1. 安全物理环境测评表

|  |  |  |  |
| --- | --- | --- | --- |
| **测评项目** |  | **测评对象** | 安全物理环境 |
| **测评单位** |  | | |
| **测评地点** |  | | |
| **测评人员** |  | **配合人员** |  |
| **测评日期** | 2023.6.19 | | |
| **测评人员签字** |  | **配合人员签字** |  |

1.1. 安全通用要求部分

1.1.1. 阿里公共云机房

|  |  |  |
| --- | --- | --- |
| **安全控制点** | **测评指标** | **结果记录** |
| 物理位置选择 | a）机房场地应选择在具有防震、防风和防雨等能力的建筑内； | 客户为云租户，物理机房安全由阿里云负责，阿里公共云已经通过等级保护第三级测评。 |
| b）机房场地应避免设在建筑物的顶层或地下室，否则应加强防水和防潮措施。 | 客户为云租户，物理机房安全由阿里云负责，阿里公共云已经通过等级保护第三级测评。 |
| 物理访问控制 | a）机房出入口应配置电子门禁系统，控制、鉴别和记录进入的人员。 | 客户为云租户，物理机房安全由阿里云负责，阿里公共云已经通过等级保护第三级测评。 |
| 防盗窃和防破坏 | a）应将设备或主要部件进行固定，并设置明显的不易除去的标识； | 客户为云租户，物理机房安全由阿里云负责，阿里公共云已经通过等级保护第三级测评。 |
| b）应将通信线缆铺设在隐蔽安全处； | 客户为云租户，物理机房安全由阿里云负责，阿里公共云已经通过等级保护第三级测评。 |
| c）应设置机房防盗报警系统或设置有专人值守的视频监控系统。 | 客户为云租户，物理机房安全由阿里云负责，阿里公共云已经通过等级保护第三级测评。 |
| 防雷击 | a）应将各类机柜、设施和设备等通过接地系统安全接地； | 客户为云租户，物理机房安全由阿里云负责，阿里公共云已经通过等级保护第三级测评。 |
| b）应采取措施防止感应雷，例如设置防雷保安器或过压保护装置等。 | 客户为云租户，物理机房安全由阿里云负责，阿里公共云已经通过等级保护第三级测评。 |
| 防火 | a）机房应设置火灾自动消防系统，能够自动检测火情、自动报警，并自动灭火； | 客户为云租户，物理机房安全由阿里云负责，阿里公共云已经通过等级保护第三级测评。 |
| b）机房及相关的工作房间和辅助房应采用具有耐火等级的建筑材料； | 客户为云租户，物理机房安全由阿里云负责，阿里公共云已经通过等级保护第三级测评。 |
| c）应对机房划分区域进行管理，区域和区域之间设置隔离防火措施。 | 客户为云租户，物理机房安全由阿里云负责，阿里公共云已经通过等级保护第三级测评。 |
| 防水和防潮 | a）应采取措施防止雨水通过机房窗户、屋顶和墙壁渗透； | 客户为云租户，物理机房安全由阿里云负责，阿里公共云已经通过等级保护第三级测评。 |
| b）应采取措施防止机房内水蒸气结露和地下积水的转移与渗透； | 客户为云租户，物理机房安全由阿里云负责，阿里公共云已经通过等级保护第三级测评。 |
| c）应安装对水敏感的检测仪表或元件，对机房进行防水检测和报警。 | 客户为云租户，物理机房安全由阿里云负责，阿里公共云已经通过等级保护第三级测评。 |
| 防静电 | a）应采用防静电地板或地面并采用必要的接地防静电措施； | 客户为云租户，物理机房安全由阿里云负责，阿里公共云已经通过等级保护第三级测评。 |
| b）应采取措施防止静电的产生，例如采用静电消除器、佩戴防静电手环等。 | 客户为云租户，物理机房安全由阿里云负责，阿里公共云已经通过等级保护第三级测评。 |
| 温湿度控制 | a）应设置温湿度自动调节设施，使机房温湿度的变化在设备运行所允许的范围之内。 | 客户为云租户，物理机房安全由阿里云负责，阿里公共云已经通过等级保护第三级测评。 |
| 电力供应 | a）应在机房供电线路上配置稳压器和过电压防护设备； | 客户为云租户，物理机房安全由阿里云负责，阿里公共云已经通过等级保护第三级测评。 |
| b）应提供短期的备用电力供应，至少满足设备在断电情况下的正常运行要求； | 客户为云租户，物理机房安全由阿里云负责，阿里公共云已经通过等级保护第三级测评。 |
| c）应设置冗余或并行的电力电缆线路为计算机系统供电。 | 客户为云租户，物理机房安全由阿里云负责，阿里公共云已经通过等级保护第三级测评。 |
| 电磁防护 | a）电源线和通信线缆应隔离铺设，避免互相干扰； | 客户为云租户，物理机房安全由阿里云负责，阿里公共云已经通过等级保护第三级测评。 |
| b）应对关键设备实施电磁屏蔽。 | 客户为云租户，物理机房安全由阿里云负责，阿里公共云已经通过等级保护第三级测评。 |

1.1.2. 世纪互联IDC机房

|  |  |  |
| --- | --- | --- |
| **安全控制点** | **测评指标** | **结果记录** |
| 物理位置选择 | a）机房场地应选择在具有防震、防风和防雨等能力的建筑内； | 机房位于上海市荷丹路130号世纪互联202机房及401机房，所在建筑具有防风、防雨和防震能力。 |
| b）机房场地应避免设在建筑物的顶层或地下室，否则应加强防水和防潮措施。 | 机房所在建筑共4层，机房位于2层及顶层4层，机房屋顶粉刷防水涂料，墙壁粉刷了耐燃性涂料，可有效防水、防潮。 |
| 物理访问控制 | a）机房出入口应配置电子门禁系统，控制、鉴别和记录进入的人员。 | 机房出入口配置电子门禁系统，工作人员通过刷卡进入机房，并且外部人员进出机房需进行登记记录后由专人负责陪同方可进入机房；电子门禁系统记录内容包括传输记录日期、传输记录、持卡人、状态、区域等。 |
| 防盗窃和防破坏 | a）应将设备或主要部件进行固定，并设置明显的不易除去的标识； | 机房内设备均固定在机柜内，无松动情况；设备和主要部件均设置了不易除去的标签。 |
| b）应将通信线缆铺设在隐蔽安全处； | 机房通信线缆铺设在上桥架中，且与电力线缆保持一定距离。 |
| c）应设置机房防盗报警系统或设置有专人值守的视频监控系统。 | 机房内部署有视频监控系统，机房内所有入口、通道均安装有摄像头，保证机房内无死角，且机房监控室有专人24小时值守；监控视频可以保存90天。 |
| 防雷击 | a）应将各类机柜、设施和设备等通过接地系统安全接地； | 机房各机柜和主要设备均已进行安全接地。 |
| b）应采取措施防止感应雷，例如设置防雷保安器或过压保护装置等。 | 机房内采用了浪涌保护装置，安装了防雷器，可防止感应雷造成的危害；存在《防雷装置安全性能检测报告》。 |
| 防火 | a）机房应设置火灾自动消防系统，能够自动检测火情、自动报警，并自动灭火； | 机房内部署了自动消防系统，可通过烟雾感应器、感温探测器对火情进行检测，在检测到火情后及时进行报警，自动灭火。 |
| b）机房及相关的工作房间和辅助房应采用具有耐火等级的建筑材料； | 机房各面墙体均采用具有难燃性、不燃性的防火涂料进行覆盖。 |
| c）应对机房划分区域进行管理，区域和区域之间设置隔离防火措施。 | 机房划分主机房、操作监控室、UPS室等区域，并且在区域与区域之间采用防火墙进行物理隔离。 |
| 防水和防潮 | a）应采取措施防止雨水通过机房窗户、屋顶和墙壁渗透； | 机房采用封闭设计，无对外朝向的窗户，机房所在位置周边、上方均无用水设备，机房内无水管横穿，屋顶粉刷防水涂料，墙壁粉刷了耐燃性涂料，可有效防水、防潮。 |
| b）应采取措施防止机房内水蒸气结露和地下积水的转移与渗透； | 机房部署有英维克精密空调，控制机房湿度，可以有效防止风口结露。 |
| c）应安装对水敏感的检测仪表或元件，对机房进行防水检测和报警。 | 机房部署有漏水检测系统，在如空调下方、UPS室等处安装有漏水绳，发现漏水时进行报警。 |
| 防静电 | a）应采用防静电地板或地面并采用必要的接地防静电措施； | 机房门口铺设防尘胶，机房采用防静电地板，且机房所处的大楼已进行防雷接地处理。 |
| b）应采取措施防止静电的产生，例如采用静电消除器、佩戴防静电手环等。 | 机房人员作业前佩戴防静电手环进行静电消除，静电消除后进行设备操作。 |
| 温湿度控制 | a）应设置温湿度自动调节设施，使机房温湿度的变化在设备运行所允许的范围之内。 | 机房部署了英维克精密空调对温湿度进行控制，控制机房温度为23℃左右，湿度为50%左右。 |
| 电力供应 | a）应在机房供电线路上配置稳压器和过电压防护设备； | 机房供电室配备有稳压器和过电压保护装置。 |
| b）应提供短期的备用电力供应，至少满足设备在断电情况下的正常运行要求； | 机房配置有UPS系统，可满足断电情况下15分钟的电力供应。 |
| c）应设置冗余或并行的电力电缆线路为计算机系统供电。 | 机房采用两路市电，保证机房系统电力供应。 |
| 电磁防护 | a）电源线和通信线缆应隔离铺设，避免互相干扰； | 电源线和通信线缆隔离铺设，通信线缆铺设于机柜上方桥架内，避免互相干扰。 |
| b）应对关键设备实施电磁屏蔽。 | 未对机房关键设备实施电磁屏蔽措施。 |

|  |  |  |  |
| --- | --- | --- | --- |
| **测评项目** |  | **测评对象** | 安全物理环境 |
| **测评单位** |  | | |
| **测评地点** |  | | |
| **测评人员** |  | **配合人员** |  |
| **测评日期** | 2023.6.16 | | |
| **测评人员签字** |  | **配合人员签字** |  |

1.2. 云计算安全扩展要求部分

1.2.1. 阿里公共云机房

|  |  |  |
| --- | --- | --- |
| **安全控制点** | **测评指标** | **结果记录** |
| 基础设施位置 | a）应保证云计算基础设施位于中国境内。 | 客户为云租户，云计算基础设施安全由阿里云负责，阿里公共云已经通过等级保护第三级测评。 |

1.2.2. 世纪互联IDC机房

|  |  |  |
| --- | --- | --- |
| **安全控制点** | **测评指标** | **结果记录** |
| 基础设施位置 | a）应保证云计算基础设施位于中国境内。 | 经访谈及核查，世纪互联IDC机房不涉及云计算安全扩展要求，该项不适用。 |

|  |  |  |  |
| --- | --- | --- | --- |
| **测评项目** |  | **测评对象** | 安全物理环境 |
| **测评单位** |  | | |
| **测评地点** |  | | |
| **测评人员** |  | **配合人员** |  |
| **测评日期** | 2023.6.16 | | |
| **测评人员签字** |  | **配合人员签字** |  |

1.3. 移动互联安全扩展要求部分

1.3.1. 阿里公共云机房

|  |  |  |
| --- | --- | --- |
| **安全控制点** | **测评指标** | **结果记录** |
| 无线接入点的物理位置 | a）应为无线接入设备的安装选择合理位置，避免过度覆盖和电磁干扰。 | 经核查，阿里云公共云不涉及无线接入设备安装，故调整为不适用。 |

1.3.2. 世纪互联IDC机房

|  |  |  |
| --- | --- | --- |
| **安全控制点** | **测评指标** | **结果记录** |
| 无线接入点的物理位置 | a）应为无线接入设备的安装选择合理位置，避免过度覆盖和电磁干扰。 | 1、经访谈网络管理员，公司制定《分拨中心网络建设方案》，经核查建设方案，无线AP设备均采用吸顶式部署，无线AP之间间隔20米，经现场核查上海分拨中心无线AP部署情况与建设方案中规划要求一致；2、经查看H3C射频资源智能调整技术白皮书，针对无线AP实现自动功率调整及自动频宽调整等，能够有效降低电磁干扰。 |

2. 安全通信网络测评表

|  |  |  |  |
| --- | --- | --- | --- |
| **测评项目** |  | **测评对象** | 安全通信网络 |
| **测评单位** |  | | |
| **测评地点** |  | | |
| **测评人员** |  | **配合人员** |  |
| **测评日期** | 2023.6.15 | | |
| **测评人员签字** |  | **配合人员签字** |  |

2.1. 安全通用要求部分

4.1.1. 安全通信网络

|  |  |  |
| --- | --- | --- |
| **安全控制点** | **测评指标** | **结果记录** |
| 网络架构 | a）应保证网络设备的业务处理能力满足业务高峰期需要； | 1、通过查看阿里云公共云基础服务平台测评报告（报告编号：33011613016-00001-22-0001-01）中关于安全通信网络中总体评价：网络关键设备未出现宕机情况，设备业务处理能力满足业务高峰期需要；网络链路带宽高峰期使用率满足业务需求； 2、经与被测单位网络管理员访谈，目前阿里公共云虚拟网络服务满足业务高峰期需要，未出现因阿里公共云虚拟网络服务业务处理能力不足导致业务中断现象； 3、通过核查世纪互联IDC机房中核心交换机、负载均衡、出口防火墙、专线防火墙中近半个月的CPU使用率及内存使用率等使用情况，其中核心交换机中CPU最高率为10%、内存最高使用率为60%，负载均衡CPU最高使用率为9%，内存使用率最高为45%，出口防火墙CPU最高使用率为11%，内存使用率最高为40%，专线防火墙CPU最高使用率为10.5%，内存使用率最高为55%，经访谈核实，目前在监控系统中配置CPU告警阈值为70%，内存使用率告警阈值为80%，所有设备CPU及内存使用率均未达到设定预警值，能够满足业务高峰期需要。 |
| b）应保证网络各个部分的带宽满足业务高峰期需要； | 1、经现场核查，被测系统共两个出口，分别为世纪互联IDC机房互联网出口，带宽为500M；另一个出口为阿里公共云互联网出口，此处采购的阿里云弹性带宽服务，可按需扩容； 2、经现场查看监控系统中近1个月流量监控，世纪互联IDC机房互联网出口流量最高使用量为150M，占总带宽量30%； 3、阿里云与世界互联IDC机房间通过四条40G专线进行联通，每条40G专线链路带宽使用量最高为4G，占总带宽量10%； 4、世纪互联IDC机房中核心交换机处理设备为TB级设备，核查核心交换机上，针对大数据算法测试业务的服务进行了带宽限速，限定20M，优先保障业务流量通过： 5、查看阿里云公共云基础服务平台测评报告（报告编号：33011613016-00001-22-0001-01）中关于安全通信网络中总体评价：网络链路带宽高峰期使用率满足业务需求； 6、经与被测单位网络管理员访谈，目前整体网络带宽能够满足业务高峰期需要，未发生过因带宽不足导致业务中断情况； 综上，网络各个部分带宽满足业务高峰期需要。 |
| c）应划分不同的网络区域，并按照方便管理和控制的原则为各网络区域分配地址； | 经与网络管理员访谈及核查网络拓扑图，被测系统绘制了与实际网络一致的网络拓扑图，整体网络架构按照管理需求及业务需求分别划分互联网接入区，专线接入区、核心交换区、业务服务区、带外管理区、阿里公共云业务区共6个逻辑区域，同时由网络管理员按照区域划分在核心交换机中划分了不同的IP地址段，如：分别划分10.33.0.0、10.30.0.0、10.39.0.0等；在阿里公共云业务区中针对各业务功能模块单独创建42个安全组。 |
| d）应避免将重要网络区域部署在边界处，重要网络区域与其他网络区域之间应采取可靠的技术隔离手段； | 经现场核查，被测系统在重要网络区域边界处均部署了防火墙设备，并配置访问控制策略，如：互联网接入区边界部署出口防火墙（H3C SecPath F1000-E-G2）、专线接入区部署专线防火墙（H3C M9000）、带外管理区部署管理网防火墙（H3C SecPath F1000-E-G2）、阿里公共云业务区通过云防火墙（企业版）及配置安全组策略进行访问控制，经核查防火墙上的访问控制策略，默认情况下为拒绝所有通信，然后根据业务访问需求及管理需求配置访问控制规则，保证网络边界及区域之间的有效控制。 |
| e）应提供通信线路、关键网络设备和关键计算设备的硬件冗余，保证系统的可用性。 | 经核查拓扑图及资产清单，被测系统中核心交换机采用堆叠技术部署，出口防火墙、专线防火墙、管理网防火墙等采用HA冗余部署，业务服务器采用K8S容器部署，数据库采用集群方式部署，保证系统高可用性。 |
| 通信传输 | a）应采用校验技术或密码技术保证通信过程中数据的完整性； | 经核查，被测系统中网络设备、服务器等均采用SSH协议进行通信，安全设备及安全服务、业务系统均采用HTTPS协议进行通信，保证数据在通信过程中的完整性。 |
| b）应采用密码技术保证通信过程中数据的保密性。 | 经核查，被测系统中网络设备、服务器等均采用SSH协议进行通信，安全设备及安全服务、业务系统均采用HTTPS协议进行通信，保证数据在通信过程中的保密性。 |
| 可信验证 | a）可基于可信根对通信设备的系统引导程序、系统程序、重要配置参数和通信应用程序等进行可信验证，并在应用程序的关键执行环节进行动态可信验证，在检测到其可信性受到破坏后进行报警，并将验证结果形成审计记录送至安全管理中心。 | 未基于可信根对通信设备进行可信验证。 |

|  |  |  |  |
| --- | --- | --- | --- |
| **测评项目** |  | **测评对象** | 安全通信网络 |
| **测评单位** |  | | |
| **测评地点** |  | | |
| **测评人员** |  | **配合人员** |  |
| **测评日期** | 2023.6.15 | | |
| **测评人员签字** |  | **配合人员签字** |  |

2.2. 云计算安全扩展要求部分

2.2.1. 安全通信网络

|  |  |  |
| --- | --- | --- |
| **安全控制点** | **测评指标** | **结果记录** |
| 网络架构 | a）应保证云计算平台不承载高于其安全保护等级的业务应用系统； | 本次被测系统JMS综合物流平台系统安全保护等级为第三级，同时阿里公共云安全保护等级为第三级，阿里公共云未承载高于其安全保护等级的业务系统。 |
| b）应实现不同云服务客户虚拟网络之间的隔离； | 客户为云租户，云计算安全由阿里云负责，阿里公共云已经通过等级保护第三级测评。 |
| c）应具有根据云服务客户业务需求提供通信传输、边界防护、入侵防范等安全机制的能力； | 客户为云租户，云计算安全由阿里云负责，阿里公共云已经通过等级保护第三级测评。 |
| d）应具有根据云服务客户业务需求自主设置安全策略的能力，包括定义访问路径、选择安全组件、配置安全策略； | 客户为云租户，云计算安全由阿里云负责，阿里公共云已经通过等级保护第三级测评。 |
| e）应提供开放接口或开放性安全服务，允许云服务客户接入第三方安全产品或在云计算平台选择第三方安全服务。 | 客户为云租户，云计算安全由阿里云负责，阿里公共云已经通过等级保护第三级测评。 |

3. 安全区域边界测评表

|  |  |  |  |
| --- | --- | --- | --- |
| **测评项目** |  | **测评对象** | 安全区域边界 |
| **测评单位** |  | | |
| **测评地点** |  | | |
| **测评人员** |  | **配合人员** | 刘亮 |
| **测评日期** | 2023.6.15-2023.6.16 | | |
| **测评人员签字** |  | **配合人员签字** |  |

3.1. 安全通用要求部分

3.1.1. 互联网接入区

|  |  |  |
| --- | --- | --- |
| **安全控制点** | **测评指标** | **结果记录** |
| 边界防护 | a）应保证跨越边界的访问和数据流通过边界设备提供的受控接口进行通信； | 经现场访谈及核查出口防火墙（H3C SecPath F1000-E-G2）访问控制策略，在出口防火墙中针对跨越边界的访问及数据流通配置了访问控制策略。 |
| b）应能够对非授权设备私自联到内部网络的行为进行检查或限制； | 1、在物理边界方面，经现场访谈机房管理人员及核查物理机房，在机房门口安装有门禁系统，外部人员进出机房或接入设备时需进行申请、审批流程，通过审批后方可进入机房或接入设备，并且进出机房均由专人陪同，拒绝外部设备非授权私自接入网络中； 2、在技术层面，核查交换机及防火墙中各端口状态，未使用端口均为shutdown状态。 |
| c）应能够对内部用户非授权联到外部网络的行为进行检查或限制； | 经现场访谈网络管理员及核查出口防火墙（H3C SecPath F1000-E-G2）访问控制策略，因内部设备需要联到外部网络进行补丁修复或调用外部网络接口，因此开放内部用户访问外部网络权限，经现场核查出口防火墙中的访问控制策略，针对trust-untrust配置10条访问控制策略，如：ID108策略为内网10.33.130.0/24网段访问钉钉公网地址，同时ID102策略为拒绝内网10.33.130.0/24网段访问互联网。 |
| d）应限制无线网络的使用，保证无线网络通过受控的边界设备接入内部网络。 | 经现场访谈网络管理员，互联网边界区中未涉及无线网络使用，因此该项调整为不适用。 |
| 访问控制 | a）应在网络边界或区域之间根据访问控制策略设置访问控制规则，默认情况下除允许通信外受控接口拒绝所有通信； | 1、经现场访谈及核查出口防火墙（H3C SecPath F1000-E-G2）访问控制策略，在出口防火墙中针对网络边界的访问配置了相应的访问控制策略； 2、出口防火墙中最后一条访问控制策略为拒绝所有通信； 3、核查出口防火墙策略，目前共计55条策略，定义了trust、untrust、local，management域，针对域之间的访问制定了访问控制策略，可信任域之间访问控制粒度为IP地址段级，访问控制策略未达到端口级。 |
| b）应删除多余或无效的访问控制规则，优化访问控制列表，并保证访问控制规则数量最小化； | 经现场访谈及核查出口防火墙（H3C SecPath F1000-E-G2）访问控制策略，出口防火墙中根据管理需求及业务需求配置相应的策略，在配置访问控制策略时经过安全组及网络组沟通确认后进行配置，目前访问控制策略已经过优化确认，目前优化后策略共39条，所有策略均为有效策略。 |
| c）应对源地址、目的地址、源端口、目的端口和协议等进行检查，以允许/拒绝数据包进出； | 经现场访谈及核查出口防火墙（H3C SecPath F1000-E-G2）访问控制策略，在出口防火墙访问控制策略中能够对源安全域、目的安全域、类型、ID、描述、源地址、目的地址、服务、用户、动作、内容安全、命中次数、流量等字段进行检查，在动作字段中能够配置允许/拒绝通信策略。 |
| d）应能根据会话状态信息为进出数据流提供明确的允许/拒绝访问的能力； | 经现场访谈及核查出口防火墙（H3C SecPath F1000-E-G2）访问控制策略，在出口防火墙的访问控制策略的服务字段中根据协议类型、端口、会话状态信息等对进出数据流提供检查，在动作字段配置明确的允许/拒绝通信策略。 |
| e）应对进出网络的数据流实现基于应用协议和应用内容的访问控制。 | 经现场访谈及核查出口防火墙（H3C SecPath F1000-E-G2）访问控制策略，未对进出网络的数据流实现基于应用协议和应用内容的访问控制。 |
| 入侵防范 | a）应在关键网络节点处检测、防止或限制从外部发起的网络攻击行为； | 1、经现场访谈及核查出口防火墙（H3C SecPath F1000-E-G2）访问控制策略，出口防火墙中具备安全防护功能，在出口防火墙导航菜单栏中安全防护菜单中启用攻击防护策略，能够对从外部发起的攻击行为进行监测，发现外部攻击行为及时报警； 2、被测系统中部署了360AISA全流量威胁分析系统和360本地安全大脑，通过将被测系统中全部流量镜像发送到360AISA全流量威胁分析系统及360本地安全大脑中进行分析监测，发现入侵事件后及时通过钉钉报警，并且能够自动阻断。 |
| b）应在关键网络节点处检测、防止或限制从内部发起的网络攻击行为； | 经现场访谈及核查，被测系统中部署了360AISA全流量威胁分析系统和360本地安全大脑，通过将被测系统中全部流量镜像发送到360AISA全流量威胁分析系统及360本地安全大脑中进行分析监测，发现入侵事件后及时通过钉钉报警，并且能够实现自动阻断。 |
| c）应采取技术措施对网络行为进行分析，实现对网络攻击特别是新型网络攻击行为的分析； | 经现场访谈及核查，被测系统中部署了360AISA全流量威胁分析系统和360本地安全大脑，通过将被测系统中全部流量镜像发送到360AISA全流量威胁分析系统及360本地安全大脑中进行威胁分析（包括APT痕迹扫描、APT样本扫描、APT行为分析等）。 |
| d）当检测到攻击行为时，记录攻击源IP、攻击类型、攻击目标、攻击时间，在发生严重入侵事件时应提供报警。 | 1、经现场访谈及核查出口防火墙（H3C SecPath F1000-E-G2）防护策略，出口防火墙中攻击日志中会记录：时间、攻击类型、入安全域名称、目的IP地址、源IP地址等信息； 2、经现场访谈及核查360AISA全流量威胁分析系统及360本地安全大脑中入侵防护策略，检测到攻击行为时会记录：发生时间、事件名称、事件级别、源地址、目的地址、源端口、目的端口、原始日志等内容，发生严重入侵事件后通过钉钉报警。 |
| 恶意代码和垃圾邮件防范 | a）应在关键网络节点处对恶意代码进行检测和清除，并维护恶意代码防护机制的升级和更新； | 经现场访谈及核查，被测系统中部署青藤云天眼云镜安全防护软件，能够实时进行恶意代码检测，发现恶意代码及时进行隔离，同时配置恶意代码特征库更新策略，每天凌晨自动更新恶意代码特征库，但是未在网络层面部署防恶意代码软件或设备。 |
| b）应在关键网络节点处对垃圾邮件进行检测和防护，并维护垃圾邮件防护机制的升级和更新。 | 经现场访谈及核查，被测系统中不涉及邮件系统及邮件收发服务，故该项调整为不适用。 |
| 安全审计 | a）应在网络边界、重要网络节点进行安全审计，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； | 目前被测系统通过堡垒机（Jumpserver V2.23.4）对用户操作行为进行审计，360AISA全流量威胁分析系统及360本地安全大脑对入侵安全事件进行审计，同时出口防火墙（H3C SecPath F1000-E-G2）本地能够对用户操作行为及入侵事件进行审计。 |
| 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； | 1、经现场核查堡垒机（Jumpserver V2.23.4）中审计记录，堡垒机中用户操作行为审计记录包括：用户名、动作、资源类型、资源、远端地址、日期等；2、经现场核查出口防火墙（H3C SecPath F1000-E-G2）中审计记录，出口防火墙中攻击日志包括：时间、严重级别、攻击类型、动作类型、入安全域名称、目的地址、源地址等；用户操作日志包括：日期、时间、协议类型、IP地址、用户、命令详情；3、经现场查看360AISA全流量威胁分析系统及360本地安全大脑检测的审计记录，360AISA全流量威胁分析系统及360本地安全大脑检测到攻击行为时会记录：发生时间、事件名称、事件级别、源地址、目的地址、源端口、目的端口、原始日志等。 |
| 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； | 经现场核查堡垒机（Jumpserver V2.23.4）、出口防火墙（H3C SecPath F1000-E-G2）、360AISA全流量威胁分析系统及360本地安全大脑中审计模块中，所有用户均无权限对审计记录进行删除、修改，出口防火墙（H3C SecPath F1000-E-G2）中审计记录会实时传输至10.33.110.21进行备份；360AISA全流量威胁分析系统及360本地安全大脑中审计记录为流量分析记录，在本地永久保存；堡垒机中审计记录会在本地保存200天，但是未对审计记录进行备份。 |
| d）应能对远程访问的用户行为、访问互联网的用户行为等单独进行行为审计和数据分析。 | 经现场访谈网络管理员及核查，远程访问的用户行为通过堡垒机进行审计记录，同时随机抽取360AISA全流量威胁分析系统及360本地安全大脑中10.33.102.14和10.33.61.34的流量分析记录，能够对源地址、目的地址、源端口、目的端口等进行审计记录。 |
| 可信验证 | a）可基于可信根对边界设备的系统引导程序、系统程序、重要配置参数和边界防护应用程序等进行可信验证，并在应用程序的关键执行环节进行动态可信验证，在检测到其可信性受到破坏后进行报警，并将验证结果形成审计记录送至安全管理中心。 | 未基于可信根对边界设备进行可信验证。 |

3.1.2. 专线接入区

|  |  |  |
| --- | --- | --- |
| **安全控制点** | **测评指标** | **结果记录** |
| 边界防护 | a）应保证跨越边界的访问和数据流通过边界设备提供的受控接口进行通信； | 经现场访谈网络管理员，专线接入区主要用于阿里公共云与世纪互联IDC机房之间业务通信；经核查专线防火墙（H3C M9000）访问控制策略，在专线防火墙中针对跨越边界的访问及数据流通配置了访问控制策略，阿里云端的区域定义为untrust域，IDC机房定义为trust域，现场核查防火墙上存在26条策略，如存在云上测试网段访问idc测试网段，允许10.22.0.0/16访问10.21.0.0/16，存在默认策略为拒绝所有网络通信等。 |
| b）应能够对非授权设备私自联到内部网络的行为进行检查或限制； | 1、在物理边界方面，经现场访谈机房管理人员及核查物理机房，在机房门口安装有门禁系统，外部人员进出机房或接入设备时需进行申请、审批流程，通过审批后方可进入机房或接入设备，并且进出机房均由专人陪同，拒绝外部设备非授权私自接入网络中；2、在技术层面，核查交换机及防火墙中个端口状态，未使用端口均设置为shutdown。 |
| c）应能够对内部用户非授权联到外部网络的行为进行检查或限制； | 专线接入区主要用于阿里云与世纪互联IDC机房间的访问通信，主要为网络设备及专线防火墙设备，不存在服务器等计算设备，经现场访谈网络管理员及核查专线防火墙（H3C M9000）访问控制策略，防火墙上存在26条策略，存在默认策略为拒绝所有网络通信等，仅有符合放行的策略才能进行联通访问。 |
| d）应限制无线网络的使用，保证无线网络通过受控的边界设备接入内部网络。 | 经现场访谈网络管理员，世纪互联IDC机房中未涉及无线网络使用，因此该项调整为不适用。 |
| 访问控制 | a）应在网络边界或区域之间根据访问控制策略设置访问控制规则，默认情况下除允许通信外受控接口拒绝所有通信； | 1、经现场访谈网络管理员及核查专线防火墙（H3C M9000）访问控制策略，在专线防火墙中针对网络边界的访问配置了相应的访问控制策略； 2、专线防火墙中第一条访问控制策略为拒绝所有网络通信； 3、访问控制策略中访问控制粒度仅达到IP地址段级，未达到端口级。 |
| b）应删除多余或无效的访问控制规则，优化访问控制列表，并保证访问控制规则数量最小化； | 经现场访谈及核查专线防火墙（H3C M9000）访问控制策略，专线防火墙中根据管理需求及业务需求配置相应的策略，在配置访问控制策略时经过安全组及网络组沟通确认后进行配置，目前访问控制策略已经过优化确认，目前优化后策略共26条，所有策略均为有效策略。 |
| c）应对源地址、目的地址、源端口、目的端口和协议等进行检查，以允许/拒绝数据包进出； | 经现场访谈及核查专线防火墙（H3C M9000）访问控制策略，在专线防火墙访问控制策略中能够对源安全域、目的安全域、类型、ID、描述、源地址、目的地址、服务、用户、动作、内容安全、命中次数、流量等字段进行检查，在动作字段中能够配置允许/拒绝通信策略。 |
| d）应能根据会话状态信息为进出数据流提供明确的允许/拒绝访问的能力； | 经现场访谈及核查专线防火墙（H3C M9000）访问控制策略，在专线防火墙的访问控制策略的服务字段中根据协议类型、端口、会话状态信息等对进出数据流提供检查，在动作字段配置明确的允许/拒绝通信策略。 |
| e）应对进出网络的数据流实现基于应用协议和应用内容的访问控制。 | 针对进出网络的数据流均通过云端Web应用防火墙设备进行检测、过滤。 |
| 入侵防范 | a）应在关键网络节点处检测、防止或限制从外部发起的网络攻击行为； | 1、经现场访谈及核查专线防火墙（H3C M9000）访问控制策略，专线防火墙中具备安全防护功能，在专线防火墙导航菜单栏中安全防护菜单中启用攻击防护策略，能够对从外部发起的攻击行为进行监测，发现外部攻击行为及时报警； 2、被测系统中部署了360AISA全流量威胁分析系统和360本地安全大脑，通过将被测系统中全部流量镜像发送到360AISA全流量威胁分析系统及360本地安全大脑中进行分析监测，发现入侵事件后及时通过钉钉报警，并且能够自动阻断。 |
| b）应在关键网络节点处检测、防止或限制从内部发起的网络攻击行为； | 经现场访谈及核查，被测系统中部署了360AISA全流量威胁分析系统和360本地安全大脑，通过将被测系统中全部流量镜像发送到360AISA全流量威胁分析系统及360本地安全大脑中进行分析监测，发现入侵事件后及时通过钉钉报警，并且能够实现自动阻断。 |
| c）应采取技术措施对网络行为进行分析，实现对网络攻击特别是新型网络攻击行为的分析； | 经现场访谈及核查，被测系统中部署了360AISA全流量威胁分析系统和360本地安全大脑，通过将被测系统中全部流量镜像发送到360AISA全流量威胁分析系统及360本地安全大脑中进行威胁分析（包括APT痕迹扫描、APT样本扫描、APT行为分析等）。 |
| d）当检测到攻击行为时，记录攻击源IP、攻击类型、攻击目标、攻击时间，在发生严重入侵事件时应提供报警。 | 1、经现场访谈及核查专线防火墙（H3C M9000）防护策略，专线防火墙中攻击日志中会记录：时间、攻击类型、入安全域名称、目的IP地址、源IP地址等信息； 2、经现场访谈及核查360AISA全流量威胁分析系统及360本地安全大脑中入侵防护策略，检测到攻击行为时会记录：发生时间、事件名称、事件级别、源地址、目的地址、源端口、目的端口、原始日志等内容，发生严重入侵事件后通过钉钉报警。 |
| 恶意代码和垃圾邮件防范 | a）应在关键网络节点处对恶意代码进行检测和清除，并维护恶意代码防护机制的升级和更新； | 经现场访谈及核查，被测系统中部署青藤云天眼云镜安全防护软件，能够实时进行恶意代码检测，发现恶意代码及时进行隔离，同时配置恶意代码特征库更新策略，每天凌晨自动更新恶意代码特征库，但是未在网络层面部署防恶意代码软件或设备。 |
| b）应在关键网络节点处对垃圾邮件进行检测和防护，并维护垃圾邮件防护机制的升级和更新。 | 经现场访谈及核查，被测系统中不涉及邮件系统及邮件收发服务，故该项调整为不适用。 |
| 安全审计 | a）应在网络边界、重要网络节点进行安全审计，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； | 目前被测系统通过堡垒机（Jumpserver V2.23.4）对用户操作行为进行审计，360AISA全流量威胁分析系统及360本地安全大脑对入侵安全事件进行审计，同时专线防火墙（H3C M9000）能够对用户操作行为及入侵事件进行审计。 |
| 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； | 1、经现场核查堡垒机（Jumpserver V2.23.4）中审计记录，堡垒机中用户操作行为审计记录包括：用户名、动作、资源类型、资源、远端地址、日期等； 2、经现场核查专线防火墙（H3C M9000）中审计记录，专线防火墙中攻击日志包括：时间、严重级别、攻击类型、动作类型、入安全域名称、目的地址、源地址等；用户操作日志包括：日期、时间、协议类型、IP地址、用户、命令详情； 3、经现场查看360AISA全流量威胁分析系统及360本地安全大脑检测的审计记录，360AISA全流量威胁分析系统及360本地安全大脑检测到攻击行为时会记录：发生时间、事件名称、事件级别、源地址、目的地址、源端口、目的端口、原始日志等。 |
| 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； | 经现场核查堡垒机（Jumpserver V2.23.4）、专线防火墙（H3C M9000）、360AISA全流量威胁分析系统及360本地安全大脑中审计模块中，所有用户均无权限对审计记录进行删除、修改，专线防火墙（H3C M9000）中审计记录会实时传输至10.33.110.21进行备份；360AISA全流量威胁分析系统及360本地安全大脑中审计记录为流量分析记录，在本地永久保存；堡垒机中审计记录会在本地保存200天，但是未对审计记录进行备份。 |
| d）应能对远程访问的用户行为、访问互联网的用户行为等单独进行行为审计和数据分析。 | 经现场访谈网络管理员及核查，远程访问的用户行为通过堡垒机进行审计记录，同时随机抽取360AISA全流量威胁分析系统及360本地安全大脑中10.33.102.14和10.33.61.34的流量分析记录，能够对源地址、目的地址、源端口、目的端口等进行审计记录。 |
| 可信验证 | a）可基于可信根对边界设备的系统引导程序、系统程序、重要配置参数和边界防护应用程序等进行可信验证，并在应用程序的关键执行环节进行动态可信验证，在检测到其可信性受到破坏后进行报警，并将验证结果形成审计记录送至安全管理中心。 | 未基于可信根对边界设备进行可信验证。 |

3.1.3. 核心交换区

|  |  |  |
| --- | --- | --- |
| **安全控制点** | **测评指标** | **结果记录** |
| 边界防护 | a）应保证跨越边界的访问和数据流通过边界设备提供的受控接口进行通信； | 1、经现场访谈网络管理员，核心交换区用于整体网络中数据交换及网络流量分发；现场核查核心交换机（H3C LS-12504X-AF）VLAN划分及ACL访问控制策略配置，在核心交换机中根据业务需求及管理需求划分了66个VLAN，并配置ACL访问控制策略，实现对各区域的数据流的控制；2、跨越边界的访问和数据流主要基于在互联网接入区和专线接入区实现访问控制。 |
| b）应能够对非授权设备私自联到内部网络的行为进行检查或限制； | 1、在物理边界方面，经现场访谈机房管理人员及核查物理机房，在机房门口安装有门禁系统，外部人员进出机房或接入设备时需进行申请、审批流程，通过审批后方可进入机房或接入设备，并且进出机房均由专人陪同，拒绝外部设备非授权私自接入网络中；2、在技术层面，核查交换机及防火墙中个端口状态，未使用端口均设置为shutdown。 |
| c）应能够对内部用户非授权联到外部网络的行为进行检查或限制； | 经访谈网络管理员，核心交换区用于世纪互联IDC机房中整体网络中数据交换及网络流量分发，内部用户访问外部网络的行为主要基于互联网接入区及专线接入区防火墙配置访问策略，经核查出口防火墙（H3C SecPath F1000-E-G2）及专线防火墙（H3C M9000）中访问控制策略，已针对内部用户联到外部网络的行为配置相应策略。 |
| d）应限制无线网络的使用，保证无线网络通过受控的边界设备接入内部网络。 | 经现场访谈网络管理员，世纪互联IDC机房中未涉及无线网络使用，因此该项调整为不适用。 |
| 访问控制 | a）应在网络边界或区域之间根据访问控制策略设置访问控制规则，默认情况下除允许通信外受控接口拒绝所有通信； | 1、经现场访谈网络管理员及核查核心交换机（H3C LS-12504X-AF）VLAN划分及ACL访问控制策略配置，在核心交换机中根据业务需求及管理需求划分了66个VLAN，并配置ACL访问控制策略，所有通信均基于核心交换机ACL访问控制策略进行控制； 2、核心交换机中未使用的接口均处于shutdown状态； 3、ACL访问控制策略控制粒度为IP地址段级，未达到端口级。 |
| b）应删除多余或无效的访问控制规则，优化访问控制列表，并保证访问控制规则数量最小化； | 经现场访谈及核查核心交换机（H3C LS-12504X-AF）VLAN划分及ACL访问控制策略，核心交换机中根据管理需求及业务需求配置相应的策略，在配置访问控制策略时经过安全组及网络组沟通确认后进行配置，目前访问控制策略已经过优化确认，目前优化后策略共66条，所有策略均为有效策略。 |
| c）应对源地址、目的地址、源端口、目的端口和协议等进行检查，以允许/拒绝数据包进出； | 经现场访谈及核查核心交换机（H3C LS-12504X-AF）VLAN划分及ACL访问控制策略，在核心交换机中能够时间、来源IP、访问地址、请求内容和请求主要头部字段等进行检查或限制，并且配置明确允许/拒绝通信策略。 |
| d）应能根据会话状态信息为进出数据流提供明确的允许/拒绝访问的能力； | 经现场访谈及核查核心交换机（H3C LS-12504X-AF）VLAN划分及ACL访问控制策略，在核心交换机中根据请求内容及请求头部字段进行检查，并配置明确的允许/拒绝通信策略。 |
| e）应对进出网络的数据流实现基于应用协议和应用内容的访问控制。 | 针对进出网络的数据流均通过云端Web应用防火墙设备进行检测、过滤。 |
| 入侵防范 | a）应在关键网络节点处检测、防止或限制从外部发起的网络攻击行为； | 1、经现场访谈及核查，核心交换区入侵防范基于互联网接入区及专线接入区进行防护，在出口防火墙、专线防火墙中具备安全防护功能，能够对从外部发起的攻击行为进行监测； 2、被测系统中部署了360AISA全流量威胁分析系统和360本地安全大脑，通过将被测系统中全部流量镜像发送到360AISA全流量威胁分析系统及360本地安全大脑中进行分析监测，发现入侵事件后及时通过钉钉报警，并且能够自动阻断。 |
| b）应在关键网络节点处检测、防止或限制从内部发起的网络攻击行为； | 经现场访谈及核查，被测系统中部署了360AISA全流量威胁分析系统和360本地安全大脑，通过将被测系统中全部流量镜像发送到360AISA全流量威胁分析系统及360本地安全大脑中进行分析监测，发现入侵事件后及时通过钉钉报警，并且能够实现自动阻断。 |
| c）应采取技术措施对网络行为进行分析，实现对网络攻击特别是新型网络攻击行为的分析； | 经现场访谈及核查，被测系统中部署了360AISA全流量威胁分析系统和360本地安全大脑，通过将被测系统中全部流量镜像发送到360AISA全流量威胁分析系统及360本地安全大脑中进行威胁分析（包括APT痕迹扫描、APT样本扫描、APT行为分析等）。 |
| d）当检测到攻击行为时，记录攻击源IP、攻击类型、攻击目标、攻击时间，在发生严重入侵事件时应提供报警。 | 1、经现场访谈及核查，核心交换区入侵防范基于互联网接入区及专线接入区进行防护，出口防火墙和专线防火墙中攻击日志中会记录：时间、攻击类型、入安全域名称、目的IP地址、源IP地址等信息； 2、360AISA全流量威胁分析系统及360本地安全大脑检测到攻击行为时会记录：发生时间、事件名称、事件级别、源地址、目的地址、源端口、目的端口、原始日志等内容。 |
| 恶意代码和垃圾邮件防范 | a）应在关键网络节点处对恶意代码进行检测和清除，并维护恶意代码防护机制的升级和更新； | 经现场访谈及核查，被测系统中部署青藤云天眼云镜安全防护软件，能够实时进行恶意代码检测，发现恶意代码及时进行隔离，同时配置恶意代码特征库更新策略，每天凌晨自动更新恶意代码特征库，但是未在网络层面部署防恶意代码软件或设备。 |
| b）应在关键网络节点处对垃圾邮件进行检测和防护，并维护垃圾邮件防护机制的升级和更新。 | 经现场访谈及核查，被测系统中不涉及邮件系统及邮件收发服务，故该项调整为不适用。 |
| 安全审计 | a）应在网络边界、重要网络节点进行安全审计，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； | 目前被测系统通过堡垒机（Jumpserver V2.23.4）对用户操作行为进行审计，360AISA全流量威胁分析系统及360本地安全大脑对入侵安全事件进行审计，出口防火墙（H3C SecPath F1000-E-G2）、专线防火墙（H3C M9000）能够在网络边界对用户操作行为及入侵事件进行审计，核心交换机（H3C LS-12504X-AF）中能够对用户操作行为等进行审计记录。 |
| 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； | 1、经现场核查堡垒机（Jumpserver V2.23.4）中审计记录，堡垒机中用户操作行为审计记录包括：用户名、动作、资源类型、资源、远端地址、日期等； 2、经现场核查出口防火墙（H3C SecPath F1000-E-G2）中审计记录，出口防火墙中攻击日志包括：时间、严重级别、攻击类型、动作类型、入安全域名称、目的地址、源地址等；用户操作日志包括：日期、时间、协议类型、IP地址、用户、命令详情； 3、经现场核查专线防火墙（H3C M9000）中审计记录，出口防火墙中攻击日志包括：时间、严重级别、攻击类型、动作类型、入安全域名称、目的地址、源地址等；用户操作日志包括：日期、时间、协议类型、IP地址、用户、命令详情； 4、经现场查看360AISA全流量威胁分析系统及360本地安全大脑检测的审计记录，360AISA全流量威胁分析系统及360本地安全大脑检测到攻击行为时会记录：发生时间、事件名称、事件级别、源地址、目的地址、源端口、目的端口、原始日志等； 5、经核查核心交换机（H3C LS-12504X-AF）中审计记录，包括：日期、时间、协议类型、IP地址、用户、命令详情等。 |
| 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、经现场核查堡垒机（Jumpserver V2.23.4）、出口防火墙（H3C SecPath F1000-E-G2）、专线防火墙（H3C M9000）、360AISA全流量威胁分析系统及360本地安全大脑、核心交换机（H3C LS-12504X-AF）的审计模块中，所有用户均无权限对审计记录进行删除、修改； 2、出口防火墙（H3C SecPath F1000-E-G2）、专线防火墙（H3C M9000）、核心交换机（H3C LS-12504X-AF）中审计记录会实时传输至10.33.110.21进行备份；360AISA全流量威胁分析系统及360本地安全大脑中审计记录为流量分析记录，共部署7个存储节点实现审计记录冷备及热备；堡垒机中审计记录会在本地保存200天，但是未对审计记录进行备份。 |
| d）应能对远程访问的用户行为、访问互联网的用户行为等单独进行行为审计和数据分析。 | 经现场访谈网络管理员及核查，远程访问的用户行为通过堡垒机进行审计记录，同时随机抽取360AISA全流量威胁分析系统及360本地安全大脑中10.33.102.14和10.33.61.34的流量分析记录，能够对源地址、目的地址、源端口、目的端口等进行审计记录。 |
| 可信验证 | a）可基于可信根对边界设备的系统引导程序、系统程序、重要配置参数和边界防护应用程序等进行可信验证，并在应用程序的关键执行环节进行动态可信验证，在检测到其可信性受到破坏后进行报警，并将验证结果形成审计记录送至安全管理中心。 | 未基于可信根对边界设备进行可信验证。 |

3.1.4. 业务服务区

|  |  |  |
| --- | --- | --- |
| **安全控制点** | **测评指标** | **结果记录** |
| 边界防护 | a）应保证跨越边界的访问和数据流通过边界设备提供的受控接口进行通信； | 经访谈网络管理员，业务服务区用于部署业务服务器及数据库服务器等，对跨域边界的访问和数据流基于在核心交换机中配置的ACL访问控制策略进行限制，现场核查核心交换机（H3C LS-12504X-AF）VLAN划分及ACL访问控制策略配置，在核心交换机中根据业务需求及管理需求划分了66个VLAN，并配置ACL访问控制策略，实现对IDC机房各计算、存储区域的数据流的控制； 2、跨越边界的访问和数据流主要基于在互联网接入区和专线接入区实现访问控制。 |
| b）应能够对非授权设备私自联到内部网络的行为进行检查或限制； | 1、在物理边界方面，经现场访谈机房管理人员及核查物理机房，在机房门口安装有门禁系统，外部人员进出机房或接入设备时需进行申请、审批流程，通过审批后方可进入机房或接入设备，并且进出机房均由专人陪同，拒绝外部设备非授权私自接入网络中；2、在技术层面，核查交换机及防火墙中个端口状态，未使用端口均设置为shutdown。 |
| c）应能够对内部用户非授权联到外部网络的行为进行检查或限制； | 经访谈网络管理员，业务服务区用于部署业务服务器及数据库服务器等，内部用户访问外部网络的行为主要基于互联网接入区及专线接入区防火墙配置访问策略，经核查出口防火墙（H3C SecPath F1000-E-G2）及专线防火墙（H3C M9000）中访问控制策略，已针对内部用户联到外部网络的行为配置相应策略。 |
| d）应限制无线网络的使用，保证无线网络通过受控的边界设备接入内部网络。 | 经现场访谈网络管理员，世纪互联IDC机房中未涉及无线网络使用，因此该项调整为不适用。 |
| 访问控制 | a）应在网络边界或区域之间根据访问控制策略设置访问控制规则，默认情况下除允许通信外受控接口拒绝所有通信； | 1、经现场访谈网络管理员，业务服务区的访问控制基于核心交换机中配置ACL访问控制策略进行控制，经核查核心交换机（H3C LS-12504X-AF）VLAN划分及ACL访问控制策略配置，在核心交换机中根据业务需求及管理需求划分了66个VLAN，并配置ACL访问控制策略，所有通信均基于核心交换机ACL访问控制策略进行控制； 2、核心交换机中未使用的接口均处于shutdown状态； 3、ACL访问控制策略控制粒度为IP地址段级，未达到端口级。 |
| b）应删除多余或无效的访问控制规则，优化访问控制列表，并保证访问控制规则数量最小化； | 经现场访谈网络管理员，业务服务区的访问控制基于核心交换机中配置ACL访问控制策略进行控制，经现场核查核心交换机（H3C LS-12504X-AF）VLAN划分及ACL访问控制策略，核心交换机中根据管理需求及业务需求配置相应的策略，在配置访问控制策略时经过安全组及网络组沟通确认后进行配置，目前访问控制策略已经过优化确认，目前优化后策略共66条，所有策略均为有效策略。 |
| c）应对源地址、目的地址、源端口、目的端口和协议等进行检查，以允许/拒绝数据包进出； | 经现场访谈网络管理员，业务服务区的访问控制基于核心交换机中配置ACL访问控制策略进行控制，经现场核查核心交换机（H3C LS-12504X-AF）VLAN划分及ACL访问控制策略，在核心交换机中能够时间、来源IP、访问地址、请求内容和请求主要头部字段等进行检查或限制，并且配置明确允许/拒绝通信策略。 |
| d）应能根据会话状态信息为进出数据流提供明确的允许/拒绝访问的能力； | 经现场访谈网络管理员，业务服务区的访问控制基于核心交换机中配置ACL访问控制策略进行控制，经现场核查核心交换机（H3C LS-12504X-AF）VLAN划分及ACL访问控制策略，在核心交换机中根据请求内容及请求头部字段进行检查，并配置明确的允许/拒绝通信策略。 |
| e）应对进出网络的数据流实现基于应用协议和应用内容的访问控制。 | 针对进出网络的数据流均通过云端Web应用防火墙设备进行检测、过滤。 |
| 入侵防范 | a）应在关键网络节点处检测、防止或限制从外部发起的网络攻击行为； | 1、经现场访谈及核查，业务服务区边界入侵防范基于互联网接入区及专线接入区进行防护，在出口防火墙、专线防火墙中具备安全防护功能，能够对从外部发起的攻击行为进行监测； 2、被测系统中部署了360AISA全流量威胁分析系统和360本地安全大脑，通过将被测系统中全部流量镜像发送到360AISA全流量威胁分析系统及360本地安全大脑中进行分析监测，发现入侵事件后及时通过钉钉报警，并且能够自动阻断。 |
| b）应在关键网络节点处检测、防止或限制从内部发起的网络攻击行为； | 经现场访谈及核查，被测系统中部署了360AISA全流量威胁分析系统和360本地安全大脑，通过将被测系统中全部流量镜像发送到360AISA全流量威胁分析系统及360本地安全大脑中进行分析监测，发现入侵事件后及时通过钉钉报警，并且能够实现自动阻断。 |
| c）应采取技术措施对网络行为进行分析，实现对网络攻击特别是新型网络攻击行为的分析； | 经现场访谈及核查，被测系统中部署了360AISA全流量威胁分析系统和360本地安全大脑，通过将被测系统中全部流量镜像发送到360AISA全流量威胁分析系统及360本地安全大脑中进行威胁分析（包括APT痕迹扫描、APT样本扫描、APT行为分析等）。 |
| d）当检测到攻击行为时，记录攻击源IP、攻击类型、攻击目标、攻击时间，在发生严重入侵事件时应提供报警。 | 1、经现场访谈及核查，业务服务区入侵防范基于互联网接入区及专线接入区进行防护，出口防火墙和专线防火墙中攻击日志中会记录：时间、攻击类型、入安全域名称、目的IP地址、源IP地址等信息； 2、360AISA全流量威胁分析系统及360本地安全大脑检测到攻击行为时会记录：发生时间、事件名称、事件级别、源地址、目的地址、源端口、目的端口、原始日志等内容。 |
| 恶意代码和垃圾邮件防范 | a）应在关键网络节点处对恶意代码进行检测和清除，并维护恶意代码防护机制的升级和更新； | 经现场访谈及核查，被测系统中部署青藤云天眼云镜安全防护软件，能够实时进行恶意代码检测，发现恶意代码及时进行隔离，同时配置恶意代码特征库更新策略，每天凌晨自动更新恶意代码特征库。 |
| b）应在关键网络节点处对垃圾邮件进行检测和防护，并维护垃圾邮件防护机制的升级和更新。 | 经现场访谈及核查，被测系统中不涉及邮件系统及邮件收发服务，故该项调整为不适用。 |
| 安全审计 | a）应在网络边界、重要网络节点进行安全审计，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； | 目前被测系统通过堡垒机（Jumpserver V2.23.4）对用户操作行为进行审计，360AISA全流量威胁分析系统及360本地安全大脑对入侵安全事件进行审计，出口防火墙（H3C SecPath F1000-E-G2）、专线防火墙（H3C M9000）能够在网络边界对用户操作行为及入侵事件进行审计，核心交换机（H3C LS-12504X-AF）中能够对用户操作行为等进行审计记录。 |
| 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； | 1、经现场核查堡垒机（Jumpserver V2.23.4）中审计记录，堡垒机中用户操作行为审计记录包括：用户名、动作、资源类型、资源、远端地址、日期等； 2、经现场核查出口防火墙（H3C SecPath F1000-E-G2）中审计记录，出口防火墙中攻击日志包括：时间、严重级别、攻击类型、动作类型、入安全域名称、目的地址、源地址等；用户操作日志包括：日期、时间、协议类型、IP地址、用户、命令详情； 3、经现场核查专线防火墙（H3C M9000）中审计记录，出口防火墙中攻击日志包括：时间、严重级别、攻击类型、动作类型、入安全域名称、目的地址、源地址等；用户操作日志包括：日期、时间、协议类型、IP地址、用户、命令详情； 4、经现场查看360AISA全流量威胁分析系统及360本地安全大脑检测的审计记录，360AISA全流量威胁分析系统及360本地安全大脑检测到攻击行为时会记录：发生时间、事件名称、事件级别、源地址、目的地址、源端口、目的端口、原始日志等； 5、经核查核心交换机（H3C LS-12504X-AF）中审计记录，包括：日期、时间、协议类型、IP地址、用户、命令详情等。 |
| 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、经现场核查堡垒机（Jumpserver V2.23.4）、出口防火墙（H3C SecPath F1000-E-G2）、专线防火墙（H3C M9000）、360AISA全流量威胁分析系统及360本地安全大脑、核心交换机（H3C LS-12504X-AF）的审计模块中，所有用户均无权限对审计记录进行删除、修改，2、出口防火墙（H3C SecPath F1000-E-G2）、专线防火墙（H3C M9000）、核心交换机（H3C LS-12504X-AF）中审计记录会实时传输至10.33.110.21进行备份；360AISA全流量威胁分析系统及360本地安全大脑中审计记录为流量分析记录，共部署7个存储节点实现审计记录冷备及热备，但是堡垒机中审计记录会在本地保存200天，但是未对审计记录进行备份。 |
| d）应能对远程访问的用户行为、访问互联网的用户行为等单独进行行为审计和数据分析。 | 经现场访谈网络管理员及核查，远程访问的用户行为通过堡垒机进行审计记录，同时随机抽取360AISA全流量威胁分析系统及360本地安全大脑中10.33.102.14和10.33.61.34的流量分析记录，能够对源地址、目的地址、源端口、目的端口等进行审计记录。 |
| 可信验证 | a）可基于可信根对边界设备的系统引导程序、系统程序、重要配置参数和边界防护应用程序等进行可信验证，并在应用程序的关键执行环节进行动态可信验证，在检测到其可信性受到破坏后进行报警，并将验证结果形成审计记录送至安全管理中心。 | 未基于可信根对边界设备进行可信验证。 |

