安全计算环境-中间件（S3A3G3）作业指导书

控制点	安全要求	要求解读	测评方法	预期结果或主要证据	符合情况
身份鉴别	a)应对登录的用户进行身份标识和鉴别，身份标识具有唯一性，身份鉴别信息具有复杂度要求并定期更换	1)应核查用户在登录时是否采用了身份鉴别措施； 2)应核查用户列表确认用户身份标识是否具有唯一性； 3)应核查用户配置信息或测试验证是否不存在空口令用户； 4)应核查用户鉴别信息是否具有复杂度要求并定期更换。	1)cat /login.defs (查看口令可用天数、修改口令间隔天数、口令最小长度) 2)cat /etc/security/pwquality.conf (查看口令复杂度)	1)身份标识具有唯一性 2)采取身份鉴别措施（如通过用户名加口令方式进行身份鉴别） 3)当前口令复杂度达到8位以上，至少三种字符类型组成，并且定期更换（更换周期3个月以内） 4)强制口令复杂度达到8位以上，至少三种字符类型组成，并且定期更换（更换周期3个月以内）	符合情况：需同时保证身份标识唯一性、存在身份鉴别措施、口令复杂度达到8位以上，至少三种字符类型组成，并且定期更换、更换口令时校验口令复杂度达到8位以上，至少三种字符类型组成。 部分符合情况：至少满足以上一点，但未全部满足。 不符合情况：未符合以上所有情况。
	b)应具有登录失败处理功能，应配置并启用结束会话、限制非法登录次数和当登录连接超时自动退出等相关措施	1)应核查是否配置并启用了登录失败处理功能； 2)应核查是否配置并启用了限制非法登录功能，非法登录达到一定次数后采取特定动作，如账户锁定等； 3)应核查是否配置并启用了登录连接超时及自动退出功能。	1)cat /pam.d/system-auth (查看登陆失败处理次数和限制时间)　　2)cat /etc/profile | grep TMOUT (查看登陆超时自动退出策略--本地) 3)cat /etc/ssh/sshd_config | grep Client（查看登陆超时自动退出策略--通过ssh链接的登录）	1)启用登录失败功能，登录失败X（不超过10）次，锁定账户X（不超过60）分钟 2)启用登录超时策略，登录超时X（30分钟以内）分钟自动退出	符合情况：启用登录失败功能和登录连接超时策略。 部分符合情况：至少满足以上一点，但未全部满足。 不符合情况：未符合以上所有情况。
	c)当进行远程管理时，应采取必要措施、防止鉴别信息在网络传输过程中被窃听	中间件是否采用加密等安全方式对系统进行远程管理，能否防止鉴别信息在网络传输过程中被窃听；	应核查是否采用加密等安全方式对系统进行远程管理，防止鉴别信息在网络传输过程中被窃听；	采用HTTPS加密传输方式	符合情况：采用安全加密协议进行传输。 不符合情况：未采用安全加密协议无法保证数据在传输过程中的完整性。
	d)应采用口令、密码技术、生物技术等两种或两种以上组合的鉴别技术对用户进行身份鉴别，且其中一种鉴别技术至少应使用密码技术来实现	中间件是否采用动态口令、数字证书、生物技术和设备指纹等两种或两种以上组合的鉴别技术对用户身份进行鉴别；	1)应核查是否采用动态口令、数字证书、生物技术和设备指纹等两种或两种以上组合的鉴别技术对用户身份进行鉴别； 2)应核查其中一种鉴别技术是否使用密码技术来实现。	1)采用双因子认证（短信验证码不算） 2)其中一种必须要有密码技术，并记录采用何种算法（如Google Authenticator 动态口令使用OTP-HMAC密码技术）	符合情况：采用双因子认证方式，并且其中一种有密码技术。 不符合情况：未采用双因子认证方式。
访问控制	a)应对登录的用户分配账户和权限	1)中间件是否对用户账户和权限进行相关设置； 2)是否限制默认账户的访问权限。	1)应核查是否为用户分配了账户和权限及相关设置情况； 2)应核查是否已禁用或限制匿名、默认账户的访问权限。	1)为管理员分配相应账户 2)为账户分配管理员所需的权限 3)禁用或限制匿名、默认账户的权限	符合情况：为管理员分配相应账户和所需的权限并且禁用或限制匿名、默认账户的权限。 不符合情况：未分配相应账户和权限，或者
