数据安全课程-v2.0

前导章节 数据安全法及数据安全事件

1.《数据安全法》

中华人民共和国数据安全法

（2021年6月10日第十三届全国人民代表大会常务委员会第二十九次会议通过）

目录

第一章 总则

第一条 为了规范数据处理活动，保障数据安全，促进数据开发利用，保护个人、组织的合法权益，维护国家主权、安全和发展利益，制定本法。

第二条 在中华人民共和国境内开展数据处理活动及其安全监管，适用本法。

在中华人民共和国境外开展数据处理活动，损害中华人民共和国国家安全、公共利益或者公民、组织合法权益的，依法追究法律责任。

第三条 本法所称数据，是指任何以电子或者其他方式对信息的记录。

数据处理，包括数据的收集、存储、使用、加工、传输、提供、公开等。

数据安全，是指通过采取必要措施，确保数据处于有效保护和合法利用的状态，以及具备保障持续安全状态的能力。

第四条 维护数据安全，应当坚持总体国家安全观，建立健全数据安全治理体系，提高数据安全保障能力。

第五条 中央国家安全领导机构负责国家数据安全工作的决策和议事协调，研究制定、指导实施国家数据安全战略和有关重大方针政策，统筹协调国家数据安全的重大事项和重要工作，建立国家数据安全工作协调机制。

第六条 各地区、各部门对本地区、本部门工作中收集和产生的数据及数据安全负责。

工业、电信、交通、金融、自然资源、卫生健康、教育、科技等主管部门承担本行业、本领域数据安全监管职责。

公安机关、国家安全机关等依照本法和有关法律、行政法规的规定，在各自职责范围内承担数据安全监管职责。

国家网信部门依照本法和有关法律、行政法规的规定，负责统筹协调网络数据安全和相关监管工作。

第七条 国家保护个人、组织与数据有关的权益，鼓励数据依法合理有效利用，保障数据依法有序自由流动，促进以数据为关键要素的数字经济发展。

第八条 开展数据处理活动，应当遵守法律、法规，尊重社会公德和伦理，遵守商业道德和职业道德，诚实守信，履行数据安全保护义务，承担社会责任，不得危害国家安全、公共利益，不得损害个人、组织的合法权益。

第九条 国家支持开展数据安全知识宣传普及，提高全社会的数据安全保护意识和水平，推动有关部门、行业组织、科研机构、企业、个人等共同参与数据安全保护工作，形成全社会共同维护数据安全和促进发展的良好环境。

第十条 相关行业组织按照章程，依法制定数据安全行为规范和团体标准，加强行业自律，指导会员加强数据安全保护，提高数据安全保护水平，促进行业健康发展。

第十一条 国家积极开展数据安全治理、数据开发利用等领域的国际交流与合作，参与数据安全相关国际规则和标准的制定，促进数据跨境安全、自由流动。

第十二条 任何个人、组织都有权对违反本法规定的行为向有关主管部门投诉、举报。收到投诉、举报的部门应当及时依法处理。

有关主管部门应当对投诉、举报人的相关信息予以保密，保护投诉、举报人的合法权益。

第二章 数据安全与发展

第十三条 国家统筹发展和安全，坚持以数据开发利用和产业发展促进数据安全，以数据安全保障数据开发利用和产业发展。

第十四条 国家实施大数据战略，推进数据基础设施建设，鼓励和支持数据在各行业、各领域的创新应用。

省级以上人民政府应当将数字经济发展纳入本级国民经济和社会发展规划，并根据需要制定数字经济发展规划。

第十五条 国家支持开发利用数据提升公共服务的智能化水平。提供智能化公共服务，应当充分考虑老年人、残疾人的需求，避免对老年人、残疾人的日常生活造成障碍。

第十六条 国家支持数据开发利用和数据安全技术研究，鼓励数据开发利用和数据安全等领域的技术推广和商业创新，培育、发展数据开发利用和数据安全产品、产业体系。

第十七条 国家推进数据开发利用技术和数据安全标准体系建设。国务院标准化行政主管部门和国务院有关部门根据各自的职责，组织制定并适时修订有关数据开发利用技术、产品和数据安全相关标准。国家支持企业、社会团体和教育、科研机构等参与标准制定。

第十八条 国家促进数据安全检测评估、认证等服务的发展，支持数据安全检测评估、认证等专业机构依法开展服务活动。

国家支持有关部门、行业组织、企业、教育和科研机构、有关专业机构等在数据安全风险评估、防范、处置等方面开展协作。

第十九条 国家建立健全数据交易管理制度，规范数据交易行为，培育数据交易市场。

第二十条 国家支持教育、科研机构和企业等开展数据开发利用技术和数据安全相关教育和培训，采取多种方式培养数据开发利用技术和数据安全专业人才，促进人才交流。

第三章 数据安全制度

第二十一条 国家建立数据分类分级保护制度，根据数据在经济社会发展中的重要程度，以及一旦遭到篡改、破坏、泄露或者非法获取、非法利用，对国家安全、公共利益或者个人、组织合法权益造成的危害程度，对数据实行分类分级保护。国家数据安全工作协调机制统筹协调有关部门制定重要数据目录，加强对重要数据的保护。

关系国家安全、国民经济命脉、重要民生、重大公共利益等数据属于国家核心数据，实行更加严格的管理制度。

各地区、各部门应当按照数据分类分级保护制度，确定本地区、本部门以及相关行业、领域的重要数据具体目录，对列入目录的数据进行重点保护。

第二十二条 国家建立集中统一、高效权威的数据安全风险评估、报告、信息共享、监测预警机制。国家数据安全工作协调机制统筹协调有关部门加强数据安全风险信息的获取、分析、研判、预警工作。

第二十三条 国家建立数据安全应急处置机制。发生数据安全事件，有关主管部门应当依法启动应急预案，采取相应的应急处置措施，防止危害扩大，消除安全隐患，并及时向社会发布与公众有关的警示信息。