3.1.5. 带外管理区

|  |  |  |
| --- | --- | --- |
| **安全控制点** | **测评指标** | **结果记录** |
| 边界防护 | a）应保证跨越边界的访问和数据流通过边界设备提供的受控接口进行通信； | 经现场访谈网络管理员，带外管理区用于安全运维管理，经核查管理网防火墙（H3C SecPath F1000-E-G2）访问控制策略，在防火墙中针对跨越区域边界的访问及数据流通配置了访问控制策略，如：业务服务内网网段到带外管理区之间的通信全放行，默认策略为拒绝所有网络通信等。 |
| b）应能够对非授权设备私自联到内部网络的行为进行检查或限制； | 1、在物理边界方面，经现场访谈机房管理人员及核查物理机房，在机房门口安装有门禁系统，外部人员进出机房或接入设备时需进行申请、审批流程，通过审批后方可进入机房或接入设备，并且进出机房均由专人陪同，拒绝外部设备非授权私自接入网络中； 2、在技术层面，核查交换机及防火墙中个端口状态，未使用端口均设置为shutdown。 |
| c）应能够对内部用户非授权联到外部网络的行为进行检查或限制； | 经访谈网络管理员，带外管理区用于整体网络安全运维管理，核查管理网防火墙（H3C SecPath F1000-E-G2）访问控制策略，均为带外管理区与其他逻辑区域之间的策略，内部用户访问外部网络的行为主要基于互联网接入区及专线接入区防火墙配置访问策略，经核查出口防火墙（H3C SecPath F1000-E-G2）及专线防火墙（H3C M9000）中访问控制策略，已针对内部用户联到外部网络的行为配置相应策略。 |
| d）应限制无线网络的使用，保证无线网络通过受控的边界设备接入内部网络。 | 经现场访谈网络管理员，世纪互联IDC机房中未涉及无线网络使用，因此该项调整为不适用。 |
| 访问控制 | a）应在网络边界或区域之间根据访问控制策略设置访问控制规则，默认情况下除允许通信外受控接口拒绝所有通信； | 1、经现场访谈及核查管理网防火墙（H3C SecPath F1000-E-G2）访问控制策略，在管理网防火墙中针对网络边界的访问配置了相应的访问控制策略，访问控制策略分别为带外管理区与核心交换区、业务服务区、互联网接入区、专线接入区之间的通信控制； 2、管理网防火墙中最后一条访问控制策略为拒绝所有通信； 3、管理网防火墙中访问控制粒度为IP地址段级，未达到端口级。 |
| b）应删除多余或无效的访问控制规则，优化访问控制列表，并保证访问控制规则数量最小化； | 经现场访谈及核查管理网防火墙（H3C SecPath F1000-E-G2）访问控制策略，管理网防火墙中根据管理需求及业务需求配置相应的策略，在配置访问控制策略时经过安全组及网络组沟通确认后进行配置，目前访问控制策略已经过优化确认。 |
| c）应对源地址、目的地址、源端口、目的端口和协议等进行检查，以允许/拒绝数据包进出； | 经现场访谈及核查管理网防火墙（H3C SecPath F1000-E-G2）访问控制策略，在管理网防火墙访问控制策略中能够对源安全域、目的安全域、类型、ID、描述、源地址、目的地址、服务、用户、动作、内容安全、命中次数、流量等字段进行检查，在动作字段中能够配置允许/拒绝通信策略。 |
| d）应能根据会话状态信息为进出数据流提供明确的允许/拒绝访问的能力； | 经现场访谈及核查管理网防火墙（H3C SecPath F1000-E-G2）访问控制策略，在管理网防火墙的访问控制策略的服务字段中根据协议类型、端口、会话状态信息等对进出数据流提供检查，在动作字段配置明确的允许/拒绝通信策略。 |
| e）应对进出网络的数据流实现基于应用协议和应用内容的访问控制。 | 针对进出网络的数据流均通过云端Web应用防火墙设备进行检测、过滤。 |
| 入侵防范 | a）应在关键网络节点处检测、防止或限制从外部发起的网络攻击行为； | 1、经现场访谈及核查管理网防火墙（H3C SecPath F1000-E-G2）访问控制策略，在管理网防火墙导航菜单栏中安全防护菜单中启用攻击防护策略，能够对从外部发起的攻击行为进行监测，发现外部攻击行为及时报警； 2、被测系统中部署了360AISA全流量威胁分析系统和360本地安全大脑，通过将被测系统中全部流量镜像发送到360AISA全流量威胁分析系统及360本地安全大脑中进行分析监测，发现入侵事件后及时通过钉钉报警，并且能够自动阻断。 |
| b）应在关键网络节点处检测、防止或限制从内部发起的网络攻击行为； | 经现场访谈及核查，被测系统中部署了360AISA全流量威胁分析系统和360本地安全大脑，通过将被测系统中全部流量镜像发送到360AISA全流量威胁分析系统及360本地安全大脑中进行分析监测，发现入侵事件后及时通过钉钉报警，并且能够实现自动阻断。 |
| c）应采取技术措施对网络行为进行分析，实现对网络攻击特别是新型网络攻击行为的分析； | 经现场访谈及核查，被测系统中部署了360AISA全流量威胁分析系统和360本地安全大脑，通过将被测系统中全部流量镜像发送到360AISA全流量威胁分析系统及360本地安全大脑中进行威胁分析（包括APT痕迹扫描、APT样本扫描、APT行为分析等）。 |
| d）当检测到攻击行为时，记录攻击源IP、攻击类型、攻击目标、攻击时间，在发生严重入侵事件时应提供报警。 | 1、经现场访谈及核查管理网防火墙（H3C SecPath F1000-E-G2）防护策略，管理网防火墙中攻击日志中会记录：时间、攻击类型、入安全域名称、目的IP地址、源IP地址等信息； 2、经现场访谈及核查360AISA全流量威胁分析系统及360本地安全大脑中入侵防护策略，检测到攻击行为时会记录：发生时间、事件名称、事件级别、源地址、目的地址、源端口、目的端口、原始日志等内容，发生严重入侵事件后通过钉钉报警。 |
| 恶意代码和垃圾邮件防范 | a）应在关键网络节点处对恶意代码进行检测和清除，并维护恶意代码防护机制的升级和更新； | 经现场访谈及核查，被测系统中部署青藤云天眼云镜安全防护软件，能够实时进行恶意代码检测，发现恶意代码及时进行隔离，同时配置恶意代码特征库更新策略，每天凌晨自动更新恶意代码特征库，但是未在网络层面部署防恶意代码软件或设备。 |
| b）应在关键网络节点处对垃圾邮件进行检测和防护，并维护垃圾邮件防护机制的升级和更新。 | 经现场访谈及核查，被测系统中不涉及邮件系统及邮件收发服务，故该项调整为不适用。 |
| 安全审计 | a）应在网络边界、重要网络节点进行安全审计，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； | 目前被测系统通过堡垒机（Jumpserver V2.23.4）对用户操作行为进行审计，360AISA全流量威胁分析系统及360本地安全大脑对入侵安全事件进行审计，同时管理网防火墙（H3C SecPath F1000-E-G2）本地能够对用户操作行为及入侵事件进行审计。 |
| 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； | 1、经现场核查堡垒机（Jumpserver V2.23.4）中审计记录，堡垒机中用户操作行为审计记录包括：用户名、动作、资源类型、资源、远端地址、日期等； 2、经现场核查管理网防火墙（H3C SecPath F1000-E-G2）中审计记录，管理网防火墙中攻击日志包括：时间、严重级别、攻击类型、动作类型、入安全域名称、目的地址、源地址等；用户操作日志包括：日期、时间、协议类型、IP地址、用户、命令详情； 3、经现场查看360AISA全流量威胁分析系统及360本地安全大脑检测的审计记录，360AISA全流量威胁分析系统及360本地安全大脑检测到攻击行为时会记录：发生时间、事件名称、事件级别、源地址、目的地址、源端口、目的端口、原始日志等。 |
| 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； | 经现场核查堡垒机（Jumpserver V2.23.4）、管理网防火墙（H3C SecPath F1000-E-G2）、360AISA全流量威胁分析系统及360本地安全大脑中审计模块中，所有用户均无权限对审计记录进行删除、修改，管理网防火墙（H3C SecPath F1000-E-G2）中审计记录会实时传输至10.33.110.21进行备份；360AISA全流量威胁分析系统及360本地安全大脑中审计记录为流量分析记录，在本地永久保存，堡垒机中审计记录会在本地保存200天，但是未对审计记录进行备份。 |
| d）应能对远程访问的用户行为、访问互联网的用户行为等单独进行行为审计和数据分析。 | 经现场访谈网络管理员及核查，远程访问的用户行为通过堡垒机进行审计记录，同时随机抽取360AISA全流量威胁分析系统及360本地安全大脑中10.33.102.14和10.33.61.34的流量分析记录，能够对源地址、目的地址、源端口、目的端口等进行审计记录。 |
| 可信验证 | a）可基于可信根对边界设备的系统引导程序、系统程序、重要配置参数和边界防护应用程序等进行可信验证，并在应用程序的关键执行环节进行动态可信验证，在检测到其可信性受到破坏后进行报警，并将验证结果形成审计记录送至安全管理中心。 | 未基于可信根对边界设备进行可信验证。 |

3.1.6. 阿里公共云业务区

|  |  |  |
| --- | --- | --- |
| **安全控制点** | **测评指标** | **结果记录** |
| 边界防护 | a）应保证跨越边界的访问和数据流通过边界设备提供的受控接口进行通信； | 经现场访谈网络管理员及核查SLB、安全组策略，在阿里公共云网络边界处部署Web应用防火墙、SLB、云防火墙等，外部用户访问时首先访问的SLB，在SLB中仅开放固定IP地址+端口（80/443端口），拒绝访问其他端口，保证跨越边界的访问和数据流通过边界设备提供接口进行通信。 |
| b）应能够对非授权设备私自联到内部网络的行为进行检查或限制； | 经现场访谈网络管理员及核查SLB、安全组策略，在SLB策略中仅允许互联网用户通过80/443端口进行业务请求；在阿里公共云安全组中配置入方向策略，管理用户仅能通过指定对虚拟实例等进行运维管理，拒绝外部非授权设备私自联到内部网络。如：允许10.66.70.120/24（IDC专线地址），10.30.19.0/24 （云上跳板机网段），10.33.110.0/24（IDC机房运维段）等与阿里公共云进行通信。 |
| c）应能够对内部用户非授权联到外部网络的行为进行检查或限制； | 经现场核查阿里公共云安全组出方向策略，该区域内对外安全组策略中未对内部用户非授权联到外部网的行为进行检查或限制。 |
| d）应限制无线网络的使用，保证无线网络通过受控的边界设备接入内部网络。 | 经访谈及核查，阿里公共云业务区未涉及无线网络使用，因此该项调整为不适用 |
| 访问控制 | a）应在网络边界或区域之间根据访问控制策略设置访问控制规则，默认情况下除允许通信外受控接口拒绝所有通信； | 1、经现场访谈网络管理员及核查SLB、安全组策略，目前共划分了49个安全组，现场核k8s\_sg\_2安全组，入方向针对管理网段开放10.30.19.0/24，10.33.110.0/24，办公网针对特殊的运维管理需求，如办公网网段访问10.30.10.204，针对外网用户访问80、443端口采用白名单放行机制； 2、阿里公共云业务区与专线接入区通信时，在安全组策略中针对世纪互联IDC机房IP地址段（10.33.0.0、10.36.0.0等）添加放行策略，访问控制粒度未达到端口级。 |
| b）应删除多余或无效的访问控制规则，优化访问控制列表，并保证访问控制规则数量最小化； | 经现场访谈网络管理员及核查阿里云SLB及安全组策略，目前SLB及安全组策略中均根据管理需求及业务需求配置相应的策略，在配置访问控制策略时经过安全组及网络组沟通确认后进行配置，目前访问控制策略已经过优化确认，目前优化后策略SLB中对外提供访问控制策略共216条，安全组共42个。 |
| c）应对源地址、目的地址、源端口、目的端口和协议等进行检查，以允许/拒绝数据包进出； | 经现场访谈网络管理员及核查阿里云SLB及安全组策略，阿里云SLB及安全组策略中能够对授权策略、协议类型、端口范围、授权类型、授权对象、描述、优先级、创建时间、操作等内容进行检查限制，并提供明确允许/拒绝通信策略。 |
| d）应能根据会话状态信息为进出数据流提供明确的允许/拒绝访问的能力； | 经现场访谈网络管理员及核查阿里云SLB及安全组策略，在授权策略字段中能够对进出数据流提供明确的允许/拒绝访问的能力。 |
| e）应对进出网络的数据流实现基于应用协议和应用内容的访问控制。 | 经现场访谈网络管理员及核查阿里云SLB及安全组策略，在阿里公共云采购并部署了Web应用防火墙，在Web应用防火墙中启用了基于HTTP/HTTPS协议的访问控制策略。 |
| 入侵防范 | a）应在关键网络节点处检测、防止或限制从外部发起的网络攻击行为； | 经现场访谈网络管理员及核查阿里云SLB及安全组策略，Web应用防火墙及云防火墙中均具备入侵防御功能，能够对从外部发起的网络攻击行为进行实时监测，发现入侵攻击事件及时进行阻断，并提供钉钉报警，现场查看网络管理员钉钉记录中，具备实时告警信息。 |
| b）应在关键网络节点处检测、防止或限制从内部发起的网络攻击行为； | 经现场访谈网络管理员及核查阿里云SLB及安全组策略，Web应用防火墙及云防火墙中均具备入侵防御功能，能够对从内部发起的网络攻击行为进行实时监测，发现入侵攻击事件及时进行阻断，并提供钉钉报警，现场查看网络管理员钉钉记录中，具备实时告警信息。 |
| c）应采取技术措施对网络行为进行分析，实现对网络攻击特别是新型网络攻击行为的分析； | 经现场访谈及核查，被测系统中部署了360AISA全流量威胁分析系统和360本地安全大脑，通过将被测系统中全部流量镜像发送到360AISA全流量威胁分析系统及360本地安全大脑中进行威胁分析（包括APT痕迹扫描、APT样本扫描、APT行为分析等）。 |
| d）当检测到攻击行为时，记录攻击源IP、攻击类型、攻击目标、攻击时间，在发生严重入侵事件时应提供报警。 | Web应用防火墙检测到攻击行为时，可以记录攻击IP、所属地区、攻击时间、攻击URL、攻击类型、请求方法、请求参数以及规则动作等，同时可以通过钉钉进行告警。 |
| 恶意代码和垃圾邮件防范 | a）应在关键网络节点处对恶意代码进行检测和清除，并维护恶意代码防护机制的升级和更新； | 经现场访谈及核查，被测系统中部署青藤云天眼云镜安全防护软件，能够实时进行恶意代码检测，发现恶意代码及时进行隔离，同时配置恶意代码特征库更新策略，每天凌晨自动更新恶意代码特征库，但是未在网络层面部署防恶意代码软件或设备。 |
| b）应在关键网络节点处对垃圾邮件进行检测和防护，并维护垃圾邮件防护机制的升级和更新。 | 经现场访谈及核查，被测系统中不涉及邮件系统及邮件收发服务，故该项调整为不适用。 |
| 安全审计 | a）应在网络边界、重要网络节点进行安全审计，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； | 目前被测系统通过阿里云控制台、堡垒机（Jumpserver V2.23.4）对用户操作行为进行审计，通过云防火墙、Web应用防火墙对入侵事件进行安全审计。 |
| 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； | 1、经核查阿里云控制台审计记录包括：事件时间、地域、错误代码、事件ID、事件名称、事件源、请求ID、源地址、用户名等； 2、经核查堡垒机中用户操作行为审计记录包括：用户名、动作、资源类型、资源、远端地址、日期等； 3、经核查云防火墙中审计记录包括：发生时间、源IP、目的IP、事件名称/攻击类型/方向/判断来源、事件数/风险级别、防御状态、操作（详情）等； 4、核查Web应用防火墙审计记录包括：攻击IP、所属区域、攻击时间、攻击类型、攻击URL、请求方法、请求参数、规则动作、规则ID、攻击概率、操作（查看详情、误报屏蔽）等。 |
| 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； | 经访谈网络管理员及核查阿里云审计记录备份策略，由管理员配置操作审计转储，定期对阿里云控制台的审计记录存储至OSS中进行备份，并且所有用户均无权限对审计记录进行修改、删除。 |
| d）应能对远程访问的用户行为、访问互联网的用户行为等单独进行行为审计和数据分析。 | 经现场访谈网络管理员及核查，远程访问的用户行为通过阿里云控制台、堡垒机进行审计记录，但是未对访问互联网的用户行为进行审计记录。 |
| 可信验证 | a）可基于可信根对边界设备的系统引导程序、系统程序、重要配置参数和边界防护应用程序等进行可信验证，并在应用程序的关键执行环节进行动态可信验证，在检测到其可信性受到破坏后进行报警，并将验证结果形成审计记录送至安全管理中心。 | 未基于可信根对边界设备进行可信验证。 |

3.1.7. 分拨中心接入区

|  |  |  |
| --- | --- | --- |
| **安全控制点** | **测评指标** | **结果记录** |
| 边界防护 | a）应保证跨越边界的访问和数据流通过边界设备提供的受控接口进行通信； | 经现场访谈及核查出口防火墙（H3C F1000-AK109）访问控制策略，在出口防火墙中针对跨越边界的访问及数据流通配置了访问控制策略，如：1、分拨中心接入区与阿里公共云业务区之间通信；2、默认拒绝所有通信等。 |
| b）应能够对非授权设备私自联到内部网络的行为进行检查或限制； | 1、经访谈网络管理员，场站中7X24小时有专人负责管理，外部人员均无法私自进入场站进行设备接入；2、经核查出口防火墙（H3C F1000-AK109）配置及无线控制器（AC）（H3C WX3010H-L） 中的配置，出口防火墙、无线控制路由（AC）中未使用端口均设置为shutdown状态，同时在AC中对场站中PDA设备进行MAC地址绑定，非授权设备均不允许接到内部网络。 |
| c）应能够对内部用户非授权联到外部网络的行为进行检查或限制； | 经现场访谈网络管理员及核查出口防火墙（（H3C F1000-AK109）访问控制策略，未对内部用户联到外部网络的行为进行检查或限制。 |
| d）应限制无线网络的使用，保证无线网络通过受控的边界设备接入内部网络。 | 经现场访谈网络管理员及核查，分拨中心接入区通过无线AP（H3C6320）为PDA设备提供无线网络，在各场站中部署了无线控制器（AC）（H3C WX3010H-L） ，对无线AP（H3C6320）进行统一控制，在无线控制器（AC）（H3C WX3010H-L）中将无线AP及PDA设备进行MAC地址绑定，同时在场站边界处部署出口防火墙（H3C F1000-AK109），通过在出口防火墙（H3C F1000-AK109）中配置访问策略，与阿里公共云业务区进行通信，保证无线网络通过受控的边界设备接入内部网络。 |
| 访问控制 | a）应在网络边界或区域之间根据访问控制策略设置访问控制规则，默认情况下除允许通信外受控接口拒绝所有通信； | 1、经现场访谈及核查出口防火墙（H3C F1000-AK109）访问控制策略，在出口防火墙中针对网络边界的访问配置了相应的访问控制策略； 2、出口防火墙中最后一条访问控制策略为拒绝所有通信； 3、访问控制策略中访问控制粒度为IP地址段级，未达到端口级。 |
| b）应删除多余或无效的访问控制规则，优化访问控制列表，并保证访问控制规则数量最小化； | 经现场访谈及核查出口防火墙（H3C F1000-AK109）访问控制策略，访问控制策略设置地址范围较宽，访问控制列表未进行优化。 |
| c）应对源地址、目的地址、源端口、目的端口和协议等进行检查，以允许/拒绝数据包进出； | 经现场访谈及核查出口防火墙（H3C F1000-AK109）访问控制策略，在出口防火墙访问控制策略中能够对源安全域、目的安全域、类型、ID、描述、源地址、目的地址、服务、用户、动作、内容安全、命中次数、流量等字段进行检查，在动作字段中能够配置允许/拒绝通信策略。 |
| d）应能根据会话状态信息为进出数据流提供明确的允许/拒绝访问的能力； | 经现场访谈及核查出口防火墙（H3C F1000-AK109）访问控制策略，在出口防火墙的访问控制策略的服务字段中根据协议类型、端口、会话状态信息等对进出数据流提供检查，在动作字段配置明确的允许/拒绝通信策略。 |
| e）应对进出网络的数据流实现基于应用协议和应用内容的访问控制。 | 经现场访谈及核查出口防火墙（H3C F1000-AK109）访问控制策略，未对进出网络的数据流实现基于应用协议和应用内容的访问控制。 |
| 入侵防范 | a）应在关键网络节点处检测、防止或限制从外部发起的网络攻击行为； | 经现场访谈及核查出口防火墙（H3C F1000-AK109）访问控制策略，出口防火墙中具备安全防护功能，在出口防火墙导航菜单栏中安全防护菜单中启用攻击防护策略，能够对从外部发起的攻击行为进行监测，发现外部攻击行为及时报警。 |
| b）应在关键网络节点处检测、防止或限制从内部发起的网络攻击行为； | 经现场访谈网络管理员，未在关键网络节点处监测、防止或限制从内部发起的网络攻击行为。 |
| c）应采取技术措施对网络行为进行分析，实现对网络攻击特别是新型网络攻击行为的分析； | 经现场访谈网络管理员及核查，未采用技术措施对网络行为进行分析，特别是新型网络攻击行为。 |
| d）当检测到攻击行为时，记录攻击源IP、攻击类型、攻击目标、攻击时间，在发生严重入侵事件时应提供报警。 | 经现场访谈及核查出口防火墙（H3C F1000-AK109）防护策略，出口防火墙中攻击日志中会记录：时间、攻击类型、入安全域名称、目的IP地址、源IP地址等信息。 |
| 恶意代码和垃圾邮件防范 | a）应在关键网络节点处对恶意代码进行检测和清除，并维护恶意代码防护机制的升级和更新； | 经现场访谈网络管理员及核查，未在网络层面部署防恶意代码软件或设备。 |
| b）应在关键网络节点处对垃圾邮件进行检测和防护，并维护垃圾邮件防护机制的升级和更新。 | 经现场访谈及核查，被测系统中不涉及邮件系统及邮件收发服务，故该项调整为不适用。 |
| 安全审计 | a）应在网络边界、重要网络节点进行安全审计，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； | 目前被测系统通过堡垒机（Jumpserver V2.23.4）对用户操作行为进行审计，同时出口防火墙（H3C F1000-AK109）能够对用户操作行为及入侵事件进行审计。 |
| 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； | 1、经现场核查堡垒机（Jumpserver V2.23.4）中审计记录，堡垒机中用户操作行为审计记录包括：用户名、动作、资源类型、资源、远端地址、日期等；2、经现场核查出口防火墙（H3C F1000-AK109）中审计记录，出口防火墙中攻击日志包括：时间、严重级别、攻击类型、动作类型、入安全域名称、目的地址、源地址等；用户操作日志包括：日期、时间、协议类型、IP地址、用户、命令详情。 |
| 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； | 经现场核查，堡垒机（Jumpserver V2.23.4）、出口防火墙（H3C SecPath F1000-E-G2）中审计模块中，所有用户均无权限对审计记录进行删除、修改，出口防火墙（H3C SecPath F1000-E-G2）中审计记录仅在本地保存一天。 |
| d）应能对远程访问的用户行为、访问互联网的用户行为等单独进行行为审计和数据分析。 | 经现场访谈网络管理员及核查，远程访问的用户行为通过堡垒机进行审计记录，但是未对访问互联网的用户行为单独进行审计。 |
| 可信验证 | a）可基于可信根对边界设备的系统引导程序、系统程序、重要配置参数和边界防护应用程序等进行可信验证，并在应用程序的关键执行环节进行动态可信验证，在检测到其可信性受到破坏后进行报警，并将验证结果形成审计记录送至安全管理中心。 | 未基于可信根对边界设备进行可信验证。 |

|  |  |  |  |
| --- | --- | --- | --- |
| **测评项目** |  | **测评对象** | 安全区域边界 |
| **测评单位** |  | | |
| **测评地点** |  | | |
| **测评人员** |  | **配合人员** | 刘亮 |
| **测评日期** | 2023.6.15-2023.6.16 | | |
| **测评人员签字** |  | **配合人员签字** |  |

3.2. 云计算安全扩展要求部分

3.2.1. 互联网接入区

|  |  |  |
| --- | --- | --- |
| **安全控制点** | **测评指标** | **结果记录** |
| 访问控制 | a）应在虚拟化网络边界部署访问控制机制，并设置访问控制规则； | 经现场访谈及核查，互联网接入区部署在世纪互联IDC机房中，不涉及云计算安全扩展要求，故该项调整为不适用。 |
| b）应在不同等级的网络区域边界部署访问控制机制，设置访问控制规则。 | 经现场访谈及核查，互联网接入区部署在世纪互联IDC机房中，不涉及云计算安全扩展要求，故该项调整为不适用。 |
| 入侵防范 | a）应能检测到云服务客户发起的网络攻击行为，并能记录攻击类型、攻击时间、攻击流量等； | 经现场访谈及核查，互联网接入区部署在世纪互联IDC机房中，不涉及云计算安全扩展要求，故该项调整为不适用。 |
| b）应能检测到对虚拟网络节点的网络攻击行为，并能记录攻击类型、攻击时间、攻击流量等； | 经现场访谈及核查，互联网接入区部署在世纪互联IDC机房中，不涉及云计算安全扩展要求，故该项调整为不适用。 |
| c）应能检测到虚拟机与宿主机、虚拟机与虚拟机之间的异常流量； | 经现场访谈及核查，互联网接入区部署在世纪互联IDC机房中，不涉及云计算安全扩展要求，故该项调整为不适用。 |
| d）应在检测到网络攻击行为、异常流量情况时进行告警。 | 经现场访谈及核查，互联网接入区部署在世纪互联IDC机房中，不涉及云计算安全扩展要求，故该项调整为不适用。 |
| 安全审计 | a）应对云服务商和云服务客户在远程管理时执行的特权命令进行审计，至少包括虚拟机删除、虚拟机重启； | 经现场访谈及核查，互联网接入区部署在世纪互联IDC机房中，不涉及云计算安全扩展要求，故该项调整为不适用。 |
| b）应保证云服务商对云服务客户系统和数据的操作可被云服务客户审计。 | 经现场访谈及核查，互联网接入区部署在世纪互联IDC机房中，不涉及云计算安全扩展要求，故该项调整为不适用。 |

3.2.2. 专线接入区

|  |  |  |
| --- | --- | --- |
| **安全控制点** | **测评指标** | **结果记录** |
| 访问控制 | a）应在虚拟化网络边界部署访问控制机制，并设置访问控制规则； | 经现场访谈及核查，专线接入区部署在世纪互联IDC机房中，不涉及云计算安全扩展要求，故该项调整为不适用。 |
| b）应在不同等级的网络区域边界部署访问控制机制，设置访问控制规则。 | 经现场访谈及核查，专线接入区部署在世纪互联IDC机房中，不涉及云计算安全扩展要求，故该项调整为不适用。 |
| 入侵防范 | a）应能检测到云服务客户发起的网络攻击行为，并能记录攻击类型、攻击时间、攻击流量等； | 经现场访谈及核查，专线接入区部署在世纪互联IDC机房中，不涉及云计算安全扩展要求，故该项调整为不适用。 |
| b）应能检测到对虚拟网络节点的网络攻击行为，并能记录攻击类型、攻击时间、攻击流量等； | 经现场访谈及核查，专线接入区部署在世纪互联IDC机房中，不涉及云计算安全扩展要求，故该项调整为不适用。 |
| c）应能检测到虚拟机与宿主机、虚拟机与虚拟机之间的异常流量； | 经现场访谈及核查，专线接入区部署在世纪互联IDC机房中，不涉及云计算安全扩展要求，故该项调整为不适用。 |
| d）应在检测到网络攻击行为、异常流量情况时进行告警。 | 经现场访谈及核查，专线接入区部署在世纪互联IDC机房中，不涉及云计算安全扩展要求，故该项调整为不适用。 |
| 安全审计 | a）应对云服务商和云服务客户在远程管理时执行的特权命令进行审计，至少包括虚拟机删除、虚拟机重启； | 经现场访谈及核查，专线接入区部署在世纪互联IDC机房中，不涉及云计算安全扩展要求，故该项调整为不适用。 |
| b）应保证云服务商对云服务客户系统和数据的操作可被云服务客户审计。 | 经现场访谈及核查，专线接入区部署在世纪互联IDC机房中，不涉及云计算安全扩展要求，故该项调整为不适用。 |

3.2.3. 核心交换区

|  |  |  |
| --- | --- | --- |
| **安全控制点** | **测评指标** | **结果记录** |
| 访问控制 | a）应在虚拟化网络边界部署访问控制机制，并设置访问控制规则； | 经现场访谈及核查，核心交换区部署在世纪互联IDC机房中，不涉及云计算安全扩展要求，故该项调整为不适用。 |
| b）应在不同等级的网络区域边界部署访问控制机制，设置访问控制规则。 | 经现场访谈及核查，核心交换区部署在世纪互联IDC机房中，不涉及云计算安全扩展要求，故该项调整为不适用。 |
| 入侵防范 | a）应能检测到云服务客户发起的网络攻击行为，并能记录攻击类型、攻击时间、攻击流量等； | 经现场访谈及核查，核心交换区部署在世纪互联IDC机房中，不涉及云计算安全扩展要求，故该项调整为不适用。 |
| b）应能检测到对虚拟网络节点的网络攻击行为，并能记录攻击类型、攻击时间、攻击流量等； | 经现场访谈及核查，核心交换区部署在世纪互联IDC机房中，不涉及云计算安全扩展要求，故该项调整为不适用。 |
| c）应能检测到虚拟机与宿主机、虚拟机与虚拟机之间的异常流量； | 经现场访谈及核查，核心交换区部署在世纪互联IDC机房中，不涉及云计算安全扩展要求，故该项调整为不适用。 |
| d）应在检测到网络攻击行为、异常流量情况时进行告警。 | 经现场访谈及核查，核心交换区部署在世纪互联IDC机房中，不涉及云计算安全扩展要求，故该项调整为不适用。 |
| 安全审计 | a）应对云服务商和云服务客户在远程管理时执行的特权命令进行审计，至少包括虚拟机删除、虚拟机重启； | 经现场访谈及核查，核心交换区部署在世纪互联IDC机房中，不涉及云计算安全扩展要求，故该项调整为不适用。 |
| b）应保证云服务商对云服务客户系统和数据的操作可被云服务客户审计。 | 经现场访谈及核查，核心交换区部署在世纪互联IDC机房中，不涉及云计算安全扩展要求，故该项调整为不适用。 |

3.2.4. 业务服务区

|  |  |  |
| --- | --- | --- |
| **安全控制点** | **测评指标** | **结果记录** |
| 访问控制 | a）应在虚拟化网络边界部署访问控制机制，并设置访问控制规则； | 经现场访谈及核查，业务服务区部署在世纪互联IDC机房中，不涉及云计算安全扩展要求，故该项调整为不适用。 |
| b）应在不同等级的网络区域边界部署访问控制机制，设置访问控制规则。 | 经现场访谈及核查，业务服务区部署在世纪互联IDC机房中，不涉及云计算安全扩展要求，故该项调整为不适用。 |
| 入侵防范 | a）应能检测到云服务客户发起的网络攻击行为，并能记录攻击类型、攻击时间、攻击流量等； | 经现场访谈及核查，业务服务区部署在世纪互联IDC机房中，不涉及云计算安全扩展要求，故该项调整为不适用。 |
| b）应能检测到对虚拟网络节点的网络攻击行为，并能记录攻击类型、攻击时间、攻击流量等； | 经现场访谈及核查，业务服务区部署在世纪互联IDC机房中，不涉及云计算安全扩展要求，故该项调整为不适用。 |
| c）应能检测到虚拟机与宿主机、虚拟机与虚拟机之间的异常流量； | 经现场访谈及核查，业务服务区部署在世纪互联IDC机房中，不涉及云计算安全扩展要求，故该项调整为不适用。 |
| d）应在检测到网络攻击行为、异常流量情况时进行告警。 | 经现场访谈及核查，业务服务区部署在世纪互联IDC机房中，不涉及云计算安全扩展要求，故该项调整为不适用。 |
| 安全审计 | a）应对云服务商和云服务客户在远程管理时执行的特权命令进行审计，至少包括虚拟机删除、虚拟机重启； | 经现场访谈及核查，业务服务区部署在世纪互联IDC机房中，不涉及云计算安全扩展要求，故该项调整为不适用。 |
| b）应保证云服务商对云服务客户系统和数据的操作可被云服务客户审计。 | 经现场访谈及核查，业务服务区部署在世纪互联IDC机房中，不涉及云计算安全扩展要求，故该项调整为不适用。 |

3.2.5. 带外管理区

|  |  |  |
| --- | --- | --- |
| **安全控制点** | **测评指标** | **结果记录** |
| 访问控制 | a）应在虚拟化网络边界部署访问控制机制，并设置访问控制规则； | 经现场访谈及核查，带外管理区部署在世纪互联IDC机房中，不涉及云计算安全扩展要求，故该项调整为不适用。 |
| b）应在不同等级的网络区域边界部署访问控制机制，设置访问控制规则。 | 经现场访谈及核查，带外管理区部署在世纪互联IDC机房中，不涉及云计算安全扩展要求，故该项调整为不适用。 |
| 入侵防范 | a）应能检测到云服务客户发起的网络攻击行为，并能记录攻击类型、攻击时间、攻击流量等； | 经现场访谈及核查，带外管理区部署在世纪互联IDC机房中，不涉及云计算安全扩展要求，故该项调整为不适用。 |
| b）应能检测到对虚拟网络节点的网络攻击行为，并能记录攻击类型、攻击时间、攻击流量等； | 经现场访谈及核查，带外管理区部署在世纪互联IDC机房中，不涉及云计算安全扩展要求，故该项调整为不适用。 |
| c）应能检测到虚拟机与宿主机、虚拟机与虚拟机之间的异常流量； | 经现场访谈及核查，带外管理区部署在世纪互联IDC机房中，不涉及云计算安全扩展要求，故该项调整为不适用。 |
| d）应在检测到网络攻击行为、异常流量情况时进行告警。 | 经现场访谈及核查，带外管理区部署在世纪互联IDC机房中，不涉及云计算安全扩展要求，故该项调整为不适用。 |
| 安全审计 | a）应对云服务商和云服务客户在远程管理时执行的特权命令进行审计，至少包括虚拟机删除、虚拟机重启； | 经现场访谈及核查，带外管理区部署在世纪互联IDC机房中，不涉及云计算安全扩展要求，故该项调整为不适用。 |
| b）应保证云服务商对云服务客户系统和数据的操作可被云服务客户审计。 | 经现场访谈及核查，带外管理区部署在世纪互联IDC机房中，不涉及云计算安全扩展要求，故该项调整为不适用。 |

3.2.6. 阿里公共云业务区

|  |  |  |
| --- | --- | --- |
| **安全控制点** | **测评指标** | **结果记录** |
| 访问控制 | a）应在虚拟化网络边界部署访问控制机制，并设置访问控制规则； | 经现场核查，在阿里公共云边界处通过在SLB、阿里云安全组上配置了访问控制策略，对跨越边界的访问及数据流进行访问控制。 |
| b）应在不同等级的网络区域边界部署访问控制机制，设置访问控制规则。 | 经现场访谈网络管理员及核查阿里公共云安全组配置，在阿里公共云业务区中根据业务访问需求对JMS综合物流平台系统业务功能模块单独划分了42安全组，并且根据业务管理需求及业务功能之间通信需求分别在安全组之间添加安全组策略。 |
| 入侵防范 | a）应能检测到云服务客户发起的网络攻击行为，并能记录攻击类型、攻击时间、攻击流量等； | 系统中部署了Web应用防火墙、云防火墙等安全防护服务，实时对从内部网络攻击行为进行检测，并记录发生时间、源IP、目的IP、攻击类型、防御状态、详情等。 |
| b）应能检测到对虚拟网络节点的网络攻击行为，并能记录攻击类型、攻击时间、攻击流量等； | 经现场访谈网络管理员及核查，阿里公共云业务区中中部署了云防火墙、Web应用防火墙等安全防护服务，能够实时对网络攻击行为进行检测，并记录发生时间、源IP、目的IP、攻击类型、防御状态、详情等内容。 |
| c）应能检测到虚拟机与宿主机、虚拟机与虚拟机之间的异常流量； | 经现场核查阿里云控制台监控服务，能够对云防火墙、每个SLB、每台虚拟主机的流量使用情况进行实时监控，发生异常流量及时通过钉钉进行告警。 |
| d）应在检测到网络攻击行为、异常流量情况时进行告警。 | 经现场核查阿里云控制台监控服务、云防火墙、Web应防火墙，阿里云控制台监控服务，能够对云防火墙、每个SLB、每台虚拟主机的流量使用情况进行实时监控，发生异常流量及时通过钉钉进行告警；云防火墙、Web应用防火墙能够实时进行网络攻击监测，发现网络攻击行为及时通过钉钉报警，经现场核查网络管理员钉钉告警记录能够与云防火墙、Web应用防火墙中入侵攻击审计记录对应。 |
| 安全审计 | a）应对云服务商和云服务客户在远程管理时执行的特权命令进行审计，至少包括虚拟机删除、虚拟机重启； | 在阿里云控制台中启用了操作审计，能够对云服务客户的远程管理操作行为进行审计记录，包括：虚拟机删除、虚拟机重启等。 |
| b）应保证云服务商对云服务客户系统和数据的操作可被云服务客户审计。 | 客户为云租户，系统部署在阿里云上，云计算安全由阿里云负责，阿里云已经通过等级保护第三级测评。 |

3.2.7. 分拨中心接入区

|  |  |  |
| --- | --- | --- |
| **安全控制点** | **测评指标** | **结果记录** |
| 访问控制 | a）应在虚拟化网络边界部署访问控制机制，并设置访问控制规则； | 经现场访谈及核查，分拨中心接入区不涉及云计算安全扩展要求，故该项调整为不适用。 |
| b）应在不同等级的网络区域边界部署访问控制机制，设置访问控制规则。 | 经现场访谈及核查，分拨中心接入区不涉及云计算安全扩展要求，故该项调整为不适用。 |
| 入侵防范 | a）应能检测到云服务客户发起的网络攻击行为，并能记录攻击类型、攻击时间、攻击流量等； | 经现场访谈及核查，分拨中心接入区不涉及云计算安全扩展要求，故该项调整为不适用。 |
| b）应能检测到对虚拟网络节点的网络攻击行为，并能记录攻击类型、攻击时间、攻击流量等； | 经现场访谈及核查，分拨中心接入区不涉及云计算安全扩展要求，故该项调整为不适用。 |
| c）应能检测到虚拟机与宿主机、虚拟机与虚拟机之间的异常流量； | 经现场访谈及核查，分拨中心接入区不涉及云计算安全扩展要求，故该项调整为不适用。 |
| d）应在检测到网络攻击行为、异常流量情况时进行告警。 | 经现场访谈及核查，分拨中心接入区不涉及云计算安全扩展要求，故该项调整为不适用。 |
| 安全审计 | a）应对云服务商和云服务客户在远程管理时执行的特权命令进行审计，至少包括虚拟机删除、虚拟机重启； | 经现场访谈及核查，分拨中心接入区不涉及云计算安全扩展要求，故该项调整为不适用。 |
| b）应保证云服务商对云服务客户系统和数据的操作可被云服务客户审计。 | 经现场访谈及核查，分拨中心接入区不涉及云计算安全扩展要求，故该项调整为不适用。 |

|  |  |  |  |
| --- | --- | --- | --- |
| **测评项目** |  | **测评对象** | 安全区域边界 |
| **测评单位** |  | | |
| **测评地点** |  | | |
| **测评人员** |  | **配合人员** | 刘亮 |
| **测评日期** | 2023.6.15-2023.6.16 | | |
| **测评人员签字** |  | **配合人员签字** |  |

3.3. 移动互联安全扩展要求部分

3.3.1. 互联网接入区

|  |  |  |
| --- | --- | --- |
| **安全控制点** | **测评指标** | **结果记录** |
| 边界防护 | a）应保证有线网络与无线网络边界之间的访问和数据流通过无线接入网关设备。 | 经现场访谈及核查，互联网接入区不涉及无线接入设备接入，故该项调整为不适用。 |
| 访问控制 | a）无线接入设备应开启接入认证功能，并支持采用认证服务器认证或国家密码管理机构批准的密码模块进行认证。 | 经现场访谈及核查，互联网接入区不涉及无线接入设备接入，故该项调整为不适用。 |
| 入侵防范 | a）应能够检测到非授权无线接入设备和非授权移动终端的接入行为； | 经现场访谈及核查，互联网接入区不涉及无线接入设备接入，故该项调整为不适用。 |
| b）应能够检测到针对无线接入设备的网络扫描、DDoS攻击、密钥破解、中间人攻击和欺骗攻击等行为； | 经现场访谈及核查，互联网接入区不涉及无线接入设备接入，故该项调整为不适用。 |
| c）应能够检测到无线接入设备的SSID广播、WPS等高风险功能的开启状态； | 经现场访谈及核查，互联网接入区不涉及无线接入设备接入，故该项调整为不适用。 |
| d）应禁用无线接入设备和无线接入网关存在风险的功能，如：SSID广播、WEP认证等； | 经现场访谈及核查，互联网接入区不涉及无线接入设备接入，故该项调整为不适用。 |
| e）应禁止多个AP使用同一个认证密钥； | 经现场访谈及核查，互联网接入区不涉及无线接入设备接入，故该项调整为不适用。 |
| f）应能够阻断非授权无线接入设备或非授权移动终端。 | 经现场访谈及核查，互联网接入区不涉及无线接入设备接入，故该项调整为不适用。 |

3.3.2. 专线接入区

|  |  |  |
| --- | --- | --- |
| **安全控制点** | **测评指标** | **结果记录** |
| 边界防护 | a）应保证有线网络与无线网络边界之间的访问和数据流通过无线接入网关设备。 | 经现场访谈及核查，专线接入区不涉及无线接入设备接入，故该项调整为不适用。 |
| 访问控制 | a）无线接入设备应开启接入认证功能，并支持采用认证服务器认证或国家密码管理机构批准的密码模块进行认证。 | 经现场访谈及核查，专线接入区不涉及无线接入设备接入，故该项调整为不适用。 |
| 入侵防范 | a）应能够检测到非授权无线接入设备和非授权移动终端的接入行为； | 经现场访谈及核查，专线接入区不涉及无线接入设备接入，故该项调整为不适用。 |
| b）应能够检测到针对无线接入设备的网络扫描、DDoS攻击、密钥破解、中间人攻击和欺骗攻击等行为； | 经现场访谈及核查，专线接入区不涉及无线接入设备接入，故该项调整为不适用。 |
| c）应能够检测到无线接入设备的SSID广播、WPS等高风险功能的开启状态； | 经现场访谈及核查，专线接入区不涉及无线接入设备接入，故该项调整为不适用。 |
| d）应禁用无线接入设备和无线接入网关存在风险的功能，如：SSID广播、WEP认证等； | 经现场访谈及核查，专线接入区不涉及无线接入设备接入，故该项调整为不适用。 |
| e）应禁止多个AP使用同一个认证密钥； | 经现场访谈及核查，专线接入区不涉及无线接入设备接入，故该项调整为不适用。 |
| f）应能够阻断非授权无线接入设备或非授权移动终端。 | 经现场访谈及核查，专线接入区不涉及无线接入设备接入，故该项调整为不适用。 |

3.3.3. 核心交换区

|  |  |  |
| --- | --- | --- |
| **安全控制点** | **测评指标** | **结果记录** |
| 边界防护 | a）应保证有线网络与无线网络边界之间的访问和数据流通过无线接入网关设备。 | 经现场访谈及核查，核心交换区不涉及无线接入设备接入，故该项调整为不适用。 |
| 访问控制 | a）无线接入设备应开启接入认证功能，并支持采用认证服务器认证或国家密码管理机构批准的密码模块进行认证。 | 经现场访谈及核查，核心交换区不涉及无线接入设备接入，故该项调整为不适用。 |
| 入侵防范 | a）应能够检测到非授权无线接入设备和非授权移动终端的接入行为； | 经现场访谈及核查，核心交换区不涉及无线接入设备接入，故该项调整为不适用。 |
| b）应能够检测到针对无线接入设备的网络扫描、DDoS攻击、密钥破解、中间人攻击和欺骗攻击等行为； | 经现场访谈及核查，核心交换区不涉及无线接入设备接入，故该项调整为不适用。 |
| c）应能够检测到无线接入设备的SSID广播、WPS等高风险功能的开启状态； | 经现场访谈及核查，核心交换区不涉及无线接入设备接入，故该项调整为不适用。 |
| d）应禁用无线接入设备和无线接入网关存在风险的功能，如：SSID广播、WEP认证等； | 经现场访谈及核查，核心交换区不涉及无线接入设备接入，故该项调整为不适用。 |
| e）应禁止多个AP使用同一个认证密钥； | 经现场访谈及核查，核心交换区不涉及无线接入设备接入，故该项调整为不适用。 |
| f）应能够阻断非授权无线接入设备或非授权移动终端。 | 经现场访谈及核查，核心交换区不涉及无线接入设备接入，故该项调整为不适用。 |

3.3.4. 业务服务区

|  |  |  |
| --- | --- | --- |
| **安全控制点** | **测评指标** | **结果记录** |
| 边界防护 | a）应保证有线网络与无线网络边界之间的访问和数据流通过无线接入网关设备。 | 经现场访谈及核查，业务服务区不涉及无线接入设备接入，故该项调整为不适用。 |
| 访问控制 | a）无线接入设备应开启接入认证功能，并支持采用认证服务器认证或国家密码管理机构批准的密码模块进行认证。 | 经现场访谈及核查，业务服务区不涉及无线接入设备接入，故该项调整为不适用。 |
| 入侵防范 | a）应能够检测到非授权无线接入设备和非授权移动终端的接入行为； | 经现场访谈及核查，业务服务区不涉及无线接入设备接入，故该项调整为不适用。 |
| b）应能够检测到针对无线接入设备的网络扫描、DDoS攻击、密钥破解、中间人攻击和欺骗攻击等行为； | 经现场访谈及核查，业务服务区不涉及无线接入设备接入，故该项调整为不适用。 |
| c）应能够检测到无线接入设备的SSID广播、WPS等高风险功能的开启状态； | 经现场访谈及核查，业务服务区不涉及无线接入设备接入，故该项调整为不适用。 |
| d）应禁用无线接入设备和无线接入网关存在风险的功能，如：SSID广播、WEP认证等； | 经现场访谈及核查，业务服务区不涉及无线接入设备接入，故该项调整为不适用。 |
| e）应禁止多个AP使用同一个认证密钥； | 经现场访谈及核查，业务服务区不涉及无线接入设备接入，故该项调整为不适用。 |
| f）应能够阻断非授权无线接入设备或非授权移动终端。 | 经现场访谈及核查，业务服务区不涉及无线接入设备接入，故该项调整为不适用。 |

3.3.5. 带外管理区

|  |  |  |
| --- | --- | --- |
| **安全控制点** | **测评指标** | **结果记录** |
| 边界防护 | a）应保证有线网络与无线网络边界之间的访问和数据流通过无线接入网关设备。 | 经现场访谈及核查，带外管理区不涉及无线接入设备接入，故该项调整为不适用。 |
| 访问控制 | a）无线接入设备应开启接入认证功能，并支持采用认证服务器认证或国家密码管理机构批准的密码模块进行认证。 | 经现场访谈及核查，带外管理区不涉及无线接入设备接入，故该项调整为不适用。 |
| 入侵防范 | a）应能够检测到非授权无线接入设备和非授权移动终端的接入行为； | 经现场访谈及核查，带外管理区不涉及无线接入设备接入，故该项调整为不适用。 |
| b）应能够检测到针对无线接入设备的网络扫描、DDoS攻击、密钥破解、中间人攻击和欺骗攻击等行为； | 经现场访谈及核查，带外管理区不涉及无线接入设备接入，故该项调整为不适用。 |
| c）应能够检测到无线接入设备的SSID广播、WPS等高风险功能的开启状态； | 经现场访谈及核查，带外管理区不涉及无线接入设备接入，故该项调整为不适用。 |
| d）应禁用无线接入设备和无线接入网关存在风险的功能，如：SSID广播、WEP认证等； | 经现场访谈及核查，带外管理区不涉及无线接入设备接入，故该项调整为不适用。 |
| e）应禁止多个AP使用同一个认证密钥； | 经现场访谈及核查，带外管理区不涉及无线接入设备接入，故该项调整为不适用。 |
| f）应能够阻断非授权无线接入设备或非授权移动终端。 | 经现场访谈及核查，带外管理区不涉及无线接入设备接入，故该项调整为不适用。 |

3.3.6. 阿里公共云业务区

|  |  |  |
| --- | --- | --- |
| **安全控制点** | **测评指标** | **结果记录** |
| 边界防护 | a）应保证有线网络与无线网络边界之间的访问和数据流通过无线接入网关设备。 | 经现场访谈及核查，阿里公共云业务区不涉及无线接入设备接入，故该项调整为不适用。 |
| 访问控制 | a）无线接入设备应开启接入认证功能，并支持采用认证服务器认证或国家密码管理机构批准的密码模块进行认证。 | 经现场访谈及核查，阿里公共云业务区不涉及无线接入设备接入，故该项调整为不适用。 |
| 入侵防范 | a）应能够检测到非授权无线接入设备和非授权移动终端的接入行为； | 经现场访谈及核查，阿里公共云业务区不涉及无线接入设备接入，故该项调整为不适用。 |
| b）应能够检测到针对无线接入设备的网络扫描、DDoS攻击、密钥破解、中间人攻击和欺骗攻击等行为； | 经现场访谈及核查，阿里公共云业务区不涉及无线接入设备接入，故该项调整为不适用。 |
| c）应能够检测到无线接入设备的SSID广播、WPS等高风险功能的开启状态； | 经现场访谈及核查，阿里公共云业务区不涉及无线接入设备接入，故该项调整为不适用。 |
| d）应禁用无线接入设备和无线接入网关存在风险的功能，如：SSID广播、WEP认证等； | 经现场访谈及核查，阿里公共云业务区不涉及无线接入设备接入，故该项调整为不适用。 |
| e）应禁止多个AP使用同一个认证密钥； | 经现场访谈及核查，阿里公共云业务区不涉及无线接入设备接入，故该项调整为不适用。 |
| f）应能够阻断非授权无线接入设备或非授权移动终端。 | 经现场访谈及核查，阿里公共云业务区不涉及无线接入设备接入，故该项调整为不适用。 |

3.3.7. 分拨中心接入区

|  |  |  |
| --- | --- | --- |
| **安全控制点** | **测评指标** | **结果记录** |
| 边界防护 | a）应保证有线网络与无线网络边界之间的访问和数据流通过无线接入网关设备。 | 经现场访谈网络管理员及核查网络拓扑图，在各场站边界处分别部署无线控制器AC（H3C WX3010H-L）和出口防火墙（ H3C F1000-AK109），各场站中PDA设备连接无线网络时均在无线控制器AC（H3C WX3010H-L）中进行MAC地址绑定，并且仅允许通过指定无线AP认证通过后才能连联网。 |
| 访问控制 | a）无线接入设备应开启接入认证功能，并支持采用认证服务器认证或国家密码管理机构批准的密码模块进行认证。 | 经现场访谈网络管理员及核查无线AP（H3C 6320 ）配置，在无线AP中启用认证功能、管理用户通过账号、口令进行身份鉴别，PDA设备需访问SSID信道，然后通过账号、口令进行认证（绑定mac地址进行通信），但是无线AP及无线控制器AC未采用认证服务器认证或国家密码管理机构批准的密码模块进行认证。 |
| 入侵防范 | a）应能够检测到非授权无线接入设备和非授权移动终端的接入行为； | 经现场访谈网络管理员及核查无线控制器AC（H3C WX3010H-L）中配置，在无线控制器AC（H3C WX3010H-L）将PDA设备进行MAC地址绑定，设备进行认证时，会通过MAC地址进行识别，未进行MAC地址绑定设备均不允许接到网络中；核查无线控制器AC未使用端口，均为shutdown状态。 |
| b）应能够检测到针对无线接入设备的网络扫描、DDoS攻击、密钥破解、中间人攻击和欺骗攻击等行为； | 经现场访谈网络管理员及核查出口防火墙（ H3C F1000-AK109）安全配置，在导航菜单栏安全防护菜单中具备入侵防护功能，场地出口部署H3C防火墙，在防火墙中启用入侵防护功能，但是无法对DDoS攻击、密钥破解、中间人攻击等进行监测。 |
| c）应能够检测到无线接入设备的SSID广播、WPS等高风险功能的开启状态； | 经现场访谈网络管理员，无法对无线接入设备的SSID广播、WPS等高风险功能的开启状态进行检测。 |
| d）应禁用无线接入设备和无线接入网关存在风险的功能，如：SSID广播、WEP认证等； | 经现场核查无线控制器AC（H3C WX3010H-L）及无线AP（H3C 6320）中配置策略，未禁用SSID广播，WEP认证等。 |
| e）应禁止多个AP使用同一个认证密钥； | 经现场核查无线控制器AC（H3C WX3010H-L）及无线AP（H3C 6320）中用户信息，设备中共创建了两个账户，分别由场站管理员及网络管理员使用，两个账户分别设置了不同的口令，未使用同一个认证密钥。 |
| f）应能够阻断非授权无线接入设备或非授权移动终端。 | 经现场访谈网络管理员及核查无线控制器AC（H3C WX3010H-L）中配置，将PDA设备进行MAC地址绑定，设备接入无线网络时需进行校验，拒绝未绑定MAC地址无线设备接入到网络中，经现场通过手机连接无线网络，提示无法接入到该网络中。 |

4. 安全计算环境测评表

4.1. 安全通用要求部分

|  |  |  |  |
| --- | --- | --- | --- |
| **测评项目** |  | **测评对象** | 网络设备 |
| **测评单位** |  | | |
| **测评地点** |  | | |
| **测评人员** |  | **配合人员** | 刘亮 |
| **测评日期** | 2023.6.15 | | |
| **测评人员签字** |  | **配合人员签字** |  |

4.1.1. 网络设备

4.1.1.1. 业务接入交换机1

|  |  |  |
| --- | --- | --- |
| **安全控制点** | **测评指标** | **结果记录** |
| 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、经现场访谈网络管理员，交换机采用用户名、口令进行身份标识及身份鉴别；2、经核查交换机配置，输入display password-control命令，返回信息为 Password aging:Enabled (90 days) Password length: Enabled (10 characters) Password composition:Enabled (3 types, 1 characters per type) Password history: Enabled (max history records:4)，通过返回信息确认：用户口令长度为至少10位，包含数字、字母、字符三种类型，用户口令更改周期为90天；3、通过现场在交换机中创建与网络管理员ylops同名账户时，交换机中会提示用户名已存在，无法创重名用户，确认用户标识具备唯一性。 |
| 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、经现场核查交换机配置策略，输入display password-control命令，返回信息为 Maximum login attempts: 3，Action for exceeding login attempts: Lock user for 1 minutes、User authentication timeout：600 seconds；2、通过返回信息确认用户连续错误登录3次锁定账户1分钟，用户登录连接超时时间限制为600秒。 |
| 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； | 1、经现场访谈网络管理员及核查其远程连接交换机的方式，管理员在远程管理交换机时采用SSH协议进行通信，防止鉴别信息在网络传输过程中被窃听；2、访谈网络管理员，Telnet协议默认为关闭状态，通过输入命令telnet server enable尝试启用Telnet协议，返回信息为Telnet is insecure because it transmits data in plaintext form，Telnet协议未启成功；3，通过在终端Telnet该交换机，无法连接成功。 |
| 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。 | 经现场核查网络管理员远程登录交换机方式，交换机仅采用用户名、口令方式进行身份鉴别，未采用两种或两种以上组合的鉴别技术对用户进行身份鉴别。 |
| 访问控制 | a）应对登录的用户分配账户和权限； | 1、经现场核查交换机中用户信息，通过输入display local-user命令，返回信息中显示交换机中存在security、tulei、xuweilai、ylops等用户，其中security的 user role list：level-1，network-operator；tulei、xuweilai、ylops的 user role list：network-admin,network-operator；2、经访谈网络管理员，其中tulei、xuweilai为两位网络管理员账号，ylops为网络主管账户，security为安全管理账号。 |
| b）应重命名或删除默认账户，修改默认账户的默认口令； | 1、经现场核查交换机中用户信息，通过输入display local-user命令，返回信息中显示交换机中存在security、tulei、xuweilai、ylops等用户,不存在默认账户，2、经核查交换机配置，输入display password-control命令，返回信息为 Password aging:Enabled (90 days) Password length: Enabled (10 characters) Password composition:Enabled (3 types, 1 characters per type) Password history: Enabled (max history records：3，用户口令已按照复杂度策略更改。 |
| 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； | 经现场核查交换机中用户信息，通过输入display local-user命令，返回信息中显示交换机中存在security、tulei、xuweilai、ylops等用户,经访谈网络管理员，其中tulei、xuweilai为两位网络管理员账号，ylops为网络主管账户，security为安全管理账号，不存在多余、过期、共享账户。 |
| 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； | 经现场核查交换机中用户信息，通过输入display local-user命令，返回信息中显示交换机中存在security、tulei、xuweilai、ylops等用户，经访谈网络管理员，交换机中未单独创建审计管理员账户，并且网络管理员权限为超管用户权限，未实现管理用户权限最小化及权限分离。 |
| e）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； | 经核查配置文件及访谈网络管理员，交换机中由网络管理员角色账户为管理用户配置相应账号，并按照用户角色级别赋予管理用户操作权限。 |
| f）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； | 经核查配置文件及访谈网络管理员，交换机中访问控制策略为管理用户的交换机中配置文件等进行配置管理及访问管理等，访问控制粒度达到主体为用户级、客体为文件级。 |
| g）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。 | 经核查配置文件及访谈网络管理员，未对重要主体和客体设置安全标记。 |
| 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； | 经现场访谈网络管理员及核查交换机配置，输入命令display logbuffer reverse，返回信息为logbuffer:enable；确认交换机中其中安全审计功能，通过查看审计记录内容，确认审计记录中包含设备运行记录及用户操作行为审计记录等。 |
| 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； | 经现场核查交换机中审计记录内容，审计记录中包含：日期、时间、主机名、类型、IP地址、用户名、详情等。 |
| 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、经访谈网络管理员，交换机中所有用户均无权限对审计记录进行删除或修改，并且管理员在备份服务器（10.33.110.160）中添加审计记录下载脚本（python脚本），实时将交换机中审计记录下载至备份服务器中进行备份；2、经现场核查备份服务器（10.33.110.160）中/home/network\_backup目录中存在审计记录备份文件，备份文件宿主为root，权限为744，其他用户仅拥有读权限。 |
| d）应对审计进程进行保护，防止未经授权的中断。 | 经现场访谈网络管理员，交换机中审计进程受系统进程保护，所有用户均无权限将审计进程单独中断。 |
| 入侵防范 | a）应遵循最小安装的原则，仅安装需要的组件和应用程序； | 经访谈网络管理员及核查配置文件，交换机为厂商提供独立封装系统，不允许安装其他组件及应用程序，遵循最小安装原则。 |
| b）应关闭不需要的系统服务、默认共享和高危端口； | 经现场访谈网络管理员及核查交换机配置，输入display current-fonfiguration，返回信息HTTP、Telnet协议均已关闭，交换机中未启用不需要的系统服务、默认共享及高危端口。 |
| c）应通过设定终端接入方式或网络地址范围对通过网络进行管理的管理终端进行限制； | 经访谈网络管理员，在防火墙中添加访问控制策略，仅允许管理用户通过堡垒机远程管理网络设备、安全设备及服务器等，经核查防火墙中访问控制策略，具备堡垒机地址-设备管理网段（10.33.0.0）的访问控制策略。 |
| d）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； | 该测评项测评对象为业务应用系统、中间件和系统管理软件，故将该项调整为不适用。 |
| e）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； | 1、经访谈网络管理员，会定期对官方网站通报的安全漏洞进行评估，然后从官方网站下载安全补丁，经过综合评估测试后对交换机系统进行补丁修复，避免系统中存在安全漏洞，2、经现场漏洞扫描，未发现交换机中存在安全漏洞。 |
| f）应能够检测到对重要节点进行入侵的行为，并在发生严重入侵事件时提供报警。 | 经访谈网络管理员，被测系统中部署了360AISA全流量威胁分析系统和360本地安全大脑，通过将被测系统中全部流量镜像发送到360AISA全流量威胁分析系统及360本地安全大脑中进行分析监测，发现入侵事件后及时通过钉钉报警，并且能够自动阻断。 |
| 可信验证 | a）可基于可信根对计算设备的系统引导程序、系统程序、重要配置参数和应用程序等进行可信验证，并在应用程序的关键执行环节进行动态可信验证，在检测到其可信性受到破坏后进行报警，并将验证结果形成审计记录送至安全管理中心。 | 未基于可信根对计算设备提供可信验证。 |
| 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； | 经现场访谈网络管理员及对交换机配置，交换机中关闭Telnet协议，采用SSH协议进行通信，保证重要数据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。 | 经访谈网络管理员及核查H3C S6800系列交换机产品文档，文件中目录05-参考指南--05文件系统管理命令中包含：“交换机中文件系统通常使用摘要算法（SHA-256）对文件计算摘要值，用于验证文件的正确性和完整性”。 |
| 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； | 经现场访谈网络管理员及对交换机配置，交换机中关闭Telnet协议，采用SSH协议进行通信，保证重要数据在传输过程中的保密性。 |
| b）应采用密码技术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个人信息等。 | 经访谈网管理员，管理员在设置用户口令时添加simple参数，经核查H3C S6800系列交换机产品文档，在文档05-参考指南--03-登录设备命令--1、登录设备--1.1等设备命令--1.1.28 set authentication password中正对simple参数进行说明：“simple：以明文方式设置密码，该密码将以密文方式存储。 |
| 数据备份恢复 | a）应提供重要数据的本地数据备份与恢复功能； | 经现场访谈网络管理员及核查相应配置，在备份服务器中配置python脚本，并设置每天凌晨4点将交换机中配置文件下载至备份服务器中进行备份，管理员每周对备份文件进行巡检，确保配置文件完整备份至备份服务器中。 |
| b）应提供异地实时备份功能，利用通信网络将重要数据实时备份至备份场地； | 1、经现场访谈网络管理员，管理员添加了数据同步策略，每天将备份服务器中备份文件拷贝至阿里公共云备份服务器中进行备份；2、经核查阿里公共云备份服务器（10.30.19.10）中备份目录/data/network-backup中具备网络设备配置备份文件；3、综上，因世纪互联IDC机房及阿里云公共云均在上海市，未实现异地实时备份功能。 |
| c）应提供重要数据处理系统的热冗余，保证系统的高可用性。 | 经访谈访问管理员及核查网络拓扑图，重要数据处理系统中采用双机冗余部署，保证系统的高可用性。 |