	b)应重命名或删除默认账户，修改默认账户的默认口令	默认账户和默认口令是否已修改；	1)应核查是否已经重命名默认账户或默认账户已被删除； 2)应核查是否已修改默认账户的默认口令。	1)默认账户已重命名或者删除默认账户 2)默认账户的默认口令已进行修改	符合情况：默认账户已重命名或者删除默认账户并且默认口令已进行修改。 部分符合情况：至少满足以上一点，但未全部满足。 不符合情况：未符合以上所有情况。
	c)应及时删除或停用多余的、过期的账户，避免共享账户的存在	管理员和账户一一对应；	1)应核查是否不存在多余或过期账户，管理员用户与账户之间是否一一对应； 2)应测试验证多余的、过期的账户是否被删除或停用。	1)不存在多余或者无效的账户 2)一个管理员一个账户	符合情况：不存在多余或者无效的账户并且一个管理员一个账户不存在共享账户。 部分符合情况：至少满足以上一点，但未全部满足。 不符合情况：未符合以上所有情况。
	d)应授予管理用户所需的最小权限，实现管理用户的权限分离	账户进行权限划分；	1)应核查是否进行角色划分； 2)应核查管理用户的权限是否已进行分离； 3)应核查管理用户权限是否为其工作任务所需的最小权限。	1)账户角色进行划分 2)账户权限进行三权分立 3)账户所需的权限为工作所需最小权限	符合情况：账户角色进行划分，部署三权分立，分配账户所需的权限为工作所需最小权限。 不符合情况：未划分相应账户的权限。
	d)应由授权主体配置访问控制策略，访问控制策略规定主体对客体的访问规则	1)应核查是否由授权主体（如管理用户）负责配置访问控制策略； 2)应核查授权主体是否依据安全策略配置了主体对客体的访问规则； 3)应测试验证用户是否有可越权访问情形	1)ls -l /etc/passwd（记录不同账户下的该文件夹权限） 2)ls -l /etc/shadow 3)ls -l/etc/profile	1)管理用户负责配置访问控制策略，管理用户为账户分配不同的角色，每个角色分配不同的功能权限，当账户与角色关联时，该账户就具备与角色相关联的功能操作 2)非管理用户不能访问权限管理相关的功能	符合情况：配置访问控制策略，非管理用户不能访问权限管理相关的功能。 不符合情况：未配置访问控制策略。
	e)访问控制的粒度应达到主体为用户级或进程级，客体为文件、数据库表级	主体和客体的访问控制策略；	应核查访问控制策略的控制粒度是否达到主体为用户级或进程级，客体为文件、数据库表、记录或字段级；	访问控制策略的控制粒度主体为登录账户，客体为功能权限以及功能权限关联的数据库表	符合情况：配置访问控制策略，控制粒度主体达到用户级或进程级，客体为功能权限以及功能权限关联的数据库表。 不符合情况：未配置访问控制策略，不存在控制主客体粒度。
	f)应对重要主体和客体设置安全标记，并控制主体对有安全标记信息资源的访问	1)应核查是否对主体、客体设置了安全标记； 2)应测试验证是否依据主体、客体安全标记控制主体对客体访问的强制访问控制策	getenforce （查看当前selinux运行状态--Enforcing强制、Permissive宽容、Disabled关闭）	1)安全策略对重要账户和重要信息设置了安全标记 2)安全标记控制了账户对有安全标记信息资源的访问	符合情况：依据安全策略对重要账户和重要信息设置了安全标记。 不符合情况：重要账户和重要信息未设置安全标记。