第二十四条 国家建立数据安全审查制度，对影响或者可能影响国家安全的数据处理活动进行国家安全审查。

依法作出的安全审查决定为最终决定。

第二十五条 国家对与维护国家安全和利益、履行国际义务相关的属于管制物项的数据依法实施出口管制。

第二十六条 任何国家或者地区在与数据和数据开发利用技术等有关的投资、贸易等方面对中华人民共和国采取歧视性的禁止、限制或者其他类似措施的，中华人民共和国可以根据实际情况对该国家或者地区对等采取措施。

第四章 数据安全保护义务

第二十七条 开展数据处理活动应当依照法律、法规的规定，建立健全全流程数据安全管理制度，组织开展数据安全教育培训，采取相应的技术措施和其他必要措施，保障数据安全。利用互联网等信息网络开展数据处理活动，应当在网络安全等级保护制度的基础上，履行上述数据安全保护义务。

重要数据的处理者应当明确数据安全负责人和管理机构，落实数据安全保护责任。

第二十八条 开展数据处理活动以及研究开发数据新技术，应当有利于促进经济社会发展，增进人民福祉，符合社会公德和伦理。

第二十九条 开展数据处理活动应当加强风险监测，发现数据安全缺陷、漏洞等风险时，应当立即采取补救措施；发生数据安全事件时，应当立即采取处置措施，按照规定及时告知用户并向有关主管部门报告。

第三十条 重要数据的处理者应当按照规定对其数据处理活动定期开展风险评估，并向有关主管部门报送风险评估报告。

风险评估报告应当包括处理的重要数据的种类、数量，开展数据处理活动的情况，面临的数据安全风险及其应对措施等。

第三十一条 关键信息基础设施的运营者在中华人民共和国境内运营中收集和产生的重要数据的出境安全管理，适用《中华人民共和国网络安全法》的规定；其他数据处理者在中华人民共和国境内运营中收集和产生的重要数据的出境安全管理办法，由国家网信部门会同国务院有关部门制定。

第三十二条 任何组织、个人收集数据，应当采取合法、正当的方式，不得窃取或者以其他非法方式获取数据。

法律、行政法规对收集、使用数据的目的、范围有规定的，应当在法律、行政法规规定的目的和范围内收集、使用数据。

第三十三条 从事数据交易中介服务的机构提供服务，应当要求数据提供方说明数据来源，审核交易双方的身份，并留存审核、交易记录。

第三十四条 法律、行政法规规定提供数据处理相关服务应当取得行政许可的，服务提供者应当依法取得许可。

第三十五条 公安机关、国家安全机关因依法维护国家安全或者侦查犯罪的需要调取数据，应当按照国家有关规定，经过严格的批准手续，依法进行，有关组织、个人应当予以配合。

第三十六条 中华人民共和国主管机关根据有关法律和中华人民共和国缔结或者参加的国际条约、协定，或者按照平等互惠原则，处理外国司法或者执法机构关于提供数据的请求。非经中华人民共和国主管机关批准，境内的组织、个人不得向外国司法或者执法机构提供存储于中华人民共和国境内的数据。

第五章 政务数据安全与开放

第三十七条 国家大力推进电子政务建设，提高政务数据的科学性、准确性、时效性，提升运用数据服务经济社会发展的能力。

第三十八条 国家机关为履行法定职责的需要收集、使用数据，应当在其履行法定职责的范围内依照法律、行政法规规定的条件和程序进行；对在履行职责中知悉的个人隐私、个人信息、商业秘密、保密商务信息等数据应当依法予以保密，不得泄露或者非法向他人提供。

第三十九条 国家机关应当依照法律、行政法规的规定，建立健全数据安全管理制度，落实数据安全保护责任，保障政务数据安全。

第四十条 国家机关委托他人建设、维护电子政务系统，存储、加工政务数据，应当经过严格的批准程序，并应当监督受托方履行相应的数据安全保护义务。受托方应当依照法律、法规的规定和合同约定履行数据安全保护义务，不得擅自留存、使用、泄露或者向他人提供政务数据。

第四十一条 国家机关应当遵循公正、公平、便民的原则，按照规定及时、准确地公开政务数据。依法不予公开的除外。

第四十二条 国家制定政务数据开放目录，构建统一规范、互联互通、安全可控的政务数据开放平台，推动政务数据开放利用。

第四十三条 法律、法规授权的具有管理公共事务职能的组织为履行法定职责开展数据处理活动，适用本章规定。

第六章 法律责任

第四十四条 有关主管部门在履行数据安全监管职责中，发现数据处理活动存在较大安全风险的，可以按照规定的权限和程序对有关组织、个人进行约谈，并要求有关组织、个人采取措施进行整改，消除隐患。

第四十五条 开展数据处理活动的组织、个人不履行本法第二十七条、第二十九条、第三十条规定的数据安全保护义务的，由有关主管部门责令改正，给予警告，可以并处五万元以上五十万元以下罚款，对直接负责的主管人员和其他直接责任人员可以处一万元以上十万元以

下罚款；拒不改正或者造成大量数据泄露等严重后果的，处五十万元以上二百万元以下罚款，并可以责令暂停相关业务、停业整顿、吊销相关业务许可证或者吊销营业执照，对直接负责的主管人员和其他直接责任人员处五万元以上二十万元以下罚款。

违反国家核心数据管理制度，危害国家主权、安全和发展利益的，由有关主管部门处二百万元以上一千万元以下罚款，并根据情况责令暂停相关业务、停业整顿、吊销相关业务许可证或者吊销营业执照；构成犯罪的，依法追究刑事责任。

第四十六条 违反本法第三十一条规定，向境外提供重要数据的，由有关主管部门责令改正，给予警告，可以并处十万元以上一百万元以下罚款，对直接负责的主管人员和其他直接责任人员可以处一万元以上十万元以下罚款；情节严重的，处一百万元以上一千万元以下罚款，并可以责令暂停相关业务、停业整顿、吊销相关业务许可证或者吊销营业执照，对直接负责的主管人员和其他直接责任人员处十万元以上一百万元以下罚款。

