云规划及网络和数据安全运维工程师笔试模拟卷（二）

在线考试编号：1630123 时间：60（分钟） 总分：89.0 姓名：_____ 成绩：_____

一、单项选择题（1～15小题，小计 45.0 分）

（每题3分，共45分）

1 根据2025年发布的《网络安全等级保护测评报告模板》(2025版)及公网安〔2025〕1001号文要求，关于云计算环境下的等级保护定级与测评，以下说法正确的是？〔3.0分〕

A．云服务商（CSP）和云租户（CST）可以合并为一个定级对象进行统一测评。

B．云平台的定级等级必然高于其上运行的云租户系统的定级等级。

C．云租户应依据其业务系统重要性独立定级，并重点关注“安全计算环境”和“数据安全”扩展要求。

D．2025年新规取消了云安全扩展要求，统一采用通用安全要求。

2 在Kubernetes (K8s) 集群安全加固中，为了防止容器逃逸并限制Pod的系统调用，应配置哪种原生安全机制？〔3.0分〕

A．NetworkPolicy；

B．Pod Security Admission (PSA) / Pod Security Standards (PSS)；

C．Resource Quota；

D．Horizontal Pod Autoscaler (HPA)；

3 某企业需要确保敏感数据（如身份证号）在开发测试环境中不可见，但在生产数据库中保持明文存储以便业务查询，应采用哪种数据安全技术？〔3.0分〕

A．透明数据加密 (TDE)；

B．静态数据脱敏；

C．动态数据脱敏；

D．同态加密；

4 关于主流云服务商的数据安全产品，以下对应关系错误的是？〔3.0分〕

A．AWS: AWS KMS (密钥管理) + Macie (敏感数据发现)；

B．Azure: Azure Key Vault + Microsoft Purview (数据治理)；

C．阿里云: 密钥管理服务KMS + 敏感数据保护 (SDDP)；

D．Google Cloud: Cloud HSM + Dataflow (主要用于数据脱敏和加密管理)；

5 在构建多层防御体系时，关于入侵防御系统（IPS）与防火墙（FW）的联动，下列描述最准确的是？〔3.0分〕

A．防火墙工作在网络层，仅能基于IP和端口过滤；IPS工作在应用层，可识别攻击特征并主动阻断。

B．IPS应部署在防火墙之前，以便先清洗攻击流量，减轻防火墙压力。

C．现代下一代防火墙（NGFW）已完全取代IPS，无需单独部署IPS设备。

D．防火墙和IPS都无法防御加密流量中的攻击，必须先在设备上解密所有流量。

6 针对分布式存储系统中的数据备份与恢复，以下哪种策略最能平衡RPO（恢复点目标）接近于0与成本效益？〔3.0分〕

A．每日全量备份到磁带库；

B．持续数据保护 (CDP) 结合增量快照；

C．每周全量备份 + 每日增量备份；

D．仅依靠云服务商的多副本机制（如三副本）；

7 使用漏洞扫描工具评估云环境时，对于容器镜像的扫描，最佳实践时机是？〔3.0分〕

A．仅在容器运行在生产环境后定期扫描；

B．仅在CI/CD流水线构建完成后扫描一次；

C．在开发者本地编写代码时、CI/CD构建时、以及运行时（Registry/Cluster）进行多阶段扫描；

D．不需要扫描容器镜像，只需扫描宿主机；

8 在Linux系统安全加固中，为了限制特定用户只能执行特定的命令，且能详细审计其操作行为，最合适的机制是？〔3.0分〕

A．修改 /etc/passwd 文件；

B．使用 chmod 限制文件权限；

C．配置 sudo 权限并结合日志审计；

D．禁用该用户的Shell登录；

9 下列关于数据加密传输的说法，正确的是？〔3.0分〕

A．在内网（VPC内部）传输数据时，由于网络隔离，无需加密。

B．TLS 1.2是目前唯一安全的传输协议版本，TLS 1.3尚未普及。

C．应强制使用TLS 1.3，并禁用弱加密套件（如RC4, 3DES），以实现前向安全性。

D．数据库客户端与应用服务器之间的连接加密会显著降低性能，建议仅在公网开启。

10 在云资源管理与优化中，为了实现成本节约并动态调配资源，以下哪项技术最适合处理具有明显波峰波谷特征的Web应用？〔3.0分〕

A．预留实例 (Reserved Instances)；

B．专属宿主机 (Dedicated Host)；

C．弹性伸缩组 (Auto Scaling Group) 结合按量付费/竞价实例；

D．手动调整虚拟机规格；

11 某公司发生了一起数据泄露事件，调查发现是因为开发人员将包含AK/SK（访问密钥）的代码上传到了GitHub公共仓库。以下哪项措施能从根源上防范此类问题再次发生？〔3.0分〕

