**集群注册运营管理平台**

**技术服务标准**

2020年1月沈阳

目录

[第1章 企业资质标准 3](#_Toc29546553)

[第2章 建设原则 4](#_Toc29546554)

[2.1 设计原则 4](#_Toc29546555)

[2.1.1 可靠性原则 4](#_Toc29546556)

[2.1.2 先进性原则 4](#_Toc29546557)

[2.1.3 高安全性原则 5](#_Toc29546558)

[2.1.4 可扩展性原则 5](#_Toc29546559)

[2.1.5 开放性原则 5](#_Toc29546560)

[2.1.6 高可复制性原则 6](#_Toc29546561)

[2.1.7 实用性原则 6](#_Toc29546562)

[2.1.8 国产化原则 6](#_Toc29546563)

[2.2 总体架构 7](#_Toc29546564)

[2.2.1 基础设施服务层(IaaS层) 7](#_Toc29546565)

[2.2.2 平台能力支撑层(PaaS层) 7](#_Toc29546566)

[2.2.3 软件能力服务层(SaaS层) 7](#_Toc29546567)

[2.2.4 保障体系 7](#_Toc29546568)

[2.3 运行环境 8](#_Toc29546569)

[2.3.1 硬件环境 8](#_Toc29546570)

[2.3.2 软件环境 9](#_Toc29546571)

[2.4 数据存储要求 9](#_Toc29546572)

[2.5 系统性能要求 10](#_Toc29546573)

[2.5.1 稳定性 10](#_Toc29546574)

[2.5.2 可靠性 11](#_Toc29546575)

[2.5.3 容错和自适应性能 11](#_Toc29546576)

[2.5.4 易于维护性 12](#_Toc29546577)

[2.5.5 安全性 12](#_Toc29546578)

[2.5.6 可支持加密系统，保证通讯的安全、可靠。方便扩展性 12](#_Toc29546579)

[2.5.7 易用性 13](#_Toc29546580)

[2.5.8 兼容性 13](#_Toc29546581)

[2.6 系统可靠性要求 13](#_Toc29546582)

[2.6.1 服务器可靠性 13](#_Toc29546583)

[2.6.2 存储可靠性 14](#_Toc29546584)

[2.6.3 网络可靠性设计 15](#_Toc29546585)

[2.6.4 虚拟化可靠性 16](#_Toc29546586)

[2.6.5 管理可靠性 16](#_Toc29546587)

[2.7 网络传输性能要求 17](#_Toc29546588)

[2.8 标准化与规范化原则 18](#_Toc29546589)

[第3章 关键技术 19](#_Toc29546590)

[3.1 人脸核身技术 19](#_Toc29546591)

[3.2 公安部信息身份认证 19](#_Toc29546592)

[3.3 银行卡认证 19](#_Toc29546593)

[3.4 权威认证电子签章与电子合同技术 20](#_Toc29546594)

[3.5 云存储技术 20](#_Toc29546595)

[3.6 微服务 21](#_Toc29546596)

[3.7 AI动态基线建立技术 22](#_Toc29546597)

[3.8 分布式对象技术 23](#_Toc29546598)

[3.9 接入技术 23](#_Toc29546599)

[3.10 接口技术 24](#_Toc29546600)

[3.11 运维保障技术 24](#_Toc29546601)

[3.12 系统安全策略 24](#_Toc29546602)

[3.12.1 法律制度与道德规范 25](#_Toc29546603)

[3.12.2 管理制度的建立与实施 25](#_Toc29546604)

[3.12.3 物理实体的安全与硬件系统的保护 25](#_Toc29546605)

[3.12.4 网络的安全与保护 26](#_Toc29546606)

[3.12.5 应用系统的安全措施 29](#_Toc29546607)

[3.12.6 相关法律问题 29](#_Toc29546608)

[3.13 网络安全策略 29](#_Toc29546609)

[3.13.1 数据中心安全域 29](#_Toc29546610)

[3.13.2 虚拟化网络安全防护 30](#_Toc29546611)

[3.13.3 逻辑分层 31](#_Toc29546612)

[3.14 虚拟化服务器安全防护 32](#_Toc29546613)

[3.15 数据存储、容灾与备份 33](#_Toc29546614)

[3.15.1 数据存储 33](#_Toc29546615)

[3.15.2 数据备份与容灾 33](#_Toc29546616)

[第4章 数据库建设与数据整合入库 35](#_Toc29546617)

[4.1 概述 35](#_Toc29546618)

[4.2 数据架构 35](#_Toc29546619)

[4.3 数据库建设内容 36](#_Toc29546620)

[4.3.1 业务数据库 36](#_Toc29546621)

[4.3.2 操作数据存储区数据库 36](#_Toc29546622)

[4.4 数据仓库设计 36](#_Toc29546623)

[4.4.1 明细数据区 36](#_Toc29546624)

[4.4.2 主题数据区 36](#_Toc29546625)

[4.5 数据字典设计 37](#_Toc29546626)

# 企业资质标准

“集群注册运营管理平台”相关信息涉及到国家行政机关和个人的敏感信，依据国家信息安全等级保护标准，接入信息系统企业必须具备以下资质：

1. 具有在有效期内的ISO9001质量体系认证证书
2. 具有在有效期内的服务管理体系ISO/IEC 20000-1:2011认证证书
3. 具有在有效期内安全管理体系 ISO/IEC 27001:2013认证证书
4. CMMI4及以上资质\*
5. 高新技术企业资质\*
6. 国家级双软企业资质\*
7. 具有3A信用企业证书\*
8. 环境管理体系认证\*
9. 安可联盟会员单位\*

注：全文内容中的\*项（段落表述）为加分评定项

# 建设原则

* 1. 设计原则

“集群注册运营管理平台”的建设将以计算机网络为基础，遵照国家有关标准以及规范对数据进行科学地存储与管理，实现快速地数据采集、校验、建库、查询、检索、更新、统计等。平台可集中控制用户的权限，提供企业、访客人员、管理员的统一接入和管理。

### 可靠性原则

建设时应充分考虑系统和技术的可靠性。系统宜采用国际上先进成熟的软件产品作为基础开发平台，利用高性能的大型数据库作为数据存储的载体，实现数据的审核和数据的备份，具有完善的数据转换接口，保证系统数据与外业数据的规则一致性。采用模块化的开发方式，严格按照软件开发的技术流程和质量保证体系进行系统建设，保证系统的稳定性与可靠性。

### 先进性原则

系统在设计思想、系统架构、采用技术上均要尽可能采用最先进的技术、方法、软件平台等，确保系统有一定的先进性、前瞻性、扩展性，符合技术发展方向，延长系统的生命周期，保证建成的系统具有良好的稳定性、可扩展性和安全性。

系统的建设应采用先进而成熟的技术，以充分提高生产效率。系统能够轻松高效地管理海量的信息数据。先进性是系统发展的条件，只有先进的系统，才能充分发挥软硬件的能力，才能发展，才能体现良好的建设效果。从一些系统建设的实际经验和教训来看，先进性如不能保证，则会在系统的使用阶段出现后期投资追加过大，系统维护费用加大等问题。