4.1.1.2. 业务接入交换机2

|  |  |  |
| --- | --- | --- |
| **安全控制点** | **测评指标** | **结果记录** |
| 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、经现场访谈网络管理员，交换机采用用户名、口令进行身份标识及身份鉴别；2、经核查交换机配置，输入display password-control命令，返回信息为 Password aging:Enabled (90 days) Password length: Enabled (10 characters) Password composition:Enabled (3 types, 1 characters per type) Password history: Enabled (max history records:4)，通过返回信息确认：用户口令长度为至少10位，包含数字、字母、字符三种类型，用户口令更改周期为90天；3、通过现场在交换机中创建与网络管理员ylops同名账户时，交换机中会提示用户名已存在，无法创重名用户，确认用户标识具备唯一性。 |
| 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、经现场核查交换机配置策略，输入display password-control命令，返回信息为 Maximum login attempts: 3，Action for exceeding login attempts: Lock user for 1 minutes、User authentication timeout：600 seconds；2、通过返回信息确认用户连续错误登录3次锁定账户1分钟，用户登录连接超时时间限制为600秒。 |
| 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； | 1、经现场访谈网络管理员及核查其远程连接交换机的方式，管理员在远程管理交换机时采用SSH协议进行通信，防止鉴别信息在网络传输过程中被窃听；2、访谈网络管理员，Telnet协议默认为关闭状态，通过输入命令telnet server enable尝试启用Telnet协议，返回信息为Telnet is insecure because it transmits data in plaintext form，Telnet协议未启成功；3，通过在终端Telnet该交换机，无法连接成功。 |
| 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。 | 经现场核查网络管理员远程登录交换机方式，交换机仅采用用户名、口令方式进行身份鉴别，未采用两种或两种以上组合的鉴别技术对用户进行身份鉴别。 |
| 访问控制 | a）应对登录的用户分配账户和权限； | 1、经现场核查交换机中用户信息，通过输入display local-user命令，返回信息中显示交换机中存在security、tulei、xuweilai、ylops等用户，其中security的 user role list：level-1，network-operator；tulei、xuweilai、ylops的 user role list：network-admin,network-operator；2、经访谈网络管理员，其中tulei、xuweilai为两位网络管理员账号，ylops为网络主管账户，security为安全管理账号。 |
| b）应重命名或删除默认账户，修改默认账户的默认口令； | 1、经现场核查交换机中用户信息，通过输入display local-user命令，返回信息中显示交换机中存在security、tulei、xuweilai、ylops等用户,不存在默认账户，2、经核查交换机配置，输入display password-control命令，返回信息为 Password aging:Enabled (90 days) Password length: Enabled (10 characters) Password composition:Enabled (3 types, 1 characters per type) Password history: Enabled (max history records：3，用户口令已按照复杂度策略更改。 |
| 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； | 经现场核查交换机中用户信息，通过输入display local-user命令，返回信息中显示交换机中存在security、tulei、xuweilai、ylops等用户,经访谈网络管理员，其中tulei、xuweilai为两位网络管理员账号，ylops为网络主管账户，security为安全管理账号，不存在多余、过期、共享账户。 |
| 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； | 经现场核查交换机中用户信息，通过输入display local-user命令，返回信息中显示交换机中存在security、tulei、xuweilai、ylops等用户，经访谈网络管理员，交换机中未单独创建审计管理员账户，并且网络管理员权限为超管用户权限，未实现管理用户权限最小化及权限分离。 |
| e）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； | 经核查配置文件及访谈网络管理员，交换机中由网络管理员角色账户为管理用户配置相应账号，并按照用户角色级别赋予管理用户操作权限。 |
| f）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； | 经核查配置文件及访谈网络管理员，交换机中访问控制策略为管理用户的交换机中配置文件等进行配置管理及访问管理等，访问控制粒度达到主体为用户级、客体为文件级。 |
| g）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。 | 经核查配置文件及访谈网络管理员，未对重要主体和客体设置安全标记。 |
| 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； | 经现场访谈网络管理员及核查交换机配置，输入命令display logbuffer reverse，返回信息为logbuffer:enable；确认交换机中其中安全审计功能，通过查看审计记录内容，确认审计记录中包含设备运行记录及用户操作行为审计记录等。 |
| 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； | 经现场核查交换机中审计记录内容，审计记录中包含：日期、时间、主机名、类型、IP地址、用户名、详情等。 |
| 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、经访谈网络管理员，交换机中所有用户均无权限对审计记录进行删除或修改，并且管理员在备份服务器（10.33.110.160）中添加审计记录下载脚本（python脚本），实时将交换机中审计记录下载至备份服务器中进行备份；2、经现场核查备份服务器（10.33.110.160）中/home/network\_backup目录中存在审计记录备份文件，备份文件宿主为root，权限为744，其他用户仅拥有读权限。 |
| d）应对审计进程进行保护，防止未经授权的中断。 | 经现场访谈网络管理员，交换机中审计进程受系统进程保护，所有用户均无权限将审计进程单独中断。 |
| 入侵防范 | a）应遵循最小安装的原则，仅安装需要的组件和应用程序； | 经访谈网络管理员及核查配置文件，交换机为厂商提供独立封装系统，不允许安装其他组件及应用程序，遵循最小安装原则。 |
| b）应关闭不需要的系统服务、默认共享和高危端口； | 经现场访谈网络管理员及核查交换机配置，输入display current-fonfiguration，返回信息HTTP、Telnet协议均已关闭，交换机中未启用不需要的系统服务、默认共享及高危端口。 |
| c）应通过设定终端接入方式或网络地址范围对通过网络进行管理的管理终端进行限制； | 经访谈网络管理员，在防火墙中添加访问控制策略，仅允许管理用户通过堡垒机远程管理网络设备、安全设备及服务器等，经核查防火墙中访问控制策略，具备堡垒机地址-设备管理网段（10.33.0.0）的访问控制策略。 |
| d）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； | 该测评项测评对象为业务应用系统、中间件和系统管理软件，故将该项调整为不适用。 |
| e）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； | 1、经访谈网络管理员，会定期对官方网站通报的安全漏洞进行评估，然后从官方网站下载安全补丁，经过综合评估测试后对交换机系统进行补丁修复，避免系统中存在安全漏洞，2、经现场漏洞扫描，未发现交换机中存在安全漏洞。 |
| f）应能够检测到对重要节点进行入侵的行为，并在发生严重入侵事件时提供报警。 | 经访谈网络管理员，被测系统中部署了360AISA全流量威胁分析系统和360本地安全大脑，通过将被测系统中全部流量镜像发送到360AISA全流量威胁分析系统及360本地安全大脑中进行分析监测，发现入侵事件后及时通过钉钉报警，并且能够自动阻断。 |
| 可信验证 | a）可基于可信根对计算设备的系统引导程序、系统程序、重要配置参数和应用程序等进行可信验证，并在应用程序的关键执行环节进行动态可信验证，在检测到其可信性受到破坏后进行报警，并将验证结果形成审计记录送至安全管理中心。 | 未基于可信根对计算设备提供可信验证。 |
| 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； | 经现场访谈网络管理员及对交换机配置，交换机中关闭Telnet协议，采用SSH协议进行通信，保证重要数据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。 | 经访谈网络管理员及核查H3C S6800系列交换机产品文档，文件中目录05-参考指南--05文件系统管理命令中包含：“交换机中文件系统通常使用摘要算法（SHA-256）对文件计算摘要值，用于验证文件的正确性和完整性”。 |
| 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； | 经现场访谈网络管理员及对交换机配置，交换机中关闭Telnet协议，采用SSH协议进行通信，保证重要数据在传输过程中的保密性。 |
| b）应采用密码技术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个人信息等。 | 经访谈网管理员，管理员在设置用户口令时添加simple参数，经核查H3C S6800系列交换机产品文档，在文档05-参考指南--03-登录设备命令--1、登录设备--1.1等设备命令--1.1.28 set authentication password中正对simple参数进行说明：“simple：以明文方式设置密码，该密码将以密文方式存储。 |
| 数据备份恢复 | a）应提供重要数据的本地数据备份与恢复功能； | 经现场访谈网络管理员及核查相应配置，在备份服务器中配置python脚本，并设置每天凌晨4点将交换机中配置文件下载至备份服务器中进行备份，管理员每周对备份文件进行巡检，确保配置文件完整备份至备份服务器中。 |
| b）应提供异地实时备份功能，利用通信网络将重要数据实时备份至备份场地； | 1、经现场访谈网络管理员，管理员添加了数据同步策略，每天将备份服务器中备份文件拷贝至阿里公共云备份服务器中进行备份；2、经核查阿里公共云备份服务器（10.30.19.10）中备份目录/data/network-backup中具备网络设备配置备份文件；3、综上，因世纪互联IDC机房及阿里云公共云均在上海市，未实现异地实时备份功能。 |
| c）应提供重要数据处理系统的热冗余，保证系统的高可用性。 | 经访谈访问管理员及核查网络拓扑图，重要数据处理系统中采用双机冗余部署，保证系统的高可用性。 |

4.1.1.3. 业务接入交换机3

|  |  |  |
| --- | --- | --- |
| **安全控制点** | **测评指标** | **结果记录** |
| 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、经现场访谈网络管理员，交换机采用用户名、口令进行身份标识及身份鉴别；2、经核查交换机配置，输入display password-control命令，返回信息为 Password aging:Enabled (90 days) Password length: Enabled (10 characters) Password composition:Enabled (3 types, 1 characters per type) Password history: Enabled (max history records:4)，通过返回信息确认：用户口令长度为至少10位，包含数字、字母、字符三种类型，用户口令更改周期为90天；3、通过现场在交换机中创建与网络管理员ylops同名账户时，交换机中会提示用户名已存在，无法创重名用户，确认用户标识具备唯一性。 |
| 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、经现场核查交换机配置策略，输入display password-control命令，返回信息为 Maximum login attempts: 3，Action for exceeding login attempts: Lock user for 1 minutes、User authentication timeout：600 seconds；2、通过返回信息确认用户连续错误登录3次锁定账户1分钟，用户登录连接超时时间限制为600秒。 |
| 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； | 1、经现场访谈网络管理员及核查其远程连接交换机的方式，管理员在远程管理交换机时采用SSH协议进行通信，防止鉴别信息在网络传输过程中被窃听；2、访谈网络管理员，Telnet协议默认为关闭状态，通过输入命令telnet server enable尝试启用Telnet协议，返回信息为Telnet is insecure because it transmits data in plaintext form，Telnet协议未启成功；3，通过在终端Telnet该交换机，无法连接成功。 |
| 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。 | 经现场核查网络管理员远程登录交换机方式，交换机仅采用用户名、口令方式进行身份鉴别，未采用两种或两种以上组合的鉴别技术对用户进行身份鉴别。 |
| 访问控制 | a）应对登录的用户分配账户和权限； | 1、经现场核查交换机中用户信息，通过输入display local-user命令，返回信息中显示交换机中存在security、tulei、xuweilai、ylops等用户，其中security的 user role list：level-1，network-operator；tulei、xuweilai、ylops的 user role list：network-admin,network-operator；2、经访谈网络管理员，其中tulei、xuweilai为两位网络管理员账号，ylops为网络主管账户，security为安全管理账号。 |
| b）应重命名或删除默认账户，修改默认账户的默认口令； | 1、经现场核查交换机中用户信息，通过输入display local-user命令，返回信息中显示交换机中存在security、tulei、xuweilai、ylops等用户,不存在默认账户，2、经核查交换机配置，输入display password-control命令，返回信息为 Password aging:Enabled (90 days) Password length: Enabled (10 characters) Password composition:Enabled (3 types, 1 characters per type) Password history: Enabled (max history records：3，用户口令已按照复杂度策略更改。 |
| 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； | 经现场核查交换机中用户信息，通过输入display local-user命令，返回信息中显示交换机中存在security、tulei、xuweilai、ylops等用户,经访谈网络管理员，其中tulei、xuweilai为两位网络管理员账号，ylops为网络主管账户，security为安全管理账号，不存在多余、过期、共享账户。 |
| 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； | 经现场核查交换机中用户信息，通过输入display local-user命令，返回信息中显示交换机中存在security、tulei、xuweilai、ylops等用户，经访谈网络管理员，交换机中未单独创建审计管理员账户，并且网络管理员权限为超管用户权限，未实现管理用户权限最小化及权限分离。 |
| e）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； | 经核查配置文件及访谈网络管理员，交换机中由网络管理员角色账户为管理用户配置相应账号，并按照用户角色级别赋予管理用户操作权限。 |
| f）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； | 经核查配置文件及访谈网络管理员，交换机中访问控制策略为管理用户的交换机中配置文件等进行配置管理及访问管理等，访问控制粒度达到主体为用户级、客体为文件级。 |
| g）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。 | 经核查配置文件及访谈网络管理员，未对重要主体和客体设置安全标记。 |
| 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； | 经现场访谈网络管理员及核查交换机配置，输入命令display logbuffer reverse，返回信息为logbuffer:enable；确认交换机中其中安全审计功能，通过查看审计记录内容，确认审计记录中包含设备运行记录及用户操作行为审计记录等。 |
| 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； | 经现场核查交换机中审计记录内容，审计记录中包含：日期、时间、主机名、类型、IP地址、用户名、详情等。 |
| 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、经访谈网络管理员，交换机中所有用户均无权限对审计记录进行删除或修改，并且管理员在备份服务器（10.33.110.160）中添加审计记录下载脚本（python脚本），实时将交换机中审计记录下载至备份服务器中进行备份；2、经现场核查备份服务器（10.33.110.160）中/home/network\_backup目录中存在审计记录备份文件，备份文件宿主为root，权限为744，其他用户仅拥有读权限。 |
| d）应对审计进程进行保护，防止未经授权的中断。 | 经现场访谈网络管理员，交换机中审计进程受系统进程保护，所有用户均无权限将审计进程单独中断。 |
| 入侵防范 | a）应遵循最小安装的原则，仅安装需要的组件和应用程序； | 经访谈网络管理员及核查配置文件，交换机为厂商提供独立封装系统，不允许安装其他组件及应用程序，遵循最小安装原则。 |
| b）应关闭不需要的系统服务、默认共享和高危端口； | 经现场访谈网络管理员及核查交换机配置，输入display current-fonfiguration，返回信息HTTP、Telnet协议均已关闭，交换机中未启用不需要的系统服务、默认共享及高危端口。 |
| c）应通过设定终端接入方式或网络地址范围对通过网络进行管理的管理终端进行限制； | 经访谈网络管理员，在防火墙中添加访问控制策略，仅允许管理用户通过堡垒机远程管理网络设备、安全设备及服务器等，经核查防火墙中访问控制策略，具备堡垒机地址-设备管理网段（10.33.0.0）的访问控制策略。 |
| d）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； | 该测评项测评对象为业务应用系统、中间件和系统管理软件，故将该项调整为不适用。 |
| e）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； | 1、经访谈网络管理员，会定期对官方网站通报的安全漏洞进行评估，然后从官方网站下载安全补丁，经过综合评估测试后对交换机系统进行补丁修复，避免系统中存在安全漏洞，2、经现场漏洞扫描，未发现交换机中存在安全漏洞。 |
| f）应能够检测到对重要节点进行入侵的行为，并在发生严重入侵事件时提供报警。 | 经访谈网络管理员，被测系统中部署了360AISA全流量威胁分析系统和360本地安全大脑，通过将被测系统中全部流量镜像发送到360AISA全流量威胁分析系统及360本地安全大脑中进行分析监测，发现入侵事件后及时通过钉钉报警，并且能够自动阻断。 |
| 可信验证 | a）可基于可信根对计算设备的系统引导程序、系统程序、重要配置参数和应用程序等进行可信验证，并在应用程序的关键执行环节进行动态可信验证，在检测到其可信性受到破坏后进行报警，并将验证结果形成审计记录送至安全管理中心。 | 未基于可信根对计算设备提供可信验证。 |
| 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； | 经现场访谈网络管理员及对交换机配置，交换机中关闭Telnet协议，采用SSH协议进行通信，保证重要数据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。 | 经访谈网络管理员及核查H3C S6800系列交换机产品文档，文件中目录05-参考指南--05文件系统管理命令中包含：“交换机中文件系统通常使用摘要算法（SHA-256）对文件计算摘要值，用于验证文件的正确性和完整性”。 |
| 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； | 经现场访谈网络管理员及对交换机配置，交换机中关闭Telnet协议，采用SSH协议进行通信，保证重要数据在传输过程中的保密性。 |
| b）应采用密码技术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个人信息等。 | 经访谈网管理员，管理员在设置用户口令时添加simple参数，经核查H3C S6800系列交换机产品文档，在文档05-参考指南--03-登录设备命令--1、登录设备--1.1等设备命令--1.1.28 set authentication password中正对simple参数进行说明：“simple：以明文方式设置密码，该密码将以密文方式存储。 |
| 数据备份恢复 | a）应提供重要数据的本地数据备份与恢复功能； | 经现场访谈网络管理员及核查相应配置，在备份服务器中配置python脚本，并设置每天凌晨4点将交换机中配置文件下载至备份服务器中进行备份，管理员每周对备份文件进行巡检，确保配置文件完整备份至备份服务器中。 |
| b）应提供异地实时备份功能，利用通信网络将重要数据实时备份至备份场地； | 1、经现场访谈网络管理员，管理员添加了数据同步策略，每天将备份服务器中备份文件拷贝至阿里公共云备份服务器中进行备份；2、经核查阿里公共云备份服务器（10.30.19.10）中备份目录/data/network-backup中具备网络设备配置备份文件；3、综上，因世纪互联IDC机房及阿里云公共云均在上海市，未实现异地实时备份功能。 |
| c）应提供重要数据处理系统的热冗余，保证系统的高可用性。 | 经访谈访问管理员及核查网络拓扑图，重要数据处理系统中采用双机冗余部署，保证系统的高可用性。 |

4.1.1.4. 业务接入交换机10

|  |  |  |
| --- | --- | --- |
| **安全控制点** | **测评指标** | **结果记录** |
| 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、经现场访谈网络管理员，交换机采用用户名、口令进行身份标识及身份鉴别；2、经核查交换机配置，输入display password-control命令，返回信息为 Password aging:Enabled (90 days) Password length: Enabled (10 characters) Password composition:Enabled (3 types, 1 characters per type) Password history: Enabled (max history records:4)，通过返回信息确认：用户口令长度为至少10位，包含数字、字母、字符三种类型，用户口令更改周期为90天；3、通过现场在交换机中创建与网络管理员ylops同名账户时，交换机中会提示用户名已存在，无法创重名用户，确认用户标识具备唯一性。 |
| 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、经现场核查交换机配置策略，输入display password-control命令，返回信息为 Maximum login attempts: 3，Action for exceeding login attempts: Lock user for 1 minutes、User authentication timeout：600 seconds；2、通过返回信息确认用户连续错误登录3次锁定账户1分钟，用户登录连接超时时间限制为600秒。 |
| 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； | 1、经现场访谈网络管理员及核查其远程连接交换机的方式，管理员在远程管理交换机时采用SSH协议进行通信，防止鉴别信息在网络传输过程中被窃听；2、访谈网络管理员，Telnet协议默认为关闭状态，通过输入命令telnet server enable尝试启用Telnet协议，返回信息为Telnet is insecure because it transmits data in plaintext form，Telnet协议未启成功；3，通过在终端Telnet该交换机，无法连接成功。 |
| 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。 | 经现场核查网络管理员远程登录交换机方式，交换机仅采用用户名、口令方式进行身份鉴别，未采用两种或两种以上组合的鉴别技术对用户进行身份鉴别。 |
| 访问控制 | a）应对登录的用户分配账户和权限； | 1、经现场核查交换机中用户信息，通过输入display local-user命令，返回信息中显示交换机中存在security、tulei、xuweilai、ylops等用户，其中security的 user role list：level-1，network-operator；tulei、xuweilai、ylops的 user role list：network-admin,network-operator；2、经访谈网络管理员，其中tulei、xuweilai为两位网络管理员账号，ylops为网络主管账户，security为安全管理账号。 |
| b）应重命名或删除默认账户，修改默认账户的默认口令； | 1、经现场核查交换机中用户信息，通过输入display local-user命令，返回信息中显示交换机中存在security、tulei、xuweilai、ylops等用户,不存在默认账户，2、经核查交换机配置，输入display password-control命令，返回信息为 Password aging:Enabled (90 days) Password length: Enabled (10 characters) Password composition:Enabled (3 types, 1 characters per type) Password history: Enabled (max history records：3，用户口令已按照复杂度策略更改。 |
| 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； | 经现场核查交换机中用户信息，通过输入display local-user命令，返回信息中显示交换机中存在security、tulei、xuweilai、ylops等用户,经访谈网络管理员，其中tulei、xuweilai为两位网络管理员账号，ylops为网络主管账户，security为安全管理账号，不存在多余、过期、共享账户。 |
| 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； | 经现场核查交换机中用户信息，通过输入display local-user命令，返回信息中显示交换机中存在security、tulei、xuweilai、ylops等用户，经访谈网络管理员，交换机中未单独创建审计管理员账户，并且网络管理员权限为超管用户权限，未实现管理用户权限最小化及权限分离。 |
| e）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； | 经核查配置文件及访谈网络管理员，交换机中由网络管理员角色账户为管理用户配置相应账号，并按照用户角色级别赋予管理用户操作权限。 |
| f）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； | 经核查配置文件及访谈网络管理员，交换机中访问控制策略为管理用户的交换机中配置文件等进行配置管理及访问管理等，访问控制粒度达到主体为用户级、客体为文件级。 |
| g）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。 | 经核查配置文件及访谈网络管理员，未对重要主体和客体设置安全标记。 |
| 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； | 经现场访谈网络管理员及核查交换机配置，输入命令display logbuffer reverse，返回信息为logbuffer:enable；确认交换机中其中安全审计功能，通过查看审计记录内容，确认审计记录中包含设备运行记录及用户操作行为审计记录等。 |
| 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； | 经现场核查交换机中审计记录内容，审计记录中包含：日期、时间、主机名、类型、IP地址、用户名、详情等。 |
| 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、经访谈网络管理员，交换机中所有用户均无权限对审计记录进行删除或修改，并且管理员在备份服务器（10.33.110.160）中添加审计记录下载脚本（python脚本），实时将交换机中审计记录下载至备份服务器中进行备份；2、经现场核查备份服务器（10.33.110.160）中/home/network\_backup目录中存在审计记录备份文件，备份文件宿主为root，权限为744，其他用户仅拥有读权限。 |
| d）应对审计进程进行保护，防止未经授权的中断。 | 经现场访谈网络管理员，交换机中审计进程受系统进程保护，所有用户均无权限将审计进程单独中断。 |
| 入侵防范 | a）应遵循最小安装的原则，仅安装需要的组件和应用程序； | 经访谈网络管理员及核查配置文件，交换机为厂商提供独立封装系统，不允许安装其他组件及应用程序，遵循最小安装原则。 |
| b）应关闭不需要的系统服务、默认共享和高危端口； | 经现场访谈网络管理员及核查交换机配置，输入display current-fonfiguration，返回信息HTTP、Telnet协议均已关闭，交换机中未启用不需要的系统服务、默认共享及高危端口。 |
| c）应通过设定终端接入方式或网络地址范围对通过网络进行管理的管理终端进行限制； | 经访谈网络管理员，在防火墙中添加访问控制策略，仅允许管理用户通过堡垒机远程管理网络设备、安全设备及服务器等，经核查防火墙中访问控制策略，具备堡垒机地址-设备管理网段（10.33.0.0）的访问控制策略。 |
| d）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； | 该测评项测评对象为业务应用系统、中间件和系统管理软件，故将该项调整为不适用。 |
| e）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； | 1、经访谈网络管理员，会定期对官方网站通报的安全漏洞进行评估，然后从官方网站下载安全补丁，经过综合评估测试后对交换机系统进行补丁修复，避免系统中存在安全漏洞，2、经现场漏洞扫描，未发现交换机中存在安全漏洞。 |
| f）应能够检测到对重要节点进行入侵的行为，并在发生严重入侵事件时提供报警。 | 经访谈网络管理员，被测系统中部署了360AISA全流量威胁分析系统和360本地安全大脑，通过将被测系统中全部流量镜像发送到360AISA全流量威胁分析系统及360本地安全大脑中进行分析监测，发现入侵事件后及时通过钉钉报警，并且能够自动阻断。 |
| 可信验证 | a）可基于可信根对计算设备的系统引导程序、系统程序、重要配置参数和应用程序等进行可信验证，并在应用程序的关键执行环节进行动态可信验证，在检测到其可信性受到破坏后进行报警，并将验证结果形成审计记录送至安全管理中心。 | 未基于可信根对计算设备提供可信验证。 |
| 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； | 经现场访谈网络管理员及对交换机配置，交换机中关闭Telnet协议，采用SSH协议进行通信，保证重要数据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。 | 经访谈网络管理员及核查H3C S6800系列交换机产品文档，文件中目录05-参考指南--05文件系统管理命令中包含：“交换机中文件系统通常使用摘要算法（SHA-256）对文件计算摘要值，用于验证文件的正确性和完整性”。 |
| 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； | 经现场访谈网络管理员及对交换机配置，交换机中关闭Telnet协议，采用SSH协议进行通信，保证重要数据在传输过程中的保密性。 |
| b）应采用密码技术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个人信息等。 | 经访谈网管理员，管理员在设置用户口令时添加simple参数，经核查H3C S6800系列交换机产品文档，在文档05-参考指南--03-登录设备命令--1、登录设备--1.1等设备命令--1.1.28 set authentication password中正对simple参数进行说明：“simple：以明文方式设置密码，该密码将以密文方式存储。 |
| 数据备份恢复 | a）应提供重要数据的本地数据备份与恢复功能； | 经现场访谈网络管理员及核查相应配置，在备份服务器中配置python脚本，并设置每天凌晨4点将交换机中配置文件下载至备份服务器中进行备份，管理员每周对备份文件进行巡检，确保配置文件完整备份至备份服务器中。 |
| b）应提供异地实时备份功能，利用通信网络将重要数据实时备份至备份场地； | 1、经现场访谈网络管理员，管理员添加了数据同步策略，每天将备份服务器中备份文件拷贝至阿里公共云备份服务器中进行备份；2、经核查阿里公共云备份服务器（10.30.19.10）中备份目录/data/network-backup中具备网络设备配置备份文件；3、综上，因世纪互联IDC机房及阿里云公共云均在上海市，未实现异地实时备份功能。 |
| c）应提供重要数据处理系统的热冗余，保证系统的高可用性。 | 经访谈访问管理员及核查网络拓扑图，重要数据处理系统中采用双机冗余部署，保证系统的高可用性。 |

4.1.1.5. 业务接入交换机11

|  |  |  |
| --- | --- | --- |
| **安全控制点** | **测评指标** | **结果记录** |
| 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、经现场访谈网络管理员，交换机采用用户名、口令进行身份标识及身份鉴别；2、经核查交换机配置，输入display password-control命令，返回信息为 Password aging:Enabled (90 days) Password length: Enabled (10 characters) Password composition:Enabled (3 types, 1 characters per type) Password history: Enabled (max history records:4)，通过返回信息确认：用户口令长度为至少10位，包含数字、字母、字符三种类型，用户口令更改周期为90天；3、通过现场在交换机中创建与网络管理员ylops同名账户时，交换机中会提示用户名已存在，无法创重名用户，确认用户标识具备唯一性。 |
| 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、经现场核查交换机配置策略，输入display password-control命令，返回信息为 Maximum login attempts: 3，Action for exceeding login attempts: Lock user for 1 minutes、User authentication timeout：600 seconds；2、通过返回信息确认用户连续错误登录3次锁定账户1分钟，用户登录连接超时时间限制为600秒。 |
| 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； | 1、经现场访谈网络管理员及核查其远程连接交换机的方式，管理员在远程管理交换机时采用SSH协议进行通信，防止鉴别信息在网络传输过程中被窃听；2、访谈网络管理员，Telnet协议默认为关闭状态，通过输入命令telnet server enable尝试启用Telnet协议，返回信息为Telnet is insecure because it transmits data in plaintext form，Telnet协议未启成功；3，通过在终端Telnet该交换机，无法连接成功。 |
| 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。 | 经现场核查网络管理员远程登录交换机方式，交换机仅采用用户名、口令方式进行身份鉴别，未采用两种或两种以上组合的鉴别技术对用户进行身份鉴别。 |
| 访问控制 | a）应对登录的用户分配账户和权限； | 1、经现场核查交换机中用户信息，通过输入display local-user命令，返回信息中显示交换机中存在security、tulei、xuweilai、ylops等用户，其中security的 user role list：level-1，network-operator；tulei、xuweilai、ylops的 user role list：network-admin,network-operator；2、经访谈网络管理员，其中tulei、xuweilai为两位网络管理员账号，ylops为网络主管账户，security为安全管理账号。 |
| b）应重命名或删除默认账户，修改默认账户的默认口令； | 1、经现场核查交换机中用户信息，通过输入display local-user命令，返回信息中显示交换机中存在security、tulei、xuweilai、ylops等用户,不存在默认账户，2、经核查交换机配置，输入display password-control命令，返回信息为 Password aging:Enabled (90 days) Password length: Enabled (10 characters) Password composition:Enabled (3 types, 1 characters per type) Password history: Enabled (max history records：3，用户口令已按照复杂度策略更改。 |
| 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； | 经现场核查交换机中用户信息，通过输入display local-user命令，返回信息中显示交换机中存在security、tulei、xuweilai、ylops等用户,经访谈网络管理员，其中tulei、xuweilai为两位网络管理员账号，ylops为网络主管账户，security为安全管理账号，不存在多余、过期、共享账户。 |
| 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； | 经现场核查交换机中用户信息，通过输入display local-user命令，返回信息中显示交换机中存在security、tulei、xuweilai、ylops等用户，经访谈网络管理员，交换机中未单独创建审计管理员账户，并且网络管理员权限为超管用户权限，未实现管理用户权限最小化及权限分离。 |
| e）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； | 经核查配置文件及访谈网络管理员，交换机中由网络管理员角色账户为管理用户配置相应账号，并按照用户角色级别赋予管理用户操作权限。 |
| f）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； | 经核查配置文件及访谈网络管理员，交换机中访问控制策略为管理用户的交换机中配置文件等进行配置管理及访问管理等，访问控制粒度达到主体为用户级、客体为文件级。 |
| g）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。 | 经核查配置文件及访谈网络管理员，未对重要主体和客体设置安全标记。 |
| 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； | 经现场访谈网络管理员及核查交换机配置，输入命令display logbuffer reverse，返回信息为logbuffer:enable；确认交换机中其中安全审计功能，通过查看审计记录内容，确认审计记录中包含设备运行记录及用户操作行为审计记录等。 |
| 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； | 经现场核查交换机中审计记录内容，审计记录中包含：日期、时间、主机名、类型、IP地址、用户名、详情等。 |
| 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、经访谈网络管理员，交换机中所有用户均无权限对审计记录进行删除或修改，并且管理员在备份服务器（10.33.110.160）中添加审计记录下载脚本（python脚本），实时将交换机中审计记录下载至备份服务器中进行备份；2、经现场核查备份服务器（10.33.110.160）中/home/network\_backup目录中存在审计记录备份文件，备份文件宿主为root，权限为744，其他用户仅拥有读权限。 |
| d）应对审计进程进行保护，防止未经授权的中断。 | 经现场访谈网络管理员，交换机中审计进程受系统进程保护，所有用户均无权限将审计进程单独中断。 |
| 入侵防范 | a）应遵循最小安装的原则，仅安装需要的组件和应用程序； | 经访谈网络管理员及核查配置文件，交换机为厂商提供独立封装系统，不允许安装其他组件及应用程序，遵循最小安装原则。 |
| b）应关闭不需要的系统服务、默认共享和高危端口； | 经现场访谈网络管理员及核查交换机配置，输入display current-fonfiguration，返回信息HTTP、Telnet协议均已关闭，交换机中未启用不需要的系统服务、默认共享及高危端口。 |
| c）应通过设定终端接入方式或网络地址范围对通过网络进行管理的管理终端进行限制； | 经访谈网络管理员，在防火墙中添加访问控制策略，仅允许管理用户通过堡垒机远程管理网络设备、安全设备及服务器等，经核查防火墙中访问控制策略，具备堡垒机地址-设备管理网段（10.33.0.0）的访问控制策略。 |
| d）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； | 该测评项测评对象为业务应用系统、中间件和系统管理软件，故将该项调整为不适用。 |
| e）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； | 1、经访谈网络管理员，会定期对官方网站通报的安全漏洞进行评估，然后从官方网站下载安全补丁，经过综合评估测试后对交换机系统进行补丁修复，避免系统中存在安全漏洞，2、经现场漏洞扫描，未发现交换机中存在安全漏洞。 |
| f）应能够检测到对重要节点进行入侵的行为，并在发生严重入侵事件时提供报警。 | 经访谈网络管理员，被测系统中部署了360AISA全流量威胁分析系统和360本地安全大脑，通过将被测系统中全部流量镜像发送到360AISA全流量威胁分析系统及360本地安全大脑中进行分析监测，发现入侵事件后及时通过钉钉报警，并且能够自动阻断。 |
| 可信验证 | a）可基于可信根对计算设备的系统引导程序、系统程序、重要配置参数和应用程序等进行可信验证，并在应用程序的关键执行环节进行动态可信验证，在检测到其可信性受到破坏后进行报警，并将验证结果形成审计记录送至安全管理中心。 | 未基于可信根对计算设备提供可信验证。 |
| 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； | 经现场访谈网络管理员及对交换机配置，交换机中关闭Telnet协议，采用SSH协议进行通信，保证重要数据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。 | 经访谈网络管理员及核查H3C S6800系列交换机产品文档，文件中目录05-参考指南--05文件系统管理命令中包含：“交换机中文件系统通常使用摘要算法（SHA-256）对文件计算摘要值，用于验证文件的正确性和完整性”。 |
| 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； | 经现场访谈网络管理员及对交换机配置，交换机中关闭Telnet协议，采用SSH协议进行通信，保证重要数据在传输过程中的保密性。 |
| b）应采用密码技术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个人信息等。 | 经访谈网管理员，管理员在设置用户口令时添加simple参数，经核查H3C S6800系列交换机产品文档，在文档05-参考指南--03-登录设备命令--1、登录设备--1.1等设备命令--1.1.28 set authentication password中正对simple参数进行说明：“simple：以明文方式设置密码，该密码将以密文方式存储。 |
| 数据备份恢复 | a）应提供重要数据的本地数据备份与恢复功能； | 经现场访谈网络管理员及核查相应配置，在备份服务器中配置python脚本，并设置每天凌晨4点将交换机中配置文件下载至备份服务器中进行备份，管理员每周对备份文件进行巡检，确保配置文件完整备份至备份服务器中。 |
| b）应提供异地实时备份功能，利用通信网络将重要数据实时备份至备份场地； | 1、经现场访谈网络管理员，管理员添加了数据同步策略，每天将备份服务器中备份文件拷贝至阿里公共云备份服务器中进行备份；2、经核查阿里公共云备份服务器（10.30.19.10）中备份目录/data/network-backup中具备网络设备配置备份文件；3、综上，因世纪互联IDC机房及阿里云公共云均在上海市，未实现异地实时备份功能。 |
| c）应提供重要数据处理系统的热冗余，保证系统的高可用性。 | 经访谈访问管理员及核查网络拓扑图，重要数据处理系统中采用双机冗余部署，保证系统的高可用性。 |

4.1.1.6. 业务接入交换机12

|  |  |  |
| --- | --- | --- |
| **安全控制点** | **测评指标** | **结果记录** |
| 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、经现场访谈网络管理员，交换机采用用户名、口令进行身份标识及身份鉴别；2、经核查交换机配置，输入display password-control命令，返回信息为 Password aging:Enabled (90 days) Password length: Enabled (10 characters) Password composition:Enabled (3 types, 1 characters per type) Password history: Enabled (max history records:4)，通过返回信息确认：用户口令长度为至少10位，包含数字、字母、字符三种类型，用户口令更改周期为90天；3、通过现场在交换机中创建与网络管理员ylops同名账户时，交换机中会提示用户名已存在，无法创重名用户，确认用户标识具备唯一性。 |
| 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、经现场核查交换机配置策略，输入display password-control命令，返回信息为 Maximum login attempts: 3，Action for exceeding login attempts: Lock user for 1 minutes、User authentication timeout：600 seconds；2、通过返回信息确认用户连续错误登录3次锁定账户1分钟，用户登录连接超时时间限制为600秒。 |
| 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； | 1、经现场访谈网络管理员及核查其远程连接交换机的方式，管理员在远程管理交换机时采用SSH协议进行通信，防止鉴别信息在网络传输过程中被窃听；2、访谈网络管理员，Telnet协议默认为关闭状态，通过输入命令telnet server enable尝试启用Telnet协议，返回信息为Telnet is insecure because it transmits data in plaintext form，Telnet协议未启成功；3，通过在终端Telnet该交换机，无法连接成功。 |
| 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。 | 经现场核查网络管理员远程登录交换机方式，交换机仅采用用户名、口令方式进行身份鉴别，未采用两种或两种以上组合的鉴别技术对用户进行身份鉴别。 |
| 访问控制 | a）应对登录的用户分配账户和权限； | 1、经现场核查交换机中用户信息，通过输入display local-user命令，返回信息中显示交换机中存在security、tulei、xuweilai、ylops等用户，其中security的 user role list：level-1，network-operator；tulei、xuweilai、ylops的 user role list：network-admin,network-operator；2、经访谈网络管理员，其中tulei、xuweilai为两位网络管理员账号，ylops为网络主管账户，security为安全管理账号。 |
| b）应重命名或删除默认账户，修改默认账户的默认口令； | 1、经现场核查交换机中用户信息，通过输入display local-user命令，返回信息中显示交换机中存在security、tulei、xuweilai、ylops等用户,不存在默认账户，2、经核查交换机配置，输入display password-control命令，返回信息为 Password aging:Enabled (90 days) Password length: Enabled (10 characters) Password composition:Enabled (3 types, 1 characters per type) Password history: Enabled (max history records：3，用户口令已按照复杂度策略更改。 |
| 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； | 经现场核查交换机中用户信息，通过输入display local-user命令，返回信息中显示交换机中存在security、tulei、xuweilai、ylops等用户,经访谈网络管理员，其中tulei、xuweilai为两位网络管理员账号，ylops为网络主管账户，security为安全管理账号，不存在多余、过期、共享账户。 |
| 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； | 经现场核查交换机中用户信息，通过输入display local-user命令，返回信息中显示交换机中存在security、tulei、xuweilai、ylops等用户，经访谈网络管理员，交换机中未单独创建审计管理员账户，并且网络管理员权限为超管用户权限，未实现管理用户权限最小化及权限分离。 |
| e）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； | 经核查配置文件及访谈网络管理员，交换机中由网络管理员角色账户为管理用户配置相应账号，并按照用户角色级别赋予管理用户操作权限。 |
| f）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； | 经核查配置文件及访谈网络管理员，交换机中访问控制策略为管理用户的交换机中配置文件等进行配置管理及访问管理等，访问控制粒度达到主体为用户级、客体为文件级。 |
| g）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。 | 经核查配置文件及访谈网络管理员，未对重要主体和客体设置安全标记。 |
| 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； | 经现场访谈网络管理员及核查交换机配置，输入命令display logbuffer reverse，返回信息为logbuffer:enable；确认交换机中其中安全审计功能，通过查看审计记录内容，确认审计记录中包含设备运行记录及用户操作行为审计记录等。 |
| 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； | 经现场核查交换机中审计记录内容，审计记录中包含：日期、时间、主机名、类型、IP地址、用户名、详情等。 |
| 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、经访谈网络管理员，交换机中所有用户均无权限对审计记录进行删除或修改，并且管理员在备份服务器（10.33.110.160）中添加审计记录下载脚本（python脚本），实时将交换机中审计记录下载至备份服务器中进行备份；2、经现场核查备份服务器（10.33.110.160）中/home/network\_backup目录中存在审计记录备份文件，备份文件宿主为root，权限为744，其他用户仅拥有读权限。 |
| d）应对审计进程进行保护，防止未经授权的中断。 | 经现场访谈网络管理员，交换机中审计进程受系统进程保护，所有用户均无权限将审计进程单独中断。 |
| 入侵防范 | a）应遵循最小安装的原则，仅安装需要的组件和应用程序； | 经访谈网络管理员及核查配置文件，交换机为厂商提供独立封装系统，不允许安装其他组件及应用程序，遵循最小安装原则。 |
| b）应关闭不需要的系统服务、默认共享和高危端口； | 经现场访谈网络管理员及核查交换机配置，输入display current-fonfiguration，返回信息HTTP、Telnet协议均已关闭，交换机中未启用不需要的系统服务、默认共享及高危端口。 |
| c）应通过设定终端接入方式或网络地址范围对通过网络进行管理的管理终端进行限制； | 经访谈网络管理员，在防火墙中添加访问控制策略，仅允许管理用户通过堡垒机远程管理网络设备、安全设备及服务器等，经核查防火墙中访问控制策略，具备堡垒机地址-设备管理网段（10.33.0.0）的访问控制策略。 |
| d）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； | 该测评项测评对象为业务应用系统、中间件和系统管理软件，故将该项调整为不适用。 |
| e）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； | 1、经访谈网络管理员，会定期对官方网站通报的安全漏洞进行评估，然后从官方网站下载安全补丁，经过综合评估测试后对交换机系统进行补丁修复，避免系统中存在安全漏洞，2、经现场漏洞扫描，未发现交换机中存在安全漏洞。 |
| f）应能够检测到对重要节点进行入侵的行为，并在发生严重入侵事件时提供报警。 | 经访谈网络管理员，被测系统中部署了360AISA全流量威胁分析系统和360本地安全大脑，通过将被测系统中全部流量镜像发送到360AISA全流量威胁分析系统及360本地安全大脑中进行分析监测，发现入侵事件后及时通过钉钉报警，并且能够自动阻断。 |
| 可信验证 | a）可基于可信根对计算设备的系统引导程序、系统程序、重要配置参数和应用程序等进行可信验证，并在应用程序的关键执行环节进行动态可信验证，在检测到其可信性受到破坏后进行报警，并将验证结果形成审计记录送至安全管理中心。 | 未基于可信根对计算设备提供可信验证。 |
| 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； | 经现场访谈网络管理员及对交换机配置，交换机中关闭Telnet协议，采用SSH协议进行通信，保证重要数据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。 | 经访谈网络管理员及核查H3C S6800系列交换机产品文档，文件中目录05-参考指南--05文件系统管理命令中包含：“交换机中文件系统通常使用摘要算法（SHA-256）对文件计算摘要值，用于验证文件的正确性和完整性”。 |
| 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； | 经现场访谈网络管理员及对交换机配置，交换机中关闭Telnet协议，采用SSH协议进行通信，保证重要数据在传输过程中的保密性。 |
| b）应采用密码技术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个人信息等。 | 经访谈网管理员，管理员在设置用户口令时添加simple参数，经核查H3C S6800系列交换机产品文档，在文档05-参考指南--03-登录设备命令--1、登录设备--1.1等设备命令--1.1.28 set authentication password中正对simple参数进行说明：“simple：以明文方式设置密码，该密码将以密文方式存储。 |
| 数据备份恢复 | a）应提供重要数据的本地数据备份与恢复功能； | 经现场访谈网络管理员及核查相应配置，在备份服务器中配置python脚本，并设置每天凌晨4点将交换机中配置文件下载至备份服务器中进行备份，管理员每周对备份文件进行巡检，确保配置文件完整备份至备份服务器中。 |
| b）应提供异地实时备份功能，利用通信网络将重要数据实时备份至备份场地； | 1、经现场访谈网络管理员，管理员添加了数据同步策略，每天将备份服务器中备份文件拷贝至阿里公共云备份服务器中进行备份；2、经核查阿里公共云备份服务器（10.30.19.10）中备份目录/data/network-backup中具备网络设备配置备份文件；3、综上，因世纪互联IDC机房及阿里云公共云均在上海市，未实现异地实时备份功能。 |
| c）应提供重要数据处理系统的热冗余，保证系统的高可用性。 | 经访谈访问管理员及核查网络拓扑图，重要数据处理系统中采用双机冗余部署，保证系统的高可用性。 |

4.1.1.7. 管理接入交换机1

|  |  |  |
| --- | --- | --- |
| **安全控制点** | **测评指标** | **结果记录** |
| 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、经现场访谈网络管理员，交换机采用用户名、口令进行身份标识及身份鉴别；2、经核查交换机配置，输入display password-control命令，返回信息为 Password aging:Enabled (90 days) Password length: Enabled (10 characters) Password composition:Enabled (3 types, 1 characters per type) Password history: Enabled (max history records:4)，通过返回信息确认：用户口令长度为至少10位，包含数字、字母、字符三种类型，用户口令更改周期为90天；3、通过现场在交换机中创建与网络管理员ylops同名账户时，交换机中会提示用户名已存在，无法创重名用户，确认用户标识具备唯一性。 |
| 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、经现场核查交换机配置策略，输入display password-control命令，返回信息为 Maximum login attempts: 3，Action for exceeding login attempts: Lock user for 1 minutes、User authentication timeout：600 seconds；2、通过返回信息确认用户连续错误登录3次锁定账户1分钟，用户登录连接超时时间限制为600秒。 |
| 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； | 1、经现场访谈网络管理员及核查其远程连接交换机的方式，管理员在远程管理交换机时采用SSH协议进行通信，防止鉴别信息在网络传输过程中被窃听；2、访谈网络管理员，Telnet协议默认为关闭状态，通过输入命令telnet server enable尝试启用Telnet协议，返回信息为Telnet is insecure because it transmits data in plaintext form，Telnet协议未启成功；3，通过在终端Telnet该交换机，无法连接成功。 |
| 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。 | 经现场核查网络管理员远程登录交换机方式，交换机仅采用用户名、口令方式进行身份鉴别，未采用两种或两种以上组合的鉴别技术对用户进行身份鉴别。 |
| 访问控制 | a）应对登录的用户分配账户和权限； | 1、经现场核查交换机中用户信息，通过输入display local-user命令，返回信息中显示交换机中存在security、tulei、xuweilai、ylops等用户，其中security的 user role list：level-1，network-operator；tulei、xuweilai、ylops的 user role list：network-admin,network-operator；2、经访谈网络管理员，其中tulei、xuweilai为两位网络管理员账号，ylops为网络主管账户，security为安全管理账号。 |
| b）应重命名或删除默认账户，修改默认账户的默认口令； | 1、经现场核查交换机中用户信息，通过输入display local-user命令，返回信息中显示交换机中存在security、tulei、xuweilai、ylops等用户,不存在默认账户，2、经核查交换机配置，输入display password-control命令，返回信息为 Password aging:Enabled (90 days) Password length: Enabled (10 characters) Password composition:Enabled (3 types, 1 characters per type) Password history: Enabled (max history records：3，用户口令已按照复杂度策略更改。 |
| 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； | 经现场核查交换机中用户信息，通过输入display local-user命令，返回信息中显示交换机中存在security、tulei、xuweilai、ylops等用户,经访谈网络管理员，其中tulei、xuweilai为两位网络管理员账号，ylops为网络主管账户，security为安全管理账号，不存在多余、过期、共享账户。 |
| 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； | 经现场核查交换机中用户信息，通过输入display local-user命令，返回信息中显示交换机中存在security、tulei、xuweilai、ylops等用户，经访谈网络管理员，交换机中未单独创建审计管理员账户，并且网络管理员权限为超管用户权限，未实现管理用户权限最小化及权限分离。 |
| e）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； | 经核查配置文件及访谈网络管理员，交换机中由网络管理员角色账户为管理用户配置相应账号，并按照用户角色级别赋予管理用户操作权限。 |
| f）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； | 经核查配置文件及访谈网络管理员，交换机中访问控制策略为管理用户的交换机中配置文件等进行配置管理及访问管理等，访问控制粒度达到主体为用户级、客体为文件级。 |
| g）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。 | 经核查配置文件及访谈网络管理员，未对重要主体和客体设置安全标记。 |
| 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； | 经现场访谈网络管理员及核查交换机配置，输入命令display logbuffer reverse，返回信息为logbuffer:enable；确认交换机中其中安全审计功能，通过查看审计记录内容，确认审计记录中包含设备运行记录及用户操作行为审计记录等。 |
| 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； | 经现场核查交换机中审计记录内容，审计记录中包含：日期、时间、主机名、类型、IP地址、用户名、详情等。 |
| 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、经访谈网络管理员，交换机中所有用户均无权限对审计记录进行删除或修改，并且管理员在备份服务器（10.33.110.160）中添加审计记录下载脚本（python脚本），实时将交换机中审计记录下载至备份服务器中进行备份；2、经现场核查备份服务器（10.33.110.160）中/home/network\_backup目录中存在审计记录备份文件，备份文件宿主为root，权限为744，其他用户仅拥有读权限。 |
| d）应对审计进程进行保护，防止未经授权的中断。 | 经现场访谈网络管理员，交换机中审计进程受系统进程保护，所有用户均无权限将审计进程单独中断。 |
| 入侵防范 | a）应遵循最小安装的原则，仅安装需要的组件和应用程序； | 经访谈网络管理员及核查配置文件，交换机为厂商提供独立封装系统，不允许安装其他组件及应用程序，遵循最小安装原则。 |
| b）应关闭不需要的系统服务、默认共享和高危端口； | 经现场访谈网络管理员及核查交换机配置，输入display current-fonfiguration，返回信息HTTP、Telnet协议均已关闭，交换机中未启用不需要的系统服务、默认共享及高危端口。 |
| c）应通过设定终端接入方式或网络地址范围对通过网络进行管理的管理终端进行限制； | 经访谈网络管理员，在防火墙中添加访问控制策略，仅允许管理用户通过堡垒机远程管理网络设备、安全设备及服务器等，经核查防火墙中访问控制策略，具备堡垒机地址-设备管理网段（10.33.0.0）的访问控制策略。 |
| d）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； | 该测评项测评对象为业务应用系统、中间件和系统管理软件，故将该项调整为不适用。 |
| e）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； | 1、经访谈网络管理员，会定期对官方网站通报的安全漏洞进行评估，然后从官方网站下载安全补丁，经过综合评估测试后对交换机系统进行补丁修复，避免系统中存在安全漏洞，2、经现场漏洞扫描，未发现交换机中存在安全漏洞。 |
| f）应能够检测到对重要节点进行入侵的行为，并在发生严重入侵事件时提供报警。 | 经访谈网络管理员，被测系统中部署了360AISA全流量威胁分析系统和360本地安全大脑，通过将被测系统中全部流量镜像发送到360AISA全流量威胁分析系统及360本地安全大脑中进行分析监测，发现入侵事件后及时通过钉钉报警，并且能够自动阻断。 |
| 可信验证 | a）可基于可信根对计算设备的系统引导程序、系统程序、重要配置参数和应用程序等进行可信验证，并在应用程序的关键执行环节进行动态可信验证，在检测到其可信性受到破坏后进行报警，并将验证结果形成审计记录送至安全管理中心。 | 未基于可信根对计算设备提供可信验证。 |
| 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； | 经现场访谈网络管理员及对交换机配置，交换机中关闭Telnet协议，采用SSH协议进行通信，保证重要数据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。 | 经访谈网络管理员及核查H3C S6800系列交换机产品文档，文件中目录05-参考指南--05文件系统管理命令中包含：“交换机中文件系统通常使用摘要算法（SHA-256）对文件计算摘要值，用于验证文件的正确性和完整性”。 |
| 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； | 经现场访谈网络管理员及对交换机配置，交换机中关闭Telnet协议，采用SSH协议进行通信，保证重要数据在传输过程中的保密性。 |
| b）应采用密码技术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个人信息等。 | 经访谈网管理员，管理员在设置用户口令时添加simple参数，经核查H3C S6800系列交换机产品文档，在文档05-参考指南--03-登录设备命令--1、登录设备--1.1等设备命令--1.1.28 set authentication password中正对simple参数进行说明：“simple：以明文方式设置密码，该密码将以密文方式存储。 |
| 数据备份恢复 | a）应提供重要数据的本地数据备份与恢复功能； | 经现场访谈网络管理员及核查相应配置，在备份服务器中配置python脚本，并设置每天凌晨4点将交换机中配置文件下载至备份服务器中进行备份，管理员每周对备份文件进行巡检，确保配置文件完整备份至备份服务器中。 |
| b）应提供异地实时备份功能，利用通信网络将重要数据实时备份至备份场地； | 1、经现场访谈网络管理员，管理员添加了数据同步策略，每天将备份服务器中备份文件拷贝至阿里公共云备份服务器中进行备份；2、经核查阿里公共云备份服务器（10.30.19.10）中备份目录/data/network-backup中具备网络设备配置备份文件；3、综上，因世纪互联IDC机房及阿里云公共云均在上海市，未实现异地实时备份功能。 |
| c）应提供重要数据处理系统的热冗余，保证系统的高可用性。 | 经访谈访问管理员及核查网络拓扑图，重要数据处理系统中采用双机冗余部署，保证系统的高可用性。 |

4.1.1.8. 管理接入交换机2

|  |  |  |
| --- | --- | --- |
| **安全控制点** | **测评指标** | **结果记录** |
| 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、经现场访谈网络管理员，交换机采用用户名、口令进行身份标识及身份鉴别；2、经核查交换机配置，输入display password-control命令，返回信息为 Password aging:Enabled (90 days) Password length: Enabled (10 characters) Password composition:Enabled (3 types, 1 characters per type) Password history: Enabled (max history records:4)，通过返回信息确认：用户口令长度为至少10位，包含数字、字母、字符三种类型，用户口令更改周期为90天；3、通过现场在交换机中创建与网络管理员ylops同名账户时，交换机中会提示用户名已存在，无法创重名用户，确认用户标识具备唯一性。 |
| 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、经现场核查交换机配置策略，输入display password-control命令，返回信息为 Maximum login attempts: 3，Action for exceeding login attempts: Lock user for 1 minutes、User authentication timeout：600 seconds；2、通过返回信息确认用户连续错误登录3次锁定账户1分钟，用户登录连接超时时间限制为600秒。 |
| 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； | 1、经现场访谈网络管理员及核查其远程连接交换机的方式，管理员在远程管理交换机时采用SSH协议进行通信，防止鉴别信息在网络传输过程中被窃听；2、访谈网络管理员，Telnet协议默认为关闭状态，通过输入命令telnet server enable尝试启用Telnet协议，返回信息为Telnet is insecure because it transmits data in plaintext form，Telnet协议未启成功；3，通过在终端Telnet该交换机，无法连接成功。 |
| 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。 | 经现场核查网络管理员远程登录交换机方式，交换机仅采用用户名、口令方式进行身份鉴别，未采用两种或两种以上组合的鉴别技术对用户进行身份鉴别。 |
| 访问控制 | a）应对登录的用户分配账户和权限； | 1、经现场核查交换机中用户信息，通过输入display local-user命令，返回信息中显示交换机中存在security、tulei、xuweilai、ylops等用户，其中security的 user role list：level-1，network-operator；tulei、xuweilai、ylops的 user role list：network-admin,network-operator；2、经访谈网络管理员，其中tulei、xuweilai为两位网络管理员账号，ylops为网络主管账户，security为安全管理账号。 |
| b）应重命名或删除默认账户，修改默认账户的默认口令； | 1、经现场核查交换机中用户信息，通过输入display local-user命令，返回信息中显示交换机中存在security、tulei、xuweilai、ylops等用户,不存在默认账户，2、经核查交换机配置，输入display password-control命令，返回信息为 Password aging:Enabled (90 days) Password length: Enabled (10 characters) Password composition:Enabled (3 types, 1 characters per type) Password history: Enabled (max history records：3，用户口令已按照复杂度策略更改。 |
| 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； | 经现场核查交换机中用户信息，通过输入display local-user命令，返回信息中显示交换机中存在security、tulei、xuweilai、ylops等用户,经访谈网络管理员，其中tulei、xuweilai为两位网络管理员账号，ylops为网络主管账户，security为安全管理账号，不存在多余、过期、共享账户。 |
| 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； | 经现场核查交换机中用户信息，通过输入display local-user命令，返回信息中显示交换机中存在security、tulei、xuweilai、ylops等用户，经访谈网络管理员，交换机中未单独创建审计管理员账户，并且网络管理员权限为超管用户权限，未实现管理用户权限最小化及权限分离。 |
| e）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； | 经核查配置文件及访谈网络管理员，交换机中由网络管理员角色账户为管理用户配置相应账号，并按照用户角色级别赋予管理用户操作权限。 |
| f）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； | 经核查配置文件及访谈网络管理员，交换机中访问控制策略为管理用户的交换机中配置文件等进行配置管理及访问管理等，访问控制粒度达到主体为用户级、客体为文件级。 |
| g）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。 | 经核查配置文件及访谈网络管理员，未对重要主体和客体设置安全标记。 |
| 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； | 经现场访谈网络管理员及核查交换机配置，输入命令display logbuffer reverse，返回信息为logbuffer:enable；确认交换机中其中安全审计功能，通过查看审计记录内容，确认审计记录中包含设备运行记录及用户操作行为审计记录等。 |
| 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； | 经现场核查交换机中审计记录内容，审计记录中包含：日期、时间、主机名、类型、IP地址、用户名、详情等。 |
| 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、经访谈网络管理员，交换机中所有用户均无权限对审计记录进行删除或修改，并且管理员在备份服务器（10.33.110.160）中添加审计记录下载脚本（python脚本），实时将交换机中审计记录下载至备份服务器中进行备份；2、经现场核查备份服务器（10.33.110.160）中/home/network\_backup目录中存在审计记录备份文件，备份文件宿主为root，权限为744，其他用户仅拥有读权限。 |
| d）应对审计进程进行保护，防止未经授权的中断。 | 经现场访谈网络管理员，交换机中审计进程受系统进程保护，所有用户均无权限将审计进程单独中断。 |
| 入侵防范 | a）应遵循最小安装的原则，仅安装需要的组件和应用程序； | 经访谈网络管理员及核查配置文件，交换机为厂商提供独立封装系统，不允许安装其他组件及应用程序，遵循最小安装原则。 |
| b）应关闭不需要的系统服务、默认共享和高危端口； | 经现场访谈网络管理员及核查交换机配置，输入display current-fonfiguration，返回信息HTTP、Telnet协议均已关闭，交换机中未启用不需要的系统服务、默认共享及高危端口。 |
| c）应通过设定终端接入方式或网络地址范围对通过网络进行管理的管理终端进行限制； | 经访谈网络管理员，在防火墙中添加访问控制策略，仅允许管理用户通过堡垒机远程管理网络设备、安全设备及服务器等，经核查防火墙中访问控制策略，具备堡垒机地址-设备管理网段（10.33.0.0）的访问控制策略。 |
| d）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； | 该测评项测评对象为业务应用系统、中间件和系统管理软件，故将该项调整为不适用。 |
| e）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； | 1、经访谈网络管理员，会定期对官方网站通报的安全漏洞进行评估，然后从官方网站下载安全补丁，经过综合评估测试后对交换机系统进行补丁修复，避免系统中存在安全漏洞，2、经现场漏洞扫描，未发现交换机中存在安全漏洞。 |
| f）应能够检测到对重要节点进行入侵的行为，并在发生严重入侵事件时提供报警。 | 经访谈网络管理员，被测系统中部署了360AISA全流量威胁分析系统和360本地安全大脑，通过将被测系统中全部流量镜像发送到360AISA全流量威胁分析系统及360本地安全大脑中进行分析监测，发现入侵事件后及时通过钉钉报警，并且能够自动阻断。 |
| 可信验证 | a）可基于可信根对计算设备的系统引导程序、系统程序、重要配置参数和应用程序等进行可信验证，并在应用程序的关键执行环节进行动态可信验证，在检测到其可信性受到破坏后进行报警，并将验证结果形成审计记录送至安全管理中心。 | 未基于可信根对计算设备提供可信验证。 |
| 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； | 经现场访谈网络管理员及对交换机配置，交换机中关闭Telnet协议，采用SSH协议进行通信，保证重要数据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。 | 经访谈网络管理员及核查H3C S6800系列交换机产品文档，文件中目录05-参考指南--05文件系统管理命令中包含：“交换机中文件系统通常使用摘要算法（SHA-256）对文件计算摘要值，用于验证文件的正确性和完整性”。 |
| 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； | 经现场访谈网络管理员及对交换机配置，交换机中关闭Telnet协议，采用SSH协议进行通信，保证重要数据在传输过程中的保密性。 |
| b）应采用密码技术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个人信息等。 | 经访谈网管理员，管理员在设置用户口令时添加simple参数，经核查H3C S6800系列交换机产品文档，在文档05-参考指南--03-登录设备命令--1、登录设备--1.1等设备命令--1.1.28 set authentication password中正对simple参数进行说明：“simple：以明文方式设置密码，该密码将以密文方式存储。 |
| 数据备份恢复 | a）应提供重要数据的本地数据备份与恢复功能； | 经现场访谈网络管理员及核查相应配置，在备份服务器中配置python脚本，并设置每天凌晨4点将交换机中配置文件下载至备份服务器中进行备份，管理员每周对备份文件进行巡检，确保配置文件完整备份至备份服务器中。 |
| b）应提供异地实时备份功能，利用通信网络将重要数据实时备份至备份场地； | 1、经现场访谈网络管理员，管理员添加了数据同步策略，每天将备份服务器中备份文件拷贝至阿里公共云备份服务器中进行备份；2、经核查阿里公共云备份服务器（10.30.19.10）中备份目录/data/network-backup中具备网络设备配置备份文件；3、综上，因世纪互联IDC机房及阿里云公共云均在上海市，未实现异地实时备份功能。 |
| c）应提供重要数据处理系统的热冗余，保证系统的高可用性。 | 经访谈访问管理员及核查网络拓扑图，重要数据处理系统中采用双机冗余部署，保证系统的高可用性。 |