安全审计	a)应启用安全审计功能，审计覆盖到每个用户，对重要的用户行为和重要安全事件进行审计	1)应核查是否开启了安全审计功能； 2)应核查安全审计范围是否覆盖到每个用户； 3)应核查是否对重要的用户行为和重要安全事件进行审计。	1)在Nginx的配置文件nginx.conf中查看是否开启error_log和access_log。 2)在Nginx安装目录中查看是否有：/logs/error_log和/logs/access_log。	1)启用了安全审计功能。建立了日志审计模块。 2)安全审计范围覆盖每个用户 3)对重要的用户行为和重要安全事件提供了审计	符合情况：启用了安全审计功能。建立了日志审计模块，安全审计范围覆盖到每个用户，对重要的用户行为和重要安全事件提供了审计。 不符合情况：未开启安全审计功能，不存在日志审计模块，无法对重要的用户行为和重
	b)审计记录应包括事件的日期和时间，用户、事件类型，事件是否成功及其他与审计相关的信息	应核查审计记录信息是否包括事件的日期和时间、用户、事件类型、事件是否成功及其他与审计相关的信息；	1)查看error_log文件记录内容，查看是否包括：错误发生的日期、时间、错误等级、IP地址、内容等。 2)查看access_log文件内容，查看是否包括：客户端连接的日期、时间、IP地址、状态代码、浏览器信息等。	审计记录至少包括事件日期，时间，发起者信息(如用户名、IP地址等)、类型、描述和结果(是否成功等)等内容	符合情况：启用了安全审计功能。建立了日志审计模块，审计记录至少包括事件日期，时间，发起者信息(如用户名、IP地址等)、类型、描述和结果(是否成功等)等内容。 不符合情况：未开启安全审计功能，不存在日志审计模块，不存在日志审计记录。
	c)应对审计记录进行保护，定期备份，避免受到未预期的删除、修改或覆盖等	1)应核查是否采取了保护措施对审计记录进行保护； 2)应核查是否采取技术措施对审计记录进行定期备份，并核查其备份策略。	1)查看日志在本地保存的周期和权限。查看日志轮转周期；查看日志的权限，确保操作系统普通用户无删除、修改权限。 2)查看日志是否进行异地备份，保存周期，查看操作系统中是否发送日志到备份系统、日志审计系统；若操作系统为虚拟机，查看是否通过创建快照的方式对日志进行保护	1)日志本地存储，可查看存储目录，周期和相关策略等 2)日志无法被删除和篡改	符合情况：启用了安全审计功能。建立了日志审计模块，日志无法被删除和篡改，日志信息保存6个月以上。对日志信息进行定期备份策略。 不符合情况：未开启安全审计功能，不存在日志审计模块，不存在日志审计记录。
	d)应对审计进程进行保护，防止未经授权的中断	通过非审计管理员的其他账户能否中断审计进程，验证审计进程是否受到保护；	Nginx审计进程与nginx服务相关联，无法单独中断。 检查方法：使用操作系统普通用户中断审计进程，查看是否成功。	非授权不能中断审计进程或关闭审计功能	符合情况：启用了安全审计功能。建立了日志审计模块，非授权不能中断审计进程或关闭审计功能。 不符合情况：未开启安全审计功能，不存在日志审计模块，不存在日志审计进程。
入侵防范	a)应提供数据有效性检验功能，保证通过人机接口输入或通过通信接口输入的内容符合系统设定要求	本条款要求应对数据的有效性进行验证，主要验证那些通过人机接口(如程序的界面)输入或通过通信接口输入的数据格式或长度是否符合系统设定要求，防止个别用户输入畸形数据而导致系统出错(如SQL注入攻击等),从而影响系统的正常使用甚至危害系统的安全	1)应核查设计文档的内容是否包括数据有效性检验功能的内容； 2)应测试验证是否对人机接口或通信接口输入的内容进行有效性检验	应具备软件容错能力，提供对输入数据的长度、格式等进行检查和验证的功能，通过限制特定关键字的输入等防护措施防止SQL注入等攻击	符合情况：系统具备软件容错能力，提供对输入数据的长度、格式等进行检查和验证的功能，通过限制特定关键字的输入等防护措施防止SQL注入等攻击。 不符合情况：系统不具备软件容错能力。