\*在平台设计上，整个系统软硬件设备的设计符合高新技术的发展趋势，媒体数字化、压缩、解压、传输等关键设备均处于国际领先的技术水平。在满足现期功能的前提下，设计具有前瞻性，在今后较长时间内保持一定的技术先进性。

### 高安全性原则

“集群注册运营管理平台”管理的数据是国家行政机关监督管理和应用的关键数据，信息管理系统的建设必须同步实施安全工程，建立基于授权的访问控制模式，逐步完善信息安全保障体系，要结合城市管理的具体情况，按照不同的业务内容，采取不同的安全策略，处理好发展与安全、建成与效益的关系，使安全措施成为保障信息资源系统正常运行的重要手段。并在网络安全、操作系统安全、数据库管理系统安全、使用安全、管理安全等方面符合国家关于计算机信息系统安全保护的相关要求。

平台采取全面的安全保护措施，具有防病毒感染、防黑客攻击措施，同时在防雷击、过载、断电和人为破坏方面进行加强，具有高度的安全性和保密性。对接入系统的设备和用户，进行严格的接入认证，以保证接入的安全性。系统支持对关键设备、关键数据、关键程序模块采取备份、冗余措施，有较强的容错和系统恢复能力，确保系统长期正常运行。

### 可扩展性原则

考虑到系统数据量的增长、数据类型的拓展；考虑到今后系统的管理需求和应用范围的进一步扩展，将会对系统的性能和功能提出新的要求。因此，随着信息技术的发展，系统中的硬件设备和软件系统必须具有良好的系统扩充性。在系统的设计和建设中，应保证系统的结构模块化。系统应是可成长的，应能适应业务的增长和扩充，同时，将按一定的比例预留冗余节点，以保证系统的扩充及容错能力，冗余和容错也是保证系统稳定性与可靠性的重要措施。

### 开放性原则

开放式系统不仅仅是一些标准和技术的组合，更重要的是，开放式系统为开发者提供了一种可以按照开放式系统的标准和技术进行设计和开发的思想。只有基于这种思想，才能开发出真正为用户所接受的开放式系统。

在系统的设计过程中，需要采用多种先进的技术。在开放式系统结构设计时采用微服务的机构体系，利用元数据（即动态的可配置的空间数据模型）驱动系统功能的思想为应用软件提供接口；在功能实现上，不仅要充分结合用户现有的功能需求，还要考虑到未来城市管理的各类应用情况；在软件的平台选型上，选用当今主流的平台，为系统的发展和升级提供方便；采用开放式设计方法实现统一的存储和管理，为数据的增值服务奠定坚实的基础；同时在软件的整体集成方面，应注重接口的设计，具备良好的输入输出接口，可为各种增值业务提供接口，充分考虑本系统与其它系统之间的无缝连接、互联互通。

### 高可复制性原则

由于本系统是一个开放统一的信息管理的平台，所以系统的建立必须严格遵循现有的国家标准和行业规范，制定统一的数据编码和数据规范体系，包括数据定义体系、分类体系、数据交换格式、数据存储格式、输出格式以及数据文档、项目实施的质量标准等，实现数据格式的标准化和统一性。在信息的收集、验证、处理、汇总和传递过程中建立统一的数据接口，保证各层次之间形成高效规范的体系，确保对各种信息的高效收集和利用，最终达到与其它应用系统的资源交换与共享。

系统开发使用的技术标准应符合国家、行业及城市的有关技术规定。

### 实用性原则

“集群注册运营管理平台”不仅面向专业的技术人员，还要面向市场监管、税务、社会保障等工作中各种需求层次应用的其它相关部门人员。系统应具有良好的实用性，提供清晰、简洁、友好的中文人机交互界面，操作简单快捷，界面友好，系统和数据要易于维护、更新和管理，提供各种满足不同层次用户需求的功能和工具。还应具有习惯操作的客户端界面，在快速操作处理突发事件上有较高的时效性。

### 国产化原则

伴随着云计算、移动互联网、大数据、社交网络、物联网等一系列新兴技术和产业的兴起，使得IT信息化的软硬件发生了很大的改变。对于加快国产软件厂商在产品和技术之间的适配度层面，是真正实现信息化的系统性替代的关键发展路径，只有真正达到了产品与技术之间的适配，才能够实现信息化的系统性替代，从而完全迁移到国产软件和硬件当中来。

系统须兼容鲲鹏、兆芯、龙芯、申威、飞腾等平台。支持IP或InfiniBand网络，支持IPv4及IPv6双栈。除主流RedHat、CentOS、Suse、Ubuntu外，须支持麒麟、深度等国产化操作系统。

* 1. 总体架构

### 基础设施服务层(IaaS层)

基础设施服务层，基于集群注册运营管理平台，建设数据中心运行服务平台，使平台具备弹性扩容的能力，承载不断增加的城市数据体系。该层通过云化主机、存储、网络等设备，提供计算、存储、计算负载管理、备份等服务，资源动态调整，按需提供基础云服务。

### 平台能力支撑层(PaaS层)

能力支撑层具有可扩展和开放的特性，支持与外部应用系统的集成，形成能力汇聚，从而以支撑应用层的各类大数据应用。

### 软件能力服务层(SaaS层)

可以快速的根据对接企业要求配置相关数据对接服务，提供平台注册、开通、注销一站式工商纳税法务的对外功能输出。

### 保障体系

在建设集群注册运营管理平台时，需着重建设安全保障体系，标准规范体系，大数据存储和建模体系等方面，它们是一站式工商税务注册管理体系成功建设并得以广泛推行的重要保障。

#### 安全保障体系

安全保障体系是服务管理信息化的前提，建立安全保障体系是平台建设的先决条件，该体系包括身份认证、权限控制、安全审计、平台监控、故障报警、日志管理等安全保障方法。同时，数据安全是“"险中之险”，应加强信息安全保障体系建设，推动建立大数据应用的法规制度体系，明确各级的责任、义务与使用权限，合理界定教据的使用方式与范围，规范公共教据的采集、共享和应用，保障公共教据的公平、权威和可信，保护数据产权、安全和隐私。

#### 标准规范体系

标准规范体系的建立是平台信息资源整合共享的前提，该体系主要包括元数据内容规范、信息资源标识规范、公共数据、元目录规范、信息资源分类及编码规范、数据交换格式设计规范、信息分类编码规范等。

* 1. 运行环境

系统软硬件平台设计需考虑业务发展，在设计时保证足够的存储容量，并提供足够的业务、计费处理足够能力，支持客户端操作，系统还应具有良好的扩展能力。在服务器部署上，应用部署在中心，时空数据的部署既要支持各公司分布部署，又要支持中心部署的模式，同时为了减轻平台用户端的实施和维护工作量，可采用虚拟桌面的方式来访问。

### 硬件环境

一站式工商税务注册硬件环境主要包括：基础设施层、平台资源层、业务数据层。其中，云计算基础设施层：主要包括云计算中心的物理机房环境；云计算平台资源层：在云计算中心安全的物理环境基础上，采用虚拟化、分布式存储等云计算技术，实现服务器、网络、存储的虚拟化，构建计算资源池、存储资源池和网络资源池，实现基础设施即服务。云计算业务数据层：实现业务数据的安全存储，针对云平台的各个虚拟机镜像数据和模板数据进行共享存储，支持虚拟机的动态迁移和数据的迁移；实现部门间数据共享与交换；实现业务应用接入。