4.1.1.9. 管理接入交换机3

|  |  |  |
| --- | --- | --- |
| **安全控制点** | **测评指标** | **结果记录** |
| 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、经现场访谈网络管理员，交换机采用用户名、口令进行身份标识及身份鉴别；2、经核查交换机配置，输入display password-control命令，返回信息为 Password aging:Enabled (90 days) Password length: Enabled (10 characters) Password composition:Enabled (3 types, 1 characters per type) Password history: Enabled (max history records:4)，通过返回信息确认：用户口令长度为至少10位，包含数字、字母、字符三种类型，用户口令更改周期为90天；3、通过现场在交换机中创建与网络管理员ylops同名账户时，交换机中会提示用户名已存在，无法创重名用户，确认用户标识具备唯一性。 |
| 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、经现场核查交换机配置策略，输入display password-control命令，返回信息为 Maximum login attempts: 3，Action for exceeding login attempts: Lock user for 1 minutes、User authentication timeout：600 seconds；2、通过返回信息确认用户连续错误登录3次锁定账户1分钟，用户登录连接超时时间限制为600秒。 |
| 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； | 1、经现场访谈网络管理员及核查其远程连接交换机的方式，管理员在远程管理交换机时采用SSH协议进行通信，防止鉴别信息在网络传输过程中被窃听；2、访谈网络管理员，Telnet协议默认为关闭状态，通过输入命令telnet server enable尝试启用Telnet协议，返回信息为Telnet is insecure because it transmits data in plaintext form，Telnet协议未启成功；3，通过在终端Telnet该交换机，无法连接成功。 |
| 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。 | 经现场核查网络管理员远程登录交换机方式，交换机仅采用用户名、口令方式进行身份鉴别，未采用两种或两种以上组合的鉴别技术对用户进行身份鉴别。 |
| 访问控制 | a）应对登录的用户分配账户和权限； | 1、经现场核查交换机中用户信息，通过输入display local-user命令，返回信息中显示交换机中存在security、tulei、xuweilai、ylops等用户，其中security的 user role list：level-1，network-operator；tulei、xuweilai、ylops的 user role list：network-admin,network-operator；2、经访谈网络管理员，其中tulei、xuweilai为两位网络管理员账号，ylops为网络主管账户，security为安全管理账号。 |
| b）应重命名或删除默认账户，修改默认账户的默认口令； | 1、经现场核查交换机中用户信息，通过输入display local-user命令，返回信息中显示交换机中存在security、tulei、xuweilai、ylops等用户,不存在默认账户，2、经核查交换机配置，输入display password-control命令，返回信息为 Password aging:Enabled (90 days) Password length: Enabled (10 characters) Password composition:Enabled (3 types, 1 characters per type) Password history: Enabled (max history records：3，用户口令已按照复杂度策略更改。 |
| 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； | 经现场核查交换机中用户信息，通过输入display local-user命令，返回信息中显示交换机中存在security、tulei、xuweilai、ylops等用户,经访谈网络管理员，其中tulei、xuweilai为两位网络管理员账号，ylops为网络主管账户，security为安全管理账号，不存在多余、过期、共享账户。 |
| 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； | 经现场核查交换机中用户信息，通过输入display local-user命令，返回信息中显示交换机中存在security、tulei、xuweilai、ylops等用户，经访谈网络管理员，交换机中未单独创建审计管理员账户，并且网络管理员权限为超管用户权限，未实现管理用户权限最小化及权限分离。 |
| e）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； | 经核查配置文件及访谈网络管理员，交换机中由网络管理员角色账户为管理用户配置相应账号，并按照用户角色级别赋予管理用户操作权限。 |
| f）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； | 经核查配置文件及访谈网络管理员，交换机中访问控制策略为管理用户的交换机中配置文件等进行配置管理及访问管理等，访问控制粒度达到主体为用户级、客体为文件级。 |
| g）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。 | 经核查配置文件及访谈网络管理员，未对重要主体和客体设置安全标记。 |
| 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； | 经现场访谈网络管理员及核查交换机配置，输入命令display logbuffer reverse，返回信息为logbuffer:enable；确认交换机中其中安全审计功能，通过查看审计记录内容，确认审计记录中包含设备运行记录及用户操作行为审计记录等。 |
| 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； | 经现场核查交换机中审计记录内容，审计记录中包含：日期、时间、主机名、类型、IP地址、用户名、详情等。 |
| 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、经访谈网络管理员，交换机中所有用户均无权限对审计记录进行删除或修改，并且管理员在备份服务器（10.33.110.160）中添加审计记录下载脚本（python脚本），实时将交换机中审计记录下载至备份服务器中进行备份；2、经现场核查备份服务器（10.33.110.160）中/home/network\_backup目录中存在审计记录备份文件，备份文件宿主为root，权限为744，其他用户仅拥有读权限。 |
| d）应对审计进程进行保护，防止未经授权的中断。 | 经现场访谈网络管理员，交换机中审计进程受系统进程保护，所有用户均无权限将审计进程单独中断。 |
| 入侵防范 | a）应遵循最小安装的原则，仅安装需要的组件和应用程序； | 经访谈网络管理员及核查配置文件，交换机为厂商提供独立封装系统，不允许安装其他组件及应用程序，遵循最小安装原则。 |
| b）应关闭不需要的系统服务、默认共享和高危端口； | 经现场访谈网络管理员及核查交换机配置，输入display current-fonfiguration，返回信息HTTP、Telnet协议均已关闭，交换机中未启用不需要的系统服务、默认共享及高危端口。 |
| c）应通过设定终端接入方式或网络地址范围对通过网络进行管理的管理终端进行限制； | 经访谈网络管理员，在防火墙中添加访问控制策略，仅允许管理用户通过堡垒机远程管理网络设备、安全设备及服务器等，经核查防火墙中访问控制策略，具备堡垒机地址-设备管理网段（10.33.0.0）的访问控制策略。 |
| d）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； | 该测评项测评对象为业务应用系统、中间件和系统管理软件，故将该项调整为不适用。 |
| e）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； | 1、经访谈网络管理员，会定期对官方网站通报的安全漏洞进行评估，然后从官方网站下载安全补丁，经过综合评估测试后对交换机系统进行补丁修复，避免系统中存在安全漏洞，2、经现场漏洞扫描，未发现交换机中存在安全漏洞。 |
| f）应能够检测到对重要节点进行入侵的行为，并在发生严重入侵事件时提供报警。 | 经访谈网络管理员，被测系统中部署了360AISA全流量威胁分析系统和360本地安全大脑，通过将被测系统中全部流量镜像发送到360AISA全流量威胁分析系统及360本地安全大脑中进行分析监测，发现入侵事件后及时通过钉钉报警，并且能够自动阻断。 |
| 可信验证 | a）可基于可信根对计算设备的系统引导程序、系统程序、重要配置参数和应用程序等进行可信验证，并在应用程序的关键执行环节进行动态可信验证，在检测到其可信性受到破坏后进行报警，并将验证结果形成审计记录送至安全管理中心。 | 未基于可信根对计算设备提供可信验证。 |
| 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； | 经现场访谈网络管理员及对交换机配置，交换机中关闭Telnet协议，采用SSH协议进行通信，保证重要数据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。 | 经访谈网络管理员及核查H3C S6800系列交换机产品文档，文件中目录05-参考指南--05文件系统管理命令中包含：“交换机中文件系统通常使用摘要算法（SHA-256）对文件计算摘要值，用于验证文件的正确性和完整性”。 |
| 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； | 经现场访谈网络管理员及对交换机配置，交换机中关闭Telnet协议，采用SSH协议进行通信，保证重要数据在传输过程中的保密性。 |
| b）应采用密码技术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个人信息等。 | 经访谈网管理员，管理员在设置用户口令时添加simple参数，经核查H3C S6800系列交换机产品文档，在文档05-参考指南--03-登录设备命令--1、登录设备--1.1等设备命令--1.1.28 set authentication password中正对simple参数进行说明：“simple：以明文方式设置密码，该密码将以密文方式存储。 |
| 数据备份恢复 | a）应提供重要数据的本地数据备份与恢复功能； | 经现场访谈网络管理员及核查相应配置，在备份服务器中配置python脚本，并设置每天凌晨4点将交换机中配置文件下载至备份服务器中进行备份，管理员每周对备份文件进行巡检，确保配置文件完整备份至备份服务器中。 |
| b）应提供异地实时备份功能，利用通信网络将重要数据实时备份至备份场地； | 1、经现场访谈网络管理员，管理员添加了数据同步策略，每天将备份服务器中备份文件拷贝至阿里公共云备份服务器中进行备份；2、经核查阿里公共云备份服务器（10.30.19.10）中备份目录/data/network-backup中具备网络设备配置备份文件；3、综上，因世纪互联IDC机房及阿里云公共云均在上海市，未实现异地实时备份功能。 |
| c）应提供重要数据处理系统的热冗余，保证系统的高可用性。 | 经访谈访问管理员及核查网络拓扑图，重要数据处理系统中采用双机冗余部署，保证系统的高可用性。 |

4.1.1.10. 管理接入交换机17

|  |  |  |
| --- | --- | --- |
| **安全控制点** | **测评指标** | **结果记录** |
| 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、经现场访谈网络管理员，交换机采用用户名、口令进行身份标识及身份鉴别；2、经核查交换机配置，输入display password-control命令，返回信息为 Password aging:Enabled (90 days) Password length: Enabled (10 characters) Password composition:Enabled (3 types, 1 characters per type) Password history: Enabled (max history records:4)，通过返回信息确认：用户口令长度为至少10位，包含数字、字母、字符三种类型，用户口令更改周期为90天；3、通过现场在交换机中创建与网络管理员ylops同名账户时，交换机中会提示用户名已存在，无法创重名用户，确认用户标识具备唯一性。 |
| 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、经现场核查交换机配置策略，输入display password-control命令，返回信息为 Maximum login attempts: 3，Action for exceeding login attempts: Lock user for 1 minutes、User authentication timeout：600 seconds；2、通过返回信息确认用户连续错误登录3次锁定账户1分钟，用户登录连接超时时间限制为600秒。 |
| 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； | 1、经现场访谈网络管理员及核查其远程连接交换机的方式，管理员在远程管理交换机时采用SSH协议进行通信，防止鉴别信息在网络传输过程中被窃听；2、访谈网络管理员，Telnet协议默认为关闭状态，通过输入命令telnet server enable尝试启用Telnet协议，返回信息为Telnet is insecure because it transmits data in plaintext form，Telnet协议未启成功；3，通过在终端Telnet该交换机，无法连接成功。 |
| 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。 | 经现场核查网络管理员远程登录交换机方式，交换机仅采用用户名、口令方式进行身份鉴别，未采用两种或两种以上组合的鉴别技术对用户进行身份鉴别。 |
| 访问控制 | a）应对登录的用户分配账户和权限； | 1、经现场核查交换机中用户信息，通过输入display local-user命令，返回信息中显示交换机中存在security、tulei、xuweilai、ylops等用户，其中security的 user role list：level-1，network-operator；tulei、xuweilai、ylops的 user role list：network-admin,network-operator；2、经访谈网络管理员，其中tulei、xuweilai为两位网络管理员账号，ylops为网络主管账户，security为安全管理账号。 |
| b）应重命名或删除默认账户，修改默认账户的默认口令； | 1、经现场核查交换机中用户信息，通过输入display local-user命令，返回信息中显示交换机中存在security、tulei、xuweilai、ylops等用户,不存在默认账户，2、经核查交换机配置，输入display password-control命令，返回信息为 Password aging:Enabled (90 days) Password length: Enabled (10 characters) Password composition:Enabled (3 types, 1 characters per type) Password history: Enabled (max history records：3，用户口令已按照复杂度策略更改。 |
| 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； | 经现场核查交换机中用户信息，通过输入display local-user命令，返回信息中显示交换机中存在security、tulei、xuweilai、ylops等用户,经访谈网络管理员，其中tulei、xuweilai为两位网络管理员账号，ylops为网络主管账户，security为安全管理账号，不存在多余、过期、共享账户。 |
| 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； | 经现场核查交换机中用户信息，通过输入display local-user命令，返回信息中显示交换机中存在security、tulei、xuweilai、ylops等用户，经访谈网络管理员，交换机中未单独创建审计管理员账户，并且网络管理员权限为超管用户权限，未实现管理用户权限最小化及权限分离。 |
| e）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； | 经核查配置文件及访谈网络管理员，交换机中由网络管理员角色账户为管理用户配置相应账号，并按照用户角色级别赋予管理用户操作权限。 |
| f）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； | 经核查配置文件及访谈网络管理员，交换机中访问控制策略为管理用户的交换机中配置文件等进行配置管理及访问管理等，访问控制粒度达到主体为用户级、客体为文件级。 |
| g）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。 | 经核查配置文件及访谈网络管理员，未对重要主体和客体设置安全标记。 |
| 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； | 经现场访谈网络管理员及核查交换机配置，输入命令display logbuffer reverse，返回信息为logbuffer:enable；确认交换机中其中安全审计功能，通过查看审计记录内容，确认审计记录中包含设备运行记录及用户操作行为审计记录等。 |
| 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； | 经现场核查交换机中审计记录内容，审计记录中包含：日期、时间、主机名、类型、IP地址、用户名、详情等。 |
| 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、经访谈网络管理员，交换机中所有用户均无权限对审计记录进行删除或修改，并且管理员在备份服务器（10.33.110.160）中添加审计记录下载脚本（python脚本），实时将交换机中审计记录下载至备份服务器中进行备份；2、经现场核查备份服务器（10.33.110.160）中/home/network\_backup目录中存在审计记录备份文件，备份文件宿主为root，权限为744，其他用户仅拥有读权限。 |
| d）应对审计进程进行保护，防止未经授权的中断。 | 经现场访谈网络管理员，交换机中审计进程受系统进程保护，所有用户均无权限将审计进程单独中断。 |
| 入侵防范 | a）应遵循最小安装的原则，仅安装需要的组件和应用程序； | 经访谈网络管理员及核查配置文件，交换机为厂商提供独立封装系统，不允许安装其他组件及应用程序，遵循最小安装原则。 |
| b）应关闭不需要的系统服务、默认共享和高危端口； | 经现场访谈网络管理员及核查交换机配置，输入display current-fonfiguration，返回信息HTTP、Telnet协议均已关闭，交换机中未启用不需要的系统服务、默认共享及高危端口。 |
| c）应通过设定终端接入方式或网络地址范围对通过网络进行管理的管理终端进行限制； | 经访谈网络管理员，在防火墙中添加访问控制策略，仅允许管理用户通过堡垒机远程管理网络设备、安全设备及服务器等，经核查防火墙中访问控制策略，具备堡垒机地址-设备管理网段（10.33.0.0）的访问控制策略。 |
| d）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； | 该测评项测评对象为业务应用系统、中间件和系统管理软件，故将该项调整为不适用。 |
| e）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； | 1、经访谈网络管理员，会定期对官方网站通报的安全漏洞进行评估，然后从官方网站下载安全补丁，经过综合评估测试后对交换机系统进行补丁修复，避免系统中存在安全漏洞，2、经现场漏洞扫描，未发现交换机中存在安全漏洞。 |
| f）应能够检测到对重要节点进行入侵的行为，并在发生严重入侵事件时提供报警。 | 经访谈网络管理员，被测系统中部署了360AISA全流量威胁分析系统和360本地安全大脑，通过将被测系统中全部流量镜像发送到360AISA全流量威胁分析系统及360本地安全大脑中进行分析监测，发现入侵事件后及时通过钉钉报警，并且能够自动阻断。 |
| 可信验证 | a）可基于可信根对计算设备的系统引导程序、系统程序、重要配置参数和应用程序等进行可信验证，并在应用程序的关键执行环节进行动态可信验证，在检测到其可信性受到破坏后进行报警，并将验证结果形成审计记录送至安全管理中心。 | 未基于可信根对计算设备提供可信验证。 |
| 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； | 经现场访谈网络管理员及对交换机配置，交换机中关闭Telnet协议，采用SSH协议进行通信，保证重要数据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。 | 经访谈网络管理员及核查H3C S6800系列交换机产品文档，文件中目录05-参考指南--05文件系统管理命令中包含：“交换机中文件系统通常使用摘要算法（SHA-256）对文件计算摘要值，用于验证文件的正确性和完整性”。 |
| 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； | 经现场访谈网络管理员及对交换机配置，交换机中关闭Telnet协议，采用SSH协议进行通信，保证重要数据在传输过程中的保密性。 |
| b）应采用密码技术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个人信息等。 | 经访谈网管理员，管理员在设置用户口令时添加simple参数，经核查H3C S6800系列交换机产品文档，在文档05-参考指南--03-登录设备命令--1、登录设备--1.1等设备命令--1.1.28 set authentication password中正对simple参数进行说明：“simple：以明文方式设置密码，该密码将以密文方式存储。 |
| 数据备份恢复 | a）应提供重要数据的本地数据备份与恢复功能； | 经现场访谈网络管理员及核查相应配置，在备份服务器中配置python脚本，并设置每天凌晨4点将交换机中配置文件下载至备份服务器中进行备份，管理员每周对备份文件进行巡检，确保配置文件完整备份至备份服务器中。 |
| b）应提供异地实时备份功能，利用通信网络将重要数据实时备份至备份场地； | 1、经现场访谈网络管理员，管理员添加了数据同步策略，每天将备份服务器中备份文件拷贝至阿里公共云备份服务器中进行备份；2、经核查阿里公共云备份服务器（10.30.19.10）中备份目录/data/network-backup中具备网络设备配置备份文件；3、综上，因世纪互联IDC机房及阿里云公共云均在上海市，未实现异地实时备份功能。 |
| c）应提供重要数据处理系统的热冗余，保证系统的高可用性。 | 经访谈访问管理员及核查网络拓扑图，重要数据处理系统中采用双机冗余部署，保证系统的高可用性。 |

4.1.1.11. 管理接入交换机18

|  |  |  |
| --- | --- | --- |
| **安全控制点** | **测评指标** | **结果记录** |
| 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、经现场访谈网络管理员，交换机采用用户名、口令进行身份标识及身份鉴别；2、经核查交换机配置，输入display password-control命令，返回信息为 Password aging:Enabled (90 days) Password length: Enabled (10 characters) Password composition:Enabled (3 types, 1 characters per type) Password history: Enabled (max history records:4)，通过返回信息确认：用户口令长度为至少10位，包含数字、字母、字符三种类型，用户口令更改周期为90天；3、通过现场在交换机中创建与网络管理员ylops同名账户时，交换机中会提示用户名已存在，无法创重名用户，确认用户标识具备唯一性。 |
| 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、经现场核查交换机配置策略，输入display password-control命令，返回信息为 Maximum login attempts: 3，Action for exceeding login attempts: Lock user for 1 minutes、User authentication timeout：600 seconds；2、通过返回信息确认用户连续错误登录3次锁定账户1分钟，用户登录连接超时时间限制为600秒。 |
| 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； | 1、经现场访谈网络管理员及核查其远程连接交换机的方式，管理员在远程管理交换机时采用SSH协议进行通信，防止鉴别信息在网络传输过程中被窃听；2、访谈网络管理员，Telnet协议默认为关闭状态，通过输入命令telnet server enable尝试启用Telnet协议，返回信息为Telnet is insecure because it transmits data in plaintext form，Telnet协议未启成功；3，通过在终端Telnet该交换机，无法连接成功。 |
| 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。 | 经现场核查网络管理员远程登录交换机方式，交换机仅采用用户名、口令方式进行身份鉴别，未采用两种或两种以上组合的鉴别技术对用户进行身份鉴别。 |
| 访问控制 | a）应对登录的用户分配账户和权限； | 1、经现场核查交换机中用户信息，通过输入display local-user命令，返回信息中显示交换机中存在security、tulei、xuweilai、ylops等用户，其中security的 user role list：level-1，network-operator；tulei、xuweilai、ylops的 user role list：network-admin,network-operator；2、经访谈网络管理员，其中tulei、xuweilai为两位网络管理员账号，ylops为网络主管账户，security为安全管理账号。 |
| b）应重命名或删除默认账户，修改默认账户的默认口令； | 1、经现场核查交换机中用户信息，通过输入display local-user命令，返回信息中显示交换机中存在security、tulei、xuweilai、ylops等用户,不存在默认账户，2、经核查交换机配置，输入display password-control命令，返回信息为 Password aging:Enabled (90 days) Password length: Enabled (10 characters) Password composition:Enabled (3 types, 1 characters per type) Password history: Enabled (max history records：3，用户口令已按照复杂度策略更改。 |
| 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； | 经现场核查交换机中用户信息，通过输入display local-user命令，返回信息中显示交换机中存在security、tulei、xuweilai、ylops等用户,经访谈网络管理员，其中tulei、xuweilai为两位网络管理员账号，ylops为网络主管账户，security为安全管理账号，不存在多余、过期、共享账户。 |
| 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； | 经现场核查交换机中用户信息，通过输入display local-user命令，返回信息中显示交换机中存在security、tulei、xuweilai、ylops等用户，经访谈网络管理员，交换机中未单独创建审计管理员账户，并且网络管理员权限为超管用户权限，未实现管理用户权限最小化及权限分离。 |
| e）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； | 经核查配置文件及访谈网络管理员，交换机中由网络管理员角色账户为管理用户配置相应账号，并按照用户角色级别赋予管理用户操作权限。 |
| f）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； | 经核查配置文件及访谈网络管理员，交换机中访问控制策略为管理用户的交换机中配置文件等进行配置管理及访问管理等，访问控制粒度达到主体为用户级、客体为文件级。 |
| g）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。 | 经核查配置文件及访谈网络管理员，未对重要主体和客体设置安全标记。 |
| 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； | 经现场访谈网络管理员及核查交换机配置，输入命令display logbuffer reverse，返回信息为logbuffer:enable；确认交换机中其中安全审计功能，通过查看审计记录内容，确认审计记录中包含设备运行记录及用户操作行为审计记录等。 |
| 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； | 经现场核查交换机中审计记录内容，审计记录中包含：日期、时间、主机名、类型、IP地址、用户名、详情等。 |
| 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、经访谈网络管理员，交换机中所有用户均无权限对审计记录进行删除或修改，并且管理员在备份服务器（10.33.110.160）中添加审计记录下载脚本（python脚本），实时将交换机中审计记录下载至备份服务器中进行备份；2、经现场核查备份服务器（10.33.110.160）中/home/network\_backup目录中存在审计记录备份文件，备份文件宿主为root，权限为744，其他用户仅拥有读权限。 |
| d）应对审计进程进行保护，防止未经授权的中断。 | 经现场访谈网络管理员，交换机中审计进程受系统进程保护，所有用户均无权限将审计进程单独中断。 |
| 入侵防范 | a）应遵循最小安装的原则，仅安装需要的组件和应用程序； | 经访谈网络管理员及核查配置文件，交换机为厂商提供独立封装系统，不允许安装其他组件及应用程序，遵循最小安装原则。 |
| b）应关闭不需要的系统服务、默认共享和高危端口； | 经现场访谈网络管理员及核查交换机配置，输入display current-fonfiguration，返回信息HTTP、Telnet协议均已关闭，交换机中未启用不需要的系统服务、默认共享及高危端口。 |
| c）应通过设定终端接入方式或网络地址范围对通过网络进行管理的管理终端进行限制； | 经访谈网络管理员，在防火墙中添加访问控制策略，仅允许管理用户通过堡垒机远程管理网络设备、安全设备及服务器等，经核查防火墙中访问控制策略，具备堡垒机地址-设备管理网段（10.33.0.0）的访问控制策略。 |
| d）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； | 该测评项测评对象为业务应用系统、中间件和系统管理软件，故将该项调整为不适用。 |
| e）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； | 1、经访谈网络管理员，会定期对官方网站通报的安全漏洞进行评估，然后从官方网站下载安全补丁，经过综合评估测试后对交换机系统进行补丁修复，避免系统中存在安全漏洞，2、经现场漏洞扫描，未发现交换机中存在安全漏洞。 |
| f）应能够检测到对重要节点进行入侵的行为，并在发生严重入侵事件时提供报警。 | 经访谈网络管理员，被测系统中部署了360AISA全流量威胁分析系统和360本地安全大脑，通过将被测系统中全部流量镜像发送到360AISA全流量威胁分析系统及360本地安全大脑中进行分析监测，发现入侵事件后及时通过钉钉报警，并且能够自动阻断。 |
| 可信验证 | a）可基于可信根对计算设备的系统引导程序、系统程序、重要配置参数和应用程序等进行可信验证，并在应用程序的关键执行环节进行动态可信验证，在检测到其可信性受到破坏后进行报警，并将验证结果形成审计记录送至安全管理中心。 | 未基于可信根对计算设备提供可信验证。 |
| 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； | 经现场访谈网络管理员及对交换机配置，交换机中关闭Telnet协议，采用SSH协议进行通信，保证重要数据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。 | 经访谈网络管理员及核查H3C S6800系列交换机产品文档，文件中目录05-参考指南--05文件系统管理命令中包含：“交换机中文件系统通常使用摘要算法（SHA-256）对文件计算摘要值，用于验证文件的正确性和完整性”。 |
| 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； | 经现场访谈网络管理员及对交换机配置，交换机中关闭Telnet协议，采用SSH协议进行通信，保证重要数据在传输过程中的保密性。 |
| b）应采用密码技术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个人信息等。 | 经访谈网管理员，管理员在设置用户口令时添加simple参数，经核查H3C S6800系列交换机产品文档，在文档05-参考指南--03-登录设备命令--1、登录设备--1.1等设备命令--1.1.28 set authentication password中正对simple参数进行说明：“simple：以明文方式设置密码，该密码将以密文方式存储。 |
| 数据备份恢复 | a）应提供重要数据的本地数据备份与恢复功能； | 经现场访谈网络管理员及核查相应配置，在备份服务器中配置python脚本，并设置每天凌晨4点将交换机中配置文件下载至备份服务器中进行备份，管理员每周对备份文件进行巡检，确保配置文件完整备份至备份服务器中。 |
| b）应提供异地实时备份功能，利用通信网络将重要数据实时备份至备份场地； | 1、经现场访谈网络管理员，管理员添加了数据同步策略，每天将备份服务器中备份文件拷贝至阿里公共云备份服务器中进行备份；2、经核查阿里公共云备份服务器（10.30.19.10）中备份目录/data/network-backup中具备网络设备配置备份文件；3、综上，因世纪互联IDC机房及阿里云公共云均在上海市，未实现异地实时备份功能。 |
| c）应提供重要数据处理系统的热冗余，保证系统的高可用性。 | 经访谈访问管理员及核查网络拓扑图，重要数据处理系统中采用双机冗余部署，保证系统的高可用性。 |

4.1.1.12. 管理接入交换机19

|  |  |  |
| --- | --- | --- |
| **安全控制点** | **测评指标** | **结果记录** |
| 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、经现场访谈网络管理员，交换机采用用户名、口令进行身份标识及身份鉴别；2、经核查交换机配置，输入display password-control命令，返回信息为 Password aging:Enabled (90 days) Password length: Enabled (10 characters) Password composition:Enabled (3 types, 1 characters per type) Password history: Enabled (max history records:4)，通过返回信息确认：用户口令长度为至少10位，包含数字、字母、字符三种类型，用户口令更改周期为90天；3、通过现场在交换机中创建与网络管理员ylops同名账户时，交换机中会提示用户名已存在，无法创重名用户，确认用户标识具备唯一性。 |
| 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、经现场核查交换机配置策略，输入display password-control命令，返回信息为 Maximum login attempts: 3，Action for exceeding login attempts: Lock user for 1 minutes、User authentication timeout：600 seconds；2、通过返回信息确认用户连续错误登录3次锁定账户1分钟，用户登录连接超时时间限制为600秒。 |
| 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； | 1、经现场访谈网络管理员及核查其远程连接交换机的方式，管理员在远程管理交换机时采用SSH协议进行通信，防止鉴别信息在网络传输过程中被窃听；2、访谈网络管理员，Telnet协议默认为关闭状态，通过输入命令telnet server enable尝试启用Telnet协议，返回信息为Telnet is insecure because it transmits data in plaintext form，Telnet协议未启成功；3，通过在终端Telnet该交换机，无法连接成功。 |
| 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。 | 经现场核查网络管理员远程登录交换机方式，交换机仅采用用户名、口令方式进行身份鉴别，未采用两种或两种以上组合的鉴别技术对用户进行身份鉴别。 |
| 访问控制 | a）应对登录的用户分配账户和权限； | 1、经现场核查交换机中用户信息，通过输入display local-user命令，返回信息中显示交换机中存在security、tulei、xuweilai、ylops等用户，其中security的 user role list：level-1，network-operator；tulei、xuweilai、ylops的 user role list：network-admin,network-operator；2、经访谈网络管理员，其中tulei、xuweilai为两位网络管理员账号，ylops为网络主管账户，security为安全管理账号。 |
| b）应重命名或删除默认账户，修改默认账户的默认口令； | 1、经现场核查交换机中用户信息，通过输入display local-user命令，返回信息中显示交换机中存在security、tulei、xuweilai、ylops等用户,不存在默认账户，2、经核查交换机配置，输入display password-control命令，返回信息为 Password aging:Enabled (90 days) Password length: Enabled (10 characters) Password composition:Enabled (3 types, 1 characters per type) Password history: Enabled (max history records：3，用户口令已按照复杂度策略更改。 |
| 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； | 经现场核查交换机中用户信息，通过输入display local-user命令，返回信息中显示交换机中存在security、tulei、xuweilai、ylops等用户,经访谈网络管理员，其中tulei、xuweilai为两位网络管理员账号，ylops为网络主管账户，security为安全管理账号，不存在多余、过期、共享账户。 |
| 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； | 经现场核查交换机中用户信息，通过输入display local-user命令，返回信息中显示交换机中存在security、tulei、xuweilai、ylops等用户，经访谈网络管理员，交换机中未单独创建审计管理员账户，并且网络管理员权限为超管用户权限，未实现管理用户权限最小化及权限分离。 |
| e）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； | 经核查配置文件及访谈网络管理员，交换机中由网络管理员角色账户为管理用户配置相应账号，并按照用户角色级别赋予管理用户操作权限。 |
| f）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； | 经核查配置文件及访谈网络管理员，交换机中访问控制策略为管理用户的交换机中配置文件等进行配置管理及访问管理等，访问控制粒度达到主体为用户级、客体为文件级。 |
| g）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。 | 经核查配置文件及访谈网络管理员，未对重要主体和客体设置安全标记。 |
| 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； | 经现场访谈网络管理员及核查交换机配置，输入命令display logbuffer reverse，返回信息为logbuffer:enable；确认交换机中其中安全审计功能，通过查看审计记录内容，确认审计记录中包含设备运行记录及用户操作行为审计记录等。 |
| 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； | 经现场核查交换机中审计记录内容，审计记录中包含：日期、时间、主机名、类型、IP地址、用户名、详情等。 |
| 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、经访谈网络管理员，交换机中所有用户均无权限对审计记录进行删除或修改，并且管理员在备份服务器（10.33.110.160）中添加审计记录下载脚本（python脚本），实时将交换机中审计记录下载至备份服务器中进行备份；2、经现场核查备份服务器（10.33.110.160）中/home/network\_backup目录中存在审计记录备份文件，备份文件宿主为root，权限为744，其他用户仅拥有读权限。 |
| d）应对审计进程进行保护，防止未经授权的中断。 | 经现场访谈网络管理员，交换机中审计进程受系统进程保护，所有用户均无权限将审计进程单独中断。 |
| 入侵防范 | a）应遵循最小安装的原则，仅安装需要的组件和应用程序； | 经访谈网络管理员及核查配置文件，交换机为厂商提供独立封装系统，不允许安装其他组件及应用程序，遵循最小安装原则。 |
| b）应关闭不需要的系统服务、默认共享和高危端口； | 经现场访谈网络管理员及核查交换机配置，输入display current-fonfiguration，返回信息HTTP、Telnet协议均已关闭，交换机中未启用不需要的系统服务、默认共享及高危端口。 |
| c）应通过设定终端接入方式或网络地址范围对通过网络进行管理的管理终端进行限制； | 经访谈网络管理员，在防火墙中添加访问控制策略，仅允许管理用户通过堡垒机远程管理网络设备、安全设备及服务器等，经核查防火墙中访问控制策略，具备堡垒机地址-设备管理网段（10.33.0.0）的访问控制策略。 |
| d）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； | 该测评项测评对象为业务应用系统、中间件和系统管理软件，故将该项调整为不适用。 |
| e）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； | 1、经访谈网络管理员，会定期对官方网站通报的安全漏洞进行评估，然后从官方网站下载安全补丁，经过综合评估测试后对交换机系统进行补丁修复，避免系统中存在安全漏洞，2、经现场漏洞扫描，未发现交换机中存在安全漏洞。 |
| f）应能够检测到对重要节点进行入侵的行为，并在发生严重入侵事件时提供报警。 | 经访谈网络管理员，被测系统中部署了360AISA全流量威胁分析系统和360本地安全大脑，通过将被测系统中全部流量镜像发送到360AISA全流量威胁分析系统及360本地安全大脑中进行分析监测，发现入侵事件后及时通过钉钉报警，并且能够自动阻断。 |
| 可信验证 | a）可基于可信根对计算设备的系统引导程序、系统程序、重要配置参数和应用程序等进行可信验证，并在应用程序的关键执行环节进行动态可信验证，在检测到其可信性受到破坏后进行报警，并将验证结果形成审计记录送至安全管理中心。 | 未基于可信根对计算设备提供可信验证。 |
| 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； | 经现场访谈网络管理员及对交换机配置，交换机中关闭Telnet协议，采用SSH协议进行通信，保证重要数据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。 | 经访谈网络管理员及核查H3C S6800系列交换机产品文档，文件中目录05-参考指南--05文件系统管理命令中包含：“交换机中文件系统通常使用摘要算法（SHA-256）对文件计算摘要值，用于验证文件的正确性和完整性”。 |
| 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； | 经现场访谈网络管理员及对交换机配置，交换机中关闭Telnet协议，采用SSH协议进行通信，保证重要数据在传输过程中的保密性。 |
| b）应采用密码技术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个人信息等。 | 经访谈网管理员，管理员在设置用户口令时添加simple参数，经核查H3C S6800系列交换机产品文档，在文档05-参考指南--03-登录设备命令--1、登录设备--1.1等设备命令--1.1.28 set authentication password中正对simple参数进行说明：“simple：以明文方式设置密码，该密码将以密文方式存储。 |
| 数据备份恢复 | a）应提供重要数据的本地数据备份与恢复功能； | 经现场访谈网络管理员及核查相应配置，在备份服务器中配置python脚本，并设置每天凌晨4点将交换机中配置文件下载至备份服务器中进行备份，管理员每周对备份文件进行巡检，确保配置文件完整备份至备份服务器中。 |
| b）应提供异地实时备份功能，利用通信网络将重要数据实时备份至备份场地； | 1、经现场访谈网络管理员，管理员添加了数据同步策略，每天将备份服务器中备份文件拷贝至阿里公共云备份服务器中进行备份；2、经核查阿里公共云备份服务器（10.30.19.10）中备份目录/data/network-backup中具备网络设备配置备份文件；3、综上，因世纪互联IDC机房及阿里云公共云均在上海市，未实现异地实时备份功能。 |
| c）应提供重要数据处理系统的热冗余，保证系统的高可用性。 | 经访谈访问管理员及核查网络拓扑图，重要数据处理系统中采用双机冗余部署，保证系统的高可用性。 |

4.1.1.13. 核心交换机1

|  |  |  |
| --- | --- | --- |
| **安全控制点** | **测评指标** | **结果记录** |
| 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、经现场访谈网络管理员，交换机采用用户名、口令进行身份标识及身份鉴别；2、经核查交换机配置，输入display password-control命令，返回信息为 Password aging:Enabled (90 days) Password length: Enabled (10 characters) Password composition:Enabled (3 types, 1 characters per type) Password history: Enabled (max history records:4)，通过返回信息确认：用户口令长度为至少10位，包含数字、字母、字符三种类型，用户口令更改周期为90天；3、通过现场在交换机中创建与网络管理员ylops同名账户时，交换机中会提示用户名已存在，无法创重名用户，确认用户标识具备唯一性。 |
| 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、经现场核查交换机配置策略，输入display password-control命令，返回信息为 Maximum login attempts: 3，Action for exceeding login attempts: Lock user for 1 minutes、User authentication timeout：600 seconds；2、通过返回信息确认用户连续错误登录3次锁定账户1分钟，用户登录连接超时时间限制为600秒。 |
| 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； | 1、经现场访谈网络管理员及核查其远程连接交换机的方式，管理员在远程管理交换机时采用SSH协议进行通信，防止鉴别信息在网络传输过程中被窃听；2、访谈网络管理员，Telnet协议默认为关闭状态，通过输入命令telnet server enable尝试启用Telnet协议，返回信息为Telnet is insecure because it transmits data in plaintext form，Telnet协议未启成功；3，通过在终端Telnet该交换机，无法连接成功。 |
| 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。 | 经现场核查网络管理员远程登录交换机方式，交换机仅采用用户名、口令方式进行身份鉴别，未采用两种或两种以上组合的鉴别技术对用户进行身份鉴别。 |
| 访问控制 | a）应对登录的用户分配账户和权限； | 1、经现场核查交换机中用户信息，通过输入display local-user命令，返回信息中显示交换机中存在security、tulei、xuweilai、ylops等用户，其中security的 user role list：level-1，network-operator；tulei、xuweilai、ylops的 user role list：network-admin,network-operator；2、经访谈网络管理员，其中tulei、xuweilai为两位网络管理员账号，ylops为网络主管账户，security为安全管理账号。 |
| b）应重命名或删除默认账户，修改默认账户的默认口令； | 1、经现场核查交换机中用户信息，通过输入display local-user命令，返回信息中显示交换机中存在security、tulei、xuweilai、ylops等用户,不存在默认账户，2、经核查交换机配置，输入display password-control命令，返回信息为 Password aging:Enabled (90 days) Password length: Enabled (10 characters) Password composition:Enabled (3 types, 1 characters per type) Password history: Enabled (max history records：3、用户口令已按照复杂度策略更改。 |
| 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； | 经现场核查交换机中用户信息，通过输入display local-user命令，返回信息中显示交换机中存在security、tulei、xuweilai、ylops等用户,经访谈网络管理员，其中tulei、xuweilai为两位网络管理员账号，ylops为网络主管账户，security为安全管理账号，不存在多余、过期、共享账户。 |
| 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； | 经现场核查交换机中用户信息，通过输入display local-user命令，返回信息中显示交换机中存在security、tulei、xuweilai、ylops等用户，经访谈网络管理员，交换机中未单独创建审计管理员账户，并且网络管理员权限为超管用户权限，未实现管理用户权限最小化及权限分离。 |
| e）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； | 经核查配置文件及访谈网络管理员，交换机中由网络管理员角色账户为管理用户配置相应账号，并按照用户角色级别赋予管理用户操作权限。 |
| f）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； | 经核查配置文件及访谈网络管理员，交换机中访问控制策略为管理用户的交换机中配置文件等进行配置管理及访问管理等，访问控制粒度达到主体为用户级、客体为文件级。 |
| g）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。 | 经核查配置文件及访谈网络管理员，未对重要主体和客体设置安全标记。 |
| 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； | 经现场访谈网络管理员及核查交换机配置，输入命令display logbuffer reverse，返回信息为logbuffer:enable；确认交换机中其中安全审计功能，通过查看审计记录内容，确认审计记录中包含设备运行记录及用户操作行为审计记录等。 |
| 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； | 经现场核查交换机中审计记录内容，审计记录中包含：日期、时间、主机名、类型、IP地址、用户名、详情等。 |
| 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、经访谈网络管理员，交换机中所有用户均无权限对审计记录进行删除或修改，并且管理员在备份服务器（10.33.110.160）中添加审计记录下载脚本（python脚本），实时将交换机中审计记录下载至备份服务器中进行备份；2、经现场核查备份服务器（10.33.110.160）中/home/network\_backup目录中存在审计记录备份文件，备份文件宿主为root，权限为744，其他用户仅拥有读权限。 |
| d）应对审计进程进行保护，防止未经授权的中断。 | 经现场访谈网络管理员，交换机中审计进程受系统进程保护，所有用户均无权限将审计进程单独中断。 |
| 入侵防范 | a）应遵循最小安装的原则，仅安装需要的组件和应用程序； | 经访谈网络管理员及核查配置文件，交换机为厂商提供独立封装系统，不允许安装其他组件及应用程序，遵循最小安装原则。 |
| b）应关闭不需要的系统服务、默认共享和高危端口； | 经现场访谈网络管理员及核查交换机配置，输入display current-fonfiguration，返回信息HTTP、Telnet协议均已关闭，交换机中未启用不需要的系统服务、默认共享及高危端口。 |
| c）应通过设定终端接入方式或网络地址范围对通过网络进行管理的管理终端进行限制； | 经访谈网络管理员，在防火墙中添加访问控制策略，仅允许管理用户通过堡垒机远程管理网络设备、安全设备及服务器等，经核查防火墙中访问控制策略，具备堡垒机地址-设备管理网段（10.33.0.0）的访问控制策略。 |
| d）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； | 该测评项测评对象为业务应用系统、中间件和系统管理软件，故将该项调整为不适用。 |
| e）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； | 1、经访谈网络管理员，会定期对官方网站通报的安全漏洞进行评估，然后从官方网站下载安全补丁，经过综合评估测试后对交换机系统进行补丁修复，避免系统中存在安全漏洞，2、经现场漏洞扫描，未发现交换机中存在安全漏洞。 |
| f）应能够检测到对重要节点进行入侵的行为，并在发生严重入侵事件时提供报警。 | 经访谈网络管理员，被测系统中部署了360AISA全流量威胁分析系统和360本地安全大脑，通过将被测系统中全部流量镜像发送到360AISA全流量威胁分析系统及360本地安全大脑中进行分析监测，发现入侵事件后及时通过钉钉报警，并且能够自动阻断。 |
| 可信验证 | a）可基于可信根对计算设备的系统引导程序、系统程序、重要配置参数和应用程序等进行可信验证，并在应用程序的关键执行环节进行动态可信验证，在检测到其可信性受到破坏后进行报警，并将验证结果形成审计记录送至安全管理中心。 | 未基于可信根对计算设备提供可信验证。 |
| 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； | 经现场访谈网络管理员及对交换机配置，交换机中关闭Telnet协议，采用SSH协议进行通信，保证重要数据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。 | 经访谈网络管理员及核查H3C S6800系列交换机产品文档，文件中目录05-参考指南--05文件系统管理命令中包含：“交换机中文件系统通常使用摘要算法（SHA-256）对文件计算摘要值，用于验证文件的正确性和完整性”。 |
| 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； | 经现场访谈网络管理员及对交换机配置，交换机中关闭Telnet协议，采用SSH协议进行通信，保证重要数据在传输过程中的保密性。 |
| b）应采用密码技术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个人信息等。 | 经访谈网管理员，管理员在设置用户口令时添加simple参数，经核查H3C S6800系列交换机产品文档，在文档05-参考指南--03-登录设备命令--1、登录设备--1.1等设备命令--1.1.28 set authentication password中正对simple参数进行说明：“simple：以明文方式设置密码，该密码将以密文方式存储。 |
| 数据备份恢复 | a）应提供重要数据的本地数据备份与恢复功能； | 经现场访谈网络管理员及核查相应配置，在备份服务器中配置python脚本，并设置每天凌晨4点将交换机中配置文件下载至备份服务器中进行备份，管理员每周对备份文件进行巡检，确保配置文件完整备份至备份服务器中。 |
| b）应提供异地实时备份功能，利用通信网络将重要数据实时备份至备份场地； | 1、经现场访谈网络管理员，管理员添加了数据同步策略，每天将备份服务器中备份文件拷贝至阿里公共云备份服务器中进行备份；2、经核查阿里公共云备份服务器（10.30.19.10）中备份目录/data/network-backup中具备网络设备配置备份文件；3、综上，因世纪互联IDC机房及阿里云公共云均在上海市，未实现异地实时备份功能。 |
| c）应提供重要数据处理系统的热冗余，保证系统的高可用性。 | 经访谈访问管理员及核查网络拓扑图，重要数据处理系统中采用双机冗余部署，保证系统的高可用性。 |

4.1.1.14. 核心交换机2

|  |  |  |
| --- | --- | --- |
| **安全控制点** | **测评指标** | **结果记录** |
| 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、经现场访谈网络管理员，交换机采用用户名、口令进行身份标识及身份鉴别；2、经核查交换机配置，输入display password-control命令，返回信息为 Password aging:Enabled (90 days) Password length: Enabled (10 characters) Password composition:Enabled (3 types, 1 characters per type) Password history: Enabled (max history records:4)，通过返回信息确认：用户口令长度为至少10位，包含数字、字母、字符三种类型，用户口令更改周期为90天；3、通过现场在交换机中创建与网络管理员ylops同名账户时，交换机中会提示用户名已存在，无法创重名用户，确认用户标识具备唯一性。 |
| 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、经现场核查交换机配置策略，输入display password-control命令，返回信息为 Maximum login attempts: 3，Action for exceeding login attempts: Lock user for 1 minutes、User authentication timeout：600 seconds；2、通过返回信息确认用户连续错误登录3次锁定账户1分钟，用户登录连接超时时间限制为600秒。 |
| 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； | 1、经现场访谈网络管理员及核查其远程连接交换机的方式，管理员在远程管理交换机时采用SSH协议进行通信，防止鉴别信息在网络传输过程中被窃听；2、访谈网络管理员，Telnet协议默认为关闭状态，通过输入命令telnet server enable尝试启用Telnet协议，返回信息为Telnet is insecure because it transmits data in plaintext form，Telnet协议未启成功；3，通过在终端Telnet该交换机，无法连接成功。 |
| 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。 | 经现场核查网络管理员远程登录交换机方式，交换机仅采用用户名、口令方式进行身份鉴别，未采用两种或两种以上组合的鉴别技术对用户进行身份鉴别。 |
| 访问控制 | a）应对登录的用户分配账户和权限； | 1、经现场核查交换机中用户信息，通过输入display local-user命令，返回信息中显示交换机中存在security、tulei、xuweilai、ylops等用户，其中security的 user role list：level-1，network-operator；tulei、xuweilai、ylops的 user role list：network-admin,network-operator；2、经访谈网络管理员，其中tulei、xuweilai为两位网络管理员账号，ylops为网络主管账户，security为安全管理账号。 |
| b）应重命名或删除默认账户，修改默认账户的默认口令； | 1、经现场核查交换机中用户信息，通过输入display local-user命令，返回信息中显示交换机中存在security、tulei、xuweilai、ylops等用户,不存在默认账户，2、经核查交换机配置，输入display password-control命令，返回信息为 Password aging:Enabled (90 days) Password length: Enabled (10 characters) Password composition:Enabled (3 types, 1 characters per type) Password history: Enabled (max history records：3、用户口令已按照复杂度策略更改。 |
| 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； | 经现场核查交换机中用户信息，通过输入display local-user命令，返回信息中显示交换机中存在security、tulei、xuweilai、ylops等用户,经访谈网络管理员，其中tulei、xuweilai为两位网络管理员账号，ylops为网络主管账户，security为安全管理账号，不存在多余、过期、共享账户。 |
| 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； | 经现场核查交换机中用户信息，通过输入display local-user命令，返回信息中显示交换机中存在security、tulei、xuweilai、ylops等用户，经访谈网络管理员，交换机中未单独创建审计管理员账户，并且网络管理员权限为超管用户权限，未实现管理用户权限最小化及权限分离。 |
| e）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； | 经核查配置文件及访谈网络管理员，交换机中由网络管理员角色账户为管理用户配置相应账号，并按照用户角色级别赋予管理用户操作权限。 |
| f）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； | 经核查配置文件及访谈网络管理员，交换机中访问控制策略为管理用户的交换机中配置文件等进行配置管理及访问管理等，访问控制粒度达到主体为用户级、客体为文件级。 |
| g）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。 | 经核查配置文件及访谈网络管理员，未对重要主体和客体设置安全标记。 |
| 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； | 经现场访谈网络管理员及核查交换机配置，输入命令display logbuffer reverse，返回信息为logbuffer:enable；确认交换机中其中安全审计功能，通过查看审计记录内容，确认审计记录中包含设备运行记录及用户操作行为审计记录等。 |
| 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； | 经现场核查交换机中审计记录内容，审计记录中包含：日期、时间、主机名、类型、IP地址、用户名、详情等。 |
| 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、经访谈网络管理员，交换机中所有用户均无权限对审计记录进行删除或修改，并且管理员在备份服务器（10.33.110.160）中添加审计记录下载脚本（python脚本），实时将交换机中审计记录下载至备份服务器中进行备份；2、经现场核查备份服务器（10.33.110.160）中/home/network\_backup目录中存在审计记录备份文件，备份文件宿主为root，权限为744，其他用户仅拥有读权限。 |
| d）应对审计进程进行保护，防止未经授权的中断。 | 经现场访谈网络管理员，交换机中审计进程受系统进程保护，所有用户均无权限将审计进程单独中断。 |
| 入侵防范 | a）应遵循最小安装的原则，仅安装需要的组件和应用程序； | 经访谈网络管理员及核查配置文件，交换机为厂商提供独立封装系统，不允许安装其他组件及应用程序，遵循最小安装原则。 |
| b）应关闭不需要的系统服务、默认共享和高危端口； | 经现场访谈网络管理员及核查交换机配置，输入display current-fonfiguration，返回信息HTTP、Telnet协议均已关闭，交换机中未启用不需要的系统服务、默认共享及高危端口。 |
| c）应通过设定终端接入方式或网络地址范围对通过网络进行管理的管理终端进行限制； | 经访谈网络管理员，在防火墙中添加访问控制策略，仅允许管理用户通过堡垒机远程管理网络设备、安全设备及服务器等，经核查防火墙中访问控制策略，具备堡垒机地址-设备管理网段（10.33.0.0）的访问控制策略。 |
| d）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； | 该测评项测评对象为业务应用系统、中间件和系统管理软件，故将该项调整为不适用。 |
| e）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； | 1、经访谈网络管理员，会定期对官方网站通报的安全漏洞进行评估，然后从官方网站下载安全补丁，经过综合评估测试后对交换机系统进行补丁修复，避免系统中存在安全漏洞，2、经现场漏洞扫描，未发现交换机中存在安全漏洞。 |
| f）应能够检测到对重要节点进行入侵的行为，并在发生严重入侵事件时提供报警。 | 经访谈网络管理员，被测系统中部署了360AISA全流量威胁分析系统和360本地安全大脑，通过将被测系统中全部流量镜像发送到360AISA全流量威胁分析系统及360本地安全大脑中进行分析监测，发现入侵事件后及时通过钉钉报警，并且能够自动阻断。 |
| 可信验证 | a）可基于可信根对计算设备的系统引导程序、系统程序、重要配置参数和应用程序等进行可信验证，并在应用程序的关键执行环节进行动态可信验证，在检测到其可信性受到破坏后进行报警，并将验证结果形成审计记录送至安全管理中心。 | 未基于可信根对计算设备提供可信验证。 |
| 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； | 经现场访谈网络管理员及对交换机配置，交换机中关闭Telnet协议，采用SSH协议进行通信，保证重要数据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。 | 经访谈网络管理员及核查H3C S6800系列交换机产品文档，文件中目录05-参考指南--05文件系统管理命令中包含：“交换机中文件系统通常使用摘要算法（SHA-256）对文件计算摘要值，用于验证文件的正确性和完整性”。 |
| 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； | 经现场访谈网络管理员及对交换机配置，交换机中关闭Telnet协议，采用SSH协议进行通信，保证重要数据在传输过程中的保密性。 |
| b）应采用密码技术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个人信息等。 | 经访谈网管理员，管理员在设置用户口令时添加simple参数，经核查H3C S6800系列交换机产品文档，在文档05-参考指南--03-登录设备命令--1、登录设备--1.1等设备命令--1.1.28 set authentication password中正对simple参数进行说明：“simple：以明文方式设置密码，该密码将以密文方式存储。 |
| 数据备份恢复 | a）应提供重要数据的本地数据备份与恢复功能； | 经现场访谈网络管理员及核查相应配置，在备份服务器中配置python脚本，并设置每天凌晨4点将交换机中配置文件下载至备份服务器中进行备份，管理员每周对备份文件进行巡检，确保配置文件完整备份至备份服务器中。 |
| b）应提供异地实时备份功能，利用通信网络将重要数据实时备份至备份场地； | 1、经现场访谈网络管理员，管理员添加了数据同步策略，每天将备份服务器中备份文件拷贝至阿里公共云备份服务器中进行备份；2、经核查阿里公共云备份服务器（10.30.19.10）中备份目录/data/network-backup中具备网络设备配置备份文件；3、综上，因世纪互联IDC机房及阿里云公共云均在上海市，未实现异地实时备份功能。 |
| c）应提供重要数据处理系统的热冗余，保证系统的高可用性。 | 经访谈访问管理员及核查网络拓扑图，重要数据处理系统中采用双机冗余部署，保证系统的高可用性。 |

4.1.1.15. 负载均衡1

|  |  |  |
| --- | --- | --- |
| **安全控制点** | **测评指标** | **结果记录** |
| 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、经现场访谈访问管理员及核查负载均衡配置策略，负载均衡采用用户名、口令进行身份鉴别和标识，2、负载均衡具有用户名查重功能，保证用户名具有唯一性，经现场测试，创建重名用户会提示用户已存在，3、核查负载均衡system-users-Authentication中配置，口令长度至少8位，包含大小写字母、数字、特殊字符四种组合，用户口令更改周期为30天。 |
| 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； | 经现场访谈访问管理员及核查负载均衡配置策略，负载均衡未启用登录失败处理策略，未配置空闲超时退出策略。 |
| 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； | 经现场访谈访问管理员及核查负载均衡配置策略，负载均衡在远程管理时采用HTTPS协议进行通信，防止鉴别信息在网络传输过程中被窃听。 |
| 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。 | 经现场访谈访问管理员及核查负载均衡配置策略，负载均衡仅采用用户名、口令方式进行身份鉴别，未采用两种或两种以上组合的鉴别技术对用户进行身份鉴别。 |
| 访问控制 | a）应对登录的用户分配账户和权限； | 经现场访谈访问管理员及核查负载均衡配置策略，负载均衡中仅创建admin管理账户，并赋予该用户拥有最高管理权限。 |
| b）应重命名或删除默认账户，修改默认账户的默认口令； | 经现场访谈访问管理员及核查负载均衡配置策略，负载均衡中默认账户未被重命名，但是用户口令已按照复杂度策略更改。 |
| 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； | 经现场访谈访问管理员及核查负载均衡配置策略，负载均衡中仅创建admin管理账户，不存在多余、过期账户，但是存在共享账户。 |
| 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； | 经现场访谈访问管理员及核查负载均衡配置策略，负载均衡中未创建审计管理员、安全管理员等账户，未实现管理用户权限最小化及权限分离。 |
| e）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； | 经访谈及核查相关配置界面，负载均衡设备由网络管理员账户为管理用户配置相应账号，并按照用户角色级别赋予管理用户操作权限。 |
| f）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； | 经访谈及核查负载均衡设备的配置，负债均衡访问控制策略由网络管理用户负债均衡的管理界面进行配置管理及访问管理等，访问控制粒度达到主体为用户级、客体为菜单级。 |
| g）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。 | 经核查配置文件及访谈网络管理员，负载均衡设备未对重要主体和客体设置安全标记。 |
| 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； | 经现场访谈管理员及核查负载均衡配置策略，负载均衡中启用了日志审计功能，审计覆盖所有用户操作及系统安全事件等。 |
| 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； | 经核查负载均衡中审计记录，负载均衡中审计记录包括：时间、日志级别、主机名、服务、详情等。 |
| 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、经现场访谈网络管理员及核查负载均衡审计记录，负载均衡中审计记录无删除权限，所有用户均不能对审计记录删除或修改，2、核查负载均衡备份策略，管理员配置审计记录备份策略，实时将审计记录备份至360本地安全大脑中进行备份保存，保证审计记录保存时间满足6个月以上。 |
| d）应对审计进程进行保护，防止未经授权的中断。 | 经现场访谈网络管理员及核查负载均衡审计进程，负载均衡中审计进程受系统进程保护，所有用户均无权限对审计进程单独中断。 |
| 入侵防范 | a）应遵循最小安装的原则，仅安装需要的组件和应用程序； | 经访谈及核查负载均衡系统，负载均衡系统为厂商提供独立封装系统，不允许安装其他组件及应用程序，遵循最小安装原则。 |
| b）应关闭不需要的系统服务、默认共享和高危端口； | 经现场核查负载均衡中配置，负载均衡中仅启用了SNMP V2版、NTP、HTTPS等服务，Telnet协议已关闭。 |
| c）应通过设定终端接入方式或网络地址范围对通过网络进行管理的管理终端进行限制； | 经现场核查，远程管理负载均衡时仅允许管理用户首先连接跳板机，然后通过跳板机远程管理负载均衡。 |
| d）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； | 该测评项测评对象为业务应用系统、中间件和系统管理软件，网络设备不适用。 |
| e）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； | 1、经访谈网络管理员，管理员定期对官方网站通报的安全漏洞进行评估，然后从官方网站下载安全补丁对负载均衡进行补丁修复，避免系统中存在安全漏洞，2、经现场漏洞扫描，未发现负载均衡中存在安全漏洞。 |
| f）应能够检测到对重要节点进行入侵的行为，并在发生严重入侵事件时提供报警。 | 经访谈网络管理员，被测系统中部署了360AISA全流量威胁分析系统和360本地安全大脑，通过将被测系统中全部流量镜像发送到360AISA全流量威胁分析系统及360本地安全大脑中进行分析监测，发现入侵事件后及时通过钉钉报警，并且能够自动阻断。 |
| 可信验证 | a）可基于可信根对计算设备的系统引导程序、系统程序、重要配置参数和应用程序等进行可信验证，并在应用程序的关键执行环节进行动态可信验证，在检测到其可信性受到破坏后进行报警，并将验证结果形成审计记录送至安全管理中心。 | 未基于可信根对计算设备提供可信验证。 |
| 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； | 经现场核查负载均衡通信方式，负载均衡通过HTTPS协议进行通信，保证重要数据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。 | 经核查网络管理员，负载均衡采用厂商自身校验技术保证用户鉴别数据、重要配置数据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； | 经现场核查负载均衡通信方式，负载均衡通过HTTPS协议进行通信，保证重要数据传输过程中的保密性。 |
| b）应采用密码技术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个人信息等。 | 经核查网络管理员及负载均衡中口令信息，负载均衡口令在系统中采用加密方式存储，保证用户鉴别信息在存储过程中的保密性。 |
| 数据备份恢复 | a）应提供重要数据的本地数据备份与恢复功能； | 经现场访谈网络管理员及核查相应配置，在备份服务器中配置python脚本，并设置每天凌晨4点将交换机中配置文件下载至备份服务器中进行备份，管理员每周对备份文件进行巡检，确保配置文件完整备份至备份服务器中。 |
| b）应提供异地实时备份功能，利用通信网络将重要数据实时备份至备份场地； | 1、经现场访谈网络管理员，管理员添加了数据同步策略，每天将备份服务器中备份文件拷贝至阿里公共云备份服务器中进行备份；2、经核查阿里公共云备份服务器（10.30.19.10）中备份目录/data/network-backup中具备网络设备配置备份文件；3、综上，因世纪互联IDC机房及阿里云公共云均在上海市，未实现异地实时备份功能。 |
| c）应提供重要数据处理系统的热冗余，保证系统的高可用性。 | 经核查，重要数据处理系统中采用双机冗余部署，保证系统的高可用性。 |