第四十七条 从事数据交易中介服务的机构未履行本法第三十三条规定的义务的，由有关主管部门责令改正，没收违法所得，处违法所得一倍以上十倍以下罚款，没有违法所得或者违法所得不足十万元的，处十万元以上一百万元以下罚款，并可以责令暂停相关业务、停业整顿、吊销相关业务许可证或者吊销营业执照；对直接负责的主管人员和其他直接责任人员处一万元以上十万元以下罚款。

第四十八条 违反本法第三十五条规定，拒不配合数据调取的，由有关主管部门责令改正，给予警告，并处五万元以上五十万元以下罚款，对直接负责的主管人员和其他直接责任人员处一万元以上十万元以下罚款。

违反本法第三十六条规定，未经主管机关批准向外国司法或者执法机构提供数据的，由有关主管部门给予警告，可以并处十万元以上一百万元以下罚款，对直接负责的主管人员和其他直接责任人员可以处一万元以上十万元以下罚款；造成严重后果的，处一百万元以上五百万元以下罚款，并可以责令暂停相关业务、停业整顿、吊销相关业务许可证或者吊销营业执照，对直接负责的主管人员和其他直接责任人员处五万元以上五十万元以下罚款。

第四十九条 国家机关不履行本法规定的数据安全保护义务的，对直接负责的主管人员和其他直接责任人员依法给予处分。

第五十条 履行数据安全监管职责的国家工作人员玩忽职守、滥用职权、徇私舞弊的，依法给予处分。

第五十一条 窃取或者以其他非法方式获取数据，开展数据处理活动排除、限制竞争，或者损害个人、组织合法权益的，依照有关法律、行政法规的规定处罚。

第五十二条 违反本法规定，给他人造成损害的，依法承担民事责任。

违反本法规定，构成违反治安管理行为的，依法给予治安管理处罚；构成犯罪的，依法追究刑事责任。

第七章 附则

第五十三条 开展涉及国家秘密的数据处理活动，适用《中华人民共和国保守国家秘密法》等法律、行政法规的规定。

在统计、档案工作中开展数据处理活动，开展涉及个人信息的数据处理活动，还应当遵守有关法律、行政法规的规定。

第五十四条 军事数据安全保护的办法，由中央军事委员会依据本法另行制定。

第五十五条 本法自2021年9月1日起施行。

2. 数据安全事件--DD打车事件

2021年6月30日，滴滴正式在美国纽交所挂牌上市。7月2日晚，国家网信办官网发布公告，网络安全审查办公室宣布对滴滴出行启动网络安全审查，一时间掀起巨大争议。

网络安全审查办公室关于对“滴滴出行”启动网络安全审查的公告，*为防范国家数据安全风险，维护国家安全，保障公共利益，*依据《中华人民共和国国家安全法》《中华人民共和国网络安全法》，网络安全审查办公室按照《网络安全审查办法》，对滴滴出行实施网络安全审查。*为配合网络安全审查工作，防范风险扩大，审查期间滴滴出行停止新用户注册。*随后，滴滴回应称将积极配合。

第一章 数据与数据库

1.什么是数据?

数据是指对客观事件进行记录并可以鉴别的符号，是对客观事物的性质、状态以及相互关系等进行记载的物理符号或这些物理符号的组合。它是可识别的、抽象的符号。

它不仅指狭义上的数字，还可以是具有一定意义的文字、字母、数字符号的组合、图形、图像、视频、音频等，也是客观事物的属性、数量、位置及其相互关系的抽象表示。例如，“0、1、2...”、“阴、雨、下降、气温”、“学生的档案记录、货物的运输情况”等都是数据。数据经过加工后就成为信息。

在计算机科学，数据是所有能输入计算机并被计算机程序处理的符号的介质的总称，是用于输入电子计算机进行处理，具有一定意义的数字、字母、符号和模拟量等的通称。计算机存储和处理的对象十分广泛，表示这些对象的数据也随之变得越来越复杂。

2.什么是数据库管理系统（DBMS）？

用来存储、管理、应用数据的软件。

4.主流数据库产品和厂商有哪些?

5.该从哪些方面保证数据库安全?

第二章 基础环境准备

1.MySQL 部署

1.1 确认支持列表：Supported Platforms

		8.0	5.7	5.6
Operating System	Architecture			
Oracle Linux / Red Hat / CentOS				
Oracle Linux 8 / Red Hat Enterprise Linux 8 / CentOS 8	x86_64, ARM 64	•		
Oracle Linux 7 / Red Hat Enterprise Linux 7 / CentOS 7	ARM 64	•		

		8.0	5.7	5.6
Oracle Linux 7 / Red Hat Enterprise Linux 7 / CentOS 7	x86_64	•	•	•
Oracle Linux 6 / Red Hat Enterprise Linux 6 / CentOS 6	x86_32, x86_64	•	•	•
Oracle Solaris				
Solaris 11 (Update 4+)	SPARC_64, x86_64	•	•	•
Solaris 10 (Update 11+)	SPARC_64, x86_32, x86_64			•
Canonical				
Ubuntu 18.04 LTS	x86_32, x86_64	•	•	
Ubuntu 16.04 LTS	x86_32, x86_64	•	•	
SUSE				
SUSE Enterprise Linux 15 / OpenSUSE 15	x86_64	•		
SUSE Enterprise Linux 12 (12.3+)	x86_64	•	•	•

		8.0	5.7	5.6
Debian				
Debian GNU/Linux 10	x86_64	•	•	
Debian GNU/Linux 9	x86_32, x86_64	•	•	•
Debian GNU/Linux 8	x86_32, x86_64		•	•
Microsoft Windows Server				
Microsoft Windows 2019 Server	x86_64	•		
Microsoft Windows 2016 Server	x86_64	•	•	•
Microsoft Windows 2012 Server R2	x86_64	•	•	•
Microsoft Windows				
Microsoft Windows 10	x86_64	•	•	
Apple				