### 软件环境

#### 数据库软件

依据下列数据库选型原则，选用Mysql 的DBMS。

* 支持本系统关键技术
* 海量的数据存储能力
* 支持OLAP分析、数据仓库与数据挖掘
* 支持Web应用、XML技术
* 完善的数据备份、恢复等安全机制
* 支持各种主流技术标准
* 出众的性能
* 良好的市场服务体系

#### 平台及工具

开发语言：Java，Python等面向对象语言和大数据分析人工智能语言。

开发框：Spring boot等Java成熟框架

微服务：采用dubbo、SpringCloud

大数据分析：采用ElasticSearch等大数据框架

前端语言：基于NODEJS的REACT、VUE语言的相关前端框架。

APP开发：使用FLUTTER、REACTNATIVE世界先进的开发语言进行开发。

* 1. 数据存储要求

1. 具有海量数据存储和管理能力，支持2TB以上的业务数据存储能力的存储
2. 具有万兆带宽的吞吐率等能力以确保未来业务的扩展性及高并发时刻的用户体验。高吞吐率可以让平台承受更多的流量，让传输速度更快，可以有效缓解DDoS和CC等网络上最常见的攻击。
3. 确保业务不中断—从存储IO看来，没有超过1秒以上的IO中断。有IO中断会造成业务卡顿，甚至超时报错，影响业务连续性。智能故障自愈意味着故障处理无需人工干预。

平台将视硬件故障为合理抖动，保障业务连续性。在节点故障时，立即由健康节点接管任务，无需任何等待，也不会发生IO性能急剧下降或中断的情况，业务不受影响。

* 1. 系统性能要求

### 稳定性

具备在规定条件和时间内完成用户所要求功能的能力，能长期稳定地工作；

系统结构稳定，可靠性高，系统启动快，系统掉电后再来电或网络传输中断后再恢复正常时，系统恢复工作迅速；系统软件及其功能模块在各种情况下不会出现死机现象及系统崩溃现象。

系统故障率低，维护维修方便，具有良好的可操作性和人机交互界面等。

### 可靠性

软件可靠性设计通过采用相应的技术和工具来减少错误的发生，从而保证系统数据维护、查询、分析、计算的正确性和准确性。系统可靠性设计将主要采用以下三种方法。

（1）软件可靠性分配

软件可靠性分配是将需求分析中形成的可靠性指标分配到各个软件部件，是软件可靠性工程设计的基础，是在充分考虑软件及其开发过程的特征并继承和发展可靠性工程已有成果的基础上发展起来的。目前，主要有快速分配法，以及基于重要度、运行时间和复杂度分配等方法，而后者是普遍使用的方法。

（2）软件重用设计

重用设计是在软件设计过程中对现有成果进行充分再利用的活动，是提高软件生产率、降低开发成本和提高软件可靠性的最有效途径之一。特别在面向对象程序设计方法获得广泛应用后，软件重用日益受到人们的重视，并逐渐成为可靠软件设计的重要方法。

（3）软件形式化设计

要获得较高的软件故障独立性往往很困难最佳的解决办法是采用形式化的程序设计、编程系统及验证方法。使用以数学为基础的描述是解决软件设计的精确性和正确性的最好办法。为了使软件设计的每个阶段都能得到有效的测试和验证，最高一级的技术要求（即软件需求分析）必须采用形式化的分析、说明和表达。

### 容错和自适应性能

对使用人员操作过程中出现的误操作或可能导致信息丢失的操作能推理纠正或给予正确的操作提示。对于关联信息采用自动套接方式按使用频率为用户预置缺省值。

（1）限制用户某些交互操作

如何从设计上避免用户出错，限制是一种非常必要的方式。置灰是界面上限制某些操作的好方式，防止用户跳过第一步直接进入后面操作，一方面告诉用户这可以进行当前操作，另一方面预示后面还有哪样的操作。

（2）合理利用系统反馈

提前提示某些操作可能引起错误；防止用户错误，操作后提示确认；反馈出错的同时给于用户解答；系统操作中能给予用户适当指引和建议。

### 易于维护性

网络系统的所有设备都是可管理的，支持远程监控及故障的过程诊断和恢复。通过网络管理工具，可以方便地监控网络运行情况，对出现的问题及时解决，对网络的优化通过依据。另外，网络的设计采用简单易用的网络技术，降低运行维护的费用。在设计网络系统时应充分利用现有的资源，以保护在软硬件上的原有投资。

除此之外，系统的数据、业务的日常管理与维护操作方便、简单实用。

### 安全性

（1）开发的软件应具有严格用户认证、授权和访问控制的权限管理，防止外部非法用户对平台的访问以及内部合法用户的越权访问。

（2）内部用户之间彼此业务不可见，各用户的数据端到端隔离，在数据库中通过用户标识区分用户的数据，有且只有用户所属管理员才能访问其数据，最大程度保证用户的数据安全。

（3）软件和数据库平台有容错和故障恢复手段。

（4）具有高度的安全性，系统应具有多级的密码设定机制。

### 方便扩展性

外部各系统通过接入平台完成具体应用的挂接，用户通过使用门户作相应的显示配置并能使用接入平台操作接入的应用系统，系统管理员能对接入什么及如何接入进行管理配置。系统管理人员能够通过应用安全平台管理局中心的人员组织结构，利用授权功能添加业务的角色，并为角色设置相应的功能权限，以及查看日志信息和系统审计报表。业务人员和领导能够在应用安全平台的保障下使用系统。对系统管理员提供对平台(包括用户映射\数据交换\目录管理\门户权限管理\日志管理\系统代码管理)管理的工具，业务系统开发商可以在此框架上添加自己的管理配置功能。

### 易用性

操作简便，点击鼠标次数在不多于3次完成一个操作。界面直观、对用户透明：用户接触软件后对界面上对应的功能一目了然、不需要多少培训就可以方便使用本应用系统。界面设计中软件用户是所有处理的核心，不应该由应用程序来决定处理过程，所以用户界面应当由用户来控制应用如何工作、如何响应，而不是由开发者按自己的意愿把操作流程强加给用户。

### 兼容性

系统从规模上、功能上易于扩展和升级，应制定可行的解决方案，预留相应的接口。

系统随着后续建设的不断进行，势必进行系统扩充。除需进行部分超前设计外，还必须考虑系统扩充性，以便能及时进行系统扩充。

软件版本易于升级，能满足各业务系统相关的标准，任何一个模块的维护和更新以及新模块的追加都不应影响其它模块，且在升级的过程中不影响系统的性能与运行。

* 1. 系统可靠性要求

为保证系统的可靠性，具体要求如下：

### 服务器可靠性

* 服务器可靠性包括内存、硬盘、电源等多个层面的内容。
* 提供BIOS内存自检和ECC纠错技术。
* 支持硬盘热插拔和RAID功能，提供硬盘在线故障检测和预警。
* 支持电源1+1冗余和热插拔。
* 支持对CPU，内存，风扇，电源，硬盘等热关键器件的温度实时监控，设备故障时会产生告警，可以灵活对支持热插拔设备进行在线更换，不支持热插拔设备提前安排好业务后进行下电更换。配合智能的风扇调速和监控，确保系统运行的可靠性。
* 多台服务器组成计算资源池，支持虚拟机的热迁移、HA功能。