4.1.1.16. 负载均衡2

|  |  |  |
| --- | --- | --- |
| **安全控制点** | **测评指标** | **结果记录** |
| 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、经现场访谈访问管理员及核查负载均衡配置策略，负载均衡采用用户名、口令进行身份鉴别和标识，2、负载均衡具有用户名查重功能，保证用户名具有唯一性，经现场测试，创建重名用户会提示用户已存在，3、核查负载均衡system-users-Authentication中配置，口令长度至少8位，包含大小写字母、数字、特殊字符四种组合，用户口令更改周期为30天。 |
| 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； | 经现场访谈访问管理员及核查负载均衡配置策略，负载均衡未启用登录失败处理策略，未配置空闲超时退出策略。 |
| 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； | 经现场访谈访问管理员及核查负载均衡配置策略，负载均衡在远程管理时采用HTTPS协议进行通信，防止鉴别信息在网络传输过程中被窃听。 |
| 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。 | 经现场访谈访问管理员及核查负载均衡配置策略，负载均衡仅采用用户名、口令方式进行身份鉴别，未采用两种或两种以上组合的鉴别技术对用户进行身份鉴别。 |
| 访问控制 | a）应对登录的用户分配账户和权限； | 经现场访谈访问管理员及核查负载均衡配置策略，负载均衡中仅创建admin管理账户，并赋予该用户拥有最高管理权限。 |
| b）应重命名或删除默认账户，修改默认账户的默认口令； | 经现场访谈访问管理员及核查负载均衡配置策略，负载均衡中默认账户未被重命名，但是用户口令已按照复杂度策略更改。 |
| 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； | 经现场访谈访问管理员及核查负载均衡配置策略，负载均衡中仅创建admin管理账户，不存在多余、过期账户，但是存在共享账户。 |
| 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； | 经现场访谈访问管理员及核查负载均衡配置策略，负载均衡中未创建审计管理员、安全管理员等账户，未实现管理用户权限最小化及权限分离。 |
| e）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； | 经访谈及核查相关配置界面，负载均衡设备由网络管理员账户为管理用户配置相应账号，并按照用户角色级别赋予管理用户操作权限。 |
| f）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； | 经访谈及核查负载均衡设备的配置，负债均衡访问控制策略由网络管理用户负债均衡的管理界面进行配置管理及访问管理等，访问控制粒度达到主体为用户级、客体为菜单级。 |
| g）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。 | 经核查配置文件及访谈网络管理员，负载均衡设备未对重要主体和客体设置安全标记。 |
| 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； | 经现场访谈管理员及核查负载均衡配置策略，负载均衡中启用了日志审计功能，审计覆盖所有用户操作及系统安全事件等。 |
| 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； | 经核查负载均衡中审计记录，负载均衡中审计记录包括：时间、日志级别、主机名、服务、详情等。 |
| 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、经现场访谈网络管理员及核查负载均衡审计记录，负载均衡中审计记录无删除权限，所有用户均不能对审计记录删除或修改，2、核查负载均衡备份策略，管理员配置审计记录备份策略，实时将审计记录备份至360本地安全大脑中进行备份保存，保证审计记录保存时间满足6个月以上。 |
| d）应对审计进程进行保护，防止未经授权的中断。 | 经现场访谈网络管理员及核查负载均衡审计进程，负载均衡中审计进程受系统进程保护，所有用户均无权限对审计进程单独中断。 |
| 入侵防范 | a）应遵循最小安装的原则，仅安装需要的组件和应用程序； | 经访谈及核查负载均衡系统，负载均衡系统为厂商提供独立封装系统，不允许安装其他组件及应用程序，遵循最小安装原则。 |
| b）应关闭不需要的系统服务、默认共享和高危端口； | 经现场核查负载均衡中配置，负载均衡中仅启用了SNMP V2版、NTP、HTTPS等服务，Telnet协议已关闭。 |
| c）应通过设定终端接入方式或网络地址范围对通过网络进行管理的管理终端进行限制； | 经现场核查，远程管理负载均衡时仅允许管理用户首先连接跳板机，然后通过跳板机远程管理负载均衡。 |
| d）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； | 该测评项测评对象为业务应用系统、中间件和系统管理软件，网络设备不适用。 |
| e）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； | 1、经访谈网络管理员，管理员定期对官方网站通报的安全漏洞进行评估，然后从官方网站下载安全补丁对负载均衡进行补丁修复，避免系统中存在安全漏洞，2、经现场漏洞扫描，未发现负载均衡中存在安全漏洞。 |
| f）应能够检测到对重要节点进行入侵的行为，并在发生严重入侵事件时提供报警。 | 经访谈网络管理员，被测系统中部署了360AISA全流量威胁分析系统和360本地安全大脑，通过将被测系统中全部流量镜像发送到360AISA全流量威胁分析系统及360本地安全大脑中进行分析监测，发现入侵事件后及时通过钉钉报警，并且能够自动阻断。 |
| 可信验证 | a）可基于可信根对计算设备的系统引导程序、系统程序、重要配置参数和应用程序等进行可信验证，并在应用程序的关键执行环节进行动态可信验证，在检测到其可信性受到破坏后进行报警，并将验证结果形成审计记录送至安全管理中心。 | 未基于可信根对计算设备提供可信验证。 |
| 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； | 经现场核查负载均衡通信方式，负载均衡通过HTTPS协议进行通信，保证重要数据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。 | 经核查网络管理员，负载均衡采用厂商自身校验技术保证用户鉴别数据、重要配置数据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； | 经现场核查负载均衡通信方式，负载均衡通过HTTPS协议进行通信，保证重要数据传输过程中的保密性。 |
| b）应采用密码技术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个人信息等。 | 经核查网络管理员及负载均衡中口令信息，负载均衡口令在系统中采用加密方式存储，保证用户鉴别信息在存储过程中的保密性。 |
| 数据备份恢复 | a）应提供重要数据的本地数据备份与恢复功能； | 经现场访谈网络管理员及核查相应配置，在备份服务器中配置python脚本，并设置每天凌晨4点将交换机中配置文件下载至备份服务器中进行备份，管理员每周对备份文件进行巡检，确保配置文件完整备份至备份服务器中。 |
| b）应提供异地实时备份功能，利用通信网络将重要数据实时备份至备份场地； | 1、经现场访谈网络管理员，管理员添加了数据同步策略，每天将备份服务器中备份文件拷贝至阿里公共云备份服务器中进行备份；2、经核查阿里公共云备份服务器（10.30.19.10）中备份目录/data/network-backup中具备网络设备配置备份文件；3、综上，因世纪互联IDC机房及阿里云公共云均在上海市，未实现异地实时备份功能。 |
| c）应提供重要数据处理系统的热冗余，保证系统的高可用性。 | 经核查，重要数据处理系统中采用双机冗余部署，保证系统的高可用性。 |

4.1.1.17. 管理网核心交换机1

|  |  |  |
| --- | --- | --- |
| **安全控制点** | **测评指标** | **结果记录** |
| 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、经现场访谈网络管理员，交换机采用用户名、口令进行身份标识及身份鉴别；2、经核查交换机配置，输入display password-control命令，返回信息为 Password aging:Enabled (90 days) Password length: Enabled (10 characters) Password composition:Enabled (3 types, 1 characters per type) Password history: Enabled (max history records:4)，通过返回信息确认：用户口令长度为至少10位，包含数字、字母、字符三种类型，用户口令更改周期为90天；3、通过现场在交换机中创建与网络管理员ylops同名账户时，交换机中会提示用户名已存在，无法创重名用户，确认用户标识具备唯一性。 |
| 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、经现场核查交换机配置策略，输入display password-control命令，返回信息为 Maximum login attempts: 3，Action for exceeding login attempts: Lock user for 1 minutes、User authentication timeout：600 seconds；2、通过返回信息确认用户连续错误登录3次锁定账户1分钟，用户登录连接超时时间限制为600秒。 |
| 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； | 1、经现场访谈网络管理员及核查其远程连接交换机的方式，管理员在远程管理交换机时采用SSH协议进行通信，防止鉴别信息在网络传输过程中被窃听；2、访谈网络管理员，Telnet协议默认为关闭状态，通过输入命令telnet server enable尝试启用Telnet协议，返回信息为Telnet is insecure because it transmits data in plaintext form，Telnet协议未启成功；3，通过在终端Telnet该交换机，无法连接成功。 |
| 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。 | 经现场核查网络管理员远程登录交换机方式，交换机仅采用用户名、口令方式进行身份鉴别，未采用两种或两种以上组合的鉴别技术对用户进行身份鉴别。 |
| 访问控制 | a）应对登录的用户分配账户和权限； | 1、经现场核查交换机中用户信息，通过输入display local-user命令，返回信息中显示交换机中存在security、tulei、xuweilai、ylops等用户，其中security的 user role list：level-1，network-operator；tulei、xuweilai、ylops的 user role list：network-admin,network-operator；2、经访谈网络管理员，其中tulei、xuweilai为两位网络管理员账号，ylops为网络主管账户，security为安全管理账号。 |
| b）应重命名或删除默认账户，修改默认账户的默认口令； | 1、经现场核查交换机中用户信息，通过输入display local-user命令，返回信息中显示交换机中存在security、tulei、xuweilai、ylops等用户,不存在默认账户，2、经核查交换机配置，输入display password-control命令，返回信息为 Password aging:Enabled (90 days) Password length: Enabled (10 characters) Password composition:Enabled (3 types, 1 characters per type) Password history: Enabled (max history records：3，用户口令已按照复杂度策略更改。 |
| 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； | 经现场核查交换机中用户信息，通过输入display local-user命令，返回信息中显示交换机中存在security、tulei、xuweilai、ylops等用户,经访谈网络管理员，其中tulei、xuweilai为两位网络管理员账号，ylops为网络主管账户，security为安全管理账号，不存在多余、过期、共享账户。 |
| 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； | 经现场核查交换机中用户信息，通过输入display local-user命令，返回信息中显示交换机中存在security、tulei、xuweilai、ylops等用户，经访谈网络管理员，交换机中未单独创建审计管理员账户，并且网络管理员权限为超管用户权限，未实现管理用户权限最小化及权限分离。 |
| e）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； | 经核查配置文件及访谈网络管理员，交换机中由网络管理员角色账户为管理用户配置相应账号，并按照用户角色级别赋予管理用户操作权限。 |
| f）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； | 经核查配置文件及访谈网络管理员，交换机中访问控制策略为管理用户的交换机中配置文件等进行配置管理及访问管理等，访问控制粒度达到主体为用户级、客体为文件级。 |
| g）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。 | 经核查配置文件及访谈网络管理员，未对重要主体和客体设置安全标记。 |
| 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； | 经现场访谈网络管理员及核查交换机配置，输入命令display logbuffer reverse，返回信息为logbuffer:enable；确认交换机中其中安全审计功能，通过查看审计记录内容，确认审计记录中包含设备运行记录及用户操作行为审计记录等。 |
| 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； | 经现场核查交换机中审计记录内容，审计记录中包含：日期、时间、主机名、类型、IP地址、用户名、详情等。 |
| 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、经访谈网络管理员，交换机中所有用户均无权限对审计记录进行删除或修改，并且管理员在备份服务器（10.33.110.160）中添加审计记录下载脚本（python脚本），实时将交换机中审计记录下载至备份服务器中进行备份；2、经现场核查备份服务器（10.33.110.160）中/home/network\_backup目录中存在审计记录备份文件，备份文件宿主为root，权限为744，其他用户仅拥有读权限。 |
| d）应对审计进程进行保护，防止未经授权的中断。 | 经现场访谈网络管理员，交换机中审计进程受系统进程保护，所有用户均无权限将审计进程单独中断。 |
| 入侵防范 | a）应遵循最小安装的原则，仅安装需要的组件和应用程序； | 经访谈网络管理员及核查配置文件，交换机为厂商提供独立封装系统，不允许安装其他组件及应用程序，遵循最小安装原则。 |
| b）应关闭不需要的系统服务、默认共享和高危端口； | 经现场访谈网络管理员及核查交换机配置，输入display current-fonfiguration，返回信息HTTP、Telnet协议均已关闭，交换机中未启用不需要的系统服务、默认共享及高危端口。 |
| c）应通过设定终端接入方式或网络地址范围对通过网络进行管理的管理终端进行限制； | 经访谈网络管理员，在防火墙中添加访问控制策略，仅允许管理用户通过堡垒机远程管理网络设备、安全设备及服务器等，经核查防火墙中访问控制策略，具备堡垒机地址-设备管理网段（10.33.0.0）的访问控制策略。 |
| d）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； | 该测评项测评对象为业务应用系统、中间件和系统管理软件，故将该项调整为不适用。 |
| e）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； | 1、经访谈网络管理员，会定期对官方网站通报的安全漏洞进行评估，然后从官方网站下载安全补丁，经过综合评估测试后对交换机系统进行补丁修复，避免系统中存在安全漏洞，2、经现场漏洞扫描，未发现交换机中存在安全漏洞。 |
| f）应能够检测到对重要节点进行入侵的行为，并在发生严重入侵事件时提供报警。 | 经访谈网络管理员，被测系统中部署了360AISA全流量威胁分析系统和360本地安全大脑，通过将被测系统中全部流量镜像发送到360AISA全流量威胁分析系统及360本地安全大脑中进行分析监测，发现入侵事件后及时通过钉钉报警，并且能够自动阻断。 |
| 可信验证 | a）可基于可信根对计算设备的系统引导程序、系统程序、重要配置参数和应用程序等进行可信验证，并在应用程序的关键执行环节进行动态可信验证，在检测到其可信性受到破坏后进行报警，并将验证结果形成审计记录送至安全管理中心。 | 未基于可信根对计算设备提供可信验证。 |
| 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； | 经现场访谈网络管理员及对交换机配置，交换机中关闭Telnet协议，采用SSH协议进行通信，保证重要数据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。 | 经访谈网络管理员及核查H3C S6800系列交换机产品文档，文件中目录05-参考指南--05文件系统管理命令中包含：“交换机中文件系统通常使用摘要算法（SHA-256）对文件计算摘要值，用于验证文件的正确性和完整性”。 |
| 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； | 经现场访谈网络管理员及对交换机配置，交换机中关闭Telnet协议，采用SSH协议进行通信，保证重要数据在传输过程中的保密性。 |
| b）应采用密码技术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个人信息等。 | 经访谈网管理员，管理员在设置用户口令时添加simple参数，经核查H3C S6800系列交换机产品文档，在文档05-参考指南--03-登录设备命令--1、登录设备--1.1等设备命令--1.1.28 set authentication password中正对simple参数进行说明：“simple：以明文方式设置密码，该密码将以密文方式存储。 |
| 数据备份恢复 | a）应提供重要数据的本地数据备份与恢复功能； | 经现场访谈网络管理员及核查相应配置，在备份服务器中配置python脚本，并设置每天凌晨4点将交换机中配置文件下载至备份服务器中进行备份，管理员每周对备份文件进行巡检，确保配置文件完整备份至备份服务器中。 |
| b）应提供异地实时备份功能，利用通信网络将重要数据实时备份至备份场地； | 1、经现场访谈网络管理员，管理员添加了数据同步策略，每天将备份服务器中备份文件拷贝至阿里公共云备份服务器中进行备份；2、经核查阿里公共云备份服务器（10.30.19.10）中备份目录/data/network-backup中具备网络设备配置备份文件；3、综上，因世纪互联IDC机房及阿里云公共云均在上海市，未实现异地实时备份功能。 |
| c）应提供重要数据处理系统的热冗余，保证系统的高可用性。 | 经访谈访问管理员及核查网络拓扑图，重要数据处理系统中采用双机冗余部署，保证系统的高可用性。 |

4.1.1.18. 管理网汇聚交换机2

|  |  |  |
| --- | --- | --- |
| **安全控制点** | **测评指标** | **结果记录** |
| 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、经现场访谈网络管理员，交换机采用用户名、口令进行身份标识及身份鉴别；2、经核查交换机配置，输入display password-control命令，返回信息为 Password aging:Enabled (90 days) Password length: Enabled (10 characters) Password composition:Enabled (3 types, 1 characters per type) Password history: Enabled (max history records:4)，通过返回信息确认：用户口令长度为至少10位，包含数字、字母、字符三种类型，用户口令更改周期为90天；3、通过现场在交换机中创建与网络管理员ylops同名账户时，交换机中会提示用户名已存在，无法创重名用户，确认用户标识具备唯一性。 |
| 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、经现场核查交换机配置策略，输入display password-control命令，返回信息为 Maximum login attempts: 3，Action for exceeding login attempts: Lock user for 1 minutes、User authentication timeout：600 seconds；2、通过返回信息确认用户连续错误登录3次锁定账户1分钟，用户登录连接超时时间限制为600秒。 |
| 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； | 1、经现场访谈网络管理员及核查其远程连接交换机的方式，管理员在远程管理交换机时采用SSH协议进行通信，防止鉴别信息在网络传输过程中被窃听；2、访谈网络管理员，Telnet协议默认为关闭状态，通过输入命令telnet server enable尝试启用Telnet协议，返回信息为Telnet is insecure because it transmits data in plaintext form，Telnet协议未启成功；3，通过在终端Telnet该交换机，无法连接成功。 |
| 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。 | 经现场核查网络管理员远程登录交换机方式，交换机仅采用用户名、口令方式进行身份鉴别，未采用两种或两种以上组合的鉴别技术对用户进行身份鉴别。 |
| 访问控制 | a）应对登录的用户分配账户和权限； | 1、经现场核查交换机中用户信息，通过输入display local-user命令，返回信息中显示交换机中存在security、tulei、xuweilai、ylops等用户，其中security的 user role list：level-1，network-operator；tulei、xuweilai、ylops的 user role list：network-admin,network-operator；2、经访谈网络管理员，其中tulei、xuweilai为两位网络管理员账号，ylops为网络主管账户，security为安全管理账号。 |
| b）应重命名或删除默认账户，修改默认账户的默认口令； | 1、经现场核查交换机中用户信息，通过输入display local-user命令，返回信息中显示交换机中存在security、tulei、xuweilai、ylops等用户,不存在默认账户，2、经核查交换机配置，输入display password-control命令，返回信息为 Password aging:Enabled (90 days) Password length: Enabled (10 characters) Password composition:Enabled (3 types, 1 characters per type) Password history: Enabled (max history records：3，用户口令已按照复杂度策略更改。 |
| 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； | 经现场核查交换机中用户信息，通过输入display local-user命令，返回信息中显示交换机中存在security、tulei、xuweilai、ylops等用户,经访谈网络管理员，其中tulei、xuweilai为两位网络管理员账号，ylops为网络主管账户，security为安全管理账号，不存在多余、过期、共享账户。 |
| 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； | 经现场核查交换机中用户信息，通过输入display local-user命令，返回信息中显示交换机中存在security、tulei、xuweilai、ylops等用户，经访谈网络管理员，交换机中未单独创建审计管理员账户，并且网络管理员权限为超管用户权限，未实现管理用户权限最小化及权限分离。 |
| e）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； | 经核查配置文件及访谈网络管理员，交换机中由网络管理员角色账户为管理用户配置相应账号，并按照用户角色级别赋予管理用户操作权限。 |
| f）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； | 经核查配置文件及访谈网络管理员，交换机中访问控制策略为管理用户的交换机中配置文件等进行配置管理及访问管理等，访问控制粒度达到主体为用户级、客体为文件级。 |
| g）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。 | 经核查配置文件及访谈网络管理员，未对重要主体和客体设置安全标记。 |
| 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； | 经现场访谈网络管理员及核查交换机配置，输入命令display logbuffer reverse，返回信息为logbuffer:enable；确认交换机中其中安全审计功能，通过查看审计记录内容，确认审计记录中包含设备运行记录及用户操作行为审计记录等。 |
| 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； | 经现场核查交换机中审计记录内容，审计记录中包含：日期、时间、主机名、类型、IP地址、用户名、详情等。 |
| 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、经访谈网络管理员，交换机中所有用户均无权限对审计记录进行删除或修改，并且管理员在备份服务器（10.33.110.160）中添加审计记录下载脚本（python脚本），实时将交换机中审计记录下载至备份服务器中进行备份；2、经现场核查备份服务器（10.33.110.160）中/home/network\_backup目录中存在审计记录备份文件，备份文件宿主为root，权限为744，其他用户仅拥有读权限。 |
| d）应对审计进程进行保护，防止未经授权的中断。 | 经现场访谈网络管理员，交换机中审计进程受系统进程保护，所有用户均无权限将审计进程单独中断。 |
| 入侵防范 | a）应遵循最小安装的原则，仅安装需要的组件和应用程序； | 经访谈网络管理员及核查配置文件，交换机为厂商提供独立封装系统，不允许安装其他组件及应用程序，遵循最小安装原则。 |
| b）应关闭不需要的系统服务、默认共享和高危端口； | 经现场访谈网络管理员及核查交换机配置，输入display current-fonfiguration，返回信息HTTP、Telnet协议均已关闭，交换机中未启用不需要的系统服务、默认共享及高危端口。 |
| c）应通过设定终端接入方式或网络地址范围对通过网络进行管理的管理终端进行限制； | 经访谈网络管理员，在防火墙中添加访问控制策略，仅允许管理用户通过堡垒机远程管理网络设备、安全设备及服务器等，经核查防火墙中访问控制策略，具备堡垒机地址-设备管理网段（10.33.0.0）的访问控制策略。 |
| d）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； | 该测评项测评对象为业务应用系统、中间件和系统管理软件，故将该项调整为不适用。 |
| e）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； | 1、经访谈网络管理员，会定期对官方网站通报的安全漏洞进行评估，然后从官方网站下载安全补丁，经过综合评估测试后对交换机系统进行补丁修复，避免系统中存在安全漏洞，2、经现场漏洞扫描，未发现交换机中存在安全漏洞。 |
| f）应能够检测到对重要节点进行入侵的行为，并在发生严重入侵事件时提供报警。 | 经访谈网络管理员，被测系统中部署了360AISA全流量威胁分析系统和360本地安全大脑，通过将被测系统中全部流量镜像发送到360AISA全流量威胁分析系统及360本地安全大脑中进行分析监测，发现入侵事件后及时通过钉钉报警，并且能够自动阻断。 |
| 可信验证 | a）可基于可信根对计算设备的系统引导程序、系统程序、重要配置参数和应用程序等进行可信验证，并在应用程序的关键执行环节进行动态可信验证，在检测到其可信性受到破坏后进行报警，并将验证结果形成审计记录送至安全管理中心。 | 未基于可信根对计算设备提供可信验证。 |
| 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； | 经现场访谈网络管理员及对交换机配置，交换机中关闭Telnet协议，采用SSH协议进行通信，保证重要数据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。 | 经访谈网络管理员及核查H3C S6800系列交换机产品文档，文件中目录05-参考指南--05文件系统管理命令中包含：“交换机中文件系统通常使用摘要算法（SHA-256）对文件计算摘要值，用于验证文件的正确性和完整性”。 |
| 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； | 经现场访谈网络管理员及对交换机配置，交换机中关闭Telnet协议，采用SSH协议进行通信，保证重要数据在传输过程中的保密性。 |
| b）应采用密码技术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个人信息等。 | 经访谈网管理员，管理员在设置用户口令时添加simple参数，经核查H3C S6800系列交换机产品文档，在文档05-参考指南--03-登录设备命令--1、登录设备--1.1等设备命令--1.1.28 set authentication password中正对simple参数进行说明：“simple：以明文方式设置密码，该密码将以密文方式存储。 |
| 数据备份恢复 | a）应提供重要数据的本地数据备份与恢复功能； | 经现场访谈网络管理员及核查相应配置，在备份服务器中配置python脚本，并设置每天凌晨4点将交换机中配置文件下载至备份服务器中进行备份，管理员每周对备份文件进行巡检，确保配置文件完整备份至备份服务器中。 |
| b）应提供异地实时备份功能，利用通信网络将重要数据实时备份至备份场地； | 1、经现场访谈网络管理员，管理员添加了数据同步策略，每天将备份服务器中备份文件拷贝至阿里公共云备份服务器中进行备份；2、经核查阿里公共云备份服务器（10.30.19.10）中备份目录/data/network-backup中具备网络设备配置备份文件；3、综上，因世纪互联IDC机房及阿里云公共云均在上海市，未实现异地实时备份功能。 |
| c）应提供重要数据处理系统的热冗余，保证系统的高可用性。 | 经访谈访问管理员及核查网络拓扑图，重要数据处理系统中采用双机冗余部署，保证系统的高可用性。 |

4.1.1.19. 无线控制器AC1

|  |  |  |
| --- | --- | --- |
| **安全控制点** | **测评指标** | **结果记录** |
| 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、经现场访谈网络管理员，无线控制器AC采用用户名、口令进行身份标识及身份鉴别；2、经核查无线控制器AC配置，输入display password-control命令，返回信息为 Password aging:Enabled (90 days) Password length: Enabled (10 characters) Password composition:Enabled (3 types, 1 characters per type) Password history: Enabled (max history records:4)，通过返回信息确认：用户口令长度为至少10位，包含数字、字母、字符三种类型，未定期更改用户口令；3、通过现场在无线控制器AC中创建与网络管理员同名账户时，无线控制器AC中会提示用户名已存在，无法创重名用户，确认用户标识具备唯一性。 |
| 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、经现场核查无线控制器AC配置策略，输入display password-control命令，返回信息为 Maximum login attempts: 3，Action for exceeding login attempts: Lock user for 1 minutes、User authentication timeout：600 seconds；2、通过返回信息确认用户连续错误登录3次锁定账户1分钟，用户登录连接超时时间限制为600秒。 |
| 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； | 1、经现场访谈网络管理员及核查其远程连接无线控制器AC的方式，管理员在远程管理无线控制器AC时采用SSH协议进行通信，防止鉴别信息在网络传输过程中被窃听；2、访谈网络管理员，Telnet协议默认为关闭状态，通过输入命令telnet server enable尝试启用Telnet协议，返回信息为Telnet is insecure because it transmits data in plaintext form，Telnet协议未启成功；3，通过在终端Telnet该无线控制器AC，无法连接成功。 |
| 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。 | 经现场核查网络管理员远程登录无线控制器AC方式，无线控制器AC仅采用用户名、口令方式进行身份鉴别，未采用两种或两种以上组合的鉴别技术对用户进行身份鉴别。 |
| 访问控制 | a）应对登录的用户分配账户和权限； | 1、经现场核查无线控制器AC中用户信息，通过输入display local-user命令，返回信息中显示无线控制器AC中存在场站管理员、网络管理员两个用户，该用户均分配超管权限。 |
| b）应重命名或删除默认账户，修改默认账户的默认口令； | 1、经现场核查无线控制器AC中用户信息，通过输入display local-user命令，返回信息中显示无线控制器AC中存在场站管理员、网络管理员两个账户,不存在默认账户，2、经核查无线控制器AC配置，输入display password-control命令，返回信息为 Password aging:Enabled (90 days) Password length: Enabled (10 characters) Password composition:Enabled (3 types, 1 characters per type) Password history: Enabled (max history records：3，用户口令已按照复杂度策略更改。 |
| 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； | 经现场核查无线控制器AC中用户信息，通过输入display local-user命令，返回信息中显示无线控制器AC中存在场站管理员、网络管理员等用户,经访谈网络管理员，账户与管理员一一对应，不存在多余、过期、共享账户。 |
| 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； | 经现场核查无线控制器AC中用户信息，通过输入display local-user命令，返回信息中显示无线控制器AC中存在场站管理员、网络管理员等用户,经访谈网络管理员，场站管理员、网络管理员均分配超级管理员权限，未按照权限最小化原则赋予管理用户权限及实现权限分离。 |
| e）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； | 经核查配置文件及访谈网络管理员，无线控制器AC由网络管理员角色账户为管理用户配置相应账号，并按照用户角色级别赋予管理用户操作权限。 |
| f）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； | 经核查配置文件及访谈网络管理员，无线控制器AC访问控制策略为管理用户的无线控制器AC配置文件等进行配置管理及访问管理等，访问控制粒度达到主体为用户级、客体为文件级。 |
| g）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。 | 经核查配置文件及访谈网络管理员，无线控制器AC未对重要主体和客体设置安全标记。 |
| 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； | 经现场访谈网络管理员及核查无线控制器AC配置，输入命令display logbuffer reverse，返回信息为logbuffer:enable；确认无线控制器AC中其中安全审计功能，通过查看审计记录内容，确认审计记录中包含设备运行记录及用户操作行为审计记录等。 |
| 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； | 经现场核查无线控制器AC中审计记录内容，审计记录中包含：日期、时间、主机名、类型、IP地址、用户名、详情等。 |
| 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、经访谈网络管理员，无线控制器AC中所有用户均无权限对审计记录进行删除或修改；2、经现场核查，管理员配置了审计记录备份策略，实时将无线控制器AC中审计记录上传至备份服务器中进行备份；2、经现场核查备份服务器中/home/network\_backup目录中存在审计记录备份文件，备份文件宿主为root，权限为744，其他用户仅拥有读权限。 |
| d）应对审计进程进行保护，防止未经授权的中断。 | 经现场访谈网络管理员，无线控制器AC中审计进程受系统进程保护，所有用户均无权限将审计进程单独中断。 |
| 入侵防范 | a）应遵循最小安装的原则，仅安装需要的组件和应用程序； | 经访谈网络管理员及核查配置文件，无线控制器AC为厂商提供独立封装系统，不允许安装其他组件及应用程序，遵循最小安装原则。 |
| b）应关闭不需要的系统服务、默认共享和高危端口； | 经现场访谈网络管理员及核查无线控制器AC配置，输入display current-fonfiguration，返回信息HTTP、Telnet协议均已关闭，无线控制器AC中未启用不需要的系统服务、默认共享及高危端口。 |
| c）应通过设定终端接入方式或网络地址范围对通过网络进行管理的管理终端进行限制； | 经访谈网络管理员，在防火墙中添加访问控制策略，仅允许管理用户通过堡垒机远程管理网络设备、安全设备及服务器等，经核查防火墙中访问控制策略，具备堡垒机地址-设备管理网段（10.33.0.0）的访问控制策略。 |
| d）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； | 该测评项测评对象为业务应用系统、中间件和系统管理软件，故将该项调整为不适用。 |
| e）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； | 1、经访谈网络管理员，会定期对官方网站通报的安全漏洞进行评估，然后从官方网站下载安全补丁，经过综合评估测试后对无线控制器AC系统进行补丁修复，避免系统中存在安全漏洞，2、经现场漏洞扫描，未发现无线控制器AC中存在安全漏洞。 |
| f）应能够检测到对重要节点进行入侵的行为，并在发生严重入侵事件时提供报警。 | 经访谈网络管理员，被测系统中部署了360AISA全流量威胁分析系统和360本地安全大脑，通过将被测系统中全部流量镜像发送到360AISA全流量威胁分析系统及360本地安全大脑中进行分析监测，发现入侵事件后及时通过钉钉报警，并且能够自动阻断。 |
| 可信验证 | a）可基于可信根对计算设备的系统引导程序、系统程序、重要配置参数和应用程序等进行可信验证，并在应用程序的关键执行环节进行动态可信验证，在检测到其可信性受到破坏后进行报警，并将验证结果形成审计记录送至安全管理中心。 | 未基于可信根对计算设备提供可信验证。 |
| 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； | 经现场访谈网络管理员及对无线控制器AC配置，无线控制器AC中关闭Telnet协议，采用SSH协议进行通信，保证重要数据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。 | 经访谈网络管理员及核查H3C WX3010系列无线控制器AC产品文档，文件中目录05-参考指南--05文件系统管理命令中包含：“无线控制器AC中文件系统通常使用摘要算法（SHA-256）对文件计算摘要值，用于验证文件的正确性和完整性”。 |
| 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； | 经现场访谈网络管理员及对无线控制器AC配置，无线控制器AC中关闭Telnet协议，采用SSH协议进行通信，保证重要数据在传输过程中的保密性。 |
| b）应采用密码技术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个人信息等。 | 经访谈网管理员，管理员在设置用户口令时添加simple参数，经核查H3C WX3010系列无线控制器AC产品文档，在文档05-参考指南--03-登录设备命令--1、登录设备--1.1等设备命令--1.1.28 set authentication password中正对simple参数进行说明：“simple：以明文方式设置密码，该密码将以密文方式存储。 |
| 数据备份恢复 | a）应提供重要数据的本地数据备份与恢复功能； | 经现场访谈网络管理员及核查相应配置，管理员约每半年时间将无线控制器AC中配置策略进行一次备份，备份文件在本地存储。 |
| b）应提供异地实时备份功能，利用通信网络将重要数据实时备份至备份场地； | 经现场访谈网络管理员，无线控制器AC中备份文件仅本地保存，未提供实时异地备份。 |
| c）应提供重要数据处理系统的热冗余，保证系统的高可用性。 | 经访谈访问管理员及核查网络拓扑图，分拨中心无线AC采用单机部署，存在单点故障风险。 |

4.1.1.20. 无线控制器AC2

|  |  |  |
| --- | --- | --- |
| **安全控制点** | **测评指标** | **结果记录** |
| 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、经现场访谈网络管理员，无线控制器AC采用用户名、口令进行身份标识及身份鉴别；2、经核查无线控制器AC配置，输入display password-control命令，返回信息为 Password aging:Enabled (90 days) Password length: Enabled (10 characters) Password composition:Enabled (3 types, 1 characters per type) Password history: Enabled (max history records:4)，通过返回信息确认：用户口令长度为至少10位，包含数字、字母、字符三种类型，未定期更改用户口令；3、通过现场在无线控制器AC中创建与网络管理员同名账户时，无线控制器AC中会提示用户名已存在，无法创重名用户，确认用户标识具备唯一性。 |
| 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、经现场核查无线控制器AC配置策略，输入display password-control命令，返回信息为 Maximum login attempts: 3，Action for exceeding login attempts: Lock user for 1 minutes、User authentication timeout：600 seconds；2、通过返回信息确认用户连续错误登录3次锁定账户1分钟，用户登录连接超时时间限制为600秒。 |
| 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； | 1、经现场访谈网络管理员及核查其远程连接无线控制器AC的方式，管理员在远程管理无线控制器AC时采用SSH协议进行通信，防止鉴别信息在网络传输过程中被窃听；2、访谈网络管理员，Telnet协议默认为关闭状态，通过输入命令telnet server enable尝试启用Telnet协议，返回信息为Telnet is insecure because it transmits data in plaintext form，Telnet协议未启成功；3，通过在终端Telnet该无线控制器AC，无法连接成功。 |
| 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。 | 经现场核查网络管理员远程登录无线控制器AC方式，无线控制器AC仅采用用户名、口令方式进行身份鉴别，未采用两种或两种以上组合的鉴别技术对用户进行身份鉴别。 |
| 访问控制 | a）应对登录的用户分配账户和权限； | 1、经现场核查无线控制器AC中用户信息，通过输入display local-user命令，返回信息中显示无线控制器AC中存在场站管理员、网络管理员两个用户，该用户均分配超管权限。 |
| b）应重命名或删除默认账户，修改默认账户的默认口令； | 1、经现场核查无线控制器AC中用户信息，通过输入display local-user命令，返回信息中显示无线控制器AC中存在场站管理员、网络管理员两个账户,不存在默认账户，2、经核查无线控制器AC配置，输入display password-control命令，返回信息为 Password aging:Enabled (90 days) Password length: Enabled (10 characters) Password composition:Enabled (3 types, 1 characters per type) Password history: Enabled (max history records：3，用户口令已按照复杂度策略更改。 |
| 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； | 经现场核查无线控制器AC中用户信息，通过输入display local-user命令，返回信息中显示无线控制器AC中存在场站管理员、网络管理员等用户,经访谈网络管理员，账户与管理员一一对应，不存在多余、过期、共享账户。 |
| 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； | 经现场核查无线控制器AC中用户信息，通过输入display local-user命令，返回信息中显示无线控制器AC中存在场站管理员、网络管理员等用户,经访谈网络管理员，场站管理员、网络管理员均分配超级管理员权限，未按照权限最小化原则赋予管理用户权限及实现权限分离。 |
| e）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； | 经核查配置文件及访谈网络管理员，无线控制器AC由网络管理员角色账户为管理用户配置相应账号，并按照用户角色级别赋予管理用户操作权限。 |
| f）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； | 经核查配置文件及访谈网络管理员，无线控制器AC访问控制策略为管理用户的无线控制器AC配置文件等进行配置管理及访问管理等，访问控制粒度达到主体为用户级、客体为文件级。 |
| g）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。 | 经核查配置文件及访谈网络管理员，无线控制器AC未对重要主体和客体设置安全标记。 |
| 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； | 经现场访谈网络管理员及核查无线控制器AC配置，输入命令display logbuffer reverse，返回信息为logbuffer:enable；确认无线控制器AC中其中安全审计功能，通过查看审计记录内容，确认审计记录中包含设备运行记录及用户操作行为审计记录等。 |
| 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； | 经现场核查无线控制器AC中审计记录内容，审计记录中包含：日期、时间、主机名、类型、IP地址、用户名、详情等。 |
| 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、经访谈网络管理员，无线控制器AC中所有用户均无权限对审计记录进行删除或修改；2、经现场核查，管理员配置了审计记录备份策略，实时将无线控制器AC中审计记录上传至备份服务器中进行备份；2、经现场核查备份服务器中/home/network\_backup目录中存在审计记录备份文件，备份文件宿主为root，权限为744，其他用户仅拥有读权限。 |
| d）应对审计进程进行保护，防止未经授权的中断。 | 经现场访谈网络管理员，无线控制器AC中审计进程受系统进程保护，所有用户均无权限将审计进程单独中断。 |
| 入侵防范 | a）应遵循最小安装的原则，仅安装需要的组件和应用程序； | 经访谈网络管理员及核查配置文件，无线控制器AC为厂商提供独立封装系统，不允许安装其他组件及应用程序，遵循最小安装原则。 |
| b）应关闭不需要的系统服务、默认共享和高危端口； | 经现场访谈网络管理员及核查无线控制器AC配置，输入display current-fonfiguration，返回信息HTTP、Telnet协议均已关闭，无线控制器AC中未启用不需要的系统服务、默认共享及高危端口。 |
| c）应通过设定终端接入方式或网络地址范围对通过网络进行管理的管理终端进行限制； | 经访谈网络管理员，在防火墙中添加访问控制策略，仅允许管理用户通过堡垒机远程管理网络设备、安全设备及服务器等，经核查防火墙中访问控制策略，具备堡垒机地址-设备管理网段（10.33.0.0）的访问控制策略。 |
| d）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； | 该测评项测评对象为业务应用系统、中间件和系统管理软件，故将该项调整为不适用。 |
| e）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； | 1、经访谈网络管理员，会定期对官方网站通报的安全漏洞进行评估，然后从官方网站下载安全补丁，经过综合评估测试后对无线控制器AC系统进行补丁修复，避免系统中存在安全漏洞，2、经现场漏洞扫描，未发现无线控制器AC中存在安全漏洞。 |
| f）应能够检测到对重要节点进行入侵的行为，并在发生严重入侵事件时提供报警。 | 经访谈网络管理员，被测系统中部署了360AISA全流量威胁分析系统和360本地安全大脑，通过将被测系统中全部流量镜像发送到360AISA全流量威胁分析系统及360本地安全大脑中进行分析监测，发现入侵事件后及时通过钉钉报警，并且能够自动阻断。 |
| 可信验证 | a）可基于可信根对计算设备的系统引导程序、系统程序、重要配置参数和应用程序等进行可信验证，并在应用程序的关键执行环节进行动态可信验证，在检测到其可信性受到破坏后进行报警，并将验证结果形成审计记录送至安全管理中心。 | 未基于可信根对计算设备提供可信验证。 |
| 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； | 经现场访谈网络管理员及对无线控制器AC配置，无线控制器AC中关闭Telnet协议，采用SSH协议进行通信，保证重要数据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。 | 经访谈网络管理员及核查H3C WX3010系列无线控制器AC产品文档，文件中目录05-参考指南--05文件系统管理命令中包含：“无线控制器AC中文件系统通常使用摘要算法（SHA-256）对文件计算摘要值，用于验证文件的正确性和完整性”。 |
| 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； | 经现场访谈网络管理员及对无线控制器AC配置，无线控制器AC中关闭Telnet协议，采用SSH协议进行通信，保证重要数据在传输过程中的保密性。 |
| b）应采用密码技术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个人信息等。 | 经访谈网管理员，管理员在设置用户口令时添加simple参数，经核查H3C WX3010系列无线控制器AC产品文档，在文档05-参考指南--03-登录设备命令--1、登录设备--1.1等设备命令--1.1.28 set authentication password中正对simple参数进行说明：“simple：以明文方式设置密码，该密码将以密文方式存储。 |
| 数据备份恢复 | a）应提供重要数据的本地数据备份与恢复功能； | 经现场访谈网络管理员及核查相应配置，管理员约每半年时间将无线控制器AC中配置策略进行一次备份，备份文件在本地存储。 |
| b）应提供异地实时备份功能，利用通信网络将重要数据实时备份至备份场地； | 经现场访谈网络管理员，无线控制器AC中备份文件仅本地保存，未提供实时异地备份。 |
| c）应提供重要数据处理系统的热冗余，保证系统的高可用性。 | 经访谈访问管理员及核查网络拓扑图，分拨中心无线AC采用单机部署，存在单点故障风险。 |

4.1.1.21. 无线控制器AC3

|  |  |  |
| --- | --- | --- |
| **安全控制点** | **测评指标** | **结果记录** |
| 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、经现场访谈网络管理员，无线控制器AC采用用户名、口令进行身份标识及身份鉴别；2、经核查无线控制器AC配置，输入display password-control命令，返回信息为 Password aging:Enabled (90 days) Password length: Enabled (10 characters) Password composition:Enabled (3 types, 1 characters per type) Password history: Enabled (max history records:4)，通过返回信息确认：用户口令长度为至少10位，包含数字、字母、字符三种类型，未定期更改用户口令；3、通过现场在无线控制器AC中创建与网络管理员同名账户时，无线控制器AC中会提示用户名已存在，无法创重名用户，确认用户标识具备唯一性。 |
| 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、经现场核查无线控制器AC配置策略，输入display password-control命令，返回信息为 Maximum login attempts: 3，Action for exceeding login attempts: Lock user for 1 minutes、User authentication timeout：600 seconds；2、通过返回信息确认用户连续错误登录3次锁定账户1分钟，用户登录连接超时时间限制为600秒。 |
| 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； | 1、经现场访谈网络管理员及核查其远程连接无线控制器AC的方式，管理员在远程管理无线控制器AC时采用SSH协议进行通信，防止鉴别信息在网络传输过程中被窃听；2、访谈网络管理员，Telnet协议默认为关闭状态，通过输入命令telnet server enable尝试启用Telnet协议，返回信息为Telnet is insecure because it transmits data in plaintext form，Telnet协议未启成功；3，通过在终端Telnet该无线控制器AC，无法连接成功。 |
| 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。 | 经现场核查网络管理员远程登录无线控制器AC方式，无线控制器AC仅采用用户名、口令方式进行身份鉴别，未采用两种或两种以上组合的鉴别技术对用户进行身份鉴别。 |
| 访问控制 | a）应对登录的用户分配账户和权限； | 1、经现场核查无线控制器AC中用户信息，通过输入display local-user命令，返回信息中显示无线控制器AC中存在场站管理员、网络管理员两个用户，该用户均分配超管权限。 |
| b）应重命名或删除默认账户，修改默认账户的默认口令； | 1、经现场核查无线控制器AC中用户信息，通过输入display local-user命令，返回信息中显示无线控制器AC中存在场站管理员、网络管理员两个账户,不存在默认账户，2、经核查无线控制器AC配置，输入display password-control命令，返回信息为 Password aging:Enabled (90 days) Password length: Enabled (10 characters) Password composition:Enabled (3 types, 1 characters per type) Password history: Enabled (max history records：3，用户口令已按照复杂度策略更改。 |
| 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； | 经现场核查无线控制器AC中用户信息，通过输入display local-user命令，返回信息中显示无线控制器AC中存在场站管理员、网络管理员等用户,经访谈网络管理员，账户与管理员一一对应，不存在多余、过期、共享账户。 |
| 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； | 经现场核查无线控制器AC中用户信息，通过输入display local-user命令，返回信息中显示无线控制器AC中存在场站管理员、网络管理员等用户,经访谈网络管理员，场站管理员、网络管理员均分配超级管理员权限，未按照权限最小化原则赋予管理用户权限及实现权限分离。 |
| e）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； | 经核查配置文件及访谈网络管理员，无线控制器AC由网络管理员角色账户为管理用户配置相应账号，并按照用户角色级别赋予管理用户操作权限。 |
| f）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； | 经核查配置文件及访谈网络管理员，无线控制器AC访问控制策略为管理用户的无线控制器AC配置文件等进行配置管理及访问管理等，访问控制粒度达到主体为用户级、客体为文件级。 |
| g）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。 | 经核查配置文件及访谈网络管理员，无线控制器AC未对重要主体和客体设置安全标记。 |
| 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； | 经现场访谈网络管理员及核查无线控制器AC配置，输入命令display logbuffer reverse，返回信息为logbuffer:enable；确认无线控制器AC中其中安全审计功能，通过查看审计记录内容，确认审计记录中包含设备运行记录及用户操作行为审计记录等。 |
| 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； | 经现场核查无线控制器AC中审计记录内容，审计记录中包含：日期、时间、主机名、类型、IP地址、用户名、详情等。 |
| 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、经访谈网络管理员，无线控制器AC中所有用户均无权限对审计记录进行删除或修改；2、经现场核查，管理员配置了审计记录备份策略，实时将无线控制器AC中审计记录上传至备份服务器中进行备份；2、经现场核查备份服务器中/home/network\_backup目录中存在审计记录备份文件，备份文件宿主为root，权限为744，其他用户仅拥有读权限。 |
| d）应对审计进程进行保护，防止未经授权的中断。 | 经现场访谈网络管理员，无线控制器AC中审计进程受系统进程保护，所有用户均无权限将审计进程单独中断。 |
| 入侵防范 | a）应遵循最小安装的原则，仅安装需要的组件和应用程序； | 经访谈网络管理员及核查配置文件，无线控制器AC为厂商提供独立封装系统，不允许安装其他组件及应用程序，遵循最小安装原则。 |
| b）应关闭不需要的系统服务、默认共享和高危端口； | 经现场访谈网络管理员及核查无线控制器AC配置，输入display current-fonfiguration，返回信息HTTP、Telnet协议均已关闭，无线控制器AC中未启用不需要的系统服务、默认共享及高危端口。 |
| c）应通过设定终端接入方式或网络地址范围对通过网络进行管理的管理终端进行限制； | 经访谈网络管理员，在防火墙中添加访问控制策略，仅允许管理用户通过堡垒机远程管理网络设备、安全设备及服务器等，经核查防火墙中访问控制策略，具备堡垒机地址-设备管理网段（10.33.0.0）的访问控制策略。 |
| d）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； | 该测评项测评对象为业务应用系统、中间件和系统管理软件，故将该项调整为不适用。 |
| e）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； | 1、经访谈网络管理员，会定期对官方网站通报的安全漏洞进行评估，然后从官方网站下载安全补丁，经过综合评估测试后对无线控制器AC系统进行补丁修复，避免系统中存在安全漏洞，2、经现场漏洞扫描，未发现无线控制器AC中存在安全漏洞。 |
| f）应能够检测到对重要节点进行入侵的行为，并在发生严重入侵事件时提供报警。 | 经访谈网络管理员，被测系统中部署了360AISA全流量威胁分析系统和360本地安全大脑，通过将被测系统中全部流量镜像发送到360AISA全流量威胁分析系统及360本地安全大脑中进行分析监测，发现入侵事件后及时通过钉钉报警，并且能够自动阻断。 |
| 可信验证 | a）可基于可信根对计算设备的系统引导程序、系统程序、重要配置参数和应用程序等进行可信验证，并在应用程序的关键执行环节进行动态可信验证，在检测到其可信性受到破坏后进行报警，并将验证结果形成审计记录送至安全管理中心。 | 未基于可信根对计算设备提供可信验证。 |
| 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； | 经现场访谈网络管理员及对无线控制器AC配置，无线控制器AC中关闭Telnet协议，采用SSH协议进行通信，保证重要数据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。 | 经访谈网络管理员及核查H3C WX3010系列无线控制器AC产品文档，文件中目录05-参考指南--05文件系统管理命令中包含：“无线控制器AC中文件系统通常使用摘要算法（SHA-256）对文件计算摘要值，用于验证文件的正确性和完整性”。 |
| 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； | 经现场访谈网络管理员及对无线控制器AC配置，无线控制器AC中关闭Telnet协议，采用SSH协议进行通信，保证重要数据在传输过程中的保密性。 |
| b）应采用密码技术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个人信息等。 | 经访谈网管理员，管理员在设置用户口令时添加simple参数，经核查H3C WX3010系列无线控制器AC产品文档，在文档05-参考指南--03-登录设备命令--1、登录设备--1.1等设备命令--1.1.28 set authentication password中正对simple参数进行说明：“simple：以明文方式设置密码，该密码将以密文方式存储。 |
| 数据备份恢复 | a）应提供重要数据的本地数据备份与恢复功能； | 经现场访谈网络管理员及核查相应配置，管理员约每半年时间将无线控制器AC中配置策略进行一次备份，备份文件在本地存储。 |
| b）应提供异地实时备份功能，利用通信网络将重要数据实时备份至备份场地； | 经现场访谈网络管理员，无线控制器AC中备份文件仅本地保存，未提供实时异地备份。 |
| c）应提供重要数据处理系统的热冗余，保证系统的高可用性。 | 经访谈访问管理员及核查网络拓扑图，分拨中心无线AC采用单机部署，存在单点故障风险。 |

4.1.1.22. 无线控制器AC4

|  |  |  |
| --- | --- | --- |
| **安全控制点** | **测评指标** | **结果记录** |
| 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、经现场访谈网络管理员，无线控制器AC采用用户名、口令进行身份标识及身份鉴别；2、经核查无线控制器AC配置，输入display password-control命令，返回信息为 Password aging:Enabled (90 days) Password length: Enabled (10 characters) Password composition:Enabled (3 types, 1 characters per type) Password history: Enabled (max history records:4)，通过返回信息确认：用户口令长度为至少10位，包含数字、字母、字符三种类型，未定期更改用户口令；3、通过现场在无线控制器AC中创建与网络管理员同名账户时，无线控制器AC中会提示用户名已存在，无法创重名用户，确认用户标识具备唯一性。 |
| 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、经现场核查无线控制器AC配置策略，输入display password-control命令，返回信息为 Maximum login attempts: 3，Action for exceeding login attempts: Lock user for 1 minutes、User authentication timeout：600 seconds；2、通过返回信息确认用户连续错误登录3次锁定账户1分钟，用户登录连接超时时间限制为600秒。 |
| 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； | 1、经现场访谈网络管理员及核查其远程连接无线控制器AC的方式，管理员在远程管理无线控制器AC时采用SSH协议进行通信，防止鉴别信息在网络传输过程中被窃听；2、访谈网络管理员，Telnet协议默认为关闭状态，通过输入命令telnet server enable尝试启用Telnet协议，返回信息为Telnet is insecure because it transmits data in plaintext form，Telnet协议未启成功；3，通过在终端Telnet该无线控制器AC，无法连接成功。 |
| 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。 | 经现场核查网络管理员远程登录无线控制器AC方式，无线控制器AC仅采用用户名、口令方式进行身份鉴别，未采用两种或两种以上组合的鉴别技术对用户进行身份鉴别。 |
| 访问控制 | a）应对登录的用户分配账户和权限； | 1、经现场核查无线控制器AC中用户信息，通过输入display local-user命令，返回信息中显示无线控制器AC中存在场站管理员、网络管理员两个用户，该用户均分配超管权限。 |
| b）应重命名或删除默认账户，修改默认账户的默认口令； | 1、经现场核查无线控制器AC中用户信息，通过输入display local-user命令，返回信息中显示无线控制器AC中存在场站管理员、网络管理员两个账户,不存在默认账户，2、经核查无线控制器AC配置，输入display password-control命令，返回信息为 Password aging:Enabled (90 days) Password length: Enabled (10 characters) Password composition:Enabled (3 types, 1 characters per type) Password history: Enabled (max history records：3，用户口令已按照复杂度策略更改。 |
| 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； | 经现场核查无线控制器AC中用户信息，通过输入display local-user命令，返回信息中显示无线控制器AC中存在场站管理员、网络管理员等用户,经访谈网络管理员，账户与管理员一一对应，不存在多余、过期、共享账户。 |
| 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； | 经现场核查无线控制器AC中用户信息，通过输入display local-user命令，返回信息中显示无线控制器AC中存在场站管理员、网络管理员等用户,经访谈网络管理员，场站管理员、网络管理员均分配超级管理员权限，未按照权限最小化原则赋予管理用户权限及实现权限分离。 |
| e）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； | 经核查配置文件及访谈网络管理员，无线控制器AC由网络管理员角色账户为管理用户配置相应账号，并按照用户角色级别赋予管理用户操作权限。 |
| f）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； | 经核查配置文件及访谈网络管理员，无线控制器AC访问控制策略为管理用户的无线控制器AC配置文件等进行配置管理及访问管理等，访问控制粒度达到主体为用户级、客体为文件级。 |
| g）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。 | 经核查配置文件及访谈网络管理员，无线控制器AC未对重要主体和客体设置安全标记。 |
| 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； | 经现场访谈网络管理员及核查无线控制器AC配置，输入命令display logbuffer reverse，返回信息为logbuffer:enable；确认无线控制器AC中其中安全审计功能，通过查看审计记录内容，确认审计记录中包含设备运行记录及用户操作行为审计记录等。 |
| 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； | 经现场核查无线控制器AC中审计记录内容，审计记录中包含：日期、时间、主机名、类型、IP地址、用户名、详情等。 |
| 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、经访谈网络管理员，无线控制器AC中所有用户均无权限对审计记录进行删除或修改；2、经现场核查，管理员配置了审计记录备份策略，实时将无线控制器AC中审计记录上传至备份服务器中进行备份；2、经现场核查备份服务器中/home/network\_backup目录中存在审计记录备份文件，备份文件宿主为root，权限为744，其他用户仅拥有读权限。 |
| d）应对审计进程进行保护，防止未经授权的中断。 | 经现场访谈网络管理员，无线控制器AC中审计进程受系统进程保护，所有用户均无权限将审计进程单独中断。 |
| 入侵防范 | a）应遵循最小安装的原则，仅安装需要的组件和应用程序； | 经访谈网络管理员及核查配置文件，无线控制器AC为厂商提供独立封装系统，不允许安装其他组件及应用程序，遵循最小安装原则。 |
| b）应关闭不需要的系统服务、默认共享和高危端口； | 经现场访谈网络管理员及核查无线控制器AC配置，输入display current-fonfiguration，返回信息HTTP、Telnet协议均已关闭，无线控制器AC中未启用不需要的系统服务、默认共享及高危端口。 |
| c）应通过设定终端接入方式或网络地址范围对通过网络进行管理的管理终端进行限制； | 经访谈网络管理员，在防火墙中添加访问控制策略，仅允许管理用户通过堡垒机远程管理网络设备、安全设备及服务器等，经核查防火墙中访问控制策略，具备堡垒机地址-设备管理网段（10.33.0.0）的访问控制策略。 |
| d）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； | 该测评项测评对象为业务应用系统、中间件和系统管理软件，故将该项调整为不适用。 |
| e）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； | 1、经访谈网络管理员，会定期对官方网站通报的安全漏洞进行评估，然后从官方网站下载安全补丁，经过综合评估测试后对无线控制器AC系统进行补丁修复，避免系统中存在安全漏洞，2、经现场漏洞扫描，未发现无线控制器AC中存在安全漏洞。 |
| f）应能够检测到对重要节点进行入侵的行为，并在发生严重入侵事件时提供报警。 | 经访谈网络管理员，被测系统中部署了360AISA全流量威胁分析系统和360本地安全大脑，通过将被测系统中全部流量镜像发送到360AISA全流量威胁分析系统及360本地安全大脑中进行分析监测，发现入侵事件后及时通过钉钉报警，并且能够自动阻断。 |
| 可信验证 | a）可基于可信根对计算设备的系统引导程序、系统程序、重要配置参数和应用程序等进行可信验证，并在应用程序的关键执行环节进行动态可信验证，在检测到其可信性受到破坏后进行报警，并将验证结果形成审计记录送至安全管理中心。 | 未基于可信根对计算设备提供可信验证。 |
| 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； | 经现场访谈网络管理员及对无线控制器AC配置，无线控制器AC中关闭Telnet协议，采用SSH协议进行通信，保证重要数据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。 | 经访谈网络管理员及核查H3C WX3010系列无线控制器AC产品文档，文件中目录05-参考指南--05文件系统管理命令中包含：“无线控制器AC中文件系统通常使用摘要算法（SHA-256）对文件计算摘要值，用于验证文件的正确性和完整性”。 |
| 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； | 经现场访谈网络管理员及对无线控制器AC配置，无线控制器AC中关闭Telnet协议，采用SSH协议进行通信，保证重要数据在传输过程中的保密性。 |
| b）应采用密码技术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个人信息等。 | 经访谈网管理员，管理员在设置用户口令时添加simple参数，经核查H3C WX3010系列无线控制器AC产品文档，在文档05-参考指南--03-登录设备命令--1、登录设备--1.1等设备命令--1.1.28 set authentication password中正对simple参数进行说明：“simple：以明文方式设置密码，该密码将以密文方式存储。 |
| 数据备份恢复 | a）应提供重要数据的本地数据备份与恢复功能； | 经现场访谈网络管理员及核查相应配置，管理员约每半年时间将无线控制器AC中配置策略进行一次备份，备份文件在本地存储。 |
| b）应提供异地实时备份功能，利用通信网络将重要数据实时备份至备份场地； | 经现场访谈网络管理员，无线控制器AC中备份文件仅本地保存，未提供实时异地备份。 |
| c）应提供重要数据处理系统的热冗余，保证系统的高可用性。 | 经访谈访问管理员及核查网络拓扑图，分拨中心无线AC采用单机部署，存在单点故障风险。 |

4.1.1.23. 无线控制器AC5

|  |  |  |
| --- | --- | --- |
| **安全控制点** | **测评指标** | **结果记录** |
| 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、经现场访谈网络管理员，无线控制器AC采用用户名、口令进行身份标识及身份鉴别；2、经核查无线控制器AC配置，输入display password-control命令，返回信息为 Password aging:Enabled (90 days) Password length: Enabled (10 characters) Password composition:Enabled (3 types, 1 characters per type) Password history: Enabled (max history records:4)，通过返回信息确认：用户口令长度为至少10位，包含数字、字母、字符三种类型，未定期更改用户口令；3、通过现场在无线控制器AC中创建与网络管理员同名账户时，无线控制器AC中会提示用户名已存在，无法创重名用户，确认用户标识具备唯一性。 |
| 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、经现场核查无线控制器AC配置策略，输入display password-control命令，返回信息为 Maximum login attempts: 3，Action for exceeding login attempts: Lock user for 1 minutes、User authentication timeout：600 seconds；2、通过返回信息确认用户连续错误登录3次锁定账户1分钟，用户登录连接超时时间限制为600秒。 |
| 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； | 1、经现场访谈网络管理员及核查其远程连接无线控制器AC的方式，管理员在远程管理无线控制器AC时采用SSH协议进行通信，防止鉴别信息在网络传输过程中被窃听；2、访谈网络管理员，Telnet协议默认为关闭状态，通过输入命令telnet server enable尝试启用Telnet协议，返回信息为Telnet is insecure because it transmits data in plaintext form，Telnet协议未启成功；3，通过在终端Telnet该无线控制器AC，无法连接成功。 |
| 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。 | 经现场核查网络管理员远程登录无线控制器AC方式，无线控制器AC仅采用用户名、口令方式进行身份鉴别，未采用两种或两种以上组合的鉴别技术对用户进行身份鉴别。 |
| 访问控制 | a）应对登录的用户分配账户和权限； | 1、经现场核查无线控制器AC中用户信息，通过输入display local-user命令，返回信息中显示无线控制器AC中存在场站管理员、网络管理员两个用户，该用户均分配超管权限。 |
| b）应重命名或删除默认账户，修改默认账户的默认口令； | 1、经现场核查无线控制器AC中用户信息，通过输入display local-user命令，返回信息中显示无线控制器AC中存在场站管理员、网络管理员两个账户,不存在默认账户，2、经核查无线控制器AC配置，输入display password-control命令，返回信息为 Password aging:Enabled (90 days) Password length: Enabled (10 characters) Password composition:Enabled (3 types, 1 characters per type) Password history: Enabled (max history records：3，用户口令已按照复杂度策略更改。 |
| 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； | 经现场核查无线控制器AC中用户信息，通过输入display local-user命令，返回信息中显示无线控制器AC中存在场站管理员、网络管理员等用户,经访谈网络管理员，账户与管理员一一对应，不存在多余、过期、共享账户。 |
| 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； | 经现场核查无线控制器AC中用户信息，通过输入display local-user命令，返回信息中显示无线控制器AC中存在场站管理员、网络管理员等用户,经访谈网络管理员，场站管理员、网络管理员均分配超级管理员权限，未按照权限最小化原则赋予管理用户权限及实现权限分离。 |
| e）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； | 经核查配置文件及访谈网络管理员，无线控制器AC由网络管理员角色账户为管理用户配置相应账号，并按照用户角色级别赋予管理用户操作权限。 |
| f）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； | 经核查配置文件及访谈网络管理员，无线控制器AC访问控制策略为管理用户的无线控制器AC配置文件等进行配置管理及访问管理等，访问控制粒度达到主体为用户级、客体为文件级。 |
| g）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。 | 经核查配置文件及访谈网络管理员，无线控制器AC未对重要主体和客体设置安全标记。 |
| 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； | 经现场访谈网络管理员及核查无线控制器AC配置，输入命令display logbuffer reverse，返回信息为logbuffer:enable；确认无线控制器AC中其中安全审计功能，通过查看审计记录内容，确认审计记录中包含设备运行记录及用户操作行为审计记录等。 |
| 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； | 经现场核查无线控制器AC中审计记录内容，审计记录中包含：日期、时间、主机名、类型、IP地址、用户名、详情等。 |
| 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、经访谈网络管理员，无线控制器AC中所有用户均无权限对审计记录进行删除或修改；2、经现场核查，管理员配置了审计记录备份策略，实时将无线控制器AC中审计记录上传至备份服务器中进行备份；2、经现场核查备份服务器中/home/network\_backup目录中存在审计记录备份文件，备份文件宿主为root，权限为744，其他用户仅拥有读权限。 |
| d）应对审计进程进行保护，防止未经授权的中断。 | 经现场访谈网络管理员，无线控制器AC中审计进程受系统进程保护，所有用户均无权限将审计进程单独中断。 |
| 入侵防范 | a）应遵循最小安装的原则，仅安装需要的组件和应用程序； | 经访谈网络管理员及核查配置文件，无线控制器AC为厂商提供独立封装系统，不允许安装其他组件及应用程序，遵循最小安装原则。 |
| b）应关闭不需要的系统服务、默认共享和高危端口； | 经现场访谈网络管理员及核查无线控制器AC配置，输入display current-fonfiguration，返回信息HTTP、Telnet协议均已关闭，无线控制器AC中未启用不需要的系统服务、默认共享及高危端口。 |
| c）应通过设定终端接入方式或网络地址范围对通过网络进行管理的管理终端进行限制； | 经访谈网络管理员，在防火墙中添加访问控制策略，仅允许管理用户通过堡垒机远程管理网络设备、安全设备及服务器等，经核查防火墙中访问控制策略，具备堡垒机地址-设备管理网段（10.33.0.0）的访问控制策略。 |
| d）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； | 该测评项测评对象为业务应用系统、中间件和系统管理软件，故将该项调整为不适用。 |
| e）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； | 1、经访谈网络管理员，会定期对官方网站通报的安全漏洞进行评估，然后从官方网站下载安全补丁，经过综合评估测试后对无线控制器AC系统进行补丁修复，避免系统中存在安全漏洞，2、经现场漏洞扫描，未发现无线控制器AC中存在安全漏洞。 |
| f）应能够检测到对重要节点进行入侵的行为，并在发生严重入侵事件时提供报警。 | 经访谈网络管理员，被测系统中部署了360AISA全流量威胁分析系统和360本地安全大脑，通过将被测系统中全部流量镜像发送到360AISA全流量威胁分析系统及360本地安全大脑中进行分析监测，发现入侵事件后及时通过钉钉报警，并且能够自动阻断。 |
| 可信验证 | a）可基于可信根对计算设备的系统引导程序、系统程序、重要配置参数和应用程序等进行可信验证，并在应用程序的关键执行环节进行动态可信验证，在检测到其可信性受到破坏后进行报警，并将验证结果形成审计记录送至安全管理中心。 | 未基于可信根对计算设备提供可信验证。 |
| 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； | 经现场访谈网络管理员及对无线控制器AC配置，无线控制器AC中关闭Telnet协议，采用SSH协议进行通信，保证重要数据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。 | 经访谈网络管理员及核查H3C WX3010系列无线控制器AC产品文档，文件中目录05-参考指南--05文件系统管理命令中包含：“无线控制器AC中文件系统通常使用摘要算法（SHA-256）对文件计算摘要值，用于验证文件的正确性和完整性”。 |
| 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； | 经现场访谈网络管理员及对无线控制器AC配置，无线控制器AC中关闭Telnet协议，采用SSH协议进行通信，保证重要数据在传输过程中的保密性。 |
| b）应采用密码技术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个人信息等。 | 经访谈网管理员，管理员在设置用户口令时添加simple参数，经核查H3C WX3010系列无线控制器AC产品文档，在文档05-参考指南--03-登录设备命令--1、登录设备--1.1等设备命令--1.1.28 set authentication password中正对simple参数进行说明：“simple：以明文方式设置密码，该密码将以密文方式存储。 |
| 数据备份恢复 | a）应提供重要数据的本地数据备份与恢复功能； | 经现场访谈网络管理员及核查相应配置，管理员约每半年时间将无线控制器AC中配置策略进行一次备份，备份文件在本地存储。 |
| b）应提供异地实时备份功能，利用通信网络将重要数据实时备份至备份场地； | 经现场访谈网络管理员，无线控制器AC中备份文件仅本地保存，未提供实时异地备份。 |
| c）应提供重要数据处理系统的热冗余，保证系统的高可用性。 | 经访谈访问管理员及核查网络拓扑图，分拨中心无线AC采用单机部署，存在单点故障风险。 |

