) 通用方案 2：云主机+RDS（在方案 1 基础上，增加了天翼云 RDS 关系型数据库，替换原有数据库）。
- (3) 通用方案 3：云主机+云专线（在方案 1 基础上，增加了云专线，保证网络带宽能支撑业务运行）。
- (4) 通用方案 4：云主机+云专线+RDS（在方案 3 基础上，增加了天翼云 RDS 关系型数据库）。
- (5) 通用方案 5：云主机+云专线+RDS+互联网访问（在方案 4 基础上，增加了互联网专线）。