### 存储可靠性

1. 存储多路径

每个计算节点与存储集群之间，至少配置两个完全冗余的路径，从而提供存储的多路径访问功能。多条路径间的故障切换由软件自动提供，从而避免单点故障带来的存储访问问题。

1. 存储数据的冗余备份

采用SAN作为存储设备，在SAN高可靠性的基础之上，配置热备盘做冗余备份，保证数据不丢失和故障快速恢复。

1. 存储冷迁移

在虚拟机关机情况下，通过管理员手动操作，将虚拟机的卷迁移至其他的存储单元中，可以在同一个VRM管理下的同一个存储设备内，不同存储设备间，块设备和存储虚拟化之间进行迁移。

1. 存储热迁移

在虚拟机正常运行时，通过管理员手动操作，将虚拟机的卷迁移至其他存储单元中，可以在VRM管理下的同一个存储设备内、不同存储设备间，块设备和存储虚拟化之间进行迁移。

1. 存储动态资源调度(DRS：Dynamic Resource Scheduler)

在存储热迁移的基础上，可以进一步提供存储DRS功能。虚拟化平台通过相关的数据采集（数据存储的空间使用率和IO延时）， 并制定采集的数据制定相应的存储自动调度计划，以保证业务连续性的情况下根据设置的参数来实现存储资源的合理调度，使得集群下的存储资源在使用率和IO性能上达到一定的均衡优化效果。

1. 全对称分布式架构及主动的智能干预机制

存储无中央控制节点，无中央元数据节点，无单点故障隐患。

同时为保证可靠性，平台须智能的主动监测与干预系统情况，包括但不限于：磁盘亚健康主动干预；节点亚健康主动干预；网络亚健康主动干预。支持设备/单板/芯片/接口/队列/光链路KPI指标趋势图展示;支持设备/单板/芯片/接口指标的动态基线展示和异常检测;支持毫秒级队列拥塞和丢包检测;支持光链路健康状态预测;支持接口接收/发送带宽利用率未来12周的预测结果展示。

### 网络可靠性设计

1. 网络路径全冗余

核心层交换设备通过使用交换机集群技术，保证对外与防火墙/NAT和对内汇聚交换机连接的冗余。

汇聚层交换设备通过使用交换机集群技术，保证对外与核心层交换设备和数据中心内接入层交换机连接的冗余。

接入交换机通过使用交换机堆叠技术，保证对外与汇聚层交换设备和对内虚拟网络层连接的冗余。

虚拟网络层通过采用多网卡绑定等技术避免单个网卡故障引发的业务中断。

1. 网络分平面通信

系统通信平面划分为业务平面、存储平面和管理平面。为了保证各种网络平面数据的可靠性，不同平面间采用VLAN等技术进行隔离，单个平面故障不影响其余两个平面的正常工作。

业务平面：主要为虚拟机虚拟网卡的通信平面，对外提供业务应用。

存储平面：主要为iSCSI存储提供通信平面，并为虚拟机提供存储资源，但不直接与虚拟机通信，而通过虚拟化平台转换。

管理平面：负责整个云计算系统的管理、业务部署、系统加载等流量的通信。

1. 网卡负荷分担

对于各通信平面（业务、存储、管理）均采用双网卡，双网卡采用了Bonding模式，两网卡被绑定成逻辑上的“一块网卡”后，同步一起工作。既能对服务器的访问流量进行负荷分担，又能保证其中一块发生故障的时候，另外的网卡立刻接管全部负载，过程是无缝的，服务不会中断。

考虑到不同平台使用者的要求，须支持主备与双活两种绑定模式。

### 虚拟化可靠性

1. 虚拟机热迁移

提供虚拟机的自动迁移和手动迁移方案，当前计算节点出现故障或者计算节点负载过高时，可以把虚拟机迁移到正常的计算节点或者负载相对较低的计算节点上，保证虚拟机的正常运行。

1. 虚拟机HA

虚拟机高可用性（HA）是虚拟机的一个特性，当虚拟机所在的物理服务器故障（如宕机、掉电等）或重启后，虚拟机可以自动在其他物理服务器上运行，保证虚拟机能够快速恢复，它可以保护用户的业务程序对外提供不间断的服务，把因软件/硬件/人为造成的故障对业务的影响降低到最小程度。

1. 快照

系统提供虚拟机、卷快照功能，系统正常状态下，可以触发一个系统快照，用于在系统出现故障的时候还原系统。平台的快照须支持至少65535个 。



### 管理可靠性

1. 计算和存储集群分离

通过采用计算集群和存储集群相分离的架构，提升系统的可靠性。计算集群完成虚拟机的按需分配以及集群内的热迁移，存储集群完成虚拟机的系统卷和用户卷的按需分配以及跨磁盘的存放。须支持超融合架构，相应的QoS配置要适合业务流量的比例，确保最大化利用带宽等资源。

1. 管理节点HA

管理软件均采用1+1备份或负载均衡的方式运行。当一个管理节点的软件出现故障的时候，系统自动切换到备用节点，保证整个系统不间断运行。

1. 故障检测

支持服务器、软件和资源的监控。通过在每个被监控的节点上运行检测程序，系统可以收集服务器的核心指标如CPU使用情况、基础网络流量和内存数据等，检测到诸如进程异常、管理和存储链路异常，节点异常、系统资源过载等各种故障，使系统具备完善的故障检测能力。

支持故障信息收集和存储集群节点可用性度量，并且可以在Web浏览器中显示。用户可查看集群管理和系统的分配负载，确定是否有：负载均衡问题、失控进程或硬件性能下降的趋势等问题。该功能对合理调整系统资源、提高系统整体性能起到重要作用。历史记录允许查看集群每日、每周、或者每年的硬件资源情况。

1. 黑匣子

管理节点和计算节点引入电信领域“黑匣子”技术，在系统出现异常时自动存储内核日志、系统快照、内核诊断信息及临终遗言，并保存至非易失性存储设备（计算节点）或自动传送至网络服务器（例如日志服务器），以便系统故障后，导出分析定位。相关日志需要保存的天数大于30天。

1. 数据一致性审计

系统提供数据一致性审计功能，定时审计VM及其卷文件的相关数据和状态的一致性。当发现有异常的时候，会自动记录下来，以便维护人员做相应的判断和恢复措施，从而保证了系统内部各种相互关联的数据的一致性。

1. 告警与在线维护

全面监控硬件及软件异常：模板化、可定制；实时告警转发：邮件、SNMP、REST。

维护模式灵活多样：在线软硬件升级。

* 1. 网络传输性能要求

“集群注册运营管理平台”管理范围广、信息种类数量多，需要高速稳定的通信网络保障数据的良好传输能力。具体要求如下：

1. 远程终端用户与服务器有线连接带宽不小于10Mbps；
2. 系统网络链路核心带宽不低于1000Mbps；
3. 本地用户接入网络带宽不低于100Mbps；
4. 移动无线网络采用无线网络接入，保证移动终端数据传输速度大于20KB/S。
5. 监控中心互联网通讯网络带宽不低于10M独享。
6. 平台软件具有万兆带宽的吞吐率等能力以确保未来业务的扩展性及高并发时刻的用户体验。
   1. 标准化与规范化原则