	b)应能发现可能存在的已知漏洞，并在经过充分测试评估后，及时修补漏洞	攻击者可能利用中间件存在的安全漏洞进行攻击，应对中间件漏洞扫描，及时发现存在的已知漏洞，并在经过充分测试评估后更新补丁，.避免遭受漏洞带的风险	1)应通过漏洞扫描、渗透测试等方式核查是否不存在高风险漏洞； 2)应核查是否在经过充分测试评估后及时修补漏洞	1)中间件经过漏洞扫描或者渗透测试后不存在高风险漏洞，若存在，则经过充分测试评估后及时修补漏洞。 2)放弃扫描情况下，客户自身定期进行漏扫或者安全评估等	符合情况：经过漏洞扫描或者渗透测试后不存在高风险漏洞，若存在，则经过充分测试评估后及时修补漏洞。放弃扫描情况下，客户自身定期进行漏扫或者安全评估等。 不符合情况：客户自身未定期进行漏扫或者安全评估。经过漏洞扫描或者渗透测试之后存在相应风险的漏洞信息。
数据完整性	a)应采用校验技术或密码技术保证重要数据在传输过程中的完整性，包括但不限于鉴别数据、重要业务数据、重要审计数据、重要配置数据、重要视频数据和重要个人信息等	为了保证各种重要数据在存储和传输过程中免受未授权的破坏，应对数据的完整性进行检测，当检测到数据的完整性遭到破坏时应采取恢复措施对数据进行恢复。本条款要求对鉴别数据、重要业务数据、重要审计数据、重要配置数据.重要视频数据和重要个人信息在传输过程中的完整性进行检测，并在检测到完整性受到破坏时采取恢复措施，如重传或其它方式	1）应核查设计文档，重要审计数据、重要配置数据和重要个人信息等在传输过程中是否采用了校验技术或密码技术保证完整性; 2）应测试验证在传输过程中对重要审计数据、重要配置数据和重要个人信息等进行篡改,查看是否能够检测到数据在传输过程中的完整性受到破坏并能够及时恢复。	1)通过HTTPS方式保证鉴别数据、重要业务数据、重要审计数据、重要配置数据、重要视频数据和重要个人信息在传输过程中的完整性 2)HTTPS协议中TSL/SSL版本为1.2以上	符合情况：通过HTTPS方式保证鉴别数据、重要业务数据、重要审计数据、重要配置数据、重要视频数据和重要个人信息在传输过程中的完整性，HTTPS协议中TSL/SSL版本为1.2以上。 不符合情况：未配置HTTPS方式无法保证鉴别数据、重要业务数据、重要审计数据、重要配置数据、重要视频数据和重要个人信息在传输过程中的完整性。
	b）应采用校验技术或密码技术保证重要数据在存储过程中的完整性，包括但不限于鉴别数据、重要业务数据、重要审计数据、重要配置数据、重要视频数据和重要个人信息等	本条款要求对鉴别数据、重要业务数据、重要审计数据、重要配置数据、重要视频数据和重要个人信息在存储过程中的完整性进行检测，并在检测到完整性受到破坏时采取恢复措施	1)应核查设计文档，是否采用了校验技术或密码技术保证鉴别数据、重要业务数据、重要审计数据、重要配置数据、重要视频数据和重要个人信息等在存储过程中的完整性; 2)应核查是否采用技术措施保证鉴别数据、重要业务数据、重要审计数据、重要配置数据、重要视频数据和重要个人信息等在存储过程中的完整性; 3)应测试验证在存储过程中对鉴别数据、重要业务数据、重要审计数据、重要配置数据、重要视频数据和重要个人信息等进行篡改，是否能够检测到数据在存储过程中的完	1)采用校验技术或密码技术保证了鉴别数据、重要业务数据、重要审计数据、重要配置数据和重要个人信息等在存储过程中的完整性 2)可检测到存储在数据库中的鉴别数据、重要业务数据、重要审计数据、重要配置数据、重要视频数据和重要个人信息等被修改的行为，并具备恢复措施	符合情况：系统采用校验技术或密码技术保证了鉴别数据、重要业务数据、重要审计数据、重要配置数据和重要个人信息等在存储过程中的完整性。 不符合情况：系统未采用校验技术或密码技术无法保证鉴别数据、重要业务数据、重要审计数据、重要配置数据和重要个人信息等在存储过程中的完整性。