4.1.1.24. 无线AP1

|  |  |  |
| --- | --- | --- |
| **安全控制点** | **测评指标** | **结果记录** |
| 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、经现场访谈网络管理员，无线AP采用用户名、口令进行身份标识及身份鉴别；2、经核查无线AP配置，输入display password-control命令，返回信息为 Password aging:Enabled (90 days) Password length: Enabled (10 characters) Password composition:Enabled (3 types, 1 characters per type) Password history: Enabled (max history records:4)，通过返回信息确认：用户口令长度为至少10位，包含数字、字母、字符三种类型，未定期更改用户口令；3、通过现场在无线AP中创建与网络管理员同名账户时，无线AP中会提示用户名已存在，无法创重名用户，确认用户标识具备唯一性。 |
| 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、经现场核查无线AP配置策略，输入display password-control命令，返回信息为 Maximum login attempts: 3，Action for exceeding login attempts: Lock user for 1 minutes、User authentication timeout：600 seconds；2、通过返回信息确认用户连续错误登录3次锁定账户1分钟，用户登录连接超时时间限制为600秒。 |
| 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； | 1、经现场访谈网络管理员及核查其远程连接无线AP的方式，管理员在远程管理无线AP时采用SSH协议进行通信，防止鉴别信息在网络传输过程中被窃听；2、访谈网络管理员，Telnet协议默认为关闭状态，通过输入命令telnet server enable尝试启用Telnet协议，返回信息为Telnet is insecure because it transmits data in plaintext form，Telnet协议未启成功；3，通过在终端Telnet该无线AP，无法连接成功。 |
| 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。 | 经现场核查网络管理员远程登录无线AP方式，无线AP仅采用用户名、口令方式进行身份鉴别，未采用两种或两种以上组合的鉴别技术对用户进行身份鉴别。 |
| 访问控制 | a）应对登录的用户分配账户和权限； | 1、经现场核查无线AP中用户信息，通过输入display local-user命令，返回信息中显示无线AP中存在场站管理员、网络管理员两个用户，该用户均分配超管权限。 |
| b）应重命名或删除默认账户，修改默认账户的默认口令； | 1、经现场核查无线AP中用户信息，通过输入display local-user命令，返回信息中显示无线AP中存在场站管理员、网络管理员两个账户,不存在默认账户，2、经核查无线AP配置，输入display password-control命令，返回信息为 Password aging:Enabled (90 days) Password length: Enabled (10 characters) Password composition:Enabled (3 types, 1 characters per type) Password history: Enabled (max history records：3，用户口令已按照复杂度策略更改。 |
| 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； | 经现场核查无线AP中用户信息，通过输入display local-user命令，返回信息中显示无线AP中存在场站管理员、网络管理员等用户,经访谈网络管理员，账户与管理员一一对应，不存在多余、过期、共享账户。 |
| 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； | 经现场核查无线AP中用户信息，通过输入display local-user命令，返回信息中显示无线AP中存在场站管理员、网络管理员等用户,经访谈网络管理员，场站管理员、网络管理员均分配超级管理员权限，未按照权限最小化原则赋予管理用户权限及实现权限分离。 |
| e）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； | 经核查配置文件及访谈网络管理员，无线AP中由网络管理员角色账户为管理用户配置相应账号，并按照用户角色级别赋予管理用户操作权限。 |
| f）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； | 经核查配置文件及访谈网络管理员，无线AP访问控制策略为管理用户的无线AP中配置文件等进行配置管理及访问管理等，访问控制粒度达到主体为用户级、客体为文件级。 |
| g）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。 | 经核查配置文件及访谈网络管理员，无线AP未对重要主体和客体设置安全标记。 |
| 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； | 经现场访谈网络管理员及核查无线AP配置，输入命令display logbuffer reverse，返回信息为logbuffer:enable；确认无线AP中其中安全审计功能，通过查看审计记录内容，确认审计记录中包含设备运行记录及用户操作行为审计记录等。 |
| 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； | 经现场核查无线AP中审计记录内容，审计记录中包含：日期、时间、主机名、类型、IP地址、用户名、详情等。 |
| 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、经访谈网络管理员，无线AP中所有用户均无权限对审计记录进行删除或修改；2、经现场核查，管理员配置了审计记录备份策略，实时将无线AP中审计记录上传至备份服务器中进行备份；2、经现场核查备份服务器中/home/network\_backup目录中存在审计记录备份文件，备份文件宿主为root，权限为744，其他用户仅拥有读权限。中/home/network\_backup目录中存在审计记录备份文件，备份文件宿主为root，权限为744，其他用户仅拥有读权限。 |
| d）应对审计进程进行保护，防止未经授权的中断。 | 经现场访谈网络管理员，无线AP中审计进程受系统进程保护，所有用户均无权限将审计进程单独中断。 |
| 入侵防范 | a）应遵循最小安装的原则，仅安装需要的组件和应用程序； | 经访谈网络管理员及核查配置文件，无线AP系统为厂商提供独立封装系统，不允许安装其他组件及应用程序，遵循最小安装原则。 |
| b）应关闭不需要的系统服务、默认共享和高危端口； | 经现场访谈网络管理员及核查无线AP配置，输入display current-fonfiguration，返回信息HTTP、Telnet协议均已关闭，无线AP中未启用不需要的系统服务、默认共享及高危端口。 |
| c）应通过设定终端接入方式或网络地址范围对通过网络进行管理的管理终端进行限制； | 经访谈网络管理员，在防火墙中添加访问控制策略，仅允许管理用户通过堡垒机远程管理网络设备、安全设备及服务器等，经核查防火墙中访问控制策略，具备堡垒机地址-设备管理网段（10.33.0.0）的访问控制策略。 |
| d）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； | 该测评项测评对象为业务应用系统、中间件和系统管理软件，故将该项调整为不适用。 |
| e）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； | 1、经访谈网络管理员，会定期对官方网站通报的安全漏洞进行评估，然后从官方网站下载安全补丁，经过综合评估测试后对无线AP系统进行补丁修复，避免系统中存在安全漏洞，2、经现场漏洞扫描，未发现无线AP中存在安全漏洞。 |
| f）应能够检测到对重要节点进行入侵的行为，并在发生严重入侵事件时提供报警。 | 经访谈网络管理员，被测系统中部署了360AISA全流量威胁分析系统和360本地安全大脑，通过将被测系统中全部流量镜像发送到360AISA全流量威胁分析系统及360本地安全大脑中进行分析监测，发现入侵事件后及时通过钉钉报警，并且能够自动阻断。 |
| 可信验证 | a）可基于可信根对计算设备的系统引导程序、系统程序、重要配置参数和应用程序等进行可信验证，并在应用程序的关键执行环节进行动态可信验证，在检测到其可信性受到破坏后进行报警，并将验证结果形成审计记录送至安全管理中心。 | 未基于可信根对计算设备提供可信验证。 |
| 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； | 经现场访谈网络管理员及对无线AP配置，无线AP中关闭Telnet协议，采用SSH协议进行通信，保证重要数据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。 | 经访谈网络管理员及核查H3C WX3010系列无线AP产品文档，文件中目录05-参考指南--05文件系统管理命令中包含：“无线AP中文件系统通常使用摘要算法（SHA-256）对文件计算摘要值，用于验证文件的正确性和完整性”。 |
| 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； | 经现场访谈网络管理员及对无线AP配置，无线AP中关闭Telnet协议，采用SSH协议进行通信，保证重要数据在传输过程中的保密性。 |
| b）应采用密码技术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个人信息等。 | 经访谈网管理员，管理员在设置用户口令时添加simple参数，经核查H3C WX3010系列无线AP产品文档，在文档05-参考指南--03-登录设备命令--1、登录设备--1.1等设备命令--1.1.28 set authentication password中正对simple参数进行说明：“simple：以明文方式设置密码，该密码将以密文方式存储。 |
| 数据备份恢复 | a）应提供重要数据的本地数据备份与恢复功能； | 经现场访谈网络管理员及核查相应配置，管理员约每半年时间将无线AP中配置策略进行一次备份，备份文件在本地存储。 |
| b）应提供异地实时备份功能，利用通信网络将重要数据实时备份至备份场地； | 经现场访谈网络管理员，无线AP中备份文件仅本地保存，未提供实时异地备份。 |
| c）应提供重要数据处理系统的热冗余，保证系统的高可用性。 | 经访谈访问管理员及核查网络拓扑图，重要数据处理系统中采用双机冗余部署，保证系统的高可用性。 |

4.1.1.25. 无线AP2

|  |  |  |
| --- | --- | --- |
| **安全控制点** | **测评指标** | **结果记录** |
| 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、经现场访谈网络管理员，无线AP采用用户名、口令进行身份标识及身份鉴别；2、经核查无线AP配置，输入display password-control命令，返回信息为 Password aging:Enabled (90 days) Password length: Enabled (10 characters) Password composition:Enabled (3 types, 1 characters per type) Password history: Enabled (max history records:4)，通过返回信息确认：用户口令长度为至少10位，包含数字、字母、字符三种类型，未定期更改用户口令；3、通过现场在无线AP中创建与网络管理员同名账户时，无线AP中会提示用户名已存在，无法创重名用户，确认用户标识具备唯一性。 |
| 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、经现场核查无线AP配置策略，输入display password-control命令，返回信息为 Maximum login attempts: 3，Action for exceeding login attempts: Lock user for 1 minutes、User authentication timeout：600 seconds；2、通过返回信息确认用户连续错误登录3次锁定账户1分钟，用户登录连接超时时间限制为600秒。 |
| 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； | 1、经现场访谈网络管理员及核查其远程连接无线AP的方式，管理员在远程管理无线AP时采用SSH协议进行通信，防止鉴别信息在网络传输过程中被窃听；2、访谈网络管理员，Telnet协议默认为关闭状态，通过输入命令telnet server enable尝试启用Telnet协议，返回信息为Telnet is insecure because it transmits data in plaintext form，Telnet协议未启成功；3，通过在终端Telnet该无线AP，无法连接成功。 |
| 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。 | 经现场核查网络管理员远程登录无线AP方式，无线AP仅采用用户名、口令方式进行身份鉴别，未采用两种或两种以上组合的鉴别技术对用户进行身份鉴别。 |
| 访问控制 | a）应对登录的用户分配账户和权限； | 1、经现场核查无线AP中用户信息，通过输入display local-user命令，返回信息中显示无线AP中存在场站管理员、网络管理员两个用户，该用户均分配超管权限。 |
| b）应重命名或删除默认账户，修改默认账户的默认口令； | 1、经现场核查无线AP中用户信息，通过输入display local-user命令，返回信息中显示无线AP中存在场站管理员、网络管理员两个账户,不存在默认账户，2、经核查无线AP配置，输入display password-control命令，返回信息为 Password aging:Enabled (90 days) Password length: Enabled (10 characters) Password composition:Enabled (3 types, 1 characters per type) Password history: Enabled (max history records：3，用户口令已按照复杂度策略更改。 |
| 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； | 经现场核查无线AP中用户信息，通过输入display local-user命令，返回信息中显示无线AP中存在场站管理员、网络管理员等用户,经访谈网络管理员，账户与管理员一一对应，不存在多余、过期、共享账户。 |
| 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； | 经现场核查无线AP中用户信息，通过输入display local-user命令，返回信息中显示无线AP中存在场站管理员、网络管理员等用户,经访谈网络管理员，场站管理员、网络管理员均分配超级管理员权限，未按照权限最小化原则赋予管理用户权限及实现权限分离。 |
| e）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； | 经核查配置文件及访谈网络管理员，无线AP中由网络管理员角色账户为管理用户配置相应账号，并按照用户角色级别赋予管理用户操作权限。 |
| f）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； | 经核查配置文件及访谈网络管理员，无线AP访问控制策略为管理用户的无线AP中配置文件等进行配置管理及访问管理等，访问控制粒度达到主体为用户级、客体为文件级。 |
| g）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。 | 经核查配置文件及访谈网络管理员，无线AP未对重要主体和客体设置安全标记。 |
| 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； | 经现场访谈网络管理员及核查无线AP配置，输入命令display logbuffer reverse，返回信息为logbuffer:enable；确认无线AP中其中安全审计功能，通过查看审计记录内容，确认审计记录中包含设备运行记录及用户操作行为审计记录等。 |
| 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； | 经现场核查无线AP中审计记录内容，审计记录中包含：日期、时间、主机名、类型、IP地址、用户名、详情等。 |
| 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、经访谈网络管理员，无线AP中所有用户均无权限对审计记录进行删除或修改；2、经现场核查，管理员配置了审计记录备份策略，实时将无线AP中审计记录上传至备份服务器中进行备份；2、经现场核查备份服务器中/home/network\_backup目录中存在审计记录备份文件，备份文件宿主为root，权限为744，其他用户仅拥有读权限。中/home/network\_backup目录中存在审计记录备份文件，备份文件宿主为root，权限为744，其他用户仅拥有读权限。 |
| d）应对审计进程进行保护，防止未经授权的中断。 | 经现场访谈网络管理员，无线AP中审计进程受系统进程保护，所有用户均无权限将审计进程单独中断。 |
| 入侵防范 | a）应遵循最小安装的原则，仅安装需要的组件和应用程序； | 经访谈网络管理员及核查配置文件，无线AP系统为厂商提供独立封装系统，不允许安装其他组件及应用程序，遵循最小安装原则。 |
| b）应关闭不需要的系统服务、默认共享和高危端口； | 经现场访谈网络管理员及核查无线AP配置，输入display current-fonfiguration，返回信息HTTP、Telnet协议均已关闭，无线AP中未启用不需要的系统服务、默认共享及高危端口。 |
| c）应通过设定终端接入方式或网络地址范围对通过网络进行管理的管理终端进行限制； | 经访谈网络管理员，在防火墙中添加访问控制策略，仅允许管理用户通过堡垒机远程管理网络设备、安全设备及服务器等，经核查防火墙中访问控制策略，具备堡垒机地址-设备管理网段（10.33.0.0）的访问控制策略。 |
| d）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； | 该测评项测评对象为业务应用系统、中间件和系统管理软件，故将该项调整为不适用。 |
| e）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； | 1、经访谈网络管理员，会定期对官方网站通报的安全漏洞进行评估，然后从官方网站下载安全补丁，经过综合评估测试后对无线AP系统进行补丁修复，避免系统中存在安全漏洞，2、经现场漏洞扫描，未发现无线AP中存在安全漏洞。 |
| f）应能够检测到对重要节点进行入侵的行为，并在发生严重入侵事件时提供报警。 | 经访谈网络管理员，被测系统中部署了360AISA全流量威胁分析系统和360本地安全大脑，通过将被测系统中全部流量镜像发送到360AISA全流量威胁分析系统及360本地安全大脑中进行分析监测，发现入侵事件后及时通过钉钉报警，并且能够自动阻断。 |
| 可信验证 | a）可基于可信根对计算设备的系统引导程序、系统程序、重要配置参数和应用程序等进行可信验证，并在应用程序的关键执行环节进行动态可信验证，在检测到其可信性受到破坏后进行报警，并将验证结果形成审计记录送至安全管理中心。 | 未基于可信根对计算设备提供可信验证。 |
| 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； | 经现场访谈网络管理员及对无线AP配置，无线AP中关闭Telnet协议，采用SSH协议进行通信，保证重要数据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。 | 经访谈网络管理员及核查H3C WX3010系列无线AP产品文档，文件中目录05-参考指南--05文件系统管理命令中包含：“无线AP中文件系统通常使用摘要算法（SHA-256）对文件计算摘要值，用于验证文件的正确性和完整性”。 |
| 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； | 经现场访谈网络管理员及对无线AP配置，无线AP中关闭Telnet协议，采用SSH协议进行通信，保证重要数据在传输过程中的保密性。 |
| b）应采用密码技术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个人信息等。 | 经访谈网管理员，管理员在设置用户口令时添加simple参数，经核查H3C WX3010系列无线AP产品文档，在文档05-参考指南--03-登录设备命令--1、登录设备--1.1等设备命令--1.1.28 set authentication password中正对simple参数进行说明：“simple：以明文方式设置密码，该密码将以密文方式存储。 |
| 数据备份恢复 | a）应提供重要数据的本地数据备份与恢复功能； | 经现场访谈网络管理员及核查相应配置，管理员约每半年时间将无线AP中配置策略进行一次备份，备份文件在本地存储。 |
| b）应提供异地实时备份功能，利用通信网络将重要数据实时备份至备份场地； | 经现场访谈网络管理员，无线AP中备份文件仅本地保存，未提供实时异地备份。 |
| c）应提供重要数据处理系统的热冗余，保证系统的高可用性。 | 经访谈访问管理员及核查网络拓扑图，重要数据处理系统中采用双机冗余部署，保证系统的高可用性。 |

4.1.1.26. 无线AP3

|  |  |  |
| --- | --- | --- |
| **安全控制点** | **测评指标** | **结果记录** |
| 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、经现场访谈网络管理员，无线AP采用用户名、口令进行身份标识及身份鉴别；2、经核查无线AP配置，输入display password-control命令，返回信息为 Password aging:Enabled (90 days) Password length: Enabled (10 characters) Password composition:Enabled (3 types, 1 characters per type) Password history: Enabled (max history records:4)，通过返回信息确认：用户口令长度为至少10位，包含数字、字母、字符三种类型，未定期更改用户口令；3、通过现场在无线AP中创建与网络管理员同名账户时，无线AP中会提示用户名已存在，无法创重名用户，确认用户标识具备唯一性。 |
| 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、经现场核查无线AP配置策略，输入display password-control命令，返回信息为 Maximum login attempts: 3，Action for exceeding login attempts: Lock user for 1 minutes、User authentication timeout：600 seconds；2、通过返回信息确认用户连续错误登录3次锁定账户1分钟，用户登录连接超时时间限制为600秒。 |
| 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； | 1、经现场访谈网络管理员及核查其远程连接无线AP的方式，管理员在远程管理无线AP时采用SSH协议进行通信，防止鉴别信息在网络传输过程中被窃听；2、访谈网络管理员，Telnet协议默认为关闭状态，通过输入命令telnet server enable尝试启用Telnet协议，返回信息为Telnet is insecure because it transmits data in plaintext form，Telnet协议未启成功；3，通过在终端Telnet该无线AP，无法连接成功。 |
| 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。 | 经现场核查网络管理员远程登录无线AP方式，无线AP仅采用用户名、口令方式进行身份鉴别，未采用两种或两种以上组合的鉴别技术对用户进行身份鉴别。 |
| 访问控制 | a）应对登录的用户分配账户和权限； | 1、经现场核查无线AP中用户信息，通过输入display local-user命令，返回信息中显示无线AP中存在场站管理员、网络管理员两个用户，该用户均分配超管权限。 |
| b）应重命名或删除默认账户，修改默认账户的默认口令； | 1、经现场核查无线AP中用户信息，通过输入display local-user命令，返回信息中显示无线AP中存在场站管理员、网络管理员两个账户,不存在默认账户，2、经核查无线AP配置，输入display password-control命令，返回信息为 Password aging:Enabled (90 days) Password length: Enabled (10 characters) Password composition:Enabled (3 types, 1 characters per type) Password history: Enabled (max history records：3，用户口令已按照复杂度策略更改。 |
| 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； | 经现场核查无线AP中用户信息，通过输入display local-user命令，返回信息中显示无线AP中存在场站管理员、网络管理员等用户,经访谈网络管理员，账户与管理员一一对应，不存在多余、过期、共享账户。 |
| 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； | 经现场核查无线AP中用户信息，通过输入display local-user命令，返回信息中显示无线AP中存在场站管理员、网络管理员等用户,经访谈网络管理员，场站管理员、网络管理员均分配超级管理员权限，未按照权限最小化原则赋予管理用户权限及实现权限分离。 |
| e）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； | 经核查配置文件及访谈网络管理员，无线AP中由网络管理员角色账户为管理用户配置相应账号，并按照用户角色级别赋予管理用户操作权限。 |
| f）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； | 经核查配置文件及访谈网络管理员，无线AP访问控制策略为管理用户的无线AP中配置文件等进行配置管理及访问管理等，访问控制粒度达到主体为用户级、客体为文件级。 |
| g）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。 | 经核查配置文件及访谈网络管理员，无线AP未对重要主体和客体设置安全标记。 |
| 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； | 经现场访谈网络管理员及核查无线AP配置，输入命令display logbuffer reverse，返回信息为logbuffer:enable；确认无线AP中其中安全审计功能，通过查看审计记录内容，确认审计记录中包含设备运行记录及用户操作行为审计记录等。 |
| 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； | 经现场核查无线AP中审计记录内容，审计记录中包含：日期、时间、主机名、类型、IP地址、用户名、详情等。 |
| 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、经访谈网络管理员，无线AP中所有用户均无权限对审计记录进行删除或修改；2、经现场核查，管理员配置了审计记录备份策略，实时将无线AP中审计记录上传至备份服务器中进行备份；2、经现场核查备份服务器中/home/network\_backup目录中存在审计记录备份文件，备份文件宿主为root，权限为744，其他用户仅拥有读权限。中/home/network\_backup目录中存在审计记录备份文件，备份文件宿主为root，权限为744，其他用户仅拥有读权限。 |
| d）应对审计进程进行保护，防止未经授权的中断。 | 经现场访谈网络管理员，无线AP中审计进程受系统进程保护，所有用户均无权限将审计进程单独中断。 |
| 入侵防范 | a）应遵循最小安装的原则，仅安装需要的组件和应用程序； | 经访谈网络管理员及核查配置文件，无线AP系统为厂商提供独立封装系统，不允许安装其他组件及应用程序，遵循最小安装原则。 |
| b）应关闭不需要的系统服务、默认共享和高危端口； | 经现场访谈网络管理员及核查无线AP配置，输入display current-fonfiguration，返回信息HTTP、Telnet协议均已关闭，无线AP中未启用不需要的系统服务、默认共享及高危端口。 |
| c）应通过设定终端接入方式或网络地址范围对通过网络进行管理的管理终端进行限制； | 经访谈网络管理员，在防火墙中添加访问控制策略，仅允许管理用户通过堡垒机远程管理网络设备、安全设备及服务器等，经核查防火墙中访问控制策略，具备堡垒机地址-设备管理网段（10.33.0.0）的访问控制策略。 |
| d）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； | 该测评项测评对象为业务应用系统、中间件和系统管理软件，故将该项调整为不适用。 |
| e）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； | 1、经访谈网络管理员，会定期对官方网站通报的安全漏洞进行评估，然后从官方网站下载安全补丁，经过综合评估测试后对无线AP系统进行补丁修复，避免系统中存在安全漏洞，2、经现场漏洞扫描，未发现无线AP中存在安全漏洞。 |
| f）应能够检测到对重要节点进行入侵的行为，并在发生严重入侵事件时提供报警。 | 经访谈网络管理员，被测系统中部署了360AISA全流量威胁分析系统和360本地安全大脑，通过将被测系统中全部流量镜像发送到360AISA全流量威胁分析系统及360本地安全大脑中进行分析监测，发现入侵事件后及时通过钉钉报警，并且能够自动阻断。 |
| 可信验证 | a）可基于可信根对计算设备的系统引导程序、系统程序、重要配置参数和应用程序等进行可信验证，并在应用程序的关键执行环节进行动态可信验证，在检测到其可信性受到破坏后进行报警，并将验证结果形成审计记录送至安全管理中心。 | 未基于可信根对计算设备提供可信验证。 |
| 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； | 经现场访谈网络管理员及对无线AP配置，无线AP中关闭Telnet协议，采用SSH协议进行通信，保证重要数据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。 | 经访谈网络管理员及核查H3C WX3010系列无线AP产品文档，文件中目录05-参考指南--05文件系统管理命令中包含：“无线AP中文件系统通常使用摘要算法（SHA-256）对文件计算摘要值，用于验证文件的正确性和完整性”。 |
| 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； | 经现场访谈网络管理员及对无线AP配置，无线AP中关闭Telnet协议，采用SSH协议进行通信，保证重要数据在传输过程中的保密性。 |
| b）应采用密码技术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个人信息等。 | 经访谈网管理员，管理员在设置用户口令时添加simple参数，经核查H3C WX3010系列无线AP产品文档，在文档05-参考指南--03-登录设备命令--1、登录设备--1.1等设备命令--1.1.28 set authentication password中正对simple参数进行说明：“simple：以明文方式设置密码，该密码将以密文方式存储。 |
| 数据备份恢复 | a）应提供重要数据的本地数据备份与恢复功能； | 经现场访谈网络管理员及核查相应配置，管理员约每半年时间将无线AP中配置策略进行一次备份，备份文件在本地存储。 |
| b）应提供异地实时备份功能，利用通信网络将重要数据实时备份至备份场地； | 经现场访谈网络管理员，无线AP中备份文件仅本地保存，未提供实时异地备份。 |
| c）应提供重要数据处理系统的热冗余，保证系统的高可用性。 | 经访谈访问管理员及核查网络拓扑图，重要数据处理系统中采用双机冗余部署，保证系统的高可用性。 |

4.1.1.27. 无线AP4

|  |  |  |
| --- | --- | --- |
| **安全控制点** | **测评指标** | **结果记录** |
| 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、经现场访谈网络管理员，无线AP采用用户名、口令进行身份标识及身份鉴别；2、经核查无线AP配置，输入display password-control命令，返回信息为 Password aging:Enabled (90 days) Password length: Enabled (10 characters) Password composition:Enabled (3 types, 1 characters per type) Password history: Enabled (max history records:4)，通过返回信息确认：用户口令长度为至少10位，包含数字、字母、字符三种类型，未定期更改用户口令；3、通过现场在无线AP中创建与网络管理员同名账户时，无线AP中会提示用户名已存在，无法创重名用户，确认用户标识具备唯一性。 |
| 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、经现场核查无线AP配置策略，输入display password-control命令，返回信息为 Maximum login attempts: 3，Action for exceeding login attempts: Lock user for 1 minutes、User authentication timeout：600 seconds；2、通过返回信息确认用户连续错误登录3次锁定账户1分钟，用户登录连接超时时间限制为600秒。 |
| 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； | 1、经现场访谈网络管理员及核查其远程连接无线AP的方式，管理员在远程管理无线AP时采用SSH协议进行通信，防止鉴别信息在网络传输过程中被窃听；2、访谈网络管理员，Telnet协议默认为关闭状态，通过输入命令telnet server enable尝试启用Telnet协议，返回信息为Telnet is insecure because it transmits data in plaintext form，Telnet协议未启成功；3，通过在终端Telnet该无线AP，无法连接成功。 |
| 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。 | 经现场核查网络管理员远程登录无线AP方式，无线AP仅采用用户名、口令方式进行身份鉴别，未采用两种或两种以上组合的鉴别技术对用户进行身份鉴别。 |
| 访问控制 | a）应对登录的用户分配账户和权限； | 1、经现场核查无线AP中用户信息，通过输入display local-user命令，返回信息中显示无线AP中存在场站管理员、网络管理员两个用户，该用户均分配超管权限。 |
| b）应重命名或删除默认账户，修改默认账户的默认口令； | 1、经现场核查无线AP中用户信息，通过输入display local-user命令，返回信息中显示无线AP中存在场站管理员、网络管理员两个账户,不存在默认账户，2、经核查无线AP配置，输入display password-control命令，返回信息为 Password aging:Enabled (90 days) Password length: Enabled (10 characters) Password composition:Enabled (3 types, 1 characters per type) Password history: Enabled (max history records：3，用户口令已按照复杂度策略更改。 |
| 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； | 经现场核查无线AP中用户信息，通过输入display local-user命令，返回信息中显示无线AP中存在场站管理员、网络管理员等用户,经访谈网络管理员，账户与管理员一一对应，不存在多余、过期、共享账户。 |
| 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； | 经现场核查无线AP中用户信息，通过输入display local-user命令，返回信息中显示无线AP中存在场站管理员、网络管理员等用户,经访谈网络管理员，场站管理员、网络管理员均分配超级管理员权限，未按照权限最小化原则赋予管理用户权限及实现权限分离。 |
| e）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； | 经核查配置文件及访谈网络管理员，无线AP中由网络管理员角色账户为管理用户配置相应账号，并按照用户角色级别赋予管理用户操作权限。 |
| f）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； | 经核查配置文件及访谈网络管理员，无线AP访问控制策略为管理用户的无线AP中配置文件等进行配置管理及访问管理等，访问控制粒度达到主体为用户级、客体为文件级。 |
| g）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。 | 经核查配置文件及访谈网络管理员，无线AP未对重要主体和客体设置安全标记。 |
| 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； | 经现场访谈网络管理员及核查无线AP配置，输入命令display logbuffer reverse，返回信息为logbuffer:enable；确认无线AP中其中安全审计功能，通过查看审计记录内容，确认审计记录中包含设备运行记录及用户操作行为审计记录等。 |
| 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； | 经现场核查无线AP中审计记录内容，审计记录中包含：日期、时间、主机名、类型、IP地址、用户名、详情等。 |
| 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、经访谈网络管理员，无线AP中所有用户均无权限对审计记录进行删除或修改；2、经现场核查，管理员配置了审计记录备份策略，实时将无线AP中审计记录上传至备份服务器中进行备份；2、经现场核查备份服务器中/home/network\_backup目录中存在审计记录备份文件，备份文件宿主为root，权限为744，其他用户仅拥有读权限。中/home/network\_backup目录中存在审计记录备份文件，备份文件宿主为root，权限为744，其他用户仅拥有读权限。 |
| d）应对审计进程进行保护，防止未经授权的中断。 | 经现场访谈网络管理员，无线AP中审计进程受系统进程保护，所有用户均无权限将审计进程单独中断。 |
| 入侵防范 | a）应遵循最小安装的原则，仅安装需要的组件和应用程序； | 经访谈网络管理员及核查配置文件，无线AP系统为厂商提供独立封装系统，不允许安装其他组件及应用程序，遵循最小安装原则。 |
| b）应关闭不需要的系统服务、默认共享和高危端口； | 经现场访谈网络管理员及核查无线AP配置，输入display current-fonfiguration，返回信息HTTP、Telnet协议均已关闭，无线AP中未启用不需要的系统服务、默认共享及高危端口。 |
| c）应通过设定终端接入方式或网络地址范围对通过网络进行管理的管理终端进行限制； | 经访谈网络管理员，在防火墙中添加访问控制策略，仅允许管理用户通过堡垒机远程管理网络设备、安全设备及服务器等，经核查防火墙中访问控制策略，具备堡垒机地址-设备管理网段（10.33.0.0）的访问控制策略。 |
| d）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； | 该测评项测评对象为业务应用系统、中间件和系统管理软件，故将该项调整为不适用。 |
| e）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； | 1、经访谈网络管理员，会定期对官方网站通报的安全漏洞进行评估，然后从官方网站下载安全补丁，经过综合评估测试后对无线AP系统进行补丁修复，避免系统中存在安全漏洞，2、经现场漏洞扫描，未发现无线AP中存在安全漏洞。 |
| f）应能够检测到对重要节点进行入侵的行为，并在发生严重入侵事件时提供报警。 | 经访谈网络管理员，被测系统中部署了360AISA全流量威胁分析系统和360本地安全大脑，通过将被测系统中全部流量镜像发送到360AISA全流量威胁分析系统及360本地安全大脑中进行分析监测，发现入侵事件后及时通过钉钉报警，并且能够自动阻断。 |
| 可信验证 | a）可基于可信根对计算设备的系统引导程序、系统程序、重要配置参数和应用程序等进行可信验证，并在应用程序的关键执行环节进行动态可信验证，在检测到其可信性受到破坏后进行报警，并将验证结果形成审计记录送至安全管理中心。 | 未基于可信根对计算设备提供可信验证。 |
| 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； | 经现场访谈网络管理员及对无线AP配置，无线AP中关闭Telnet协议，采用SSH协议进行通信，保证重要数据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。 | 经访谈网络管理员及核查H3C WX3010系列无线AP产品文档，文件中目录05-参考指南--05文件系统管理命令中包含：“无线AP中文件系统通常使用摘要算法（SHA-256）对文件计算摘要值，用于验证文件的正确性和完整性”。 |
| 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； | 经现场访谈网络管理员及对无线AP配置，无线AP中关闭Telnet协议，采用SSH协议进行通信，保证重要数据在传输过程中的保密性。 |
| b）应采用密码技术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个人信息等。 | 经访谈网管理员，管理员在设置用户口令时添加simple参数，经核查H3C WX3010系列无线AP产品文档，在文档05-参考指南--03-登录设备命令--1、登录设备--1.1等设备命令--1.1.28 set authentication password中正对simple参数进行说明：“simple：以明文方式设置密码，该密码将以密文方式存储。 |
| 数据备份恢复 | a）应提供重要数据的本地数据备份与恢复功能； | 经现场访谈网络管理员及核查相应配置，管理员约每半年时间将无线AP中配置策略进行一次备份，备份文件在本地存储。 |
| b）应提供异地实时备份功能，利用通信网络将重要数据实时备份至备份场地； | 经现场访谈网络管理员，无线AP中备份文件仅本地保存，未提供实时异地备份。 |
| c）应提供重要数据处理系统的热冗余，保证系统的高可用性。 | 经访谈访问管理员及核查网络拓扑图，重要数据处理系统中采用双机冗余部署，保证系统的高可用性。 |

4.1.1.28. 无线AP5

|  |  |  |
| --- | --- | --- |
| **安全控制点** | **测评指标** | **结果记录** |
| 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、经现场访谈网络管理员，无线AP采用用户名、口令进行身份标识及身份鉴别；2、经核查无线AP配置，输入display password-control命令，返回信息为 Password aging:Enabled (90 days) Password length: Enabled (10 characters) Password composition:Enabled (3 types, 1 characters per type) Password history: Enabled (max history records:4)，通过返回信息确认：用户口令长度为至少10位，包含数字、字母、字符三种类型，未定期更改用户口令；3、通过现场在无线AP中创建与网络管理员同名账户时，无线AP中会提示用户名已存在，无法创重名用户，确认用户标识具备唯一性。 |
| 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、经现场核查无线AP配置策略，输入display password-control命令，返回信息为 Maximum login attempts: 3，Action for exceeding login attempts: Lock user for 1 minutes、User authentication timeout：600 seconds；2、通过返回信息确认用户连续错误登录3次锁定账户1分钟，用户登录连接超时时间限制为600秒。 |
| 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； | 1、经现场访谈网络管理员及核查其远程连接无线AP的方式，管理员在远程管理无线AP时采用SSH协议进行通信，防止鉴别信息在网络传输过程中被窃听；2、访谈网络管理员，Telnet协议默认为关闭状态，通过输入命令telnet server enable尝试启用Telnet协议，返回信息为Telnet is insecure because it transmits data in plaintext form，Telnet协议未启成功；3，通过在终端Telnet该无线AP，无法连接成功。 |
| 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。 | 经现场核查网络管理员远程登录无线AP方式，无线AP仅采用用户名、口令方式进行身份鉴别，未采用两种或两种以上组合的鉴别技术对用户进行身份鉴别。 |
| 访问控制 | a）应对登录的用户分配账户和权限； | 1、经现场核查无线AP中用户信息，通过输入display local-user命令，返回信息中显示无线AP中存在场站管理员、网络管理员两个用户，该用户均分配超管权限。 |
| b）应重命名或删除默认账户，修改默认账户的默认口令； | 1、经现场核查无线AP中用户信息，通过输入display local-user命令，返回信息中显示无线AP中存在场站管理员、网络管理员两个账户,不存在默认账户，2、经核查无线AP配置，输入display password-control命令，返回信息为 Password aging:Enabled (90 days) Password length: Enabled (10 characters) Password composition:Enabled (3 types, 1 characters per type) Password history: Enabled (max history records：3，用户口令已按照复杂度策略更改。 |
| 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； | 经现场核查无线AP中用户信息，通过输入display local-user命令，返回信息中显示无线AP中存在场站管理员、网络管理员等用户,经访谈网络管理员，账户与管理员一一对应，不存在多余、过期、共享账户。 |
| 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； | 经现场核查无线AP中用户信息，通过输入display local-user命令，返回信息中显示无线AP中存在场站管理员、网络管理员等用户,经访谈网络管理员，场站管理员、网络管理员均分配超级管理员权限，未按照权限最小化原则赋予管理用户权限及实现权限分离。 |
| e）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； | 经核查配置文件及访谈网络管理员，无线AP中由网络管理员角色账户为管理用户配置相应账号，并按照用户角色级别赋予管理用户操作权限。 |
| f）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； | 经核查配置文件及访谈网络管理员，无线AP访问控制策略为管理用户的无线AP中配置文件等进行配置管理及访问管理等，访问控制粒度达到主体为用户级、客体为文件级。 |
| g）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。 | 经核查配置文件及访谈网络管理员，无线AP未对重要主体和客体设置安全标记。 |
| 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； | 经现场访谈网络管理员及核查无线AP配置，输入命令display logbuffer reverse，返回信息为logbuffer:enable；确认无线AP中其中安全审计功能，通过查看审计记录内容，确认审计记录中包含设备运行记录及用户操作行为审计记录等。 |
| 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； | 经现场核查无线AP中审计记录内容，审计记录中包含：日期、时间、主机名、类型、IP地址、用户名、详情等。 |
| 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、经访谈网络管理员，无线AP中所有用户均无权限对审计记录进行删除或修改；2、经现场核查，管理员配置了审计记录备份策略，实时将无线AP中审计记录上传至备份服务器中进行备份；2、经现场核查备份服务器中/home/network\_backup目录中存在审计记录备份文件，备份文件宿主为root，权限为744，其他用户仅拥有读权限。中/home/network\_backup目录中存在审计记录备份文件，备份文件宿主为root，权限为744，其他用户仅拥有读权限。 |
| d）应对审计进程进行保护，防止未经授权的中断。 | 经现场访谈网络管理员，无线AP中审计进程受系统进程保护，所有用户均无权限将审计进程单独中断。 |
| 入侵防范 | a）应遵循最小安装的原则，仅安装需要的组件和应用程序； | 经访谈网络管理员及核查配置文件，无线AP系统为厂商提供独立封装系统，不允许安装其他组件及应用程序，遵循最小安装原则。 |
| b）应关闭不需要的系统服务、默认共享和高危端口； | 经现场访谈网络管理员及核查无线AP配置，输入display current-fonfiguration，返回信息HTTP、Telnet协议均已关闭，无线AP中未启用不需要的系统服务、默认共享及高危端口。 |
| c）应通过设定终端接入方式或网络地址范围对通过网络进行管理的管理终端进行限制； | 经访谈网络管理员，在防火墙中添加访问控制策略，仅允许管理用户通过堡垒机远程管理网络设备、安全设备及服务器等，经核查防火墙中访问控制策略，具备堡垒机地址-设备管理网段（10.33.0.0）的访问控制策略。 |
| d）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； | 该测评项测评对象为业务应用系统、中间件和系统管理软件，故将该项调整为不适用。 |
| e）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； | 1、经访谈网络管理员，会定期对官方网站通报的安全漏洞进行评估，然后从官方网站下载安全补丁，经过综合评估测试后对无线AP系统进行补丁修复，避免系统中存在安全漏洞，2、经现场漏洞扫描，未发现无线AP中存在安全漏洞。 |
| f）应能够检测到对重要节点进行入侵的行为，并在发生严重入侵事件时提供报警。 | 经访谈网络管理员，被测系统中部署了360AISA全流量威胁分析系统和360本地安全大脑，通过将被测系统中全部流量镜像发送到360AISA全流量威胁分析系统及360本地安全大脑中进行分析监测，发现入侵事件后及时通过钉钉报警，并且能够自动阻断。 |
| 可信验证 | a）可基于可信根对计算设备的系统引导程序、系统程序、重要配置参数和应用程序等进行可信验证，并在应用程序的关键执行环节进行动态可信验证，在检测到其可信性受到破坏后进行报警，并将验证结果形成审计记录送至安全管理中心。 | 未基于可信根对计算设备提供可信验证。 |
| 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； | 经现场访谈网络管理员及对无线AP配置，无线AP中关闭Telnet协议，采用SSH协议进行通信，保证重要数据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。 | 经访谈网络管理员及核查H3C WX3010系列无线AP产品文档，文件中目录05-参考指南--05文件系统管理命令中包含：“无线AP中文件系统通常使用摘要算法（SHA-256）对文件计算摘要值，用于验证文件的正确性和完整性”。 |
| 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； | 经现场访谈网络管理员及对无线AP配置，无线AP中关闭Telnet协议，采用SSH协议进行通信，保证重要数据在传输过程中的保密性。 |
| b）应采用密码技术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个人信息等。 | 经访谈网管理员，管理员在设置用户口令时添加simple参数，经核查H3C WX3010系列无线AP产品文档，在文档05-参考指南--03-登录设备命令--1、登录设备--1.1等设备命令--1.1.28 set authentication password中正对simple参数进行说明：“simple：以明文方式设置密码，该密码将以密文方式存储。 |
| 数据备份恢复 | a）应提供重要数据的本地数据备份与恢复功能； | 经现场访谈网络管理员及核查相应配置，管理员约每半年时间将无线AP中配置策略进行一次备份，备份文件在本地存储。 |
| b）应提供异地实时备份功能，利用通信网络将重要数据实时备份至备份场地； | 经现场访谈网络管理员，无线AP中备份文件仅本地保存，未提供实时异地备份。 |
| c）应提供重要数据处理系统的热冗余，保证系统的高可用性。 | 经访谈访问管理员及核查网络拓扑图，重要数据处理系统中采用双机冗余部署，保证系统的高可用性。 |

4.1.1.29. 无线AP6-200

|  |  |  |
| --- | --- | --- |
| **安全控制点** | **测评指标** | **结果记录** |
| 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、经现场访谈网络管理员，无线AP采用用户名、口令进行身份标识及身份鉴别；2、经核查无线AP配置，输入display password-control命令，返回信息为 Password aging:Enabled (90 days) Password length: Enabled (10 characters) Password composition:Enabled (3 types, 1 characters per type) Password history: Enabled (max history records:4)，通过返回信息确认：用户口令长度为至少10位，包含数字、字母、字符三种类型，未定期更改用户口令；3、通过现场在无线AP中创建与网络管理员同名账户时，无线AP中会提示用户名已存在，无法创重名用户，确认用户标识具备唯一性。 |
| 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、经现场核查无线AP配置策略，输入display password-control命令，返回信息为 Maximum login attempts: 3，Action for exceeding login attempts: Lock user for 1 minutes、User authentication timeout：600 seconds；2、通过返回信息确认用户连续错误登录3次锁定账户1分钟，用户登录连接超时时间限制为600秒。 |
| 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； | 1、经现场访谈网络管理员及核查其远程连接无线AP的方式，管理员在远程管理无线AP时采用SSH协议进行通信，防止鉴别信息在网络传输过程中被窃听；2、访谈网络管理员，Telnet协议默认为关闭状态，通过输入命令telnet server enable尝试启用Telnet协议，返回信息为Telnet is insecure because it transmits data in plaintext form，Telnet协议未启成功；3，通过在终端Telnet该无线AP，无法连接成功。 |
| 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。 | 经现场核查网络管理员远程登录无线AP方式，无线AP仅采用用户名、口令方式进行身份鉴别，未采用两种或两种以上组合的鉴别技术对用户进行身份鉴别。 |
| 访问控制 | a）应对登录的用户分配账户和权限； | 1、经现场核查无线AP中用户信息，通过输入display local-user命令，返回信息中显示无线AP中存在场站管理员、网络管理员两个用户，该用户均分配超管权限。 |
| b）应重命名或删除默认账户，修改默认账户的默认口令； | 1、经现场核查无线AP中用户信息，通过输入display local-user命令，返回信息中显示无线AP中存在场站管理员、网络管理员两个账户,不存在默认账户，2、经核查无线AP配置，输入display password-control命令，返回信息为 Password aging:Enabled (90 days) Password length: Enabled (10 characters) Password composition:Enabled (3 types, 1 characters per type) Password history: Enabled (max history records：3，用户口令已按照复杂度策略更改。 |
| 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； | 经现场核查无线AP中用户信息，通过输入display local-user命令，返回信息中显示无线AP中存在场站管理员、网络管理员等用户,经访谈网络管理员，账户与管理员一一对应，不存在多余、过期、共享账户。 |
| 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； | 经现场核查无线AP中用户信息，通过输入display local-user命令，返回信息中显示无线AP中存在场站管理员、网络管理员等用户,经访谈网络管理员，场站管理员、网络管理员均分配超级管理员权限，未按照权限最小化原则赋予管理用户权限及实现权限分离。 |
| e）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； | 经核查配置文件及访谈网络管理员，无线AP中由网络管理员角色账户为管理用户配置相应账号，并按照用户角色级别赋予管理用户操作权限。 |
| f）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； | 经核查配置文件及访谈网络管理员，无线AP访问控制策略为管理用户的无线AP中配置文件等进行配置管理及访问管理等，访问控制粒度达到主体为用户级、客体为文件级。 |
| g）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。 | 经核查配置文件及访谈网络管理员，无线AP未对重要主体和客体设置安全标记。 |
| 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； | 经现场访谈网络管理员及核查无线AP配置，输入命令display logbuffer reverse，返回信息为logbuffer:enable；确认无线AP中其中安全审计功能，通过查看审计记录内容，确认审计记录中包含设备运行记录及用户操作行为审计记录等。 |
| 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； | 经现场核查无线AP中审计记录内容，审计记录中包含：日期、时间、主机名、类型、IP地址、用户名、详情等。 |
| 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、经访谈网络管理员，无线AP中所有用户均无权限对审计记录进行删除或修改；2、经现场核查，管理员配置了审计记录备份策略，实时将无线AP中审计记录上传至备份服务器中进行备份；2、经现场核查备份服务器中/home/network\_backup目录中存在审计记录备份文件，备份文件宿主为root，权限为744，其他用户仅拥有读权限。中/home/network\_backup目录中存在审计记录备份文件，备份文件宿主为root，权限为744，其他用户仅拥有读权限。 |
| d）应对审计进程进行保护，防止未经授权的中断。 | 经现场访谈网络管理员，无线AP中审计进程受系统进程保护，所有用户均无权限将审计进程单独中断。 |
| 入侵防范 | a）应遵循最小安装的原则，仅安装需要的组件和应用程序； | 经访谈网络管理员及核查配置文件，无线AP系统为厂商提供独立封装系统，不允许安装其他组件及应用程序，遵循最小安装原则。 |
| b）应关闭不需要的系统服务、默认共享和高危端口； | 经现场访谈网络管理员及核查无线AP配置，输入display current-fonfiguration，返回信息HTTP、Telnet协议均已关闭，无线AP中未启用不需要的系统服务、默认共享及高危端口。 |
| c）应通过设定终端接入方式或网络地址范围对通过网络进行管理的管理终端进行限制； | 经访谈网络管理员，在防火墙中添加访问控制策略，仅允许管理用户通过堡垒机远程管理网络设备、安全设备及服务器等，经核查防火墙中访问控制策略，具备堡垒机地址-设备管理网段（10.33.0.0）的访问控制策略。 |
| d）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； | 该测评项测评对象为业务应用系统、中间件和系统管理软件，故将该项调整为不适用。 |
| e）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； | 1、经访谈网络管理员，会定期对官方网站通报的安全漏洞进行评估，然后从官方网站下载安全补丁，经过综合评估测试后对无线AP系统进行补丁修复，避免系统中存在安全漏洞，2、经现场漏洞扫描，未发现无线AP中存在安全漏洞。 |
| f）应能够检测到对重要节点进行入侵的行为，并在发生严重入侵事件时提供报警。 | 经访谈网络管理员，被测系统中部署了360AISA全流量威胁分析系统和360本地安全大脑，通过将被测系统中全部流量镜像发送到360AISA全流量威胁分析系统及360本地安全大脑中进行分析监测，发现入侵事件后及时通过钉钉报警，并且能够自动阻断。 |
| 可信验证 | a）可基于可信根对计算设备的系统引导程序、系统程序、重要配置参数和应用程序等进行可信验证，并在应用程序的关键执行环节进行动态可信验证，在检测到其可信性受到破坏后进行报警，并将验证结果形成审计记录送至安全管理中心。 | 未基于可信根对计算设备提供可信验证。 |
| 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； | 经现场访谈网络管理员及对无线AP配置，无线AP中关闭Telnet协议，采用SSH协议进行通信，保证重要数据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。 | 经访谈网络管理员及核查H3C WX3010系列无线AP产品文档，文件中目录05-参考指南--05文件系统管理命令中包含：“无线AP中文件系统通常使用摘要算法（SHA-256）对文件计算摘要值，用于验证文件的正确性和完整性”。 |
| 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； | 经现场访谈网络管理员及对无线AP配置，无线AP中关闭Telnet协议，采用SSH协议进行通信，保证重要数据在传输过程中的保密性。 |
| b）应采用密码技术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个人信息等。 | 经访谈网管理员，管理员在设置用户口令时添加simple参数，经核查H3C WX3010系列无线AP产品文档，在文档05-参考指南--03-登录设备命令--1、登录设备--1.1等设备命令--1.1.28 set authentication password中正对simple参数进行说明：“simple：以明文方式设置密码，该密码将以密文方式存储。 |
| 数据备份恢复 | a）应提供重要数据的本地数据备份与恢复功能； | 经现场访谈网络管理员及核查相应配置，管理员约每半年时间将无线AP中配置策略进行一次备份，备份文件在本地存储。 |
| b）应提供异地实时备份功能，利用通信网络将重要数据实时备份至备份场地； | 经现场访谈网络管理员，无线AP中备份文件仅本地保存，未提供实时异地备份。 |
| c）应提供重要数据处理系统的热冗余，保证系统的高可用性。 | 经访谈访问管理员及核查网络拓扑图，重要数据处理系统中采用双机冗余部署，保证系统的高可用性。 |

|  |  |  |  |
| --- | --- | --- | --- |
| **测评项目** |  | **测评对象** | 安全设备 |
| **测评单位** |  | | |
| **测评地点** |  | | |
| **测评人员** |  | **配合人员** | 刘亮 |
| **测评日期** | 2023.6.15 | | |
| **测评人员签字** |  | **配合人员签字** |  |

4.1.2. 安全设备

4.1.2.1. Web应用防火墙

|  |  |  |
| --- | --- | --- |
| **安全控制点** | **测评指标** | **结果记录** |
| 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、经现场访谈网络管理员，Web应用防火墙基于阿里云控制台进行身份鉴别，阿里云控制台采用用户名、口令方式+MFA动态随机码对登录用户进行身份标识和鉴别，阿里云控制台对登录用户通过真实邮箱、手机号进行验证，能够保证用户身份标识唯一；2、经现场查看阿里云控制台RAM访问控制台-身份管理-设置菜单，用户口令长度要求为8-32位字符，由数字、大小写字母、字符三种以上组合，MFA生成6位动态随机码，首次登录时需要通过手机短信验证码，但未要求定期更换口令。 |
| 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、经现场访谈网络管理员，Web应用防火墙基于阿里云控制台进行身份鉴别； 2、经现场查看阿里云控制台RAM访问控制台-身份管理-设置菜单，阿里云控制台启用了用户登录失败处理功能，用户一小时内连续错误登录5次需要通过拖动滑动条进行验证，并启用短信验证码进行二次验证，登录会话的过期时间为6小时。 |
| 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； | 经现场访谈网络管理员，Web应用防火墙基于阿里云控制台进行身份鉴别，经现场核查阿里云控制台的登录方式，阿里云控制台通过HTTPS协议进行远程管理，保证鉴别信息在网络传输过程中不被窃听。 |
| 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。 | 1、经现场访谈网络管理员，Web应用防火墙基于阿里云控制台进行身份鉴别； 2、经现场核查阿里云控制台的登录方式，阿里云控制台用户通过用户名、口令+MFA动态随机码对登录用户进行身份标识和鉴别进行身份鉴别。 |
| 访问控制 | a）应对登录的用户分配账户和权限； | 1、经现场访谈网络管理员，Web应用防火墙基于阿里云控制台进行访问控制，2、经现场查看阿里云控制台RAM访问控制台-身份管理-用户组及用户菜单，在阿里云控制台中分别为创建DBA、network-user、safe三个用户组，将三个用户组分别赋予数据库管理、网络管理及安全审计管理等权限，在控制台中按照业务需求及管理需求分别创建了相应账户，然后将管理用户根据工作职责添加到对应用户组中，进而获得相应管理权限，经现场核查，阿里云控制台中共49个账户。 |
| b）应重命名或删除默认账户，修改默认账户的默认口令； | 1、经现场访谈网络管理员，Web应用防火墙基于阿里云控制台进行访问控制，阿里云控制台中管理用户为注册用户，子账户由管理用户创建，不存在默认账户；2、所有用户口令均按照复杂度策略更改。 |
| 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； | 1、经现场访谈网络管理员，Web应用防火墙基于阿里云控制台进行身份鉴别，2、经现场访谈网络管理员及核查阿里云控制台中用户信息，目前阿里云控制台中账户均为在职人员及业务账户，账户与人员一一对应，并且分别根据管理用户工作职责赋予工作权限，不存在多余、过期、共享账户。 |
| 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； | 1、经现场访谈网络管理员，Web应用防火墙基于阿里云控制台进行身份鉴别，2、经现场访谈网络管理员及核查阿里云控制台中用户权限管理，目前阿里云控制台中分别创建了系统管理员、操作用户、审计管理员、安全管理等用户，并分别赋予管理用户相应的工作权限，实现管理用户权限最小化及权限分离。 |
| e）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、经现场访谈网络管理员，Web应用防火墙基于阿里云控制台进行身份鉴别，2、经现场访谈网络管理员及核查阿里云控制台各管理员的权限分配情况，在阿里云控制台由管理员主账户为各管理员配置访问控制策略，访问控制策略为管理员对阿里云控制台中各功能菜单的访问及操作管理等，如：用户管理、安全服务管理、操作审计等功能菜单的操作管理。 |
| f）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； | 1、经现场访谈网络管理员，Web应用防火墙基于阿里云控制台进行身份鉴别；2、经现场访谈网络管理员及核查阿里云控制台各管理员的权限分配情况，阿里云控制台访问控制粒度达到主体为用户级，客体为功能菜单级。 |
| g）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。 | 经现场核查，未对重要主体和客体设置安全标记。 |
| 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、经现场访谈网络管理员，Web应用防火墙用户操作行为基于阿里云控制台进行安全审计，经现场核查阿里云控制台中操作审计功能，在阿里云控制台中启用了操作审计功能，能够对系统中用户操作内容及系统中的安全事件进行审计，2、经现场核查Web应用防火墙中日志服务，能够对用户访问等进行审计记录。 |
| 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； | 1、经现场访谈网络管理员，Web应用防火墙用户操作行为基于阿里云控制台进行安全审计，经现场核查阿里云控制台中操作审计内容，阿里云控制台操作审计记录包括：时间、用户名、事件名称、资源类型、资源名称、错误码等；2、Web应用防火墙中用户访问日志包括：acl\_action、acl\_rule\_id、acl\_rule\_type、antiscan\_action、antiscan\_rule\_id、antiscan\_rule\_type、body\_bytes\_sent、request\_body、server\_port、waf\_action、waf\_rule\_id、waf\_rule\_type、response\_set\_cookie、scene\_action、scene\_id、scene\_rule\_type等信息。 |
| 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、经现场访谈网络管理员，Web应用防火墙用户操作行为基于阿里云控制台进行安全审计，经现场核查阿里云控制台审计记录及备份设置，阿里云控制台所有用户均无权限对相关的审计记录进行删除、修改；2、经现场核查Web应用防火墙审计记录及备份设置，所有用户均无权限对相关的审计记录进行删除、修改；3、管理员配置审计记录转储，每天将审计记录传输至OSS上进行存储，并保证审计记录保存时间至少为180天。 |
| d）应对审计进程进行保护，防止未经授权的中断。 | 经现场核查阿里云控制台操作审计功能及Web应用防火墙审计服务中，操作审计功能为阿里公共云提供的审计服务，阿里云控制台及Web应用防火墙相关的审计进程由阿里公共云负责保护，不会受到未预期的中断。 |
| 入侵防范 | a）应遵循最小安装的原则，仅安装需要的组件和应用程序； | 经核查，Web应用防火墙为阿里公共云为用户提供应用层面安全防护服务，不涉及组件和应用程序安装，故该测评项调整为不适用。 |
| b）应关闭不需要的系统服务、默认共享和高危端口； | 经核查，Web应用防火墙为阿里公共云为用户提供应用层面安全防护服务，故该测评项调整为不适用。 |
| c）应通过设定终端接入方式或网络地址范围对通过网络进行管理的管理终端进行限制； | 经核查，Web应用防火墙基于阿里云控制台进行管理，在阿里云控制台中针对RAM账号单独创建登录链接以及账号，仅允许对应账号进行登录。 |
| d）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； | 经现场核查Web应用防火墙基于阿里云控制台进行集中管理，阿里云控制台中人机交互均采用下拉框或勾选方式实现，核查阿里云操作手册，能够对特殊字符进行了过滤，保证输入数据的有效性。 |
| e）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； | 经现场访谈管理管理员及核查Web应用防火墙配置，被测系统采购阿里公共云提供的云平台服务，由阿里公共云负责对Web应用防火墙进行维护管理及版本更新，阿里公共云已通过等级保护第三级测评。 |
| f）应能够检测到对重要节点进行入侵的行为，并在发生严重入侵事件时提供报警。 | 经现场访谈网络管理员及核查阿里云安全服务，在阿里公共云采购云防火墙、Web应用防火墙安全服务，云防火墙能够对网络层入侵行为进行检测，Web应用防火墙能够应用层入侵行为进行检测，发现严重入侵事件及时通过钉钉报警，经现场核查网络管理员钉钉记录，具备实时报警记录。 |
| 可信验证 | a）可基于可信根对计算设备的系统引导程序、系统程序、重要配置参数和应用程序等进行可信验证，并在应用程序的关键执行环节进行动态可信验证，在检测到其可信性受到破坏后进行报警，并将验证结果形成审计记录送至安全管理中心。 | 未基于可信根对计算设备提供可信验证。 |
| 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； | 经现场核查Web应用防火墙基于阿里云控制台进行统一管理，现场核查阿里云控制台的通信方式，阿里云控制台通过HTTPS协议进行通信，保证重要数据在网络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。 | 经现场核查Web应用防火墙基于阿里云控制台进行统一管理，经现场访问网络管理员及核查阿里云相关文档说明，阿里云控制台中用户鉴别信息会采用加密技术保证了重要数据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； | 经现场核查Web应用防火墙基于阿里云控制台进行统一管理，现场核查阿里云控制台的通信方式，阿里云控制台通过HTTPS协议进行通信，保证重要数据在网络传输过程中的完保密性。 |
| b）应采用密码技术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个人信息等。 | 经现场核查Web应用防火墙基于阿里云控制台进行统一管理，经现场访问网络管理员及核查阿里云相关文档说明，阿里云控制台中用户鉴别信息会采用加密技术保证了重要数据在存储过程中的保密性。 |
| 数据备份恢复 | a）应提供重要数据的本地数据备份与恢复功能； | 经现场核查Web应用防火墙基于阿里云控制台进行统一管理，管理员通过手动方式将Web应用防火墙中配置数据进行下载备份。 |
| b）应提供异地实时备份功能，利用通信网络将重要数据实时备份至备份场地； | 公司未对重要数据提供异地备份服务。 |
| c）应提供重要数据处理系统的热冗余，保证系统的高可用性。 | 经访谈访问管理员及核查网络拓扑图，Web应用防火墙冗余由阿里云负责。 |