标准化工作的目的是将智慧化城市管理信息系统中的各类信息进行有序整合，使之服从于统一的标准和规则，实现系统建设和未来扩展有章可循。标准和规范体系也是“数字”建设共享行政信息的一个重要基础。

出台标准体系建设的总体思路为：在参照国内外行业标准、规范及研究成果基础上，深入调研实际需求和项目本身特点，广泛征求专家、学者以及实际工作人员的意见和建议，通过反复讨论、修改完善形成科学、实用的工商税务一站式注册的标准体系。

# 关键技术

* 1. \*人脸核身技术

人脸核身技术是根据移动端或者电脑端获取用户的实时图像采集人脸部位，并核对权威机构如：国证通、公安部居民资料库、银行系统等多个系统确认办理业务人员是否为真实人员的现代身份识别技术。人脸核身技术有如下几大优势。

* 权威数据源

对接权威数据库，信息更新及时，精准高效响应，同时提供数据安全防护体系，保障数据交互稳定安全。

* 服务安全稳定

提供企业级稳定、精确的大流量服务。支持毫秒级的识别响应能力、弹性灵活的高并发承载及99.99%的可靠性保障。

* 算法领先

基于我司专业的深度学习算法和海量数据训练，深度学习能力领先。

* 完整的配套服务

灵活组合身份证识别、图片质量检测、活体检测、人脸对比等服务，提供人脸核身完整解决方案，可基于场景特点自由配置功能。

* 1. \*公安部信息身份认证

通过用户人像核身，抓取多张实时人像照片，调取公安部接口对比照片与身份证照片的相识度。确定是否本人申请业务。数据采用加密方式传输。借助互联网现代技术，以身份证数据为基础，通过国家“互联网+可信身份认证平台”签发与实体身份证芯片唯一对应的电子映射文件。可以随时随地证明“我就是我”。

* 1. \*银行卡认证

银行卡认证，是对银行卡用户资料真实性进行的验证审核，以便建立完善可靠的互联网信用基础。快速查询姓名与银行卡、身份证、手机号是否一致，实时联网银联数据，准确率99.99%；银行卡验证是由： 银行卡号【姓名+身份证号码+银行预留手机号码】组成的验证和鉴权服务。多种鉴权方式。如

银行卡二要素验证： 银行卡 + (姓名、身份证号码、手机号码) 任选其一。

银行卡三要素验证： 银行卡 + (姓名、身份证号码、手机号码) 任选其二。

银行卡四要素验证： 银行卡、姓名、身份证号码、手机号码。

* 1. 权威认证电子签章与电子合同技术

通过整合IoT、移动互联等技术给传统印章加上“智能锁”，成为内含传统印章的可携带智能印章控制仪，实现对印章使用前审批、使用中受控、使用后可追溯，从而帮助企业有效把控用印风险。同时印控仪方案也与电子印章无缝融合，对外提供相应能力服务。

提供基于AI技术的智能合同管理服务。不仅赋能接入企业合同管理能力，而且帮助接入企业进行合同范本、分类管控、智能审阅、合同风控、合同履约、合同分析统计等功能。

契约锁-合同电子签章,须获国家CA数字中心认证,安全便捷,合法有效。

* 1. 云存储技术

云存储是在云计算(cloud computing)概念上延伸和发展出来的一个新的概念，是一种新兴的网络存储技术，是指通过集群应用、网络技术或分布式文件系统等功能，将网络中大量各种不同类型的存储设备通过应用软件集合起来协同工作，共同对外提供数据存储和业务访问功能的系统。

云存储的概念与云计算类似，它是指通过集群应用、网格技术或分布式文件系统等功能，网络中大量各种不同类型的存储设备通过应用软件集合起来协同工作，共同对外提供数据存储和业务访问功能的一个系统，保证数据的安全性，并节约存储空间。简单来说，云存储就是将储存资源放到云上供人存取的一种新兴方案。使用者可以在任何时间、任何地方，透过任何可连网的装置连接到云上方便地存取数据。

当云计算系统运算和处理的核心是大量数据的存储和管理时，云计算系统中就需要配置大量的存储设备，那么云计算系统就转变成为一个云存储系统，所以云存储是一个以数据存储和管理为核心的云计算系统。简单来说，云存储就是将储存资源放到云上供人存取的一种新兴方案。使用者可以在任何时间、任何地方，透过任何可连网的装置连接到云上方便地存取数据。

* 1. 微服务

微服务架构是一项在云中部署应用和服务的新技术。大部分围绕微服务的争论都集中在容器或其他技术是否能很好的实施微服务，而红帽说API应该是重点。

微服务可以在“自己的程序”中运行，并通过“轻量级设备与HTTP型API进行沟通”。关键在于该服务可以在自己的程序中运行。通过这一点我们就可以将服务公开与微服务架构（在现有系统中分布一个API）区分开来。在服务公开中，许多服务都可以被内部独立进程所限制。如果其中任何一个服务需要增加某种功能，那么就必须缩小进程范围。在微服务架构中，只需要在特定的某种服务中增加所需功能，而不影响整体进程。在分散的组件中使用微服务云架构和平台，使部署、管理和服务功能交付变得更加简单。

平台系统要提供一套基础的架构，这种架构使得微服务可以独立的部署、运行、升级，不仅如此，这个系统架构还让微服务与微服务之间在结构上“松耦合”，而在功能上则表现为一个统一的整体。这种所谓的“统一的整体”表现出来的是统一风格的界面，统一的权限管理，统一的安全策略，统一的上线过程，统一的日志和审计方法，统一的调度方式，统一的访问入口等等。微服务的目的是有效的拆分应用，实现敏捷开发和部署 。

微服务提倡的理念团队间应该是 inter-operate, not integrate 。inter-operate是定义好系统的边界和接口，在一个团队内全栈，让团队自治，原因就是因为如果团队按照这样的方式组建，将沟通的成本维持在系统内部，每个子系统就会更加内聚，彼此的依赖耦合能变弱，跨系统的沟通成本也就能降低。

设计须采用以下原则：

（1）单一职责原则

每个微服务只需要实现自己的业务逻辑，比如订单管理模块，它只需要处理订单的业务逻辑就可以，其它的不必考虑。

（2）服务自治原则

每个微服务从开发、测试、运维等都是独立的，包括存储的数据库也都是独立的，自己就有一套完整的流程，我们完全可以把它当成一个项目来对待。不必依赖于其它模块。

（3）轻量级通信原则

首先是通信的语言非常的轻量，第二，该通信方式需要是跨语言、跨平台的，可以不受技术的钳制。

（4）接口明确原则

由于微服务之间可能存在着调用关系，为了尽量避免以后由于某个微服务的接口变化而导致其它微服务都做调整，在设计之初就要考虑到所有情况，让接口尽量做的更通用，更灵活，从而尽量避免其它模块也做调整。