		8.0	5.7	5.6
macOS 10.14	x86_64	•	•	
macOS 10.13	x86_64	•	•	
FreeBSD				
FreeBSD 12	x86_64	•		
Various Linux				
Generic Linux (tar format)	x86_32, x86_64, glibc 2.12, libstdc++ 4.4	•	•	•
Fedora Yum Repo	•	•	•	
Debian/Ubuntu APT Repo	•	•	•	
SUSE Repo	•	•	•	

> 官网：
>
> https://www.mysql.com/support/supportedplatforms/database.html
>
> https://www.mysql.com/support/eol-notice.html

1.2 确认版本

> 准备安装MySQL时，请确定要使用哪个版本和发行格式（二进制或源码）。

首先，决定要安装开发版本还是通用版本（GA）。开发版本具有最新功能，但不建议用于生产环境。GA版本（也称为生产版本或稳定版本）是供生产使用的。

MySQL 8.0中的命名方案使用的发行版名称由三个数字和一个可选的后缀组成（例如， **mysql-8.0.1-dmr**）。版本名称中的数字解释如下：

- 第一个数字（**8**）是主版本号。
- 第二个数字（**0**）是次要版本号。总而言之，主要和次要数字构成发行版本号。序列号描述了稳定的功能集。
- 第三个数字（**1**）是发行系列中的版本号。对于每个新的错误修正版本，此值均递增。在大多数情况下，系列中的最新版本是最佳选择。
  版本名称也可以包含一个后缀，以指示版本的稳定性。在一系列发行中，发布会通过一组后缀来指示稳定性水平如何提高。可能的后缀是：
- **dmr**指示开发里程碑版本（DMR）。MySQL开发使用里程碑模型，其中每个里程碑都引入了一小部分经过全面测试的功能。从一个里程碑到下一个里程碑，基于尝试这些正常发布的社区成员提供的反馈，功能界面可能会更改，甚至功能可能会被删除。里程碑版本中的功能可能被视为具有预生产质量。
- **rc**表示发布候选（RC）。通过了MySQL的所有内部测试后，发布候选版本被认为是稳定的。RC版本中可能仍会引入新功能，但是重点将转移到修复错误上，以稳定本系列中较早引入的功能。

> - 没有后缀表示具有一般可用性（GA）或正式版。GA版本稳定，已成功通过了较早的发行阶段，并且被认为是可靠的，没有严重的错误并且适合在生产系统中使用。

1.3 获取 MySQL软件

> https://downloads.mysql.com/archives/community/
>
> 一定要到官网下载

1.4 MD5验证软件包

```
md5sum mysql-xxx.tar.gz
aaab65abbec64d5e907dcd41b8699945  mysql-xxx.tar.gz
```

1.5 企业上线准备

1.5.1 硬件标准化

- 标准化数据库专用服务器
- 标准化服务器硬件带来的收益

1.5.2 操作系统及配置标准化

1.5.3 标准化操作系统及硬件参数

- 关闭NUMA
- 开启CPU高性能模式
- 阵列卡RAID配置
- 关闭THP
- 网卡绑定

- 存储多路径
- 系统层面参数调整

1.5.4 预装MySQL前硬件烤机压测

- stress 进行CPU、IO、MEM烤机压测
- FIO 进行定制化IO烤机压测
- sysbench进行综合压测

1.6 MySQL 8.0.x安装过程

1.6.1 安装准备

```
shell> groupadd mysql
shell> useradd  -s /bin/false mysql
shell> cd /usr/local
shell> tar xvf /path/to/mysql-VERSION-
OS.tar.xz
shell> xz -dc /path/to/mysql-VERSION-
OS.tar.xz | tar x
shell> ln -s full-path-to-mysql-VERSION-OS
mysql
shell> export PATH=$PATH:/usr/local/mysql/bin
shell> yum install libaio # install library
```

1.6.2 部署过程

```
shell> cd mysql
shell> mkdir mysql-files
shell> chown mysql:mysql mysql-files
shell> chmod 750 mysql-files
shell>bin/mysqld --initialize --user=mysql
  --basedir=/usr/local/mysql
  --datadir=/data/mysql/data_3306
shell> bin/mysql_ssl_rsa_setup
shell> bin/mysqld_safe --user=mysql &
# Next command is optional
shell> cp support-files/mysql.server
/etc/init.d/mysql.server
```

1.6.3 启动和关闭

```
shell> bin/mysqld_safe --user=mysql &
```

2.Oracle 部署

```
环境准备:

1.关闭NetworkManager

[root@db01 ~]# systemctl stop NetworkManager
[root@db01 ~]# systemctl disable
NetworkManager


2.修改网卡配置
```

```
vim /etc/sysconfig/network-scripts/ifcfg-
ens33
TYPE="Ethernet"
BOOTPROTO="static"
DEFROUTE="yes"
NAME="ens33"
DEVICE="ens33"
ONBOOT="yes"
IPADDR=100.0.0.88
NETMASK=255.255.255.0
GATEWAY=100.0.0.254
DNS1=223.5.5.5

systemctl restart network
```