4.1.2.2. 云防火墙

|  |  |  |
| --- | --- | --- |
| **安全控制点** | **测评指标** | **结果记录** |
| 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、经现场访谈网络管理员，云防火墙基于阿里云控制台进行身份鉴别，阿里云控制台采用用户名、口令方式+MFA动态随机码对登录用户进行身份标识和鉴别，阿里云控制台对登录用户通过真实邮箱、手机号进行验证，能够保证用户身份标识唯一； 2、经现场查看阿里云控制台RAM访问控制台-身份管理-设置菜单，用户口令长度要求为8-32位字符，由数字、大小写字母、字符三种以上组合，MFA生成6位动态随机码，首次登录时需要通过手机短信验证码，但未要求定期更换口令。 |
| 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、经现场访谈网络管理员，云防火墙基于阿里云控制台进行身份鉴别； 2、经现场查看阿里云控制台RAM访问控制台-身份管理-设置菜单，阿里云控制台启用了用户登录失败处理功能，用户一小时内连续错误登录5次需要通过拖动滑动条进行验证，并启用短信验证码进行二次验证，登录会话的过期时间为6小时。 |
| 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； | 1、经现场访谈网络管理员，云防火墙基于阿里云控制台进行身份鉴别，经现场核查阿里云控制台的登录方式， 2、阿里云控制台通过HTTPS协议进行远程管理，保证鉴别信息在网络传输过程中不被窃听。 |
| 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。 | 1、经现场访谈网络管理员，云防火墙基于阿里云控制台进行身份鉴别； 2、经现场核查阿里云控制台的登录方式，阿里云控制台用户通过用户名、口令+MFA动态随机码对登录用户进行身份标识和鉴别进行身份鉴别。 |
| 访问控制 | a）应对登录的用户分配账户和权限； | 1、经现场访谈网络管理员，云防火墙基于阿里云控制台进行访问控制，2、经现场查看阿里云控制台RAM访问控制台-身份管理-用户组及用户菜单，在阿里云控制台中分别为创建DBA、network-user、safe三个用户组，将三个用户组分别赋予数据库管理、网络管理及安全审计管理等权限，在控制台中按照业务需求及管理需求分别创建了相应账户，然后将管理用户根据工作职责添加到对应用户组中，进而获得相应管理权限，经现场核查，阿里云控制台中共49个账户。 |
| b）应重命名或删除默认账户，修改默认账户的默认口令； | 1、经现场访谈网络管理员，云防火墙基于阿里云控制台进行访问控制，阿里云控制台中管理用户为注册用户，子账户由管理用户创建，不存在默认账户；2、所有用户口令均按照复杂度策略更改。 |
| 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； | 1、经现场访谈网络管理员，云防火墙基于阿里云控制台进行身份鉴别，2、经现场访谈网络管理员及核查阿里云控制台中用户信息，目前阿里云控制台中账户均为在职人员及业务账户，账户与人员一一对应，并且分别根据管理用户工作职责赋予工作权限，不存在多余、过期、共享账户。 |
| 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； | 1、经现场访谈网络管理员，云防火墙基于阿里云控制台进行身份鉴别，2、经现场访谈网络管理员及核查阿里云控制台中用户权限管理，目前阿里云控制台中分别创建了系统管理员、操作用户、审计管理员、安全管理等用户，并分别赋予管理用户相应的工作权限，实现管理用户权限最小化及权限分离。 |
| e）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、经现场访谈网络管理员，云防火墙基于阿里云控制台进行身份鉴别，2、经现场访谈网络管理员及核查阿里云控制台各管理员的权限分配情况，在阿里云控制台由管理员主账户为各管理员配置访问控制策略，访问控制策略为管理员对阿里云控制台中各功能菜单的访问及操作管理等，如：用户管理、安全服务管理、操作审计等功能菜单的操作管理。 |
| f）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； | 1、经现场访谈网络管理员，云防火墙基于阿里云控制台进行身份鉴别，2、经现场访谈网络管理员及核查阿里云控制台各管理员的权限分配情况，阿里云控制台访问控制粒度达到主体为用户级，客体为功能菜单级。 |
| g）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。 | 经现场核查，未对重要主体和客体设置安全标记。 |
| 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、经现场访谈网络管理员，云防火墙用户操作行为基于阿里云控制台进行安全审计，经现场核查阿里云控制台中操作审计功能，在阿里云控制台中启用了操作审计功能，能够对系统中用户操作内容及系统中的安全事件进行审计，2、经现场核查云防火墙中日志服务，能够对入侵攻击行为等进行审计记录。 |
| 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； | 1、经现场访谈网络管理员，云防火墙用户操作行为基于阿里云控制台进行安全审计，经现场核查阿里云控制台中操作审计内容，阿里云控制台操作审计记录包括：时间、用户名、事件名称、资源类型、资源名称、错误码等，2、经核查云防火墙中入侵攻击审计记录包括：发生时间、源IP、目的IP、事件名称/攻击类型/方向/判断来源、事件数/风险级别、防御状态、操作（详情）等。 |
| 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、经现场访谈网络管理员，云防火墙用户操作行为基于阿里云控制台进行安全审计，经现场核查阿里云控制台审计记录及备份设置，阿里云控制台所有用户均无权限对相关的审计记录进行删除、修改，2、经现场核查云防火墙审计记录及备份设置，所有用户均无权限对相关的审计记录进行删除、修改，3、管理员配置审计记录转储，每天将审计记录传输至OSS上进行存储，并保证审计记录保存时间至少为180天 。 |
| d）应对审计进程进行保护，防止未经授权的中断。 | 经现场核查阿里云控制台操作审计功能及云防火墙审计服务中，操作审计功能为阿里公共云提供的审计服务，阿里云控制台及云防火墙相关的审计进程由阿里公共云负责保护，不会受到未预期的中断。 |
| 入侵防范 | a）应遵循最小安装的原则，仅安装需要的组件和应用程序； | 经核查，云防火墙为阿里公共云为用户提供应用层面安全防护服务，不涉及组件和应用程序的安装，故该测评项调整为不适用。 |
| b）应关闭不需要的系统服务、默认共享和高危端口； | 经核查，云防火墙为阿里公共云为用户提供应用层面安全防护服务，故该测评项调整为不适用。 |
| c）应通过设定终端接入方式或网络地址范围对通过网络进行管理的管理终端进行限制； | 经核查，Web应用防火墙基于阿里云控制台进行管理，在阿里云控制台中针对RAM账号单独创建登录链接以及账号，仅允许对应账号进行登录。 |
| d）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； | 经现场核查云防火墙基于阿里云控制台进行集中管理，阿里云控制台中人机交互均采用下拉框或勾选方式实现，核查阿里云操作手册，能够对特殊字符进行了过滤，保证输入数据的有效性。 |
| e）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； | 经现场访谈管理管理员及核查云防火墙配置，被测系统采购阿里公共云提供的云平台服务，由阿里公共云负责对云防火墙进行维护管理及版本更新，阿里公共云已通过等级保护第三级测评。 |
| f）应能够检测到对重要节点进行入侵的行为，并在发生严重入侵事件时提供报警。 | 经现场访谈网络管理员及核查阿里云安全服务，在阿里公共云采购云防火墙、Web应用防火墙安全服务，云防火墙能够对网络层入侵行为进行检测，Web应用防火墙能够应用层入侵行为进行检测，发现严重入侵事件及时通过钉钉报警，经现场核查网络管理员钉钉记录，具备实时报警记录。 |
| 可信验证 | a）可基于可信根对计算设备的系统引导程序、系统程序、重要配置参数和应用程序等进行可信验证，并在应用程序的关键执行环节进行动态可信验证，在检测到其可信性受到破坏后进行报警，并将验证结果形成审计记录送至安全管理中心。 | 未基于可信根对计算设备提供可信验证。 |
| 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； | 经现场核查，云防火墙基于阿里云控制台进行统一管理，现场核查阿里云控制台的通信方式，阿里云控制台通过HTTPS协议进行通信，保证重要数据在网络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。 | 经现场核查，云防火墙基于阿里云控制台进行统一管理，经现场访问网络管理员及核查阿里云相关文档说明，阿里云控制台中用户鉴别信息会采用加密技术保证了重要业务数据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； | 经现场核查，云防火墙基于阿里云控制台进行统一管理，现场核查阿里云控制台的通信方式，阿里云控制台通过HTTPS协议进行通信，保证重要数据在网络传输过程中的保密性。 |
| b）应采用密码技术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个人信息等。 | 经现场核查，云防火墙基于阿里云控制台进行统一管理，经现场访问网络管理员及核查阿里云相关文档说明，阿里云控制台中用户鉴别信息会采用加密技术保证了重要业务数据在存储过程中的保密性。 |
| 数据备份恢复 | a）应提供重要数据的本地数据备份与恢复功能； | 经现场核查云防火墙基于阿里云控制台进行统一管理，管理员通过手动方式将阿里云控制台中配置数据进行下载备份。 |
| b）应提供异地实时备份功能，利用通信网络将重要数据实时备份至备份场地； | 公司未对重要数据提供异地备份服务。 |
| c）应提供重要数据处理系统的热冗余，保证系统的高可用性。 | 经访谈访问管理员及核查网络拓扑图，重要数据处理系统中采用双机冗余部署，保证系统的高可用性。 |

4.1.2.3. 360AISA全流量威胁分析系统

|  |  |  |
| --- | --- | --- |
| **安全控制点** | **测评指标** | **结果记录** |
| 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、经现场访谈安全管理员及核查360全流量威胁分析系统配置，360全流量采用用户名、口令进行身份鉴别和标识，360全流量具备用户名查重功能，保证用户名具有唯一性，经现场测试，创建重名用户会提示用户名已存在；2、核查360全流量威胁分析系统中配置，在系统管理-安全性设置中配置口令策略，其中口令最小长度为8位，包含字母、数字、特殊字符三种组合，密码最长周期为7天。 |
| 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、经现场访谈安全管理员及核查360全流量威胁分析系统中配置，360全流量启用登录失败处理策略，用户连续错误登录5次锁定账户，由管理员负责解锁； 2、页面超时时间限制为480分钟。 |
| 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； | 经现场核查360全流量威胁分析系统通信方式，360全流量威胁分析系统在远程管理时采用HTTPS协议进行通信，防止鉴别信息在网络传输过程中被窃听。 |
| 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。 | 经现场核查360全流量威胁分析系统登录方式，360全流量仅采用用户名、口令方式进行身份鉴别，未采用两种或两种以上组合的鉴别技术对用户进行身份鉴别。 |
| 访问控制 | a）应对登录的用户分配账户和权限； | 经现场核查360全流量威胁分析系统用户及权限策略，360全流量由admin管理员对登录的账户创建账户并进行权限分配，目前在系统中存在admin默认超管账户（有专人保管）；wangtao、tsuser为系统管理员账户（属于admin组），yangyuhao为安全管理员，yulili、wangcongcong为审计管理员，qinzhuowei、fengkun等8各个账户为普通用户。 |
| b）应重命名或删除默认账户，修改默认账户的默认口令； | 经现场核查360全流量威胁分析系统用户及权限策略，360全流量中默认账户admin未被重命名或删除，但是该账号由专人保管，并且用户口令已按照复杂度策略更改。 |
| 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； | 经现场访谈管理员及核查360全流量威胁分析系统用户管理，系统中用户admin、wangtao、tsuser、yangyuhao等用户均为有效账户，与管理人员一一对应，不存在多余、过期、共享账户。 |
| 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； | 经现场访谈管理员及核查360全流量威胁分析系统用户管理，360全流量中系统管理员、安全管理员、审计管理员、普通用户等，并按照各自角色赋予相应权限，实现管理用户权限分离及权限最小化。 |
| e）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； | 经核查及访谈网络管理员，360全流量威胁分析系统中由网络管理员角色账户为管理用户配置相应账号，并按照用户角色级别赋予管理用户操作权限。 |
| f）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； | 经核查及访谈网络管理员，360全流量威胁分析系统中访问控制策略为管理用户的360全流量威胁分析系统中配置管理界面等进行配置管理及访问管理等，访问控制粒度达到主体为用户级、客体为菜单级。 |
| g）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。 | 经核查及访谈网络管理员，360全流量威胁分析系统未对重要主体和客体设置安全标记。 |
| 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； | 经现场核查360全流量威胁分析系统日志审计功能，系统启用了日志审计功能，审计覆盖所有用户操作及系统安全事件等。 |
| 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； | 经现场核查360全流量威胁分析系统日志审计内容，360全流量威胁分析系统中用户访问日志包括：时间、用户、IP、级别、操作、结果等；系统升级日志包括：升级时间、组件、版本变更、升级结果等。 |
| 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、经现场核查360全流量威胁分析系统日志审计内容，所有用户均无权限将审计记录进行修改或删除，2、管理员配置审计记录备份策略，实时将审计记录备份至360本地安全大脑中进行备份保存，经现场核查360本地安全大脑中具备360全流量威胁分析系统审计记录，保存时间满足半年以上。 |
| d）应对审计进程进行保护，防止未经授权的中断。 | 经现场核查360全流量威胁分析系统日志审计进程，360全流量中审计进程受系统进程保护，所有用户均无权限将审计进程进行单独中断。 |
| 入侵防范 | a）应遵循最小安装的原则，仅安装需要的组件和应用程序； | 经访谈网络管理员及核查，360全流量威胁分析系统为厂商提供独立封装系统，不允许安装其他组件及应用程序，遵循最小安装原则。 |
| b）应关闭不需要的系统服务、默认共享和高危端口； | 经现场核查360全流量威胁分析系统配置策略，360全流量威胁分析系统中仅启用了SNMP、NTP、HTTPS等协议及服务器，Telnet协议已关闭，未启用不需要的系统服务、默认共享和高危端口。 |
| c）应通过设定终端接入方式或网络地址范围对通过网络进行管理的管理终端进行限制； | 经现场访谈安全管理员及核查，远程管理360全流量威胁分析系统时仅允许管理用户使用在办公网防火墙中启用VPN隧道连接到世纪互联IDC机房中，然后对360全流量威胁分析系统进行远程管理。 |
| d）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； | 该测评项测评对象为业务应用系统、中间件和系统管理软件，安全设备不适用。 |
| e）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； | 1、经访谈安全管理员，管理员定期对官方网站通报的安全漏洞进行评估，然后从官方网站下载安全补丁对360全流量进行补丁修复，避免系统中存在安全漏洞，2、经现场核查，360全流量系统最近补丁修复时间为2022年9月28日。 |
| f）应能够检测到对重要节点进行入侵的行为，并在发生严重入侵事件时提供报警。 | 经现场访谈安全管理员及核查360AISA全流量威胁分析系统安全策略，通过将被测系统中全部流量镜像发送到360AISA全流量威胁分析系统中进行分析监测，发现入侵事件后及时通过钉钉报警。 |
| 可信验证 | a）可基于可信根对计算设备的系统引导程序、系统程序、重要配置参数和应用程序等进行可信验证，并在应用程序的关键执行环节进行动态可信验证，在检测到其可信性受到破坏后进行报警，并将验证结果形成审计记录送至安全管理中心。 | 未基于可信根对计算设备提供可信验证。 |
| 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； | 经现场核查360全流量威胁分析系统通信方式，系统通过HTTPS协议进行通信，保证重要数据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。 | 经现场核查安全管理员，360全流量威胁分析系统通过厂商自身的加密技术保证用户鉴别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； | 经现场核查360全流量威胁分析系统通信方式，系统通过HTTPS协议进行通信，保证重要数据传输过程中的保密性。 |
| b）应采用密码技术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个人信息等。 | 经现场核查安全管理员，360全流量威胁分析系统通过厂商自身的加密技术保证用户鉴别信息等在存储过程中的保密性。 |
| 数据备份恢复 | a）应提供重要数据的本地数据备份与恢复功能； | 经现场访谈管理员及核查相应配置，在备份服务器中配置python脚本，并设置每天凌晨4点将交换机中配置文件下载至备份服务器中进行备份，管理员每周对备份文件进行巡检，确保配置文件完整备份至备份服务器中。 |
| b）应提供异地实时备份功能，利用通信网络将重要数据实时备份至备份场地； | 公司未对重要数据提供异地备份服务。 |
| c）应提供重要数据处理系统的热冗余，保证系统的高可用性。 | 经核查，重要数据处理系统中采用双机冗余部署，保证系统的高可用性。 |

4.1.2.4. 360本地安全大脑

|  |  |  |
| --- | --- | --- |
| **安全控制点** | **测评指标** | **结果记录** |
| 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、经现场访谈安全管理员及核查360本地安全大脑配置，360本地安全大脑采用用户名、口令进行身份鉴别和标识，360本地安全大脑具备用户名查重功能，保证用户名具有唯一性，经现场测试，创建重名用户时，会提示用户名已存在，2、经现场核查360本地安全大脑安全策略，其中口令最小长度为8位，包含大小写字母、数字、特殊字符四种组合，口令更换周期为90天。 |
| 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； | 经现场访谈安全管理员及核查360本地安全大脑配置，360本地安全大脑在安全策略中启用登录失败处理策略，用户连续错误登录5次锁定账户15分钟，设置空闲超时时间限制为600分钟。 |
| 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； | 经现场核查360本地安全大脑通信方式，360本地安全大脑在远程管理时采用HTTPS协议进行通信，防止鉴别信息在网络传输过程中被窃听。 |
| 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。 | 经现场核查360本地安全大脑身份鉴别方式，360本地安全大脑仅采用用户名、口令方式进行身份鉴别，未采用两种或两种以上组合的鉴别技术对用户进行身份鉴别。 |
| 访问控制 | a）应对登录的用户分配账户和权限； | 经现场访谈安全管理员及核查360本地安全大脑用户管理，360本地安全大脑由admin管理员对登录用户分配账户及赋予权限，目前在360本地安全大脑中存在admin默认超管账户，由专人保管；wangtao、huangfusheng为系统管理员，yulili、wangcongcong为安全审计员，yangyuhao为安全管理员，fengkun、zhangjixiang等共10个只读账户，用于查看监控大屏等。 |
| b）应重命名或删除默认账户，修改默认账户的默认口令； | 经现场核查360本地安全大脑中用户管理，360本地安全大脑中默认账户admin未被重命名或删除，但是该账号由专人保管，并且用户口令已按照复杂度策略更改。 |
| 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； | 经现场访谈管理员及核查360本地安全大脑用户管理，系统中用户admin、wangtao、yulili、wangcongcong等用户均为有效账户，与管理人员一一对应，不存在多余、过期、共享账户。 |
| 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； | 经现场访谈管理员及核查360本地安全大脑用户管理，360本地安全大脑中系统管理员、安全管理员、审计管理员、普通用户等，并按照各自角色赋予相应权限，实现管理用户权限分离及权限最小化。 |
| e）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； | 经核查及访谈网络管理员，360本地安全大脑中由网络管理员角色账户为管理用户配置相应账号，并按照用户角色级别赋予管理用户操作权限。 |
| f）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； | 经核查及访谈网络管理员，360本地安全大脑中访问控制策略为管理用户的360本地安全大脑中配置管理界面等进行配置管理及访问管理等，访问控制粒度达到主体为用户级、客体为菜单级。 |
| g）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。 | 经核查及访谈网络管理员，360本地安全大脑未对重要主体和客体设置安全标记。 |
| 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； | 经现场核查360本地安全大脑审计功能，360本地安全大脑启用了系统日志及更新日志，审计覆盖所有用户操作及系统安全事件等。 |
| 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； | 经现场核查360本地安全大脑审计内容，360本地安全大脑中系统日志包括：用户名、IP地址、描述、操作状态、操作结果、创建时间等，更新日志包括：升级时间、组件、版本变更、升级结果等。 |
| 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、经现场核查360本地安全大脑审计记录，所有用户均无权限将审计记录进行删除、修改，2、经访谈安全管理员，360本地安全大脑采用7个节点部署，并且对审计记录进行热备及冷备，现场查看360本地安全大脑磁盘空间仅占用4.62%，审计记录保存时间满足半年以上。 |
| d）应对审计进程进行保护，防止未经授权的中断。 | 经现场核查360本地安全大脑审计进程，360本地安全大脑中审计进程受系统进程保护，所有用户均无权限将审计进程进行单独中断。 |
| 入侵防范 | a）应遵循最小安装的原则，仅安装需要的组件和应用程序； | 经访谈网络管理员及核查配置文件，360本地安全大脑为厂商提供独立封装系统，不允许安装其他组件及应用程序，遵循最小安装原则。 |
| b）应关闭不需要的系统服务、默认共享和高危端口； | 经现场核查360本地安全大脑配置策略，360本地安全大脑中仅启用了SNMP、NTP、HTTPS等协议及服务器，Telnet协议已关闭，未启用不需要的系统服务、默认共享和高危端口。 |
| c）应通过设定终端接入方式或网络地址范围对通过网络进行管理的管理终端进行限制； | 经现场访谈安全管理员及核查，远程管理360本地安全大脑时仅允许管理用户使用在办公网防火墙中启用VPN隧道连接到世纪互联IDC机房中，然后对360本地安全大脑进行远程管理。 |
| d）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； | 该测评项测评对象为业务应用系统、中间件和系统管理软件，安全设备不适用。 |
| e）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； | 1、经访谈安全管理员，管理员定期对官方网站通报的安全漏洞进行评估，然后从官方网站下载安全补丁对360全流量进行补丁修复，避免系统中存在安全漏洞，2、经现场核查，360全流量系统最近补丁修复时间为2022年9月28日。 |
| f）应能够检测到对重要节点进行入侵的行为，并在发生严重入侵事件时提供报警。 | 经现场访谈安全管理员及核查，被测系统中部署了360AISA全流量威胁分析系统和360本地安全大脑，通过将被测系统中全部流量镜像发送到360AISA全流量威胁分析系统及360本地安全大脑中进行分析监测，发现入侵事件后及时通过钉钉报警，并且能够实现自动阻断。 |
| 可信验证 | a）可基于可信根对计算设备的系统引导程序、系统程序、重要配置参数和应用程序等进行可信验证，并在应用程序的关键执行环节进行动态可信验证，在检测到其可信性受到破坏后进行报警，并将验证结果形成审计记录送至安全管理中心。 | 未基于可信根对计算设备提供可信验证。 |
| 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； | 经现场核查360本地安全大脑通信方式，系统通过HTTPS协议进行通信，保证重要数据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。 | 经现场核查安全管理员，360本地安全大脑通过厂商自身的加密技术保证用户鉴别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； | 经现场核查360本地安全大脑通信方式，系统通过HTTPS协议进行通信，保证重要数据传输过程中的保密性。 |
| b）应采用密码技术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个人信息等。 | 经现场核查安全管理员，360本地安全大脑通过厂商自身的加密技术保证用户鉴别信息等在存储过程中的保密性。 |
| 数据备份恢复 | a）应提供重要数据的本地数据备份与恢复功能； | 经现场访谈管理员及核查相应配置，在备份服务器中配置python脚本，并设置每天凌晨4点将交换机中配置文件下载至备份服务器中进行备份，管理员每周对备份文件进行巡检，确保配置文件完整备份至备份服务器中。 |
| b）应提供异地实时备份功能，利用通信网络将重要数据实时备份至备份场地； | 公司未对重要数据提供异地备份服务。 |
| c）应提供重要数据处理系统的热冗余，保证系统的高可用性。 | 经核查，重要数据处理系统中采用双机冗余部署，保证系统的高可用性。 |

4.1.2.5. 360天擎

|  |  |  |
| --- | --- | --- |
| **安全控制点** | **测评指标** | **结果记录** |
| 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、经现场访谈安全管理员及核查360天擎配置，360天擎采用用户名、口令进行身份鉴别和标识，360天擎具备用户名查重功能，保证用户名具有唯一性，经现场测试，创建重名用户会提示用户名已存在，创建用户失败，2、现场核查360天擎中账户策略-密码策略，其中密码字符长度必须在8-32个字符，包含大小写字母、数字、特殊字符至少三种组合，密码有效期为90天。 |
| 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、经现场访谈安全管理员及核查360天擎配置，360天擎启用账户锁定策略，用户连续错误登录5次锁定账户30分钟； 2、已设置登录超时30分钟。 |
| 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； | 经现场核查360天擎登录方式，360天擎在远程管理时采用HTTPS协议进行通信，防止鉴别信息在网络传输过程中被窃听。 |
| 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。 | 经现场核查360天擎登录方式，360天擎仅采用用户名、口令方式进行身份鉴别，未采用两种或两种以上组合的鉴别技术对用户进行身份鉴别。 |
| 访问控制 | a）应对登录的用户分配账户和权限； | 经现场核查360天擎账号管理，360天擎由admin管理员对登录的账户进行权限分配，目前在360天擎中存在admin默认超管账户，由专人保管；safeadmin为审计管理员账户，wangtao为普通用户。 |
| b）应重命名或删除默认账户，修改默认账户的默认口令； | 经现场核查360天擎账号管理，360天擎中默认账户admin未被重命名或删除，但是该账号由专人保管，并且用户口令已按照复杂度策略更改。 |
| 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； | 经现场核查360天擎账号管理及访谈管理员，360天擎中目前有效账户为admin、safeadmin、sfadmin、txhw等账户，经访谈以上账户均与管理用户一一对应，不存在多余、过期、共享账户。 |
| 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； | 经现场核查360天擎账号管理及访谈管理员，360天擎中未单独创建系统管理员、安全管理员等账户，未实现管理用户权限分离。 |
| e）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； | 经核查配置文件及访谈，360天擎中由网络管理员角色账户为管理用户配置相应账号，并按照用户角色级别赋予管理用户操作权限。 |
| f）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； | 经核查配置文件及访谈，360天擎中访问控制策略为管理用户的交换机中配置文件等进行配置管理及访问管理等，访问控制粒度达到主体为用户级、客体为菜单级。 |
| g）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。 | 经核查配置文件及访谈，360天擎未对重要主体和客体设置安全标记。 |
| 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； | 经现场核查360天擎中系统日志菜单，包含管理员操作日志、系统升级日志等，审计覆盖所有用户操作及系统安全事件等。 |
| 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； | 经核查360天擎审计记录，360天擎中用户操作日志包括：时间、管理员、来源IP、事件类型、详细信息等；系统升级日志包括：时间、模块名、结果、升级版本等。 |
| 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、经核查360天擎审计记录，所有用户均无权限对审计记录进行修改或删除，2、管理员配置审计记录备份策略，实时将审计记录备份至360天擎中进行备份保存，经现场核查360天擎中具备360全流量威胁分析系统审计记录，保存时间满足半年以上。 |
| d）应对审计进程进行保护，防止未经授权的中断。 | 经核查360天擎审计进程，360天擎中审计进程受系统进程保护，所有用户均无权限将审计进程进行单独中断。 |
| 入侵防范 | a）应遵循最小安装的原则，仅安装需要的组件和应用程序； | 经访谈员及核查配置文件，360天擎为厂商提供独立封装系统，不允许安装其他组件及应用程序，遵循最小安装原则。 |
| b）应关闭不需要的系统服务、默认共享和高危端口； | 经现场核查360天擎配置策略，，360天擎中仅启用了HTTPS协议用于远程管理，Telnet协议已关闭，未启用不需要的系统服务、默认共享和高危端口。 |
| c）应通过设定终端接入方式或网络地址范围对通过网络进行管理的管理终端进行限制； | 经现场访谈管理员及核查，远程管理360天擎时仅允许管理用户通过办公网络进行访问。 |
| d）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； | 该测评项测评对象为业务应用系统、中间件和系统管理软件，安全设备不适用。 |
| e）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； | 1、经现场访谈安全管理员，管理员定期对官方网站通报的安全漏洞进行评估，然后从官方网站下载安全补丁对360天擎进行补丁修复，避免系统中存在安全漏洞，2、经现场核查，360天擎最近补丁修复时间为2022年10月16日。 |
| f）应能够检测到对重要节点进行入侵的行为，并在发生严重入侵事件时提供报警。 | 经现场访谈及核查，被测系统中部署了360AISA全流量威胁分析系统和360天擎，通过将被测系统中全部流量镜像发送到360AISA全流量威胁分析系统及360天擎中进行分析监测，发现入侵事件后及时通过钉钉报警，并且能够实现自动阻断。 |
| 可信验证 | a）可基于可信根对计算设备的系统引导程序、系统程序、重要配置参数和应用程序等进行可信验证，并在应用程序的关键执行环节进行动态可信验证，在检测到其可信性受到破坏后进行报警，并将验证结果形成审计记录送至安全管理中心。 | 未基于可信根对计算设备提供可信验证。 |
| 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； | 经现场核查360天擎通信方式，系统通过HTTPS协议进行通信，保证重要数据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。 | 经现场核查安全管理员，360天擎通过厂商自身的加密技术保证用户鉴别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； | 经现场核查360天擎通信方式，系统通过HTTPS协议进行通信，保证重要数据传输过程中的保密性。 |
| b）应采用密码技术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个人信息等。 | 经现场核查安全管理员，360天擎通过厂商自身的加密技术保证用户鉴别信息等在存储过程中的保密性。 |
| 数据备份恢复 | a）应提供重要数据的本地数据备份与恢复功能； | 经现场访谈管理员及核查相应配置，在备份服务器中配置python脚本，并设置每天凌晨4点将交换机中配置文件下载至备份服务器中进行备份，管理员每周对备份文件进行巡检，确保配置文件完整备份至备份服务器中。 |
| b）应提供异地实时备份功能，利用通信网络将重要数据实时备份至备份场地； | 公司未对重要数据提供异地备份服务。 |
| c）应提供重要数据处理系统的热冗余，保证系统的高可用性。 | 经核查，重要数据处理系统中采用双机冗余部署，保证系统的高可用性。 |

4.1.2.6. GOPR数据安全治理平台

|  |  |  |
| --- | --- | --- |
| **安全控制点** | **测评指标** | **结果记录** |
| 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、经现场访谈安全管理员及核查数据安全治理平台，数据治理平台采用用户名、口令进行身份鉴别和标识，数据治理平台具备用户名查重功能，保证用户名具有唯一性，经现场测试，创建重名用户会提示用户名已存在；2、经核查数据安全治理平台安全配置，其中密码策略为：口令长度范围为8-16位，包含大小写字母、数字三种组合，口令有效期为90天。 |
| 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； | 经现场访谈安全管理员及核查数据安全治理平台中暴力破解配置：登录失败周期5分钟，登录失败次数10次，锁定时间5分钟，2、会话超时退出时间30分钟。 |
| 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； | 经现场核查数据安全治理平台通信方式，数据治理平台在远程管理时采用HTTPS协议进行通信，防止鉴别信息在网络传输过程中被窃听。 |
| 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。 | 经现场核查数据安全治理平台登录方式，数据治理平台仅采用用户名、口令方式进行身份鉴别，未采用两种或两种以上组合的鉴别技术对用户进行身份鉴别。 |
| 访问控制 | a）应对登录的用户分配账户和权限； | 经现场核查数据安全治理平台用户管理，数据治理平台由admin管理员对登录的账户创建账户并分配权限，目前数据安全治理平台中存在admin默认超管账户，由专人保管；liuyuanhan、zhongqikul、yulili、jumana为业务管理员账户。 |
| b）应重命名或删除默认账户，修改默认账户的默认口令； | 经现场核查数据治理平台中用户管理配置，数据治理平台中默认账户admin未被重命名或删除，但是该账号由专人保管，并且用户口令已按照复杂度策略更改。 |
| 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； | 经现场核查数据治理平台中用户管理及访谈管理员，数据治理平台中目前有效账户为admin，liuyuanhan、zhongqikul、yulili、jumana为业务管理员账户，经访谈以上账户均与管理用户一一对应，不存在多余、过期、共享账户。 |
| 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； | 经现场核查数据治理平台管理及访谈管理员，数据治理平台中未单独创建系统管理员、安全管理员等账户，未实现管理用户权限分离。 |
| e）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； | 经核查配置文件及访谈，数据治理平台中由管理员角色账户为管理用户配置相应账号，并按照用户角色级别赋予管理用户操作权限。 |
| f）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； | 经核查配置文件及访谈，数据治理平台中访问控制策略为管理用户的数据治理平台中配置文件等进行配置管理及访问管理等，访问控制粒度达到主体为用户级、客体为菜单级。 |
| g）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。 | 经核查配置文件及访谈，数据治理平台未对重要主体和客体设置安全标记。 |
| 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； | 经现场核查数据安全治理平台审计功能，数据安全治理平台能够对用户操作行为、系统日志等进行审计记录。 |
| 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； | 经核查数据安全治理平台中审计记录，数据治理平台中操作日志包括：用户、操作IP、时间、日志类型、描述、结果等；系统审计日志包括：用户、访问IP、目标IP、访问时间、访问应用、访问域名、访问OS、访问浏览器、访问行为、访问接口、访问敏感数据等。 |
| 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、经核查数据安全治理平台审计记录，所有用户均无权限对审计记录进行修改或删除，2、管理员配置审计记录备份策略，实时将审计记录备份至360本地安全大脑中进行备份保存，经现场核查360本地安全大脑中具备数据安全治理平台审计记录，保存时间满足半年以上。 |
| d）应对审计进程进行保护，防止未经授权的中断。 | 经核查数据治理平台审计进程，数据治理平台中审计进程受系统进程保护，所有用户均无权限将审计进程进行单独中断。 |
| 入侵防范 | a）应遵循最小安装的原则，仅安装需要的组件和应用程序； | 经访谈及核查配置文件，数据治理平台为厂商提供独立封装系统，不允许安装其他组件及应用程序，遵循最小安装原则。 |
| b）应关闭不需要的系统服务、默认共享和高危端口； | 经现场核查，数据治理平台中仅启用了HTTPS协议用于远程管理，Telnet协议已关闭，未启用不需要的系统服务、默认共享和高危端口。 |
| c）应通过设定终端接入方式或网络地址范围对通过网络进行管理的管理终端进行限制； | 经现场访谈安全管理员及核查，远程管理数据安全治理平台时仅允许管理用户使用在办公网防火墙中启用VPN隧道连接到世纪互联IDC机房中，然后对数据安全治理平台进行远程管理。 |
| d）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； | 该测评项测评对象为业务应用系统、中间件和系统管理软件，安全设备不适用。 |
| e）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； | 经访谈管理员及核查数据安全治理平台升级策略，管理员定期对官方网站通报的安全漏洞进行评估，然后从官方网站下载安全补丁对数据治理平台进行补丁修复，避免系统中存在安全漏洞，经现场核查，数据治理平台最近补丁修复时间为2023年6月24日，系统版本为2.2，当前最新版本。 |
| f）应能够检测到对重要节点进行入侵的行为，并在发生严重入侵事件时提供报警。 | 经访谈网络管理员，被测系统中部署了360AISA全流量威胁分析系统和360本地安全大脑，通过将被测系统中全部流量镜像发送到360AISA全流量威胁分析系统及360本地安全大脑中进行分析监测，发现入侵事件后及时通过钉钉报警，并且能够自动阻断。 |
| 可信验证 | a）可基于可信根对计算设备的系统引导程序、系统程序、重要配置参数和应用程序等进行可信验证，并在应用程序的关键执行环节进行动态可信验证，在检测到其可信性受到破坏后进行报警，并将验证结果形成审计记录送至安全管理中心。 | 未基于可信根对计算设备提供可信验证。 |
| 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； | 经现场核查数据安全治理平台通信方式，系统通过HTTPS协议进行通信，保证重要数据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。 | 经现场核查安全管理员，数据安全治理平台通过厂商自身的加密技术保证用户鉴别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； | 经现场核查数据安全治理平台通信方式，系统通过HTTPS协议进行通信，保证重要数据传输过程中的保密性。 |
| b）应采用密码技术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个人信息等。 | 经现场核查安全管理员，数据安全治理平台通过厂商自身的加密技术保证用户鉴别信息等在存储过程中的保密性。 |
| 数据备份恢复 | a）应提供重要数据的本地数据备份与恢复功能； | 经现场访谈管理员及核查相应配置，目前通过集群方式部署，单个节点互为备份。 |
| b）应提供异地实时备份功能，利用通信网络将重要数据实时备份至备份场地； | 公司未对重要数据提供异地备份服务。 |
| c）应提供重要数据处理系统的热冗余，保证系统的高可用性。 | 经核查，重要数据处理系统中采用集群方式部署，保证系统的高可用性。 |

4.1.2.7. 出口防火墙1

|  |  |  |
| --- | --- | --- |
| **安全控制点** | **测评指标** | **结果记录** |
| 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、经现场访谈网络管理员，防火墙采用用户名、口令进行身份标识及身份鉴别；2、经核查防火墙配置，输入display password-control命令，返回信息为 Password aging:Enabled (90 days) Password length: Enabled (10 characters) Password composition:Enabled (3 types, 1 characters per type) Password history: Enabled (max history records:4)，通过返回信息确认：用户口令长度为至少10位，包含数字、字母、字符三种类型，用户口令更改周期为90天；3、通过现场在防火墙中创建与网络管理员ylops同名账户时，防火墙中会提示用户名已存在，无法创重名用户，确认用户标识具备唯一性。 |
| 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、经现场核查防火墙配置策略，输入display password-control命令，返回信息为 Maximum login attempts: 3，Action for exceeding login attempts: Lock user for 1 minutes、User authentication timeout：600 seconds；2、通过返回信息确认用户连续错误登录3次锁定账户1分钟，用户登录连接超时时间限制为600秒。 |
| 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； | 1、经现场访谈网络管理员及核查其远程连接防火墙的方式，管理员在远程管理防火墙时采用SSH协议或HTTPS协议进行通信，防止鉴别信息在网络传输过程中被窃听；2、访谈网络管理员，Telnet协议默认为关闭状态，通过输入命令telnet server enable尝试启用Telnet协议，返回信息为Telnet is insecure because it transmits data in plaintext form，Telnet协议未启成功；3，通过在终端Telnet该防火墙，无法连接成功。 |
| 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。 | 经现场核查网络管理员远程登录防火墙方式，防火墙仅采用用户名、口令方式进行身份鉴别，未采用两种或两种以上组合的鉴别技术对用户进行身份鉴别。 |
| 访问控制 | a）应对登录的用户分配账户和权限； | 1、经现场核查防火墙中用户信息，通过输入display local-user命令，返回信息中显示防火墙中存在security、tulei、xuweilai、ylops等用户，其中security的 user role list：level-1，network-operator；tulei、xuweilai、ylops的 user role list：network-admin,network-operator。 |
| b）应重命名或删除默认账户，修改默认账户的默认口令； | 1、经现场核查防火墙中用户信息，通过输入display local-user命令，返回信息中显示防火墙中存在security、tulei、xuweilai、ylops等用户,不存在默认账户，2、经核查防火墙配置，输入display password-control命令，返回信息为 Password aging:Enabled (90 days) Password length: Enabled (10 characters) Password composition:Enabled (3 types, 1 characters per type) Password history: Enabled (max history records：3、用户口令已按照复杂度策略更改。 |
| 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； | 经现场核查防火墙中用户信息，通过输入display local-user命令，返回信息中显示防火墙中存在security、tulei、xuweilai、ylops等用户,经访谈网络管理员，其中tulei、xuweilai为两位网络管理员账号，ylops为网络主管账户，security为安全管理账号，不存在多余、过期、共享账户。 |
| 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； | 经现场核查防火墙中用户信息，通过输入display local-user命令，返回信息中显示防火墙中存在security、tulei、xuweilai、ylops等用户，经访谈网络管理员，防火墙中未单独创建审计管理员账户，并且网络管理员权限为超管用户权限，未实现管理用户权限最小化及权限分离。 |
| e）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； | 经核查配置文件及访谈，防火墙中由网络管理员角色账户为管理用户配置相应账号，并按照用户角色级别赋予管理用户操作权限。 |
| f）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； | 经核查配置文件及访谈，防火墙中访问控制策略为管理用户的防火墙中配置文件等进行配置管理及访问管理等，访问控制粒度达到主体为用户级、客体为文件级。 |
| g）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。 | 经核查配置文件及访谈，防火墙未对重要主体和客体设置安全标记。 |
| 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； | 经现场访谈网络管理员及核查防火墙配置，输入命令display logbuffer reverse，返回信息为logbuffer:enable；确认防火墙中其中安全审计功能，通过查看审计记录内容，确认审计记录中包含设备运行记录及用户操作行为审计记录等。 |
| 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； | 经现场核查防火墙中审计记录内容，攻击日志包括：时间、严重级别、攻击类型、动作类型、入安全域名称、目的地址、源地址等；用户操作日志包括：日期、时间、协议类型、IP地址、用户、命令详情等。 |
| 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、经访谈网络管理员，防火墙中所有用户均无权限对审计记录进行删除或修改，并且管理员在备份服务器（10.33.110.160）中添加审计记录下载脚本（python脚本），实时将防火墙中审计记录下载至备份服务器中进行备份；2、经现场核查备份服务器（10.33.110.160）中/home/network\_backup目录中存在审计记录备份文件，备份文件宿主为root，权限为744，其他用户仅拥有读权限。 |
| d）应对审计进程进行保护，防止未经授权的中断。 | 经现场访谈网络管理员，防火墙中审计进程受系统进程保护，所有用户均无权限将审计进程单独中断。 |
| 入侵防范 | a）应遵循最小安装的原则，仅安装需要的组件和应用程序； | 经访谈及核查配置文件，防火墙为厂商提供独立封装系统，不允许安装其他组件及应用程序，遵循最小安装原则。 |
| b）应关闭不需要的系统服务、默认共享和高危端口； | 经现场访谈网络管理员及核查防火墙配置，输入display current-fonfiguration，返回信息HTTP、Telnet协议均已关闭，防火墙中未启用不需要的系统服务、默认共享及高危端口。 |
| c）应通过设定终端接入方式或网络地址范围对通过网络进行管理的管理终端进行限制； | 经访谈网络管理员，在防火墙中添加访问控制策略，仅允许管理用户通过堡垒机远程管理网络设备、安全设备及服务器等，经核查防火墙中访问控制策略，具备堡垒机地址-设备管理网段（10.33.0.0）的访问控制策略。 |
| d）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； | 该测评项测评对象为业务应用系统、中间件和系统管理软件，故将该项调整为不适用。 |
| e）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； | 1、经访谈网络管理员，会定期对官方网站通报的安全漏洞进行评估，然后从官方网站下载安全补丁，经过综合评估测试后对防火墙系统进行补丁修复，避免系统中存在安全漏洞，2、经现场漏洞扫描，未发现防火墙中存在安全漏洞。 |
| f）应能够检测到对重要节点进行入侵的行为，并在发生严重入侵事件时提供报警。 | 经现场访谈及核查防火墙配置策略，防火墙中具备安全防护功能，在防火墙导航菜单栏中安全防护菜单中启用攻击防护策略，能够对从外部发起的攻击行为进行监测，发现外部攻击行为及时报警。 |
| 可信验证 | a）可基于可信根对计算设备的系统引导程序、系统程序、重要配置参数和应用程序等进行可信验证，并在应用程序的关键执行环节进行动态可信验证，在检测到其可信性受到破坏后进行报警，并将验证结果形成审计记录送至安全管理中心。 | 未基于可信根对计算设备提供可信验证。 |
| 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； | 经现场访谈网络管理员及对防火墙配置，防火墙中关闭Telnet协议，采用SSH协议或HTTPS协议进行通信，保证重要数据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。 | 经访谈网络管理员及核查H3C SecPath F1000系列防火墙产品文档，文件中目录05-参考指南--05文件系统管理命令中包含：“防火墙中文件系统通常使用摘要算法（SHA-256）对文件计算摘要值，用于验证文件的正确性和完整性”。 |
| 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； | 经现场访谈网络管理员及对防火墙配置，防火墙中关闭Telnet协议，采用SSH协议或HTTPS协议进行通信，保证重要数据在传输过程中的保密性。 |
| b）应采用密码技术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个人信息等。 | 经访谈网管理员，管理员在设置用户口令时添加simple参数，经核查H3C SecPath F1000系列防火墙产品文档，在文档05-参考指南--03-登录设备命令--1、登录设备--1.1等设备命令--1.1.28 set authentication password中正对simple参数进行说明：“simple：以明文方式设置密码，该密码将以密文方式存储。 |
| 数据备份恢复 | a）应提供重要数据的本地数据备份与恢复功能； | 经现场访谈网络管理员及核查相应配置，在备份服务器中配置python脚本，并设置每天凌晨4点将防火墙中配置文件下载至备份服务器中进行备份，管理员每周对备份文件进行巡检，确保配置文件完整备份至备份服务器中。 |
| b）应提供异地实时备份功能，利用通信网络将重要数据实时备份至备份场地； | 1、经现场访谈网络管理员，管理员添加了数据同步策略，每天将备份服务器中备份文件拷贝至阿里公共云备份服务器中进行备份；2、经核查阿里公共云备份服务器（10.30.19.10）中备份目录/data/network-backup中具备网络设备配置备份文件；3、综上，因世纪互联IDC机房及阿里云公共云均在上海市，未实现异地实时备份功能。 |
| c）应提供重要数据处理系统的热冗余，保证系统的高可用性。 | 经访谈访问管理员及核查网络拓扑图，重要数据处理系统中采用双机冗余部署，保证系统的高可用性。 |

4.1.2.8. 出口防火墙2

|  |  |  |
| --- | --- | --- |
| **安全控制点** | **测评指标** | **结果记录** |
| 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、经现场访谈网络管理员，防火墙采用用户名、口令进行身份标识及身份鉴别；2、经核查防火墙配置，输入display password-control命令，返回信息为 Password aging:Enabled (90 days) Password length: Enabled (10 characters) Password composition:Enabled (3 types, 1 characters per type) Password history: Enabled (max history records:4)，通过返回信息确认：用户口令长度为至少10位，包含数字、字母、字符三种类型，用户口令更改周期为90天；3、通过现场在防火墙中创建与网络管理员ylops同名账户时，防火墙中会提示用户名已存在，无法创重名用户，确认用户标识具备唯一性。 |
| 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、经现场核查防火墙配置策略，输入display password-control命令，返回信息为 Maximum login attempts: 3，Action for exceeding login attempts: Lock user for 1 minutes、User authentication timeout：600 seconds；2、通过返回信息确认用户连续错误登录3次锁定账户1分钟，用户登录连接超时时间限制为600秒。 |
| 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； | 1、经现场访谈网络管理员及核查其远程连接防火墙的方式，管理员在远程管理防火墙时采用SSH协议或HTTPS协议进行通信，防止鉴别信息在网络传输过程中被窃听；2、访谈网络管理员，Telnet协议默认为关闭状态，通过输入命令telnet server enable尝试启用Telnet协议，返回信息为Telnet is insecure because it transmits data in plaintext form，Telnet协议未启成功；3，通过在终端Telnet该防火墙，无法连接成功。 |
| 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。 | 经现场核查网络管理员远程登录防火墙方式，防火墙仅采用用户名、口令方式进行身份鉴别，未采用两种或两种以上组合的鉴别技术对用户进行身份鉴别。 |
| 访问控制 | a）应对登录的用户分配账户和权限； | 1、经现场核查防火墙中用户信息，通过输入display local-user命令，返回信息中显示防火墙中存在security、tulei、xuweilai、ylops等用户，其中security的 user role list：level-1，network-operator；tulei、xuweilai、ylops的 user role list：network-admin,network-operator。 |
| b）应重命名或删除默认账户，修改默认账户的默认口令； | 1、经现场核查防火墙中用户信息，通过输入display local-user命令，返回信息中显示防火墙中存在security、tulei、xuweilai、ylops等用户,不存在默认账户，2、经核查防火墙配置，输入display password-control命令，返回信息为 Password aging:Enabled (90 days) Password length: Enabled (10 characters) Password composition:Enabled (3 types, 1 characters per type) Password history: Enabled (max history records：3、用户口令已按照复杂度策略更改。 |
| 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； | 经现场核查防火墙中用户信息，通过输入display local-user命令，返回信息中显示防火墙中存在security、tulei、xuweilai、ylops等用户,经访谈网络管理员，其中tulei、xuweilai为两位网络管理员账号，ylops为网络主管账户，security为安全管理账号，不存在多余、过期、共享账户。 |
| 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； | 经现场核查防火墙中用户信息，通过输入display local-user命令，返回信息中显示防火墙中存在security、tulei、xuweilai、ylops等用户，经访谈网络管理员，防火墙中未单独创建审计管理员账户，并且网络管理员权限为超管用户权限，未实现管理用户权限最小化及权限分离。 |
| e）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； | 经核查配置文件及访谈，防火墙中由网络管理员角色账户为管理用户配置相应账号，并按照用户角色级别赋予管理用户操作权限。 |
| f）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； | 经核查配置文件及访谈，防火墙中访问控制策略为管理用户的防火墙中配置文件等进行配置管理及访问管理等，访问控制粒度达到主体为用户级、客体为文件级。 |
| g）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。 | 经核查配置文件及访谈，防火墙未对重要主体和客体设置安全标记。 |
| 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； | 经现场访谈网络管理员及核查防火墙配置，输入命令display logbuffer reverse，返回信息为logbuffer:enable；确认防火墙中其中安全审计功能，通过查看审计记录内容，确认审计记录中包含设备运行记录及用户操作行为审计记录等。 |
| 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； | 经现场核查防火墙中审计记录内容，攻击日志包括：时间、严重级别、攻击类型、动作类型、入安全域名称、目的地址、源地址等；用户操作日志包括：日期、时间、协议类型、IP地址、用户、命令详情等。 |
| 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、经访谈网络管理员，防火墙中所有用户均无权限对审计记录进行删除或修改，并且管理员在备份服务器（10.33.110.160）中添加审计记录下载脚本（python脚本），实时将防火墙中审计记录下载至备份服务器中进行备份；2、经现场核查备份服务器（10.33.110.160）中/home/network\_backup目录中存在审计记录备份文件，备份文件宿主为root，权限为744，其他用户仅拥有读权限。 |
| d）应对审计进程进行保护，防止未经授权的中断。 | 经现场访谈网络管理员，防火墙中审计进程受系统进程保护，所有用户均无权限将审计进程单独中断。 |
| 入侵防范 | a）应遵循最小安装的原则，仅安装需要的组件和应用程序； | 经访谈及核查配置文件，防火墙为厂商提供独立封装系统，不允许安装其他组件及应用程序，遵循最小安装原则。 |
| b）应关闭不需要的系统服务、默认共享和高危端口； | 经现场访谈网络管理员及核查防火墙配置，输入display current-fonfiguration，返回信息HTTP、Telnet协议均已关闭，防火墙中未启用不需要的系统服务、默认共享及高危端口。 |
| c）应通过设定终端接入方式或网络地址范围对通过网络进行管理的管理终端进行限制； | 经访谈网络管理员，在防火墙中添加访问控制策略，仅允许管理用户通过堡垒机远程管理网络设备、安全设备及服务器等，经核查防火墙中访问控制策略，具备堡垒机地址-设备管理网段（10.33.0.0）的访问控制策略。 |
| d）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； | 该测评项测评对象为业务应用系统、中间件和系统管理软件，故将该项调整为不适用。 |
| e）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； | 1、经访谈网络管理员，会定期对官方网站通报的安全漏洞进行评估，然后从官方网站下载安全补丁，经过综合评估测试后对防火墙系统进行补丁修复，避免系统中存在安全漏洞，2、经现场漏洞扫描，未发现防火墙中存在安全漏洞。 |
| f）应能够检测到对重要节点进行入侵的行为，并在发生严重入侵事件时提供报警。 | 经现场访谈及核查防火墙配置策略，防火墙中具备安全防护功能，在防火墙导航菜单栏中安全防护菜单中启用攻击防护策略，能够对从外部发起的攻击行为进行监测，发现外部攻击行为及时报警。 |
| 可信验证 | a）可基于可信根对计算设备的系统引导程序、系统程序、重要配置参数和应用程序等进行可信验证，并在应用程序的关键执行环节进行动态可信验证，在检测到其可信性受到破坏后进行报警，并将验证结果形成审计记录送至安全管理中心。 | 未基于可信根对计算设备提供可信验证。 |
| 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； | 经现场访谈网络管理员及对防火墙配置，防火墙中关闭Telnet协议，采用SSH协议或HTTPS协议进行通信，保证重要数据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。 | 经访谈网络管理员及核查H3C SecPath F1000系列防火墙产品文档，文件中目录05-参考指南--05文件系统管理命令中包含：“防火墙中文件系统通常使用摘要算法（SHA-256）对文件计算摘要值，用于验证文件的正确性和完整性”。 |
| 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； | 经现场访谈网络管理员及对防火墙配置，防火墙中关闭Telnet协议，采用SSH协议或HTTPS协议进行通信，保证重要数据在传输过程中的保密性。 |
| b）应采用密码技术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个人信息等。 | 经访谈网管理员，管理员在设置用户口令时添加simple参数，经核查H3C SecPath F1000系列防火墙产品文档，在文档05-参考指南--03-登录设备命令--1、登录设备--1.1等设备命令--1.1.28 set authentication password中正对simple参数进行说明：“simple：以明文方式设置密码，该密码将以密文方式存储。 |
| 数据备份恢复 | a）应提供重要数据的本地数据备份与恢复功能； | 经现场访谈网络管理员及核查相应配置，在备份服务器中配置python脚本，并设置每天凌晨4点将防火墙中配置文件下载至备份服务器中进行备份，管理员每周对备份文件进行巡检，确保配置文件完整备份至备份服务器中。 |
| b）应提供异地实时备份功能，利用通信网络将重要数据实时备份至备份场地； | 1、经现场访谈网络管理员，管理员添加了数据同步策略，每天将备份服务器中备份文件拷贝至阿里公共云备份服务器中进行备份；2、经核查阿里公共云备份服务器（10.30.19.10）中备份目录/data/network-backup中具备网络设备配置备份文件；3、综上，因世纪互联IDC机房及阿里云公共云均在上海市，未实现异地实时备份功能。 |
| c）应提供重要数据处理系统的热冗余，保证系统的高可用性。 | 经访谈访问管理员及核查网络拓扑图，重要数据处理系统中采用双机冗余部署，保证系统的高可用性。 |

4.1.2.9. 专线防火墙1

|  |  |  |
| --- | --- | --- |
| **安全控制点** | **测评指标** | **结果记录** |
| 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、经现场访谈网络管理员，防火墙采用用户名、口令进行身份标识及身份鉴别；2、经核查防火墙配置，输入display password-control命令，返回信息为 Password aging:Enabled (90 days) Password length: Enabled (10 characters) Password composition:Enabled (3 types, 1 characters per type) Password history: Enabled (max history records:4)，通过返回信息确认：用户口令长度为至少10位，包含数字、字母、字符三种类型，用户口令更改周期为90天；3、通过现场在防火墙中创建与网络管理员ylops同名账户时，防火墙中会提示用户名已存在，无法创重名用户，确认用户标识具备唯一性。 |
| 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、经现场核查防火墙配置策略，输入display password-control命令，返回信息为 Maximum login attempts: 3，Action for exceeding login attempts: Lock user for 1 minutes、User authentication timeout：600 seconds；2、通过返回信息确认用户连续错误登录3次锁定账户1分钟，用户登录连接超时时间限制为600秒。 |
| 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； | 1、经现场访谈网络管理员及核查其远程连接防火墙的方式，管理员在远程管理防火墙时采用SSH协议或HTTPS协议进行通信，防止鉴别信息在网络传输过程中被窃听； 2、访谈网络管理员，Telnet 服务已关闭，通过SSH协议访问，访问时通过AAA认证服务器用户认证、审计。通过图形管理界面远程连接采用HTTPS协议。 |
| 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。 | 经现场核查网络管理员远程登录防火墙方式，防火墙仅采用用户名、口令方式进行身份鉴别，未采用两种或两种以上组合的鉴别技术对用户进行身份鉴别。 |
| 访问控制 | a）应对登录的用户分配账户和权限； | 1、经现场核查防火墙中用户信息，通过输入display local-user命令，返回信息中显示防火墙中存在security、tulei、xuweilai、ylops等用户，其中security的 user role list：level-1，network-operator；tulei、xuweilai、ylops的 user role list：network-admin,network-operator。 |
| b）应重命名或删除默认账户，修改默认账户的默认口令； | 1、经现场核查防火墙中用户信息，通过输入display local-user命令，返回信息中显示防火墙中存在security、tulei、xuweilai、ylops等用户,不存在默认账户，2、经核查防火墙配置，输入display password-control命令，返回信息为 Password aging:Enabled (90 days) Password length: Enabled (10 characters) Password composition:Enabled (3 types, 1 characters per type) Password history: Enabled (max history records：3、用户口令已按照复杂度策略更改。 |
| 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； | 经现场核查防火墙中用户信息，通过输入display local-user命令，返回信息中显示防火墙中存在security、tulei、xuweilai、ylops等用户,经访谈网络管理员，其中tulei、xuweilai为两位网络管理员账号，ylops为网络主管账户，security为安全管理账号，不存在多余、过期、共享账户。 |
| 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； | 经现场核查防火墙中用户信息，通过输入display local-user命令，返回信息中显示防火墙中存在security、tulei、xuweilai、ylops等用户，经访谈网络管理员，防火墙中未单独创建审计管理员账户，并且网络管理员权限为超管用户权限，未实现管理用户权限最小化及权限分离。 |
| e）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； | 经核查配置文件及访谈，防火墙中由网络管理员角色账户为管理用户配置相应账号，并按照用户角色级别赋予管理用户操作权限。 |
| f）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； | 经核查配置文件及访谈，防火墙中访问控制策略为管理用户的防火墙中配置文件等进行配置管理及访问管理等，访问控制粒度达到主体为用户级、客体为文件级。 |
| g）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。 | 经核查配置文件及访谈，防火墙未对重要主体和客体设置安全标记。 |
| 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； | 经现场访谈网络管理员及核查防火墙配置，输入命令display logbuffer reverse，返回信息为logbuffer:enable；确认防火墙中启用安全审计功能，通过查看审计记录内容，确认审计记录中包含设备运行记录及用户操作行为审计记录等。 |
| 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； | 经现场核查防火墙中审计记录内容，攻击日志包括：时间、严重级别、攻击类型、动作类型、入安全域名称、目的地址、源地址等；用户操作日志包括：日期、时间、协议类型、IP地址、用户、命令详情等。 |
| 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、经访谈网络管理员，防火墙中所有用户均无权限对审计记录进行删除或修改，并且管理员在备份服务器（10.33.110.160）中添加审计记录下载脚本（python脚本），实时将防火墙中审计记录下载至备份服务器中进行备份；2、经现场核查备份服务器（10.33.110.160）中/home/network\_backup目录中存在审计记录备份文件，备份文件宿主为root，权限为744，其他用户仅拥有读权限。 |
| d）应对审计进程进行保护，防止未经授权的中断。 | 经现场访谈网络管理员，防火墙中审计进程受系统进程保护，所有用户均无权限将审计进程单独中断。 |
| 入侵防范 | a）应遵循最小安装的原则，仅安装需要的组件和应用程序； | 经访谈及核查配置文件，防火墙为厂商提供独立封装系统，不允许安装其他组件及应用程序，遵循最小安装原则。 |
| b）应关闭不需要的系统服务、默认共享和高危端口； | 经现场访谈网络管理员及核查防火墙配置，输入display current-fonfiguration，返回信息HTTP、Telnet协议均已关闭，防火墙中未启用不需要的系统服务、默认共享及高危端口。 |
| c）应通过设定终端接入方式或网络地址范围对通过网络进行管理的管理终端进行限制； | 经访谈网络管理员，在防火墙中添加访问控制策略，仅允许管理用户通过堡垒机远程管理网络设备、安全设备及服务器等，经核查防火墙中访问控制策略，具备堡垒机地址-设备管理网段（10.33.0.0）的访问控制策略。 |
| d）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； | 该测评项测评对象为业务应用系统、中间件和系统管理软件，故将该项调整为不适用。 |
| e）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； | 1、经访谈网络管理员，会定期对官方网站通报的安全漏洞进行评估，然后从官方网站下载安全补丁，经过综合评估测试后对防火墙系统进行补丁修复，避免系统中存在安全漏洞，2、经现场漏洞扫描，未发现防火墙中存在安全漏洞。 |
| f）应能够检测到对重要节点进行入侵的行为，并在发生严重入侵事件时提供报警。 | 经现场访谈及核查防火墙配置策略，防火墙中具备安全防护功能，在防火墙导航菜单栏中安全防护菜单中启用攻击防护策略，能够对从外部发起的攻击行为进行监测，发现外部攻击行为及时报警。 |
| 可信验证 | a）可基于可信根对计算设备的系统引导程序、系统程序、重要配置参数和应用程序等进行可信验证，并在应用程序的关键执行环节进行动态可信验证，在检测到其可信性受到破坏后进行报警，并将验证结果形成审计记录送至安全管理中心。 | 未基于可信根对计算设备提供可信验证。 |
| 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； | 经现场访谈网络管理员及对防火墙配置，防火墙中关闭Telnet协议，采用SSH协议或HTTPS协议进行通信，保证重要数据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。 | 经访谈网络管理员及核查H3C SecPath F1000系列防火墙产品文档，文件中目录05-参考指南--05文件系统管理命令中包含：“防火墙中文件系统通常使用摘要算法（SHA-256）对文件计算摘要值，用于验证文件的正确性和完整性”。 |
| 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； | 经现场访谈网络管理员及对防火墙配置，防火墙中关闭Telnet协议，采用SSH协议或HTTPS协议进行通信，保证重要数据在传输过程中的保密性。 |
| b）应采用密码技术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个人信息等。 | 经访谈网管理员，管理员在设置用户口令时添加simple参数，经核查H3C SecPath F1000系列防火墙产品文档，在文档05-参考指南--03-登录设备命令--1、登录设备--1.1等设备命令--1.1.28 set authentication password中正对simple参数进行说明：“simple：以明文方式设置密码，该密码将以密文方式存储。 |
| 数据备份恢复 | a）应提供重要数据的本地数据备份与恢复功能； | 经现场访谈网络管理员及核查相应配置，在备份服务器中配置python脚本，并设置每天凌晨4点将防火墙中配置文件下载至备份服务器中进行备份，管理员每周对备份文件进行巡检，确保配置文件完整备份至备份服务器中。 |
| b）应提供异地实时备份功能，利用通信网络将重要数据实时备份至备份场地； | 1、经现场访谈网络管理员，管理员添加了数据同步策略，每天将备份服务器中备份文件拷贝至阿里公共云备份服务器中进行备份；2、经核查阿里公共云备份服务器（10.30.19.10）中备份目录/data/network-backup中具备网络设备配置备份文件；3、综上，因世纪互联IDC机房及阿里云公共云均在上海市，未实现异地实时备份功能。 |
| c）应提供重要数据处理系统的热冗余，保证系统的高可用性。 | 经访谈访问管理员及核查网络拓扑图，重要数据处理系统中采用双机冗余部署，保证系统的高可用性。 |