## \*AI动态基线建立技术

系统基于历史大量数据通过AI机器学习算法，创建动态基线预测的范围。与实际网络产生的数据对比，对于超出范围内的异常数据识别。

动态基线主要用于对某一指标未来变化趋势的预测，是基于历史大量数据通过AI机器学习算法所得，是系统判定指标是否异常的标准之一。动态基线不是一条固定不变的基准线，而是一条会根据各时间点指标（比如网络流量）不断变化的基准线。

基于动态基线预测的范围与实际平台产生的数据对比，对于超出范围内的数据时刻，初步判定为网络的异常事件。

动态基线当前采用高斯回归作为异常事件的预测算法。

* 1. 分布式对象技术

分布式对象技术涵盖的主流技术包括COM／DCOM／．NET组件技术、Java技术、CORBA技术、数据库技术这四种技术。Java技术是一种可以撰写扩平台应用软件的面向对象程序设计语言，具有卓越的通用性、高效性、平台一致性和安全性，它对于移动APP的开发具有显著的作用，可兼容各种网络设备，通过该技术组件网络管理子系统，先在每台设备上构筑信息通道，保证数据传输，并由该系统实现与上层软件的信息交互和NAP功能，同时可在该子系统配置标准的应用程序接口，实现用户自定义程序与上层软件的信息交互。数据库技术，是当中比较核心的技术，系统对信息采集的实时性要求高，DRTDBS(分布式实时数据库)可满足要求，商业数据库可对历史数据进行保存，通过建立起RTDB，形成数据处理的子系统。这些技术的实质在于构建出数据中心的硬件基础，然后向云计算转型。通过虚拟化服务器、网络虚拟化、软件定义的存储、混合，负载均衡技术，全对称分布式架构等技术，架构软件定义数据中心，目的是解决大数据分析。

* 1. 接入技术

有线无线统一接入，提供企业，访客人员，管理员，以及哑终端的统一接入与管理提供全流程的访客自助服务。

支持802.1X，Portal，MAC，SACG等多种认证方式 支持PAP，CHAP、EAP-MD5，EAP-PEAP-MSCHAPV2，EAP-TLS，EAP-TTLS-PAP，EAP-PEAP-GTC等多种身份验证协 议，支持匿名认证，账号认证，证书认证，AD/LDAP联动认证，第三方数据库联动认证，Radius中继等多种认证方式 支持双因子认证、社交媒体联动认证（微信/QQ/新浪微博/Facebook/Twitter/Google+）

支持逃生机制，当AD/LDAP服务器宕机时用户直接认证通过 支持基于用户组，帐号，角色，SSID，时间段，终端IP地址，终端设备组，接入设备组等多种条件进行授权 支持动态ACL，静态ACL，VLAN，设备用户组，安全组等多种授权方式 支持对网络管理员访问设备进行身份校验及对配置命令行进行细粒度授权。

* 1. 接口技术

开放合作： 开放架构，提供API对接应用，使能行业数字化。北向提供标准RESTful API 。

* 1. 运维保障技术

提供权限，QoS，带宽，应用，安全策略的统一管理。基于场景感知（用户、时间、地点、终端类型、接入方式）的身份认证与授权。自动下发终端配置与证书（Boarding），简化用户接入方式，提升效率。采用 Streaming Telemetry 技术准实时采集设备数据，基于机器学习算法进行特征分析和基线运算，能够自动识别故障，并通过丰富的图形化界面对分析结果进行呈现。

利用云计算、SDN、大数据分析等技术手段，提升自动化管理能力，提供平台的自动化部署，融合管理等创新方案，帮助企业降低运维成本，让管理更便捷，让运维更智能。

采用SDN技术，用Overlay虚拟网络实现网络隔离：理论上支持16M的二层隔离网络。在一张物理网上部署多个逻辑组网VN，多网融合，一网多用，实现便捷的，扩展的网络隔离。

自动化部署、运维简单：提供VXLAN虚拟网络的自动化配置能力。只需要配置及运维NVE设备，中间透传设备只需要支持三层透传即可；全网物理/逻辑拓扑可视化，网络配置运维更简单。

弹性智能，按需创建：分布式VXLAN网关，减轻了单网关对全网设备表项学习的压力，且更易于扩展；基于B Underlay协议，支持VXLAN网络按需创建，灵活高效。管理员可以更加方便高效的管理运维本平台。

智简运维，物理网络可视。物理/逻辑拓扑呈现，全网业务可视化；基于拓扑的可视化运维。

* 1. 系统安全策略

由于信息数据具有较高的保密性和重要性，因此系统的安全性特别是数据的安全性对云平台建设至关重要。云平台建设是一项复杂的系统工程，它的实现不仅是一个单纯的技术问题，而且还需要法律、管理、社会因素的配合。因此该项目的安全模型是一个层次结构。如图所示。

|  |
| --- |
| 数据安全 |
| 软件系统安全措施 |
| 网络通信安全措施 |
| 硬件系统安全措施 |
| 物理实体安全措施 |
| 管理细则 保护措施 |
| 法律、规范、道德、纪律 |

安全层次模型

从图中可以看出各层之间的相互依赖，下层向上层提供支持，上层依赖下层的完善，最终实现数据信息的安全。

### 法律制度与道德规范

技术的进步，一方面导致工作方法和手段的改变，从而提高工作效率，另一方面也导致了新类型的犯罪。全社会都应加强相应的法律制度与道德规范的建设、宣传和教育。

### 管理制度的建立与实施

安全管理制度的建立与实施，是实现《集群注册运营管理平台》项目建设安全的重要保证。它包括安全管理人员的教育培训、制度的落实、职责的检查等方面的内容。计算机信息系统建设单位的领导应把系统建设和安全管理放在同等重要的位置。

### 物理实体的安全与硬件系统的保护

计算机物理上的安全与硬件系统的保护是《集群注册运营管理平台》建设项目安全不可缺少的重要环节。计算机网络的物理安全是保护主机、网络设备及其它附件免遭地震、火灾、水灾等环境事故以及人为操作失误和各种计算机犯罪行为导致的破坏过程。正常的防范措施主要有以下几点：

对主机房及重要信息存储、收发部门进行屏蔽处理，即建设一个具有高度屏蔽的屏蔽室，用它来安装主要运行设备，以防止磁鼓、磁带与高辐射设备等的信号外泄。

对本地网、局域网传输线路传导辐射的抑制，由于电缆传输辐射信息的不可避免性，建议网络的主干部分采用光缆传输方式。

对终端设备应尽量选用低辐射产品，或在终端密集的场所采用主动式的干扰设备。

最好配置不间断电源UPS。

对机房管理人员应加强技术和素质培养。

### 网络的安全与保护

计算机网络的重要功能是资源共享和通信。网络的安全性指的是保证数据和程序等资源安全可靠，对资源进行保护以免受到破坏；保密性主要是指对某些资源或信息，需要加以保密，不允许泄露给别人。