3. 防火墙关闭

```
selinux :
[root@db01 ~]# getenforce
Enforcing
[root@db01 ~]# setenforce 0
[root@db01 ~]# vim /etc/selinux/config


# This file controls the state of SELinux on
the system.
# SELINUX= can take one of these three
values:
#     enforcing - SELinux security policy is
enforced.
```

```
#     permissive - SELinux prints warnings
instead of enforcing.
#     disabled - No SELinux policy is loaded.
SELINUX=disabled
# SELINUXTYPE= can take one of three values:
#     targeted - Targeted processes are
protected,
#     minimum - Modification of targeted
policy. Only selected processes are
protected.
#     mls - Multi Level Security protection.
SELINUXTYPE=targeted


iptables :
[root@db01 ~]# iptables -F
[root@db01 ~]# systemctl disable firewalld
Removed symlink /etc/systemd/system/multi-
user.target.wants/firewalld.service.
Removed symlink /etc/systemd/system/dbus-
org.fedoraproject.FirewallD1.service.
[root@db01 ~]# systemctl stop  firewalld


4. 配置本地yum源
[root@db01 ~]# cd /etc/yum.repos.d/
[root@db01 yum.repos.d]#
[root@db01 yum.repos.d]# ll
total 32
-rw-r--r--. 1 root root 1664 Nov 23  2018
CentOS-Base.repo
```

```
-rw-r--r--. 1 root root 1309 Nov 23  2018
CentOS-CR.repo
-rw-r--r--. 1 root root  649 Nov 23  2018
CentOS-Debuginfo.repo
-rw-r--r--. 1 root root  314 Nov 23  2018
CentOS-fasttrack.repo
-rw-r--r--. 1 root root  630 Nov 23  2018
CentOS-Media.repo
-rw-r--r--. 1 root root 1331 Nov 23  2018
CentOS-Sources.repo
-rw-r--r--. 1 root root 5701 Nov 23  2018
CentOS-Vault.repo
[root@db01 yum.repos.d]# mv * /tmp
[root@db01 yum.repos.d]# ll

[root@db01 yum.repos.d]# vim
/etc/yum.repos.d/rhel-source.repo
[rhel-source]
name=local-iso
baseurl=file:///mnt
enabled=1
gpgchek=0
```

挂载光盘镜像

```
[root@db01 yum.repos.d]# mount /dev/sr0 /mnt
[root@db01 yum.repos.d]# yum clean all
```

==========

1、Oracle产品介绍

1.1 Oracle版本说明

```
7:  7.3.4
8i: 8.1.7
9i: 9.2.0.8
10g:10.2.0.4 10.2.0.5
11g:11.2.0.3  11.2.0.4
12c:12.2.0.1
18c:
19c:

企业现存版本:
10g:10.2.0.4  10.2.0.5
11g:11.2.0.3  11.2.0.4
12c:12.2.0.1
18c:
19c:

1.2 Oracle工具网站
oracle.com              ---> 官网
support.oracle.com      ---> MOS
https://edelivery.oracle.com/osdc/faces/Home.
jspx --->历史版本及补丁


1.3 Oracle 软件release版本选择
10gR2   11gR2   12cR2

1.4 Oracle 补丁类型
Patch Set Release     PSR
Patch Set Update      PSU
Critical Patch Update CPU
```

2012年10月，经更名为Security Patch Update (SPU)
Interim Patch/One-Off Patc

补丁应用方法和注意事项：

以上的补丁除了psr直接使用runInstaller，其他的补丁类型都是使用opatch命令，在oracle 10g之前，我们需要单独下载此命令，到oracle 10g之后这个命令在ORACLE_HOME/Opatch下，因此，最好在环境变量path中添加以下

10.2.0.1 ----> 升级成 10.2.0.5
11.2.0.1 ----> 11.2.0.4

2. Oracle 11g安装

2.0 Oracle11g软件包介绍

database(RDBMS):
1of7
2of7

cluser软件(grid):
3of7 : 集群功能,独立的存储功能(ASM)

2.1. 检查内存，至少1G
grep MemTotal /proc/meminfo

2.2.交换分区

```
    Available RAM              Swap Space
Required
    Between 1 GB and 2 GB    1.5 times the
size of RAM
    Between 2 GB and 16 GB   Equal to the
size of RAM
    More than 16 GB          16 GB

grep "model name" /proc/cpuinfo
grep SwapTotal /proc/meminfo

free
total       used       free     shared
buffers     cached
Mem:       1035140     512924     522216
     0      51236     335880
-/+ buffers/cache:     125808     909332
Swap:      1052248          0    1052248
```

2.3. 共享内存段至少要大于MEMORY_MAX_TARGET and MEMORY_TARGET

```
df -k /dev/shm/
Filesystem           1K-blocks      Used
Available Use% Mounted on
tmpfs                  517568         0
517568   0% /dev/shm
```

2.4. 至少1G的 /tmp

```
df -h /tmp
```

2.5. 数据库软件和data磁盘空间要求

Installation Type Requirement for Software Files (GB)
Enterprise Edition 3.95
Standard Edition 3.88

Installation Type Requirement for Data Files (GB)
Enterprise Edition 1.7
Standard Edition 1.5

2.6. 操作系统版本

Operating System Requirements

The following are the operating system requirements for Oracle Database 11g Release 2 (11.2) for Linux x86:

Asianux 2.0
Asianux 3.0
Oracle Enterprise Linux 4.0 Update 7 or later
Oracle Enterprise Linux 5.0
Red Hat Enterprise Linux 4.0 Update 7 or later
Red Hat Enterprise Linux 5.0
SUSE Linux Enterprise Server 10.0
SUSE Linux Enterprise Server 11.0
For Asianux 3, Oracle Enterprise Linux 5.0, and Red Hat Enterprise Linux 5.0: 2.6.18 or later