A．定期轮换所有AK/SK；

B．在Git提交钩子（Pre-commit Hook）中集成密钥扫描工具（如GitLeaks）；

C．加强员工安全意识培训；

D．购买更高版本的防火墙；

12 关于虚拟化安全，以下哪种攻击方式是指攻击者利用虚拟机监控器（Hypervisor）的漏洞，从Guest OS突破到Host OS或其他VM？〔3.0分〕

A．ARP欺骗；

B．虚拟机逃逸 (VM Escape)；

C．SQL注入；

D．DDoS攻击；

A．冷备（Cold Site）；

B．温备（Warm Site）；

C．热备（Hot Site）/ 双活数据中心；

D．仅本地备份；

14 下列哪项不属于网络安全等级保护2.0中“安全计算环境”层面的技术要求？〔3.0分〕

A．身份鉴别；

B．访问控制；

C．入侵防范；

D．通信网络架构设计；

15 在使用Docker容器时，为了减小镜像体积并降低被攻击面，最佳实践是？〔3.0分〕

A．直接在官方Ubuntu镜像上安装所有依赖；

B．使用多阶段构建（Multi-stage builds），最终镜像仅包含运行二进制文件和最小化基础镜像（如Alpine/Distroless）；

C．将源代码和编译工具链都打包进生产镜像以便调试；

D．以root用户运行容器进程；

二、多项选择题（16～21小题，小计 24.0 分）

（每题4分，共24分，错选不得分）

16 面对2025年日益严峻的勒索软件威胁，作为安全运维工程师，应采取哪些关键技术措施来保障数据备份的有效性？（ ） 〔4.0分〕

A．实施备份数据的不可变性（Immutability/WORM），防止备份文件被加密或删除；

B．建立离线备份或空气间隙（Air Gap）机制，物理或逻辑隔离备份存储；

C．定期对备份数据进行恢复演练，验证数据完整性；

D．将备份数据存储在同一个云账号的同一个Region下，以降低延迟；

17 在Kubernetes集群中，为了实现细粒度的访问控制（RBAC），需要配置哪些核心资源对象？（ ） 〔4.0分〕

A．Role 或 ClusterRole；

B．RoleBinding 或 ClusterRoleBinding；

C．ServiceAccount；

D．Ingress；

18 关于云环境下的网络安全监测与响应，以下哪些属于“态势感知”平台的核心能力？（ ） 〔4.0分〕

A．多源日志采集与标准化（Firewall, WAF, Host, Cloud Audit Logs）；

B．基于大数据和AI的异常行为分析与威胁情报关联；

C．自动化编排与响应（SOAR），如自动封禁IP、隔离主机；

D．仅提供静态的漏洞扫描报告，不涉及实时流量分析；

19 在进行数据库安全加固时，以下哪些措施是符合“最小权限”和“纵深防御”原则的？（）〔4.0分〕

A．禁止数据库账号直接从互联网访问，仅允许通过堡垒机或应用内网访问；

B．为应用程序分配仅具备CRUD必要权限的专用账号，严禁使用sa/root账号；

C．开启数据库审计功能，记录所有DDL和DML操作；

D．为了方便运维，将所有DBA的密码设置为统一且简单的密码，并保存在Excel中；

20 针对混合云架构（本地IDC + 公有云）的网络规划，以下哪些技术可用于构建安全、高速的连接？（）〔4.0分〕

A．IPsec VPN；

B．专线接入（Direct Connect / Express Route / 高速通道）；

C．SD-WAN（软件定义广域网）；

D．将本地数据中心直接暴露在公网，通过公网IP互访；

21 根据《数据安全法》及2025年等保新规，数据分类分级工作应包含哪些关键步骤？（）〔4.0分〕

A．资产梳理：识别组织内的所有数据资产及其分布；

B．定级：依据数据遭到破坏后的影响对象和影响程度划分级别（如核心、重要、一般）；

C．标识：对不同级别的数据打上标签，以便技术策略自动匹配；

D．忽略非结构化数据（如文档、图片），仅对数据库表格进行分类；

三、判断题（22～31小题，小计 20.0 分）

（每题2分，共20分，正确的选A，错误的选B）

22 在云环境中，只要开启了云服务商提供的“安全组”（Security Group），就不需要再在操作系统内部配置iptables或firewalld防火墙了。〔2.0分〕

A．正确√；

B．错误×；

23 数据备份的“3-2-1”原则指的是：3份数据拷贝，2种不同存储介质，1份异地备份。在云时代，这一原则已经过时，不再适用。〔2.0分〕

A．正确√；

B．错误×；

24 容器技术（Docker）相比传统虚拟机（VM），因为共享宿主内核，所以在默认情况下具有更强的隔离性和安全性。〔2.0分〕

A．正确√；

B．错误×；

25 网络安全等级保护第三级系统要求每年至少进行一次等级测评，且在发生重大变更（如架构调整、云迁移）时应重新定级或备案。〔2.0分〕

A．正确√；

B．错误×；

26 使用HTTPS协议可以完全防止中间人攻击（MITM），因此不需要校验服务器证书的有效性。〔2.0分〕

A．正确√；

B．错误×；

27 在K8s中，Secret对象默认是以加密形式存储在Etcd中的，无需额外配置。〔2.0分〕

A．正确√；

B．错误×；

28 漏洞扫描发现的高危漏洞，必须立即在生产环境进行补丁更新，无需经过测试验证。〔2.0分〕

A．正确√；

B．错误×；

29 云服务商的责任共担模型中，物理数据中心的安全、宿主机的虚拟化层安全由云服务商负责；而客户操作系统的补丁、应用代码安全、数据加密由客户负责。〔2.0分〕

A．正确√；

B．错误×；

30 为了便于排查问题，可以将数据库的监听端口（如3306, 1521）直接映射到云服务器的公网IP上，并设置复杂的密码即可。 〔2.0分〕

A．正确√；

B．错误×；

31 2025年实施的等保2.0新版测评要求中，对于采用云计算、大数据、物联网等新技术的系统，不再需要参考相应的安全扩展要求，统一按通用要求测评。 〔2.0分〕

A．正确√；

B．错误×；

本次考试考题展示结束