* **网络安全管理的原则**

网络的安全对于《集群注册运营管理平台》的正常运作、管理和发展都起着至关重要的影响。整个网络的安全性，需要所有用户来共同维护。因为网络的安全性，实际上是由用户，尤其是系统管理员来决定。因此每个系统管理员和用户需要意识到网络安全的重要性，建立完善的安全策略，主动承担责任来保护自己的系统。

网络信息系统的安全管理主要基于以下三个原则。

* **多人负责原则**

每一项与安全有关的活动，都须有两人或多人在场。这些人应是系统主管领导指派的，他们忠诚可靠，能胜任此项工作；他们应该签署工作情况记录以证明安全工作己得到保障。

以下各项是与安全有关的活动：

访问控制使用证件的发放与回收；

信息处理系统使用的媒介发放与回收；

处理保密信息；

硬件和软件的维护；

系统软件的设计，实现和修改；

重要程序和数据的删除和销毁等；

* **任期有限原则**

一般来讲，任何人最好不要长期担任与安全有关的职务，以免使他认为这个职务是专有的或永久性的。为遵循任期有限原则，工作人员应不定期地循环任职，强制实行休假制度，并规定对工作人员进行轮流培训，以使任期有限制度切实可行。

* **职责分离原则**

在信息处理系统工作的人员不要打听、了解或参与与职责以外的任何与安全有关的事情，除非系统主管领导批准。

出于对安全的考虑，下面每组内的两项信息处理工作应当分开。

计算机操作与计算机编程；

机密资料的接收和传送；

安全管理和系统管理；

应用程序和系统程序的编制；

访问证件的管理与其它工作；

计算机操作与信息处理系统使用媒介的保管等。

* **安全措施的实现**

《集群注册运营管理平台》的网络安全措施主要包括：

* 网络物理安全；
* 网络通信安全；
* 局域网安全；
* 系统主机安全；
* 数据存储安全系统。
* **网络通信安全**

网络通信安全通过下述方式实现：

防火墙：内部网络如果要接入外部网络，则要采用防火墙技术，进行特定模式IP包的过滤、内部结构隐藏和地址过滤等防护，在网络和应用两个层次上提供安全保障。

路由器、交换机运行的IOS提供一致的访问控制功能。各关键接入设备和路由交换设备在通信包的转发过程中可以利用IOS操作系统的访问控制功能进行包的阻断或续传。

各权属部门接入部分采用全交换，按端口划分VLAN，VLAN之间的路由可以设置完整的安全控制机制。

通过端到端的加密技术，防止通信线路的窃听、泄漏、篡改和破坏。

实时对进出内部网络的信息进行内容审计。

* **局域网安全**

在局域网中，交换机所提供的VLAN（虚拟网）技术及路由器的防火墙功能对整个网络进行管理和控制。通过VLAN的划分，可根据需要在不同部门、不同的应用系统之间进行隔离。

高性能的局域网交换机都具有MAC地址过滤功能，出于每个网卡的MAC地址是唯一的，因此可根据需要对交换机的每个端口进行定义，只允许特定的MAC地址的工作站通过特定的端口进行访问。由于MAC的地址是不可改变，因此相对于IP地址的过滤来说MAC地址过滤具有更高的安全性。

* **系统主机安全**

系统主机安全主要通过网络操作系统和双机容错、备份技术来实现。为了提高系统的安全性、可用性，不至于在一台服务器发生故障时，使整个系统服务停止。利用双机容错技术，当其中任一服务器发生硬软故障，另一台服务器会自动承担该服务器所做的服务，不致于使系统服务停止。作到7 x 24小时不间断运行。

* **防止入侵策略**

网络与Intenet相连，基于Web服务器的HTTP、FTP、其他独立于常规通道的Web协议和E-mail服务器的SNMP协议，通过Intemet实现信息的实时发布及其他信息的发布、各部门各种表格填报、有关消息的自动传递和邮件服务等功能。这样，入侵者就可以利用它们透过或避开防火墙进行网络侵入。为了加强系统的安全策略，因此建议在区域共享中心采用防火墙的同时还需选用网络入侵防护设备。它通过加密、身份验证、入侵检测、防护策略等技术来提升网络安全的等级。入侵防护设备包含多种功能：

* 加解密
* 身份验证
* 入侵保护
* 风险评估
* 全局VPN
* 防火墙保护

### 应用系统的安全措施

#### 应用平台

应用平台：应用平台指建立在网络系统之上的应用软件服务，数据库服务器、中间件服务器、Web服务器等，由于应用平台的系统非常复杂，通常采用多种技术(如SSL等)来增强应用平台的安全性；

#### 应用系统

应用系统：应用系统完成网络系统的最终目的——为用户服务。应用系统的安全与系统设计和实现关系密切。应用系统通过应用平台（数据库服务器、应用服务器、Web服务器等）的安全服务来保证基本安全，如：通信内容安全、通信双方的认证、审计等。

### 相关法律问题

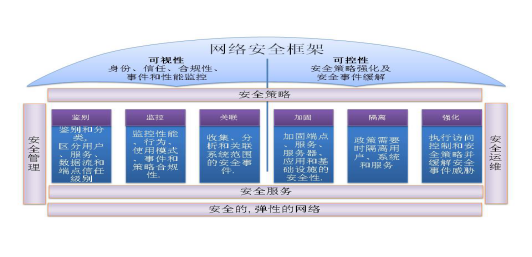
根据《关于加强涉密信息数据应用安全监管的通知》，分别对基础数据和涉密数据的管理做出相应规定。

本项目通过建设专网，采用数据切片缓存、数据加密等技术，保障数据安全性，有效的防止数据泄密和丢失的隐患存在。

* 1. 网络安全策略

### 数据中心安全域

安全域划分目标是通过对系统进行分区域划分和防护，构建起有效的纵深防护体系，有效抵御潜在威胁，降低风险，保证系统的顺畅运行，保证业务服务的持续、有效。



从IT的角度看，系统支撑或提供的业务服务表现为一系列相互关联的业务数据流程，保障业务的安全就是要保障这一系列业务数据流的安全。因此，要求全面、细致、深入了解各种业务服务所对应的业务数据流程集合以及相关的管理、控制数据流程，紧紧抓住数据流程这根主线，识别贯穿整个数据流程的关键数据处理活动，全面、细致的刻画业务服务的实现细节。通过对数据流、数据处理活动的深入、系统分析，并综合考虑其IT组成要素的实际情况，分析来自业务、IT风 险、合规等方面的安全需求，将具有相同或近似安全保护需求的IT要素归并到一个安全域中，沿着数据流程构建起纵深的防护体系，同时，对不相关的数据流进行有效的隔离。安全域的划分、防护应围绕业务服务展开，并以是否有效保障了业务的安全、稳定、顺畅运行为最终评判标准。以业务为中心，要求全面了解系统支撑或提供的各种业务服务，分析各种业务服务对机密性、完整性、可用性、可控性、真实性、抗否认、可稽核性、合规性等等各方面的要求，确定系统的安全保护等级和保护要求。