2.7. 检查软件包

The following or later version of packages for Asianux 3, Oracle Enterprise Linux 5.0, and Red Hat Enterprise Linux 5.0 should be installed:

```
yum -y install binutils-*
yum -y install compat-libstdc++-*
yum -y install elfutils-libelf-*
yum -y install elfutils-libelf-devel-*
yum -y install elfutils-libelf-devel-static-*
yum -y install gcc-*
yum -y install gcc-c++-*
yum -y install glibc-*
yum -y install glibc-common-*
yum -y install glibc-devel-*
yum -y install glibc-headers-*
yum -y install kernel-headers-*
yum -y install ksh-*
yum -y install libaio-*
yum -y install libaio-devel-*
yum -y install libgcc-*
yum -y install libgomp-*
yum -y install libstdc++-*
yum -y install libstdc++-devel-*
yum -y install make-*
yum -y install sysstat-*
yum -y install unixODBC-*
yum -y install unixODBC-devel-*
```

```
rpm -q --qf '%{NAME}-%{VERSION}-%{RELEASE} (%
{ARCH})\n' binutils \
compat-libstdc++ \
elfutils-libelf-devel \
elfutils-libelf-devel-static \
gcc \
gcc-c++ \
glibc \
glibc-common \
glibc-devel \
glibc-headers \
kernel-headers \
ksh \
libaio \
libaio-devel \
libgcc \
libgomp \
libstdc++ \
libstdc++-devel \
make \
sysstat \
unixODBC \
unixODBC-devel \
libXp
```

2.8. 创建组和用户

```
/usr/sbin/groupadd oinstall
/usr/sbin/groupadd dba
/usr/sbin/useradd -g oinstall -G dba oracle

echo oracle | passwd --stdin oracle
```

2.9. 修改内核参数

```
vim /etc/sysctl.conf

fs.aio-max-nr = 1048576
fs.file-max = 6815744
kernel.shmall = 2097152
kernel.shmmax = 536870912
kernel.shmmni = 4096
kernel.sem = 250 32000 100 128
net.ipv4.ip_local_port_range = 9000 65500
net.core.rmem_default = 262144
net.core.rmem_max = 4194304
net.core.wmem_default = 262144
net.core.wmem_max = 1048586

sysctl -p
```

2.10. 修改系统限制

```
vim /etc/security/limits.conf
oracle           soft    nproc   2047
oracle           hard    nproc   16384
oracle           soft    nofile  1024
oracle           hard    nofile  65536
```

2.11.

```
vi /etc/pam.d/login
session    required     pam_limits.so
```

2.12. 修改profile

```
if [ $USER = "oracle" ]; then
        if [ $SHELL = "/bin/ksh" ]; then
              ulimit -p 16384
              ulimit -n 65536
        else
              ulimit -u 16384 -n 65536
        fi
fi
```

2.13. 创建目录结构

分区:

```
fdisk /dev/sda
sda5  15G     ---->/u01        ---->本地   软件程序
sda6  20G     ---->/oradata    ---->存储盘 数据存储

mkfs.ext4 /dev/sda5
mkfs.ext4 /dev/sda6
mkdir /u01  /oradata
mount /dev/sda5 /u01
mount /dev/sda6 /oradata
[root@db08 ~]# blkid
/dev/sda2: UUID="40852d80-1f81-469c-afe2-f3b84847467f" TYPE="ext4"
/dev/sda1: UUID="a484cae0-ba65-4b19-91fb-8d23bdbcd118" TYPE="ext4"
/dev/sda3: UUID="76380440-f2c6-4d7b-8343-044069196e2a" TYPE="swap"
```

```
/dev/sda5: UUID="f76191bb-a035-41a4-94c4-
2b005c468eba" TYPE="ext4"
/dev/sda6: UUID="eb9cebaf-2ca0-4467-9476-
b2d5f0cc9f0f" TYPE="ext4"
vim /etc/fstab
UUID="f76191bb-a035-41a4-94c4-2b005c468eba"
/u01 ext4 defaults 0 0
UUID="eb9cebaf-2ca0-4467-9476-b2d5f0cc9f0f"
/oradata ext4 defaults 0 0


#创建必须目录:
#ORACLE_BASE:存放各类日志
mkdir -p /u01/app/oracle
#ORACLE_HOME:存放程序的目录
mkdir -p /u01/app/oracle/product/11.2.0/db_1

#更改权限:
chown -R oracle:oinstall /u01/
chmod -R 775 /u01/
chown -R oracle:oinstall /oradata

#切换用户并更改环境变量文件
su - oracle
vim .bash_profile
export ORACLE_BASE=/u01/app/oracle
export
ORACLE_HOME=/u01/app/oracle/product/11.2.0/db
_1
export ORACLE_SID=orcl
export PATH=$ORACLE_HOME/bin:$PATH
```

```
source .bash_profile


2.14. runInstaller

2.15. netca

2.16. dbca

2.17. 基本链接使用
sqlplus / as sysdba
```

第三章 等保中MySQL 的安全保护

1.等保中对于MySQL版本的要求

准备安装MySQL时，请确定要使用哪个版本和发行格式（二进制或源码）。
首先，决定要安装开发版本还是通用版本（GA）。开发版本具有最新功能，但不建议用于生产环境。
GA版本（也称为生产版本或稳定版本）是供生产使用的。一般使用GA版本（6-12月）。大约20个小版本

2.等保要求的中的数据库升级要求

3.等保要求中对于用户、权限要求

3.1 用户及密码管理

3.1.1 用户定义

> 用户名@'白名单' 密码
>
> 用户名：由字母、数字、特殊符号组成的字符串
>
> 白名单：能够允许登录数据库的地址列表，可以是单个ip，网段，主机名，域名等。
>
> oldguo@'localhost' ----> 只能在本地登录，一般管理员用户使用
>
> oldguo@'10.0.0.55' ----> 只能此地址访问数据库，中间件中会使用
>
> oldguo@'10.0.0.0/255.255.255.0' ---> 1-254访问数据
>
> oldguo@'10.0.0.5%' ----> 50-59
>
> oldguo@'10.0.%'
>
> oldguo@'%'

3.1.2 等保中对于用户密码要求细则

1. 用户密码需要12位以上
2. 用户需要3种密码复杂度以上
3. 用户需要90天密码过期设置
4. 生产有人未经许可，索要root管理员密码需要及时上报
5. 原则上不得将root管理员用户密码告知非管理员人员
6. 禁用生产中无作用用户及已离职人员具备的用户
7. 合理设置用户白名单，最小化连接主机列表