数据保密性	a)应采用密码技术保证重要数据在传输过程中的保密性，包括但不限于鉴别数据、重要业务数据、和重要个人信息等	为了保证各种重要数据在存储和传输过程中免受未授权的破坏，应对数据的完整性进行检测，当检测到数据的完整性遭到破坏时应采取恢复措施对数据进行恢复。本条款要求对鉴别数据、重要业务数据、重要审计数据、重要配置数据,重要视频数据和重要个人信息在传输过程中的完整性进行检测，并在检测到完整性受到破坏时采取恢复措施，如重传或其它方式	1)应核查设计文档，重要业务数据和重要个人信息等在传输过程中是否采用密码技术保证保密性； 2)应通过嗅探等方式抓取传输过程中的数据包,查看重要业务数据和重要个人信息等在传输过程中是否进行了加密处理。	1)通过HTTPS方式保证鉴别数据、重要业务数据、重要审计数据、重要配置数据、重要视频数据和重要个人信息在传输过程中的保密性 2)HTTPS协议中TSL/SSL版本为1.2以上	符合情况：通过HTTPS方式保证鉴别数据、重要业务数据、重要审计数据、重要配置数据、重要视频数据和重要个人信息在传输过程中的保密性，HTTPS协议中TSL/SSL版本为1.2以上。 不符合情况：未配置HTTPS方式无法保证鉴别数据、重要业务数据、重要审计数据、重要配置数据、重要视频数据和重要个人信息在传输过程中的保密性。
	b)应采用密码技术来保证重要数据在存储过程中的保密性，包括但不限于鉴别数据、重要业务数据和重要人信息等	本条款要求对鉴别数据、重要业务数据和重要个人信息在存储过程中采取保密措施，如对这些数据进行加密等	1）应核查是否采用密码技术保证重要业务数据和重要个人信息等在存储过程中的保密性； 2）应核查是否采用技术措施（如数据安全保护系统等）保证重要业务数据和重要个人信息等在存储过程中的保密性； 3）应测试验证是否对指定的数据进行加密处理。	1)系统采用了密码技术对存储在数据库中的鉴别数据、重要业务数据和重要 2)数据库中存储的鉴别数据、重要业务数据和重要个人信息等均加密存储	符合情况：系统采用校验技术或密码技术保证了鉴别数据、重要业务数据、重要审计数据、重要配置数据和重要个人信息等在存储过程中的保密性。 不符合情况：系统未采用校验技术或密码技术无法保证鉴别数据、重要业务数据、重要审计数据、重要配置数据和重要个人信息等在存储过程中的保密性。
剩余信息保护	a)应保证鉴别信息所在的存储空间被释放或重新分配前得到完全清除	要求用户的鉴别信息所在的存储空间(如硬盘清除后才能分配给其他用户)	应核查相关配置信息或系统设计文档，用户的鉴别信息所在的存储空间被释放或重新分配前是否得到完全清除	中间件采取措施保证对存储介质(如硬盘或内存)中的用户鉴别信息进行及时清除。如系统会对存储或调用过鉴别信息的函数或变量及时写零或置空，及时清除B/S系统中的Session和Cookie信息，以及对存有用户鉴别信息的临时文件进行删除或内容清除等	符合情况：采取措施保证对存储介质(如硬盘或内存)中的用户鉴别信息进行及时清除。如系统会对存储或调用过鉴别信息的函数或变量及时写零或置空，及时清除系统中的剩余信息，以及对存有用户鉴别信息的临时文件进行删除或内容清除等。 不符合情况：未对剩余信息进行及时清理。
	b)应保证存有敏感数据的存储空间被释放或重新分配前得到完全清除	要求用户的敏感数据所在的存储空间(如硬盘清除后才能分配给其他用户)	应核查相关配置信息或系统设计文档，敏感数据所在的存储空间被释放或重新分配给其他用户前是否得到完全清除	中间件采取了措施保证对存储介质(如硬盘或内存入中的敏感数据进行及时清除，如系统会对存储或调用过鉴别信息的函数或变量及时写零或置空，及时清除B/S系统中的Session和Cookie信息，以及对存有用户鉴别信息的临时文件进行删除或内容清除等	符合情况：采取措施保证对存储介质(如硬盘或内存)中的用户鉴别信息进行及时清除。如系统会对存储或调用过鉴别信息的函数或变量及时写零或置空，及时清除系统中的剩余信息，以及对存有用户鉴别信息的临时文件进行删除或内容清除等。 不符合情况：未对剩余信息进行及时清理。