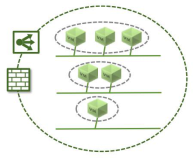
### 虚拟化网络安全防护

类别之间和类别内部的工作流通过分布式虚拟防火墙技术实现保护、日志和策略执行。虚拟化提供了构建PCI-DSS标准的信任域的关键能力。当一个新的应用需求出现的时候，不再需要物理的防火墙来对其进行安全管控和部署。虚拟防火墙可以将新规则部署到现有的新的虚拟机上，很快就能上线生产。在集中式的部署模式中，管理员可以动态的通过API进行部署。

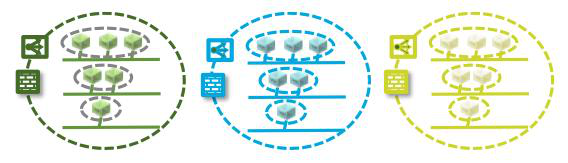


### 逻辑分层

下图的逻辑应用拓扑是一个3层架构，有三个应用层次，有逻辑的交换机、路由器、分布式的防火墙和负载均衡。



如果管理员查看虚拟机的物理位置，会发现同一个类别的虚拟机可能位于不同的主机中。



通过简单的重构这些网络可以使得划分网络非常简单，并且可以提供很强的网络控制和安全策略。可以使用现有的架构实现所需的安全隔离。在新的应用上线的时候，例如开发、生产等，这种技术可以能够在快速的交付时间里提供x86计算资源和网络资源。

* 1. 虚拟化服务器安全防护

为提升集群注册运营管理平台业务服务器安全等级，采用如下两种方式进行防护：

1. 构建标准化模版构建虚拟化服务器

在全面采用云计算平台后，所有业务系统部署均通过预定义模版进行部署，针对虚拟服务器模版采用标准安全加固配置，包括补丁更新、管理员帐户隐藏和密码安全规则等内容。

逐步形成集群注册运营管理平台服务器规范标准，并以此作为第一道安全防线。

1. 构建软件防火墙

通过在虚拟机上部署软件防火墙,提供同用户相同VLAN下VM间的访问控制。可基于业务需求和访问流量动态扩展资源。同时在软件防火墙内还可以以一虚多的方式进一步虚拟出多个轻量级的用户防火墙,满足扩容需求。

1. 主机入侵检测防护

通过在云主机里部署安全检测客户端,配合云平台的入侵防控中心,提供可视化的入侵痕迹检测。同时,支持安全扫描发现云服务器系统弱点和网页后门,降低被入侵的风险,能够实现暴力破解防御、异地登陆提醒、弱口令检测、网页后门文件检测等诸多安全防护功能。

1. 构建基于虚拟化平台的防病毒系统



利用安全厂商与虚拟化平台的融合安全防护方案，构建适合虚拟化平台的防病毒系统，实现Agent-less病毒防护，即虚拟机无需部署任何防病毒软件，开机即可获得安全防护，以此作为第二道安全防线。

* 1. 数据存储、容灾与备份

### 数据存储

1.数据的安全性和系统的高可靠性

2.系统的高性能

3.系统的可扩展性/可扩充性

4.系统的多平台支持能力。须支持国产化平台

作为集中存储的基本要求，存储系统必须能够同时连接不同的服务器平台，以满足数据集中的需要。

5.灵活性和系统管理的简单性

6.数据共享要求

7. 具有万兆带宽的吞吐率等能力以确保未来业务的扩展性及高并发时刻的用户体验

8. 确保业务不中断—从存储IO看来，没有超过1秒以上的IO中断

### 数据备份与容灾

1.根据数据的重要性以及需求恢复的速度和程度，来设计选择并实现灾难恢复计划：

(1) 备份/恢复的范围；

(2) 灾难恢复计划的状态；

(3) 应用结点与备份结点之间的距离；

(4) 应用服务器与备份备用服务器之间是如何相互连接的；

(5) 数据是怎样在两个服务器之间传送的；

(6) 允许有多少数据被丢失；

(7) 怎样保证更新的数据在备份服务器被更新；

(8) 备份服务器可以开始备份的能力。

(9) 容灾备份方案建议

(10) \*支持异地容灾

2.按系统应用和数据的关键性以及恢复操作的速度等将数据分为：

(1) 关键性的数据

主要包括：用于重要业务程序中的数据、法律要求保存的数据等。

(2) 赖以生存的数据

主要包括：用于正常业务程序并耗费政府很大的资源的数据、灾难恢复时不会马上需要的数据、牵涉业务部门的业务机密的数据等。

(3) 敏感的数据

主要包括：用于正常业务程序但丢失时可以从别处恢复的数据、比较容易重新建立起来的数据等。

(4) 非关键性的数据

主要包括：花费很少就可以重新建立起来的数据、安全系数要求不高的数据等。

# 数据库建设与数据整合入库

* 1. 概述

平台数据库建设在数据交换与集成共享平台基础上，借助数据仓库技术，来实现基础信息、业务信息、分析结论等数据的获取、汇总、存储、访问优化、转发调度、回放、分析、展现、监控、负载均衡、安全控制、备份、交换等应用管理。

* 1. 数据架构



数据库平台为集群注册运营管理平台的基础数据平台，用于统一组织、存储和管理有关业务的全部工作数据，从底层实现应急基础数据和业务数据的共享。数据库应符合本项目建设总体要求，建立一套符合开发范式的数据库结构。采用Web Service数据访问技术、数据加工分析技术、数据仓库技术等整合管理各项业务数据，并通过对数据的整理、加工、挖掘、分析，提取综合、有效的数据结果，为数据的发布提供支撑，为税务和工商业务管理决策提供数据支持。

* 1. 数据库建设内容

数据库管理系统的主要功能包括建库管理、数据输入、数据查询输出、数据维护管理、代码维护、数据库安全管理、数据库备份恢复、数据库外部接口等，是数据更新、数据库建立和维护的主要工具，也是在系统运行过程中进行原始数据处理和查询的主要手段，数据库的外部数据接口可根据应用需求情况完成。

### 业务数据库

业务系统在建设过程中均遵循税务和工商大数据中心标准规范体系，采用数据复制服务将业务数据库数据全量复制到数据中心ODS区。业务数据库中用到的基础数据库部分内容，直接从基础数据库部分复制，使用过程中采用同步机制进行更新。其他由具体业务应用根据情况自行建设。

### 操作数据存储区数据库

操作数据存储区数据库主要是将异构数据库进行基础转换，然后对业务数据库进行全量复制。具体情况需根据业务系统数据库实际情况进行建设。

* 1. 数据仓库设计

### 明细数据区

明细数据区主要存放的是操作数据存储区中的数据经过清洗，将不同业务系统中，同类数据、不同描述的数据进行归一化处理，形成标准一条数据。明细数据包括基础数据和详细数据。

### 主题数据区

主题数据区是若干主题数据库的集合，是以数据仓库明细数据为唯一数据源、面向特定分析应用、按一定方式重新组织的数据集合，是数据仓库的子集。

* 1. 数据字典设计

通过建立统一的数据编码体系，实现标准化规范化的数据管理，规范前端等应用系统建设，并为数据共享交换提供基础。在建立中心数据库过程中，本系统性能设计：

1．稳定性、2.可靠性、3.容错和自适应性能、4.易于维护性、5.安全性、6.方便扩展性、7.易用性、8.兼容性。