3.1.3 操作

```
mysql> select user,host,authentication_string
from mysql.user;
mysql> alter user root@'localhost' identified
by 'Oldguo@22654481.com';
mysql> select user,host,plugin  from
mysql.user\G
mysql> alter user root@'localhost' identified
with mysql_native_password by
'Oldguo@22654481.com';
mysql> select user,host ,password_expired
from mysql.user;
mysql> create user oldguo@'10.0.0.%'
identified with mysql_native_password by
'123';
mysql> alter user oldguo@'10.0.0.%' password
expire interval 90 day;
mysql> select user,host,password_lifetime
from mysql.user;
mysql> alter user oldguo@'10.0.0.%' password
expire never;
```

3.2 等保中权限管理

3.2.1 等保中对于权限的管理

```
1. 最小化权限，专用户专用，细化权限
2. 谨慎使用ALL权限
3. 不在使用用户，及时回收权限
```

3.2.2 操作

```
mysql> create user user_test@'10.0.0.%'
identified with mysql_native_password by
'123';
mysql> show privileges;
mysql> grant select,update,delete ,insert on
test.* to user_test@'10.0.0.%';
mysql> show grants for user_test@'10.0.0.%';
mysql> revoke delete on test.* from
user_test@'10.0.0.%'
```

4.MySQL数据库的SQL安全审计

4.1 SQL种类介绍

```
DDL 数据定义语言
create
drop
```

```
alter

DCL 数据控制语言
grant
revoke

DML 数据操作语言
select
update
delete
insert
```

4.2 SQL书写规范

```
参考阿里巴巴SQL规范。
```

4.3 SQL安全审核平台--Yearning

4.3.0 功能介绍

- SQL 查询
  - 查询工单
  - 导出
  - 自动补全，智能提示
  - 查询语句审计
  - 查询结果脱敏
- SQL 审核

    - 流程化工单
    - SQL语句语法检测
    - 根据规则检测SQL语句合规性
    - 自动生成DDL/DML回滚语句
    - 历史审核记录
- 推送
    - E-mail 工单推送
    - 钉钉 webhook 机器人工单推送
- 用户权限及管理
    - 角色划分
    - 基于用户的细粒度权限
    - 注册
- 其他
    - todoList
    - LDAP 登录
    - 动态审核规则配置
    - 自定义审核层级
- AutoTask 自动执行

4.3.1 Yearning工具部署

```
# 下载地址
https://github.com/cookieY/Yearning/releases/tag/2.3.5

1. 配置文件设计
# vim conf.toml
[Mysql]
Db = "Yearning"
```

```
Host = "10.0.0.51"
Port = "3306"
Password = "Test123"
User = "root"

[General]
SecretKey = "dbcjqheupqjsuwsm"
Hours = 4



2. 初始化及安装
./Yearning install

3. 启动服务
./Yearning run --push "10.0.0.60" --port
"8000"

4. 登录
默认账号/密码：admin/Yearning_admin
```

4.3.1 工具使用

```
请参照视频操作流程。
```

5.数据安全保护-MySQL数据备份恢复

5.0 数据损坏场景

物理损坏：主机硬件损坏，服务器宕机，磁盘损坏，rm,dd,坏块，坏道
解决方案：主从、高可用架构、灾备、备份恢复

逻辑损坏：drop truncate delete update
解决方案：备份恢复、闪回工具、binlog、延时从库。。。

目标： 将数据尽可能恢复到故障之前的状态（PITR），减少数据损失

5.1 在数据备份中需要做哪些事情?

设计备份策略
    工具 ： 逻辑备份、物理备份
    周期 ： 每天、每周、每月
日常备份巡检
    日志
    备份大小
定期恢复演练(测试库)
    季度
    半年
故障恢复
升级迁移

5.2 MySQL数据库备份方式

```
逻辑备份：  就是备份SQL
mysqldump
load data/mysqlimport
mydumper

物理备份：拷贝数据文件
Percona Xtrabackup 8.0.12+
Enterprise Backup
8017+ Clone Plugin
```

5.3 mysqldump逻辑备份应用

```
-A 全备参数
-B db1 db2 db3 备份多个单库
备份单个或多个表
-R              备份存储过程及函数
--triggers      备份触发器
-E              备份事件


--master-data=2

--max-allowed-packet=#

mysqldump -uroot -p -A -R -E --triggers --
master-data=2  --single-transaction --set-
gtid-purged=OFF --max-allowed-packet=256M
>/data/backup/full.sql
```

```
--max-allowed-packet=#
The maximum packet length to send to or
receive from server

例子:
mysqldump -uroot -p123 -A  -R  --triggers --
master-data=2  --single-transaction|gzip >
/backup/full_$(date +%F).sql.gz
mysqldump -uroot -p123 -A  -R  --triggers --
master-data=2  --single-transaction|gzip >
/backup/full_$(date +%F-%T).sql.gz

mysqldump备份的恢复方式（在生产中恢复要谨慎，恢复会
删除重复的表）
set sql_log_bin=0;
source /backup/full.sql
```

5.4 PXB 物理备份应用

5.4.1 全备应用

```
Percona xtrabackup

1.全量备份
xtrabackup --defaults-file=/etc/my.cnf --
backup --target-dir=/data/backup/full

2.数据恢复
2.1 准备
```

```
xtrabackup  --prepare --target-
dir=/data/backup/full
2.2 拷回数据
xtrabackup --copy-back --target-
dir=/data/backup/full
2.3 修改目录属性启动数据库
  chown -R mysql.mysql /data/3306/data
  chmod -R 755 /data/3306/data

2.4 启动数据库实例
```

5.4.2 增量备份应用

```
全量备份的目录为： mkdir  -p /data/backup/full
增量备份的目录为： mkdir  -p /data/backup/inc
1.备份操作：
1.1.全量备份：
xtrabackup --defaults-file=/etc/my.cnf --
backup --parallel=4 --target-
dir=/data/backup/full
1.2.增量备份：
xtrabackup --defaults-file=/etc/my.cnf --
backup --parallel=4 --target-
dir=/data/backup/inc  --incremental-
basedir=/data/backup/full

2.恢复操作：
2.1 准备全备份的日志：
xtrabackup --prepare --apply-log-only --
target-dir=/data/backup/full
```

```
2.2 准备增量备份的日志：
xtrabackup --prepare --apply-log-only --
target-dir=/data/backup/full  --incremental-
dir=/data/backup/inc
2.3 全备份准备：
xtrabackup --prepare --target-
dir=/data/backup/full
2.4 拷回数据：
xtrabackup  --copy-back --target-
dir=/data/backup/full

2.5 修改数据目录的权限和属性：
chown -R mysql:mysql /data/
```

5.5 Clone Plugin备份工具使用

5.5.1 本地克隆(8.0.17+)

```
# 加载插件
INSTALL PLUGIN clone SONAME 'mysql_clone.so';
或
[mysqld]
plugin-load-add=mysql_clone.so
clone=FORCE_PLUS_PERMANENT

SELECT PLUGIN_NAME, PLUGIN_STATUS
FROM INFORMATION_SCHEMA.PLUGINS
WHERE PLUGIN_NAME LIKE 'clone';
```

```
# 创建克隆专用用户
CREATE USER clone_user@'%' IDENTIFIED with
mysql_native_password by 'password';
GRANT BACKUP_ADMIN ON *.* TO 'clone_user';

# BACKUP_ADMIN是MySQL8.0 才有的备份锁的权限

# 本地克隆
[root@db01 3306]# mkdir -p /data/test/
[root@db01 3306]# chown -R mysql.mysql /data/
mysql -uclone_user -ppassword
CLONE LOCAL DATA DIRECTORY =
'/data/test/clonedir';

# 观测状态
db01 [(none)]> SELECT STAGE, STATE, END_TIME
FROM performance_schema.clone_progress;
```

5.5.2 远程克隆

```
源端          ----》  目标
128                   129
backup_admin          clone_plugin


# 加载插件
INSTALL PLUGIN clone SONAME 'mysql_clone.so';
或
[mysqld]
plugin-load-add=mysql_clone.so
```

```
clone=FORCE_PLUS_PERMANENT

SELECT PLUGIN_NAME, PLUGIN_STATUS
FROM INFORMATION_SCHEMA.PLUGINS
WHERE PLUGIN_NAME LIKE 'clone';

# 创建远程clone用户
## 捐赠者授权(源端)
create user test_s@'%' identified by '123';
grant backup_admin on *.* to test_s@'%';

## 接受者授权（目标端）
create user test_t@'%' identified by '123';
grant clone_admin on *.* to test_t@'%';

# 远程clone(目标端)
## 开始克隆
SET GLOBAL
clone_valid_donor_list='10.0.0.128:3306';
mysql -utest_t -p123 -h10.0.0.129  -P3306
CLONE INSTANCE FROM test_s@'10.0.0.128':3306
IDENTIFIED BY '123';
```

6.MySQL架构设计方面对于安全的保证

6.1 数据安全在架构方面的要求-高可用容灾技术

无故障时间	故障时间	典型架构
99.9%	0.1%=525.6 min	KA+双主： 人为干预
99.99%	0.01%=52.56 min	MHA 、RM、 consul+zk、ORCH、xenon： 半自动化，都要配合5.7+GTID+增强半同步
99.999%	0.001%=5.256 min	PXC 、 MGR 、MIC、MGC
99.9999%	0.0001%=0.5256 min	自动化、云化、平台化、分布式

6.2 企业容灾级别

级别	方式	RPO	RTO
L0	**无备源中心**: 没有灾难恢复能力，只在本地进行数据备份	24小时+	4小时+
L1	**本地备份+异地保存**: 本地将关键数据备份，然后送到异地保存。 灾难发生后，按预定数据恢复程序恢复系统和数据。	24小时+	8小时+
L2	**双中心主备模式**: 在异地建立一个热备份点，通过网络进行数据备份。 当出现灾难时，备份站点接替主站点的业务，维护业务连续性	秒级	数分钟到半小时

级别	方式	RPO	RTO
L3	**双中心双活** 在相隔较远的地方分别建立两个数据中心，进行相互数据备份。 当某个数据中心发生灾难时，另一个数据中心接替其工作任务。	秒级	秒级
L4	**双中心双活 + 异地热备 = 两地三中心** 在同城分别建立两个数据中心，进行相互数据备份。 当该城市的2个中心同时不可用（地震/大面积停电/网络等），快速切换到异地	秒级	分钟级

RTO (Recovery Time Objective，复原时间目标)是企业可容许服务中断的时间长度。比如说灾难发生后半天内便需要恢复，RTO值就是十二小时；
RPO (Recovery Point Objective，复原点目标)是指当服务恢复后，恢复得来的数据所对应时的间点。

6.2 MySQL Orch高可用架构设计于应用

6.3.1 ORCH介绍

Orchestrator（orch）：go编写的MySQL高可用性和复制拓扑管理工具，支持复制拓扑结构的调整，自动故障转移和手动主从切换等。后端数据库用MySQL或SQLite存储元数据，并提供web界面展示MySQL复制的拓扑关系及状态，通过web可更改MySQL实例的复制关系和部分配置信息，同时也提供命令行和api接口，方便运维管理。相对比MHA来看最重要的是解决了管理节点的单点问题，其通过raft协议保证本身的高可用。GitHub的一部分管理也在用该工具进行管理。

① 自动发现MySQL的复制拓扑，并且在web上展示。
② 重构复制关系，可以在web进行拖图来进行复制关系变更。
③ 检测主异常，并可以自动或手动恢复，通过Hooks进行自定义脚本。
④ 支持命令行和web界面管理复制。

6.3.2 ORCH功能展示

参考视频功能。