4.1.2.10. 专线防火墙2

|  |  |  |
| --- | --- | --- |
| **安全控制点** | **测评指标** | **结果记录** |
| 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、经现场访谈网络管理员，防火墙采用用户名、口令进行身份标识及身份鉴别；2、经核查防火墙配置，输入display password-control命令，返回信息为 Password aging:Enabled (90 days) Password length: Enabled (10 characters) Password composition:Enabled (3 types, 1 characters per type) Password history: Enabled (max history records:4)，通过返回信息确认：用户口令长度为至少10位，包含数字、字母、字符三种类型，用户口令更改周期为90天；3、通过现场在防火墙中创建与网络管理员ylops同名账户时，防火墙中会提示用户名已存在，无法创重名用户，确认用户标识具备唯一性。 |
| 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、经现场核查防火墙配置策略，输入display password-control命令，返回信息为 Maximum login attempts: 3，Action for exceeding login attempts: Lock user for 1 minutes、User authentication timeout：600 seconds；2、通过返回信息确认用户连续错误登录3次锁定账户1分钟，用户登录连接超时时间限制为600秒。 |
| 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； | 1、经现场访谈网络管理员及核查其远程连接防火墙的方式，管理员在远程管理防火墙时采用SSH协议或HTTPS协议进行通信，防止鉴别信息在网络传输过程中被窃听； 2、访谈网络管理员，Telnet 服务已关闭，通过SSH协议访问，访问时通过AAA认证服务器用户认证、审计。通过图形管理界面远程连接采用HTTPS协议。 |
| 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。 | 经现场核查网络管理员远程登录防火墙方式，防火墙仅采用用户名、口令方式进行身份鉴别，未采用两种或两种以上组合的鉴别技术对用户进行身份鉴别。 |
| 访问控制 | a）应对登录的用户分配账户和权限； | 1、经现场核查防火墙中用户信息，通过输入display local-user命令，返回信息中显示防火墙中存在security、tulei、xuweilai、ylops等用户，其中security的 user role list：level-1，network-operator；tulei、xuweilai、ylops的 user role list：network-admin,network-operator。 |
| b）应重命名或删除默认账户，修改默认账户的默认口令； | 1、经现场核查防火墙中用户信息，通过输入display local-user命令，返回信息中显示防火墙中存在security、tulei、xuweilai、ylops等用户,不存在默认账户，2、经核查防火墙配置，输入display password-control命令，返回信息为 Password aging:Enabled (90 days) Password length: Enabled (10 characters) Password composition:Enabled (3 types, 1 characters per type) Password history: Enabled (max history records：3、用户口令已按照复杂度策略更改。 |
| 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； | 经现场核查防火墙中用户信息，通过输入display local-user命令，返回信息中显示防火墙中存在security、tulei、xuweilai、ylops等用户,经访谈网络管理员，其中tulei、xuweilai为两位网络管理员账号，ylops为网络主管账户，security为安全管理账号，不存在多余、过期、共享账户。 |
| 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； | 经现场核查防火墙中用户信息，通过输入display local-user命令，返回信息中显示防火墙中存在security、tulei、xuweilai、ylops等用户，经访谈网络管理员，防火墙中未单独创建审计管理员账户，并且网络管理员权限为超管用户权限，未实现管理用户权限最小化及权限分离。 |
| e）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； | 经核查配置文件及访谈，防火墙中由网络管理员角色账户为管理用户配置相应账号，并按照用户角色级别赋予管理用户操作权限。 |
| f）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； | 经核查配置文件及访谈，防火墙中访问控制策略为管理用户的防火墙中配置文件等进行配置管理及访问管理等，访问控制粒度达到主体为用户级、客体为文件级。 |
| g）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。 | 经核查配置文件及访谈，防火墙未对重要主体和客体设置安全标记。 |
| 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； | 经现场访谈网络管理员及核查防火墙配置，输入命令display logbuffer reverse，返回信息为logbuffer:enable；确认防火墙中启用安全审计功能，通过查看审计记录内容，确认审计记录中包含设备运行记录及用户操作行为审计记录等。 |
| 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； | 经现场核查防火墙中审计记录内容，攻击日志包括：时间、严重级别、攻击类型、动作类型、入安全域名称、目的地址、源地址等；用户操作日志包括：日期、时间、协议类型、IP地址、用户、命令详情等。 |
| 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、经访谈网络管理员，防火墙中所有用户均无权限对审计记录进行删除或修改，并且管理员在备份服务器（10.33.110.160）中添加审计记录下载脚本（python脚本），实时将防火墙中审计记录下载至备份服务器中进行备份；2、经现场核查备份服务器（10.33.110.160）中/home/network\_backup目录中存在审计记录备份文件，备份文件宿主为root，权限为744，其他用户仅拥有读权限。 |
| d）应对审计进程进行保护，防止未经授权的中断。 | 经现场访谈网络管理员，防火墙中审计进程受系统进程保护，所有用户均无权限将审计进程单独中断。 |
| 入侵防范 | a）应遵循最小安装的原则，仅安装需要的组件和应用程序； | 经访谈及核查配置文件，防火墙为厂商提供独立封装系统，不允许安装其他组件及应用程序，遵循最小安装原则。 |
| b）应关闭不需要的系统服务、默认共享和高危端口； | 经现场访谈网络管理员及核查防火墙配置，输入display current-fonfiguration，返回信息HTTP、Telnet协议均已关闭，防火墙中未启用不需要的系统服务、默认共享及高危端口。 |
| c）应通过设定终端接入方式或网络地址范围对通过网络进行管理的管理终端进行限制； | 经访谈网络管理员，在防火墙中添加访问控制策略，仅允许管理用户通过堡垒机远程管理网络设备、安全设备及服务器等，经核查防火墙中访问控制策略，具备堡垒机地址-设备管理网段（10.33.0.0）的访问控制策略。 |
| d）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； | 该测评项测评对象为业务应用系统、中间件和系统管理软件，故将该项调整为不适用。 |
| e）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； | 1、经访谈网络管理员，会定期对官方网站通报的安全漏洞进行评估，然后从官方网站下载安全补丁，经过综合评估测试后对防火墙系统进行补丁修复，避免系统中存在安全漏洞，2、经现场漏洞扫描，未发现防火墙中存在安全漏洞。 |
| f）应能够检测到对重要节点进行入侵的行为，并在发生严重入侵事件时提供报警。 | 经现场访谈及核查防火墙配置策略，防火墙中具备安全防护功能，在防火墙导航菜单栏中安全防护菜单中启用攻击防护策略，能够对从外部发起的攻击行为进行监测，发现外部攻击行为及时报警。 |
| 可信验证 | a）可基于可信根对计算设备的系统引导程序、系统程序、重要配置参数和应用程序等进行可信验证，并在应用程序的关键执行环节进行动态可信验证，在检测到其可信性受到破坏后进行报警，并将验证结果形成审计记录送至安全管理中心。 | 未基于可信根对计算设备提供可信验证。 |
| 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； | 经现场访谈网络管理员及对防火墙配置，防火墙中关闭Telnet协议，采用SSH协议或HTTPS协议进行通信，保证重要数据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。 | 经访谈网络管理员及核查H3C SecPath F1000系列防火墙产品文档，文件中目录05-参考指南--05文件系统管理命令中包含：“防火墙中文件系统通常使用摘要算法（SHA-256）对文件计算摘要值，用于验证文件的正确性和完整性”。 |
| 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； | 经现场访谈网络管理员及对防火墙配置，防火墙中关闭Telnet协议，采用SSH协议或HTTPS协议进行通信，保证重要数据在传输过程中的保密性。 |
| b）应采用密码技术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个人信息等。 | 经访谈网管理员，管理员在设置用户口令时添加simple参数，经核查H3C SecPath F1000系列防火墙产品文档，在文档05-参考指南--03-登录设备命令--1、登录设备--1.1等设备命令--1.1.28 set authentication password中正对simple参数进行说明：“simple：以明文方式设置密码，该密码将以密文方式存储。 |
| 数据备份恢复 | a）应提供重要数据的本地数据备份与恢复功能； | 经现场访谈网络管理员及核查相应配置，在备份服务器中配置python脚本，并设置每天凌晨4点将防火墙中配置文件下载至备份服务器中进行备份，管理员每周对备份文件进行巡检，确保配置文件完整备份至备份服务器中。 |
| b）应提供异地实时备份功能，利用通信网络将重要数据实时备份至备份场地； | 1、经现场访谈网络管理员，管理员添加了数据同步策略，每天将备份服务器中备份文件拷贝至阿里公共云备份服务器中进行备份；2、经核查阿里公共云备份服务器（10.30.19.10）中备份目录/data/network-backup中具备网络设备配置备份文件；3、综上，因世纪互联IDC机房及阿里云公共云均在上海市，未实现异地实时备份功能。 |
| c）应提供重要数据处理系统的热冗余，保证系统的高可用性。 | 经访谈访问管理员及核查网络拓扑图，重要数据处理系统中采用双机冗余部署，保证系统的高可用性。 |

4.1.2.11. 管理网防火墙1

|  |  |  |
| --- | --- | --- |
| **安全控制点** | **测评指标** | **结果记录** |
| 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、经现场访谈网络管理员，防火墙采用用户名、口令进行身份标识及身份鉴别；2、经核查防火墙配置，输入display password-control命令，返回信息为 Password aging:Enabled (90 days) Password length: Enabled (10 characters) Password composition:Enabled (3 types, 1 characters per type) Password history: Enabled (max history records:4)，通过返回信息确认：用户口令长度为至少10位，包含数字、字母、字符三种类型，用户口令更改周期为90天；3、通过现场在防火墙中创建与网络管理员ylops同名账户时，防火墙中会提示用户名已存在，无法创重名用户，确认用户标识具备唯一性。 |
| 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、经现场核查防火墙配置策略，输入display password-control命令，返回信息为 Maximum login attempts: 3，Action for exceeding login attempts: Lock user for 1 minutes、User authentication timeout：600 seconds；2、通过返回信息确认用户连续错误登录3次锁定账户1分钟，用户登录连接超时时间限制为600秒。 |
| 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； | 1、经现场访谈网络管理员及核查其远程连接防火墙的方式，管理员在远程管理防火墙时采用SSH协议或HTTPS协议进行通信，防止鉴别信息在网络传输过程中被窃听；2、访谈网络管理员，Telnet协议默认为关闭状态，通过输入命令telnet server enable尝试启用Telnet协议，返回信息为Telnet is insecure because it transmits data in plaintext form，Telnet协议未启成功；3，通过在终端Telnet该防火墙，无法连接成功。 |
| 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。 | 经现场核查网络管理员远程登录防火墙方式，防火墙仅采用用户名、口令方式进行身份鉴别，未采用两种或两种以上组合的鉴别技术对用户进行身份鉴别。 |
| 访问控制 | a）应对登录的用户分配账户和权限； | 1、经现场核查防火墙中用户信息，通过输入display local-user命令，返回信息中显示防火墙中存在security、tulei、xuweilai、ylops等用户，其中security的 user role list：level-1，network-operator；tulei、xuweilai、ylops的 user role list：network-admin,network-operator。 |
| b）应重命名或删除默认账户，修改默认账户的默认口令； | 1、经现场核查防火墙中用户信息，通过输入display local-user命令，返回信息中显示防火墙中存在security、tulei、xuweilai、ylops等用户,不存在默认账户，2、经核查防火墙配置，输入display password-control命令，返回信息为 Password aging:Enabled (90 days) Password length: Enabled (10 characters) Password composition:Enabled (3 types, 1 characters per type) Password history: Enabled (max history records：3、用户口令已按照复杂度策略更改。 |
| 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； | 经现场核查防火墙中用户信息，通过输入display local-user命令，返回信息中显示防火墙中存在security、tulei、xuweilai、ylops等用户,经访谈网络管理员，其中tulei、xuweilai为两位网络管理员账号，ylops为网络主管账户，security为安全管理账号，不存在多余、过期、共享账户。 |
| 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； | 经现场核查防火墙中用户信息，通过输入display local-user命令，返回信息中显示防火墙中存在security、tulei、xuweilai、ylops等用户，经访谈网络管理员，防火墙中未单独创建审计管理员账户，并且网络管理员权限为超管用户权限，未实现管理用户权限最小化及权限分离。 |
| e）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； | 经核查配置文件及访谈，防火墙中由网络管理员角色账户为管理用户配置相应账号，并按照用户角色级别赋予管理用户操作权限。 |
| f）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； | 经核查配置文件及访谈，防火墙中访问控制策略为管理用户的防火墙中配置文件等进行配置管理及访问管理等，访问控制粒度达到主体为用户级、客体为文件级。 |
| g）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。 | 经核查配置文件及访谈，防火墙未对重要主体和客体设置安全标记。 |
| 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； | 经现场访谈网络管理员及核查防火墙配置，输入命令display logbuffer reverse，返回信息为logbuffer:enable；确认防火墙中其中安全审计功能，通过查看审计记录内容，确认审计记录中包含设备运行记录及用户操作行为审计记录等。 |
| 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； | 经现场核查防火墙中审计记录内容，攻击日志包括：时间、严重级别、攻击类型、动作类型、入安全域名称、目的地址、源地址等；用户操作日志包括：日期、时间、协议类型、IP地址、用户、命令详情等。 |
| 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、经访谈网络管理员，防火墙中所有用户均无权限对审计记录进行删除或修改，并且管理员在备份服务器（10.33.110.160）中添加审计记录下载脚本（python脚本），实时将防火墙中审计记录下载至备份服务器中进行备份；2、经现场核查备份服务器（10.33.110.160）中/home/network\_backup目录中存在审计记录备份文件，备份文件宿主为root，权限为744，其他用户仅拥有读权限。 |
| d）应对审计进程进行保护，防止未经授权的中断。 | 经现场访谈网络管理员，防火墙中审计进程受系统进程保护，所有用户均无权限将审计进程单独中断。 |
| 入侵防范 | a）应遵循最小安装的原则，仅安装需要的组件和应用程序； | 经访谈及核查配置文件，防火墙为厂商提供独立封装系统，不允许安装其他组件及应用程序，遵循最小安装原则。 |
| b）应关闭不需要的系统服务、默认共享和高危端口； | 经现场访谈网络管理员及核查防火墙配置，输入display current-fonfiguration，返回信息HTTP、Telnet协议均已关闭，防火墙中未启用不需要的系统服务、默认共享及高危端口。 |
| c）应通过设定终端接入方式或网络地址范围对通过网络进行管理的管理终端进行限制； | 经访谈网络管理员，在防火墙中添加访问控制策略，仅允许管理用户通过堡垒机远程管理网络设备、安全设备及服务器等，经核查防火墙中访问控制策略，具备堡垒机地址-设备管理网段（10.33.0.0）的访问控制策略。 |
| d）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； | 该测评项测评对象为业务应用系统、中间件和系统管理软件，故将该项调整为不适用。 |
| e）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； | 1、经访谈网络管理员，会定期对官方网站通报的安全漏洞进行评估，然后从官方网站下载安全补丁，经过综合评估测试后对防火墙系统进行补丁修复，避免系统中存在安全漏洞，2、经现场漏洞扫描，未发现防火墙中存在安全漏洞。 |
| f）应能够检测到对重要节点进行入侵的行为，并在发生严重入侵事件时提供报警。 | 经现场访谈及核查防火墙配置策略，防火墙中具备安全防护功能，在防火墙导航菜单栏中安全防护菜单中启用攻击防护策略，能够对从外部发起的攻击行为进行监测，发现外部攻击行为及时报警。 |
| 可信验证 | a）可基于可信根对计算设备的系统引导程序、系统程序、重要配置参数和应用程序等进行可信验证，并在应用程序的关键执行环节进行动态可信验证，在检测到其可信性受到破坏后进行报警，并将验证结果形成审计记录送至安全管理中心。 | 未基于可信根对计算设备提供可信验证。 |
| 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； | 经现场访谈网络管理员及对防火墙配置，防火墙中关闭Telnet协议，采用SSH协议或HTTPS协议进行通信，保证重要数据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。 | 经访谈网络管理员及核查H3C SecPath F1000系列防火墙产品文档，文件中目录05-参考指南--05文件系统管理命令中包含：“防火墙中文件系统通常使用摘要算法（SHA-256）对文件计算摘要值，用于验证文件的正确性和完整性”。 |
| 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； | 经现场访谈网络管理员及对防火墙配置，防火墙中关闭Telnet协议，采用SSH协议或HTTPS协议进行通信，保证重要数据在传输过程中的保密性。 |
| b）应采用密码技术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个人信息等。 | 经访谈网管理员，管理员在设置用户口令时添加simple参数，经核查H3C SecPath F1000系列防火墙产品文档，在文档05-参考指南--03-登录设备命令--1、登录设备--1.1等设备命令--1.1.28 set authentication password中正对simple参数进行说明：“simple：以明文方式设置密码，该密码将以密文方式存储。 |
| 数据备份恢复 | a）应提供重要数据的本地数据备份与恢复功能； | 经现场访谈网络管理员及核查相应配置，在备份服务器中配置python脚本，并设置每天凌晨4点将防火墙中配置文件下载至备份服务器中进行备份，管理员每周对备份文件进行巡检，确保配置文件完整备份至备份服务器中。 |
| b）应提供异地实时备份功能，利用通信网络将重要数据实时备份至备份场地； | 1、经现场访谈网络管理员，管理员添加了数据同步策略，每天将备份服务器中备份文件拷贝至阿里公共云备份服务器中进行备份；2、经核查阿里公共云备份服务器（10.30.19.10）中备份目录/data/network-backup中具备网络设备配置备份文件；3、综上，因世纪互联IDC机房及阿里云公共云均在上海市，未实现异地实时备份功能。 |
| c）应提供重要数据处理系统的热冗余，保证系统的高可用性。 | 经访谈访问管理员及核查网络拓扑图，重要数据处理系统中采用双机冗余部署，保证系统的高可用性。 |

4.1.2.12. 管理网防火墙2

|  |  |  |
| --- | --- | --- |
| **安全控制点** | **测评指标** | **结果记录** |
| 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、经现场访谈网络管理员，防火墙采用用户名、口令进行身份标识及身份鉴别；2、经核查防火墙配置，输入display password-control命令，返回信息为 Password aging:Enabled (90 days) Password length: Enabled (10 characters) Password composition:Enabled (3 types, 1 characters per type) Password history: Enabled (max history records:4)，通过返回信息确认：用户口令长度为至少10位，包含数字、字母、字符三种类型，用户口令更改周期为90天；3、通过现场在防火墙中创建与网络管理员ylops同名账户时，防火墙中会提示用户名已存在，无法创重名用户，确认用户标识具备唯一性。 |
| 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、经现场核查防火墙配置策略，输入display password-control命令，返回信息为 Maximum login attempts: 3，Action for exceeding login attempts: Lock user for 1 minutes、User authentication timeout：600 seconds；2、通过返回信息确认用户连续错误登录3次锁定账户1分钟，用户登录连接超时时间限制为600秒。 |
| 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； | 1、经现场访谈网络管理员及核查其远程连接防火墙的方式，管理员在远程管理防火墙时采用SSH协议或HTTPS协议进行通信，防止鉴别信息在网络传输过程中被窃听；2、访谈网络管理员，Telnet协议默认为关闭状态，通过输入命令telnet server enable尝试启用Telnet协议，返回信息为Telnet is insecure because it transmits data in plaintext form，Telnet协议未启成功；3，通过在终端Telnet该防火墙，无法连接成功。 |
| 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。 | 经现场核查网络管理员远程登录防火墙方式，防火墙仅采用用户名、口令方式进行身份鉴别，未采用两种或两种以上组合的鉴别技术对用户进行身份鉴别。 |
| 访问控制 | a）应对登录的用户分配账户和权限； | 1、经现场核查防火墙中用户信息，通过输入display local-user命令，返回信息中显示防火墙中存在security、tulei、xuweilai、ylops等用户，其中security的 user role list：level-1，network-operator；tulei、xuweilai、ylops的 user role list：network-admin,network-operator。 |
| b）应重命名或删除默认账户，修改默认账户的默认口令； | 1、经现场核查防火墙中用户信息，通过输入display local-user命令，返回信息中显示防火墙中存在security、tulei、xuweilai、ylops等用户,不存在默认账户，2、经核查防火墙配置，输入display password-control命令，返回信息为 Password aging:Enabled (90 days) Password length: Enabled (10 characters) Password composition:Enabled (3 types, 1 characters per type) Password history: Enabled (max history records：3、用户口令已按照复杂度策略更改。 |
| 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； | 经现场核查防火墙中用户信息，通过输入display local-user命令，返回信息中显示防火墙中存在security、tulei、xuweilai、ylops等用户,经访谈网络管理员，其中tulei、xuweilai为两位网络管理员账号，ylops为网络主管账户，security为安全管理账号，不存在多余、过期、共享账户。 |
| 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； | 经现场核查防火墙中用户信息，通过输入display local-user命令，返回信息中显示防火墙中存在security、tulei、xuweilai、ylops等用户，经访谈网络管理员，防火墙中未单独创建审计管理员账户，并且网络管理员权限为超管用户权限，未实现管理用户权限最小化及权限分离。 |
| e）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； | 经核查配置文件及访谈，防火墙中由网络管理员角色账户为管理用户配置相应账号，并按照用户角色级别赋予管理用户操作权限。 |
| f）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； | 经核查配置文件及访谈，防火墙中访问控制策略为管理用户的防火墙中配置文件等进行配置管理及访问管理等，访问控制粒度达到主体为用户级、客体为文件级。 |
| g）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。 | 经核查配置文件及访谈，防火墙未对重要主体和客体设置安全标记。 |
| 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； | 经现场访谈网络管理员及核查防火墙配置，输入命令display logbuffer reverse，返回信息为logbuffer:enable；确认防火墙中其中安全审计功能，通过查看审计记录内容，确认审计记录中包含设备运行记录及用户操作行为审计记录等。 |
| 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； | 经现场核查防火墙中审计记录内容，攻击日志包括：时间、严重级别、攻击类型、动作类型、入安全域名称、目的地址、源地址等；用户操作日志包括：日期、时间、协议类型、IP地址、用户、命令详情等。 |
| 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、经访谈网络管理员，防火墙中所有用户均无权限对审计记录进行删除或修改，并且管理员在备份服务器（10.33.110.160）中添加审计记录下载脚本（python脚本），实时将防火墙中审计记录下载至备份服务器中进行备份；2、经现场核查备份服务器（10.33.110.160）中/home/network\_backup目录中存在审计记录备份文件，备份文件宿主为root，权限为744，其他用户仅拥有读权限。 |
| d）应对审计进程进行保护，防止未经授权的中断。 | 经现场访谈网络管理员，防火墙中审计进程受系统进程保护，所有用户均无权限将审计进程单独中断。 |
| 入侵防范 | a）应遵循最小安装的原则，仅安装需要的组件和应用程序； | 经访谈及核查配置文件，防火墙为厂商提供独立封装系统，不允许安装其他组件及应用程序，遵循最小安装原则。 |
| b）应关闭不需要的系统服务、默认共享和高危端口； | 经现场访谈网络管理员及核查防火墙配置，输入display current-fonfiguration，返回信息HTTP、Telnet协议均已关闭，防火墙中未启用不需要的系统服务、默认共享及高危端口。 |
| c）应通过设定终端接入方式或网络地址范围对通过网络进行管理的管理终端进行限制； | 经访谈网络管理员，在防火墙中添加访问控制策略，仅允许管理用户通过堡垒机远程管理网络设备、安全设备及服务器等，经核查防火墙中访问控制策略，具备堡垒机地址-设备管理网段（10.33.0.0）的访问控制策略。 |
| d）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； | 该测评项测评对象为业务应用系统、中间件和系统管理软件，故将该项调整为不适用。 |
| e）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； | 1、经访谈网络管理员，会定期对官方网站通报的安全漏洞进行评估，然后从官方网站下载安全补丁，经过综合评估测试后对防火墙系统进行补丁修复，避免系统中存在安全漏洞，2、经现场漏洞扫描，未发现防火墙中存在安全漏洞。 |
| f）应能够检测到对重要节点进行入侵的行为，并在发生严重入侵事件时提供报警。 | 经现场访谈及核查防火墙配置策略，防火墙中具备安全防护功能，在防火墙导航菜单栏中安全防护菜单中启用攻击防护策略，能够对从外部发起的攻击行为进行监测，发现外部攻击行为及时报警。 |
| 可信验证 | a）可基于可信根对计算设备的系统引导程序、系统程序、重要配置参数和应用程序等进行可信验证，并在应用程序的关键执行环节进行动态可信验证，在检测到其可信性受到破坏后进行报警，并将验证结果形成审计记录送至安全管理中心。 | 未基于可信根对计算设备提供可信验证。 |
| 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； | 经现场访谈网络管理员及对防火墙配置，防火墙中关闭Telnet协议，采用SSH协议或HTTPS协议进行通信，保证重要数据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。 | 经访谈网络管理员及核查H3C SecPath F1000系列防火墙产品文档，文件中目录05-参考指南--05文件系统管理命令中包含：“防火墙中文件系统通常使用摘要算法（SHA-256）对文件计算摘要值，用于验证文件的正确性和完整性”。 |
| 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； | 经现场访谈网络管理员及对防火墙配置，防火墙中关闭Telnet协议，采用SSH协议或HTTPS协议进行通信，保证重要数据在传输过程中的保密性。 |
| b）应采用密码技术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个人信息等。 | 经访谈网管理员，管理员在设置用户口令时添加simple参数，经核查H3C SecPath F1000系列防火墙产品文档，在文档05-参考指南--03-登录设备命令--1、登录设备--1.1等设备命令--1.1.28 set authentication password中正对simple参数进行说明：“simple：以明文方式设置密码，该密码将以密文方式存储。 |
| 数据备份恢复 | a）应提供重要数据的本地数据备份与恢复功能； | 经现场访谈网络管理员及核查相应配置，在备份服务器中配置python脚本，并设置每天凌晨4点将防火墙中配置文件下载至备份服务器中进行备份，管理员每周对备份文件进行巡检，确保配置文件完整备份至备份服务器中。 |
| b）应提供异地实时备份功能，利用通信网络将重要数据实时备份至备份场地； | 1、经现场访谈网络管理员，管理员添加了数据同步策略，每天将备份服务器中备份文件拷贝至阿里公共云备份服务器中进行备份；2、经核查阿里公共云备份服务器（10.30.19.10）中备份目录/data/network-backup中具备网络设备配置备份文件；3、综上，因世纪互联IDC机房及阿里云公共云均在上海市，未实现异地实时备份功能。 |
| c）应提供重要数据处理系统的热冗余，保证系统的高可用性。 | 经访谈访问管理员及核查网络拓扑图，重要数据处理系统中采用双机冗余部署，保证系统的高可用性。 |

4.1.2.13. 天眼云镜

|  |  |  |
| --- | --- | --- |
| **安全控制点** | **测评指标** | **结果记录** |
| 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、经现场访谈安全管理员及核查天眼云镜，天眼云镜采用用户名、口令、OTP动态验证码进行身份鉴别和标识，天眼云镜具有用户名查重功能，保证用户名具有唯一性，经现场测试，创建重名用户时会提示用户名已存在，创建账户失败，2、经现场核查天眼云镜密码策略，要求口令长度为8-20位字符，包含大小写字母、数字、特殊字符三种以上组合，用户口令更改周期为90天，OTP动态验证码刷新时间为30秒。 |
| 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、经现场访谈安全管理员及核查天眼云镜，天眼云镜启用登录失败处理策略，用户连续错误登录5次锁定账户15分钟，2、已配置连接超时时间30分钟。 |
| 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； | 经现场核查天眼云镜通信方式，天眼云镜在远程管理时采用HTTPS协议进行通信，防止鉴别信息在网络传输过程中被窃听。 |
| 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。 | 经现场访谈安全管理员及核查天眼云镜登录方式，天眼云镜采用用户名、口令、OTP动态验证码对用户进行身份鉴别。 |
| 访问控制 | a）应对登录的用户分配账户和权限； | 经现场访谈安全管理员及核查天眼云镜中子账号管理，天眼云镜由超级管理员对登录的用户创建账号并分配权限，目前在天眼云镜中存在huangfusheng安全管理员（拥有安全管理权限）、fengkun审计员（拥有审计管理权限）、wangtao、huanqinlong、yangyuhao等共6个普通用户（拥有日常运维管理权限。 |
| b）应重命名或删除默认账户，修改默认账户的默认口令； | 核查天眼云镜中子账号管理，天眼云镜中不存在默认账户，并且用户口令已按照复杂度策略更改。 |
| 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； | 经现场核查天眼云镜中子账号管理，天眼云镜中账户和员工账户一一对应，不存在多余、过期、共享账户。 |
| 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； | 经现场核查天眼云镜中子账号管理，天眼云镜中创建了安全管理员、审计管理员、普通管理用户，并按照权限最小原则赋予各管理用户操作权限，实现管理用户权限分离。 |
| e）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； | 经核查与访谈，天眼云镜中由管理员角色账户为管理用户配置相应账号，并按照用户角色级别赋予管理用户操作权限。 |
| f）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； | 经核查及访谈，天眼云镜中访问控制策略为管理用户的天眼云镜中配置文件等进行配置管理及访问管理等，访问控制粒度达到主体为用户级、客体为菜单级。 |
| g）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。 | 经核查及访谈，天眼云镜未对重要主体和客体设置安全标记。 |
| 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； | 经现场核查天眼云镜审计功能，天眼云镜能够对用户操作、病毒查杀等进行审计记录。 |
| 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； | 经现场核查天眼云镜审计记录，天眼云镜中操作日志包括：操作时间、操作用户、操作名称、操作类型、操作（查看详情）等；病毒查杀记录包括：病毒名称、病毒文件、受感染主机、发现时间、处理时间、处理人、操作（还原文件、删除文件）等。 |
| 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、经现场核查天眼云镜审计记录，所有用户均无权限将审计记录进行修改、删除，2、管理员配置审计记录备份策略，实时将审计记录备份至360本地安全大脑中进行备份保存，经现场核查360本地安全大脑中具备天眼云镜审计记录，保存时间满足半年以上。 |
| d）应对审计进程进行保护，防止未经授权的中断。 | 经现场核查天眼云镜审计进程，天眼云镜中审计进程受系统进程保护，所有用户均无权限对审计进程单独中断。 |
| 入侵防范 | a）应遵循最小安装的原则，仅安装需要的组件和应用程序； | 经访谈及核查，天眼云镜系统为厂商提供独立封装系统，不允许安装其他组件及应用程序，遵循最小安装原则。 |
| b）应关闭不需要的系统服务、默认共享和高危端口； | 经现场核查天眼云镜配置策略，天眼云镜中仅启用了SNMP、NTP、HTTPS远程管理端口，Telnet协议已关闭。 |
| c）应通过设定终端接入方式或网络地址范围对通过网络进行管理的管理终端进行限制； | 经现场访谈安全管理员及核查，远程管理天眼云镜时仅允许管理用户使用在办公网防火墙中启用VPN隧道连接到世纪互联IDC机房中，然后对天眼云镜进行远程管理。 |
| d）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； | 该测评项测评对象为业务应用系统、中间件和系统管理软件，安全设备不适用。 |
| e）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； | 1、经现场访谈安全管理员，管理员定期对官方网站通报的安全漏洞进行评估，然后从官方网站下载安全补丁对设备进行补丁修复，避免系统中存在安全漏洞，2、经现场漏洞扫描，未发现天眼云镜中存在安全漏洞。 |
| f）应能够检测到对重要节点进行入侵的行为，并在发生严重入侵事件时提供报警。 | 经现场访谈及核查，被测系统中部署了360AISA全流量威胁分析系统和360本地安全大脑，通过将被测系统中全部流量镜像发送到360AISA全流量威胁分析系统及360本地安全大脑中进行分析监测，发现入侵事件后及时通过钉钉报警，并且能够实现自动阻断。 |
| 可信验证 | a）可基于可信根对计算设备的系统引导程序、系统程序、重要配置参数和应用程序等进行可信验证，并在应用程序的关键执行环节进行动态可信验证，在检测到其可信性受到破坏后进行报警，并将验证结果形成审计记录送至安全管理中心。 | 未基于可信根对计算设备提供可信验证。 |
| 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； | 经现场核查天眼云镜通信方式，系统通过HTTPS协议进行通信，保证重要数据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。 | 经现场核查安全管理员，天眼云镜通过厂商自身的加密技术保证用户鉴别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； | 经现场核查天眼云镜通信方式，系统通过HTTPS协议进行通信，保证重要数据传输过程中的保密性。 |
| b）应采用密码技术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个人信息等。 | 经现场核查安全管理员，天眼云镜通过厂商自身的加密技术保证用户鉴别信息等在存储过程中的保密性。 |
| 数据备份恢复 | a）应提供重要数据的本地数据备份与恢复功能； | 经现场访谈管理员及核查相应配置，在备份服务器中配置python脚本，并设置每天凌晨4点将交换机中配置文件下载至备份服务器中进行备份，管理员每周对备份文件进行巡检，确保配置文件完整备份至备份服务器中。 |
| b）应提供异地实时备份功能，利用通信网络将重要数据实时备份至备份场地； | 公司未对重要数据提供异地备份服务。 |
| c）应提供重要数据处理系统的热冗余，保证系统的高可用性。 | 经核查，重要数据处理系统中通过四台设备组成一个集群进行部署，保证系统的高可用性。 |

4.1.2.14. 数据库安全审计系统

|  |  |  |
| --- | --- | --- |
| **安全控制点** | **测评指标** | **结果记录** |
| 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、经现场访谈管理员及核查数据库安全审计系统，数据库安全审计系统采用用户名、口令进行身份标识和身份鉴别，数据库安全审计系统具备用户名查重功能，保证用户身份标识具备唯一性，经现场测试，创建重名用户会提示用户名已存在，2、经现场核查数据库审计系统口令策略，用户口令长度至少为8位，由，、大小写字母、数字、字符四种组合，但是未配置用户口令更改周期。 |
| 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； | 经现场访谈管理员及核查数据库安全审计系统登录策略，用户连续错误登录10次锁定IP地址，由管理员负责解锁，空闲超时时间限制为3分钟。 |
| 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； | 经现场核查数据库安全审计系统通信方式，数据库审计在远程管理时采用HTTPS协议进行通信，防止鉴别信息在网络传输过程中被窃听。 |
| 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。 | 经现场访谈管理员及核查数据库安全审计系统登录方式，数据库安全审计系统仅采用用户名、口令方式进行身份鉴别，未采用两种或两种以上组合的鉴别技术对用户进行身份鉴别。 |
| 访问控制 | a）应对登录的用户分配账户和权限； | 经现场访谈管理员及核查数据库安全审计系统用户管理配置，在用户管理-账号管理中分别配置sysadmin系统管理员、audadmin审计管理员、secadmin安全管理员等账户，并分别为各管理用户赋予相应权限，如：系统管理员：首页、审计、分析、报表、策略、资产系统等菜单权限；审计管理员拥有审计菜单权限；安全管理员拥有系统、用户管理、账号审核、安全配置等菜单权限。 |
| b）应重命名或删除默认账户，修改默认账户的默认口令； | 经现场访谈管理员及核查数据库安全审计系统用户管理配置，系统中不存在默认账户，并且用户口令已按照复杂度要求更改。 |
| 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； | 经现场访谈管理员及核查数据库安全审计系统用户管理配置，数据库安全审计系统中按照管理需求创建用户，不存在多余、过期、共享账户。 |
| 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； | 经现场访谈管理员及核查数据库安全审计系统用户管理配置，分别配置sysadmin系统管理员、audadmin审计管理员、secadmin安全管理员等账户，并按照最小权限原则赋予各管理用户相应权限，实现管理用户权限最小化及权限分离。 |
| e）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； | 经核查配置文件及访谈，数据库安全审计系统中由管理员角色账户为管理用户配置相应账号，并按照用户角色级别赋予管理用户操作权限。 |
| f）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； | 经核查配置文件及访谈，数据库安全审计中访问控制策略为管理用户的数据库安全审计系统中配置文件等进行配置管理及访问管理等，访问控制粒度达到主体为用户级、客体为菜单级。 |
| g）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。 | 经核查及访谈，数据库安全审计系统未对重要主体和客体设置安全标记。 |
| 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； | 经现场核查数据库安全审计系统审计功能，数据库安全审计系统启用安全审计，能够对用户操作行为及安全事件进行审计记录。 |
| 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； | 经现场核查数据库安全审计系统审计记录，数据库安全审计系统中会话审计记录包括：会话ID、开始时间、时长、客户端IP、服务端IP、协议类型、数据库账号、请求总数、操作（详情、回放）。 |
| 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； | 经现场核查数据库安全审计系统审计记录，所有用户均无权限将审计记录进行删除、修改，管理员配置审计备份，实时将审计记录传输至360本地安全大脑进行备份保存。 |
| d）应对审计进程进行保护，防止未经授权的中断。 | 经现场核查数据库安全审计系统审计进程，数据库安全审计系统审计进程受系统进程保护，所有用户均无权限对审计进程单独中断。 |
| 入侵防范 | a）应遵循最小安装的原则，仅安装需要的组件和应用程序； | 经访谈及核查，数据库安全审计系统为厂商提供独立封装系统，不允许安装其他组件及应用程序，遵循最小安装原则。 |
| b）应关闭不需要的系统服务、默认共享和高危端口； | 经现场核查数据库安全审计系统配置策略，数据库安全审计系统仅启用了HTTPS远程管理端口、ftp服务用于审计记录备份，未启用不需要服务及高危端口。 |
| c）应通过设定终端接入方式或网络地址范围对通过网络进行管理的管理终端进行限制； | 经现场访谈安全管理员及核查，远程管理数据库安全审计系统时仅允许管理用户使用在办公网防火墙中启用VPN隧道连接到世纪互联IDC机房中，然后对数据库安全审计系统进行远程管理。 |
| d）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； | 该测评项测评对象为业务应用系统、中间件和系统管理软件，安全设备不适用。 |
| e）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； | 经现场访谈安全管理员，管理员定期对官方网站通报的安全漏洞进行评估，然后从官方网站下载安全补丁对数据库安全审计系统进行补丁修复，避免系统中存在安全漏洞，经现场核查数据库安全审计系统系统版本为V3.0，为当前厂商提供最新版本。 |
| f）应能够检测到对重要节点进行入侵的行为，并在发生严重入侵事件时提供报警。 | 经访谈网络管理员，被测系统中部署了通过360AISA全流量威胁分析系统和360本地安全大脑将被测系统中全部流量镜像发送到360AISA全流量威胁分析系统及360本地安全大脑中进行分析监测，发现入侵事件后及时通过钉钉报警，并且能够自动阻断。 |
| 可信验证 | a）可基于可信根对计算设备的系统引导程序、系统程序、重要配置参数和应用程序等进行可信验证，并在应用程序的关键执行环节进行动态可信验证，在检测到其可信性受到破坏后进行报警，并将验证结果形成审计记录送至安全管理中心。 | 未基于可信根对计算设备提供可信验证。 |
| 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； | 经现场核查数据库安全审计系统通信方式，系统通过HTTPS协议进行通信，保证重要数据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。 | 经现场核查安全管理员，数据库安全审计系统过厂商自身的加密技术保证用户鉴别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； | 经现场核查数据库安全审计系统通信方式，系统通过HTTPS协议进行通信，保证重要数据传输过程中的保密性。 |
| b）应采用密码技术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个人信息等。 | 经现场核查安全管理员，数据库安全审计系统通过厂商自身的加密技术保证用户鉴别信息等在存储过程中的保密性。 |
| 数据备份恢复 | a）应提供重要数据的本地数据备份与恢复功能； | 经现场访谈管理员及核查相应配置，在备份服务器中配置python脚本，并设置每天凌晨4点将交换机中配置文件下载至备份服务器中进行备份，管理员每周对备份文件进行巡检，确保配置文件完整备份至备份服务器中。 |
| b）应提供异地实时备份功能，利用通信网络将重要数据实时备份至备份场地； | 公司未对重要数据提供异地备份服务。 |
| c）应提供重要数据处理系统的热冗余，保证系统的高可用性。 | 经核查，重要数据处理系统中采用热冗余部署，保证系统的高可用性。 |

4.1.2.15. 分拨中心出口防火墙1

|  |  |  |
| --- | --- | --- |
| **安全控制点** | **测评指标** | **结果记录** |
| 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、经现场访谈网络管理员，防火墙采用用户名、口令进行身份标识及身份鉴别；2、经核查防火墙配置，输入display password-control命令，返回信息为 Password aging:Enabled (90 days) Password length: Enabled (10 characters) Password composition:Enabled (3 types, 1 characters per type) Password history: Enabled (max history records:4)，通过返回信息确认：用户口令长度为至少10位，包含数字、字母、字符三种类型，用户口令更改周期为90天；3、通过现场在防火墙中创建与网络管理员ylops同名账户时，防火墙中会提示用户名已存在，无法创重名用户，确认用户标识具备唯一性。 |
| 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、经现场核查防火墙配置策略，输入display password-control命令，返回信息为 Maximum login attempts: 3，Action for exceeding login attempts: Lock user for 1 minutes、User authentication timeout：600 seconds；2、通过返回信息确认用户连续错误登录3次锁定账户1分钟，用户登录连接超时时间限制为600秒。 |
| 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； | 1、经现场访谈网络管理员及核查其远程连接防火墙的方式，管理员在远程管理防火墙时采用SSH协议或HTTPS协议进行通信，防止鉴别信息在网络传输过程中被窃听；2、访谈网络管理员，Telnet协议默认为关闭状态，通过输入命令telnet server enable尝试启用Telnet协议，返回信息为Telnet is insecure because it transmits data in plaintext form，Telnet协议未启成功；3，通过在终端Telnet该防火墙，无法连接成功。 |
| 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。 | 经现场核查网络管理员远程登录防火墙方式，防火墙仅采用用户名、口令方式进行身份鉴别，未采用两种或两种以上组合的鉴别技术对用户进行身份鉴别。 |
| 访问控制 | a）应对登录的用户分配账户和权限； | 1、经现场核查防火墙中用户信息，通过输入display local-user命令，返回信息中显示防火墙中存在security、tulei、xuweilai、ylops等用户，其中security的 user role list：level-1，network-operator；tulei、xuweilai、ylops的 user role list：network-admin,network-operator。 |
| b）应重命名或删除默认账户，修改默认账户的默认口令； | 1、经现场核查防火墙中用户信息，通过输入display local-user命令，返回信息中显示防火墙中存在security、tulei、xuweilai、ylops等用户,不存在默认账户，2、经核查防火墙配置，输入display password-control命令，返回信息为 Password aging:Enabled (90 days) Password length: Enabled (10 characters) Password composition:Enabled (3 types, 1 characters per type) Password history: Enabled (max history records：3、用户口令已按照复杂度策略更改。 |
| 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； | 经现场核查防火墙中用户信息，通过输入display local-user命令，返回信息中显示防火墙中存在security、tulei、xuweilai、ylops等用户,经访谈网络管理员，其中tulei、xuweilai为两位网络管理员账号，ylops为网络主管账户，security为安全管理账号，不存在多余、过期、共享账户。 |
| 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； | 经现场核查防火墙中用户信息，通过输入display local-user命令，返回信息中显示防火墙中存在security、tulei、xuweilai、ylops等用户，经访谈网络管理员，防火墙中未单独创建审计管理员账户，并且网络管理员权限为超管用户权限，未实现管理用户权限最小化及权限分离。 |
| e）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； | 经核查配置文件及访谈，防火墙中由网络管理员角色账户为管理用户配置相应账号，并按照用户角色级别赋予管理用户操作权限。 |
| f）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； | 经核查配置文件及访谈，防火墙中访问控制策略为管理用户的防火墙中配置文件等进行配置管理及访问管理等，访问控制粒度达到主体为用户级、客体为文件级。 |
| g）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。 | 经核查配置文件及访谈，防火墙未对重要主体和客体设置安全标记。 |
| 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； | 经现场访谈网络管理员及核查防火墙配置，输入命令display logbuffer reverse，返回信息为logbuffer:enable；确认防火墙中其中安全审计功能，通过查看审计记录内容，确认审计记录中包含设备运行记录及用户操作行为审计记录等。 |
| 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； | 经现场核查防火墙中审计记录内容，攻击日志包括：时间、严重级别、攻击类型、动作类型、入安全域名称、目的地址、源地址等；用户操作日志包括：日期、时间、协议类型、IP地址、用户、命令详情等。 |
| 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、经访谈网络管理员，防火墙中所有用户均无权限对审计记录进行删除或修改，并且管理员在备份服务器（10.33.110.160）中添加审计记录下载脚本（python脚本），实时将防火墙中审计记录下载至备份服务器中进行备份；2、经现场核查备份服务器（10.33.110.160）中/home/network\_backup目录中存在审计记录备份文件，备份文件宿主为root，权限为744，其他用户仅拥有读权限。 |
| d）应对审计进程进行保护，防止未经授权的中断。 | 经现场访谈网络管理员，防火墙中审计进程受系统进程保护，所有用户均无权限将审计进程单独中断。 |
| 入侵防范 | a）应遵循最小安装的原则，仅安装需要的组件和应用程序； | 经访谈及核查配置文件，防火墙为厂商提供独立封装系统，不允许安装其他组件及应用程序，遵循最小安装原则。 |
| b）应关闭不需要的系统服务、默认共享和高危端口； | 经现场访谈网络管理员及核查防火墙配置，输入display current-fonfiguration，返回信息HTTP、Telnet协议均已关闭，防火墙中未启用不需要的系统服务、默认共享及高危端口。 |
| c）应通过设定终端接入方式或网络地址范围对通过网络进行管理的管理终端进行限制； | 经访谈网络管理员，在防火墙中添加访问控制策略，仅允许管理用户通过堡垒机远程管理网络设备、安全设备及服务器等，经核查防火墙中访问控制策略，具备堡垒机地址-设备管理网段（10.33.0.0）的访问控制策略。 |
| d）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； | 该测评项测评对象为业务应用系统、中间件和系统管理软件，故将该项调整为不适用。 |
| e）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； | 1、经访谈网络管理员，会定期对官方网站通报的安全漏洞进行评估，然后从官方网站下载安全补丁，经过综合评估测试后对防火墙系统进行补丁修复，避免系统中存在安全漏洞，2、经现场漏洞扫描，未发现防火墙中存在安全漏洞。 |
| f）应能够检测到对重要节点进行入侵的行为，并在发生严重入侵事件时提供报警。 | 经现场访谈及核查防火墙配置策略，防火墙中具备安全防护功能，在防火墙导航菜单栏中安全防护菜单中启用攻击防护策略，能够对从外部发起的攻击行为进行监测，发现外部攻击行为及时报警。 |
| 可信验证 | a）可基于可信根对计算设备的系统引导程序、系统程序、重要配置参数和应用程序等进行可信验证，并在应用程序的关键执行环节进行动态可信验证，在检测到其可信性受到破坏后进行报警，并将验证结果形成审计记录送至安全管理中心。 | 未基于可信根对计算设备提供可信验证。 |
| 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； | 经现场访谈网络管理员及对防火墙配置，防火墙中关闭Telnet协议，采用SSH协议或HTTPS协议进行通信，保证重要数据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。 | 经访谈网络管理员及核查H3C SecPath F1000系列防火墙产品文档，文件中目录05-参考指南--05文件系统管理命令中包含：“防火墙中文件系统通常使用摘要算法（SHA-256）对文件计算摘要值，用于验证文件的正确性和完整性”。 |
| 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； | 经现场访谈网络管理员及对防火墙配置，防火墙中关闭Telnet协议，采用SSH协议或HTTPS协议进行通信，保证重要数据在传输过程中的保密性。 |
| b）应采用密码技术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个人信息等。 | 经访谈网管理员，管理员在设置用户口令时添加simple参数，经核查H3C SecPath F1000系列防火墙产品文档，在文档05-参考指南--03-登录设备命令--1、登录设备--1.1等设备命令--1.1.28 set authentication password中正对simple参数进行说明：“simple：以明文方式设置密码，该密码将以密文方式存储。 |
| 数据备份恢复 | a）应提供重要数据的本地数据备份与恢复功能； | 经现场访谈网络管理员及核查相应配置，在备份服务器中配置python脚本，并设置每天凌晨4点将防火墙中配置文件下载至备份服务器中进行备份，管理员每周对备份文件进行巡检，确保配置文件完整备份至备份服务器中。 |
| b）应提供异地实时备份功能，利用通信网络将重要数据实时备份至备份场地； | 1、经现场访谈网络管理员，管理员添加了数据同步策略，每天将备份服务器中备份文件拷贝至阿里公共云备份服务器中进行备份；2、经核查阿里公共云备份服务器（10.30.19.10）中备份目录/data/network-backup中具备网络设备配置备份文件；3、综上，因世纪互联IDC机房及阿里云公共云均在上海市，未实现异地实时备份功能。 |
| c）应提供重要数据处理系统的热冗余，保证系统的高可用性。 | 经访谈访问管理员及核查网络拓扑图，重要数据处理系统中采用双机冗余部署，保证系统的高可用性。 |

4.1.2.16. 分拨中心出口防火墙2

|  |  |  |
| --- | --- | --- |
| **安全控制点** | **测评指标** | **结果记录** |
| 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、经现场访谈网络管理员，防火墙采用用户名、口令进行身份标识及身份鉴别；2、经核查防火墙配置，输入display password-control命令，返回信息为 Password aging:Enabled (90 days) Password length: Enabled (10 characters) Password composition:Enabled (3 types, 1 characters per type) Password history: Enabled (max history records:4)，通过返回信息确认：用户口令长度为至少10位，包含数字、字母、字符三种类型，用户口令更改周期为90天；3、通过现场在防火墙中创建与网络管理员ylops同名账户时，防火墙中会提示用户名已存在，无法创重名用户，确认用户标识具备唯一性。 |
| 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、经现场核查防火墙配置策略，输入display password-control命令，返回信息为 Maximum login attempts: 3，Action for exceeding login attempts: Lock user for 1 minutes、User authentication timeout：600 seconds；2、通过返回信息确认用户连续错误登录3次锁定账户1分钟，用户登录连接超时时间限制为600秒。 |
| 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； | 1、经现场访谈网络管理员及核查其远程连接防火墙的方式，管理员在远程管理防火墙时采用SSH协议或HTTPS协议进行通信，防止鉴别信息在网络传输过程中被窃听；2、访谈网络管理员，Telnet协议默认为关闭状态，通过输入命令telnet server enable尝试启用Telnet协议，返回信息为Telnet is insecure because it transmits data in plaintext form，Telnet协议未启成功；3，通过在终端Telnet该防火墙，无法连接成功。 |
| 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。 | 经现场核查网络管理员远程登录防火墙方式，防火墙仅采用用户名、口令方式进行身份鉴别，未采用两种或两种以上组合的鉴别技术对用户进行身份鉴别。 |
| 访问控制 | a）应对登录的用户分配账户和权限； | 1、经现场核查防火墙中用户信息，通过输入display local-user命令，返回信息中显示防火墙中存在security、tulei、xuweilai、ylops等用户，其中security的 user role list：level-1，network-operator；tulei、xuweilai、ylops的 user role list：network-admin,network-operator。 |
| b）应重命名或删除默认账户，修改默认账户的默认口令； | 1、经现场核查防火墙中用户信息，通过输入display local-user命令，返回信息中显示防火墙中存在security、tulei、xuweilai、ylops等用户,不存在默认账户，2、经核查防火墙配置，输入display password-control命令，返回信息为 Password aging:Enabled (90 days) Password length: Enabled (10 characters) Password composition:Enabled (3 types, 1 characters per type) Password history: Enabled (max history records：3、用户口令已按照复杂度策略更改。 |
| 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； | 经现场核查防火墙中用户信息，通过输入display local-user命令，返回信息中显示防火墙中存在security、tulei、xuweilai、ylops等用户,经访谈网络管理员，其中tulei、xuweilai为两位网络管理员账号，ylops为网络主管账户，security为安全管理账号，不存在多余、过期、共享账户。 |
| 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； | 经现场核查防火墙中用户信息，通过输入display local-user命令，返回信息中显示防火墙中存在security、tulei、xuweilai、ylops等用户，经访谈网络管理员，防火墙中未单独创建审计管理员账户，并且网络管理员权限为超管用户权限，未实现管理用户权限最小化及权限分离。 |
| e）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； | 经核查配置文件及访谈，防火墙中由网络管理员角色账户为管理用户配置相应账号，并按照用户角色级别赋予管理用户操作权限。 |
| f）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； | 经核查配置文件及访谈，防火墙中访问控制策略为管理用户的防火墙中配置文件等进行配置管理及访问管理等，访问控制粒度达到主体为用户级、客体为文件级。 |
| g）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。 | 经核查配置文件及访谈，防火墙未对重要主体和客体设置安全标记。 |
| 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； | 经现场访谈网络管理员及核查防火墙配置，输入命令display logbuffer reverse，返回信息为logbuffer:enable；确认防火墙中其中安全审计功能，通过查看审计记录内容，确认审计记录中包含设备运行记录及用户操作行为审计记录等。 |
| 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； | 经现场核查防火墙中审计记录内容，攻击日志包括：时间、严重级别、攻击类型、动作类型、入安全域名称、目的地址、源地址等；用户操作日志包括：日期、时间、协议类型、IP地址、用户、命令详情等。 |
| 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、经访谈网络管理员，防火墙中所有用户均无权限对审计记录进行删除或修改，并且管理员在备份服务器（10.33.110.160）中添加审计记录下载脚本（python脚本），实时将防火墙中审计记录下载至备份服务器中进行备份；2、经现场核查备份服务器（10.33.110.160）中/home/network\_backup目录中存在审计记录备份文件，备份文件宿主为root，权限为744，其他用户仅拥有读权限。 |
| d）应对审计进程进行保护，防止未经授权的中断。 | 经现场访谈网络管理员，防火墙中审计进程受系统进程保护，所有用户均无权限将审计进程单独中断。 |
| 入侵防范 | a）应遵循最小安装的原则，仅安装需要的组件和应用程序； | 经访谈及核查配置文件，防火墙为厂商提供独立封装系统，不允许安装其他组件及应用程序，遵循最小安装原则。 |
| b）应关闭不需要的系统服务、默认共享和高危端口； | 经现场访谈网络管理员及核查防火墙配置，输入display current-fonfiguration，返回信息HTTP、Telnet协议均已关闭，防火墙中未启用不需要的系统服务、默认共享及高危端口。 |
| c）应通过设定终端接入方式或网络地址范围对通过网络进行管理的管理终端进行限制； | 经访谈网络管理员，在防火墙中添加访问控制策略，仅允许管理用户通过堡垒机远程管理网络设备、安全设备及服务器等，经核查防火墙中访问控制策略，具备堡垒机地址-设备管理网段（10.33.0.0）的访问控制策略。 |
| d）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； | 该测评项测评对象为业务应用系统、中间件和系统管理软件，故将该项调整为不适用。 |
| e）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； | 1、经访谈网络管理员，会定期对官方网站通报的安全漏洞进行评估，然后从官方网站下载安全补丁，经过综合评估测试后对防火墙系统进行补丁修复，避免系统中存在安全漏洞，2、经现场漏洞扫描，未发现防火墙中存在安全漏洞。 |
| f）应能够检测到对重要节点进行入侵的行为，并在发生严重入侵事件时提供报警。 | 经现场访谈及核查防火墙配置策略，防火墙中具备安全防护功能，在防火墙导航菜单栏中安全防护菜单中启用攻击防护策略，能够对从外部发起的攻击行为进行监测，发现外部攻击行为及时报警。 |
| 可信验证 | a）可基于可信根对计算设备的系统引导程序、系统程序、重要配置参数和应用程序等进行可信验证，并在应用程序的关键执行环节进行动态可信验证，在检测到其可信性受到破坏后进行报警，并将验证结果形成审计记录送至安全管理中心。 | 未基于可信根对计算设备提供可信验证。 |
| 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； | 经现场访谈网络管理员及对防火墙配置，防火墙中关闭Telnet协议，采用SSH协议或HTTPS协议进行通信，保证重要数据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。 | 经访谈网络管理员及核查H3C SecPath F1000系列防火墙产品文档，文件中目录05-参考指南--05文件系统管理命令中包含：“防火墙中文件系统通常使用摘要算法（SHA-256）对文件计算摘要值，用于验证文件的正确性和完整性”。 |
| 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； | 经现场访谈网络管理员及对防火墙配置，防火墙中关闭Telnet协议，采用SSH协议或HTTPS协议进行通信，保证重要数据在传输过程中的保密性。 |
| b）应采用密码技术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个人信息等。 | 经访谈网管理员，管理员在设置用户口令时添加simple参数，经核查H3C SecPath F1000系列防火墙产品文档，在文档05-参考指南--03-登录设备命令--1、登录设备--1.1等设备命令--1.1.28 set authentication password中正对simple参数进行说明：“simple：以明文方式设置密码，该密码将以密文方式存储。 |
| 数据备份恢复 | a）应提供重要数据的本地数据备份与恢复功能； | 经现场访谈网络管理员及核查相应配置，在备份服务器中配置python脚本，并设置每天凌晨4点将防火墙中配置文件下载至备份服务器中进行备份，管理员每周对备份文件进行巡检，确保配置文件完整备份至备份服务器中。 |
| b）应提供异地实时备份功能，利用通信网络将重要数据实时备份至备份场地； | 1、经现场访谈网络管理员，管理员添加了数据同步策略，每天将备份服务器中备份文件拷贝至阿里公共云备份服务器中进行备份；2、经核查阿里公共云备份服务器（10.30.19.10）中备份目录/data/network-backup中具备网络设备配置备份文件；3、综上，因世纪互联IDC机房及阿里云公共云均在上海市，未实现异地实时备份功能。 |
| c）应提供重要数据处理系统的热冗余，保证系统的高可用性。 | 经访谈访问管理员及核查网络拓扑图，重要数据处理系统中采用双机冗余部署，保证系统的高可用性。 |

4.1.2.17. 分拨中心出口防火墙3

|  |  |  |
| --- | --- | --- |
| **安全控制点** | **测评指标** | **结果记录** |
| 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、经现场访谈网络管理员，防火墙采用用户名、口令进行身份标识及身份鉴别；2、经核查防火墙配置，输入display password-control命令，返回信息为 Password aging:Enabled (90 days) Password length: Enabled (10 characters) Password composition:Enabled (3 types, 1 characters per type) Password history: Enabled (max history records:4)，通过返回信息确认：用户口令长度为至少10位，包含数字、字母、字符三种类型，用户口令更改周期为90天；3、通过现场在防火墙中创建与网络管理员ylops同名账户时，防火墙中会提示用户名已存在，无法创重名用户，确认用户标识具备唯一性。 |
| 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、经现场核查防火墙配置策略，输入display password-control命令，返回信息为 Maximum login attempts: 3，Action for exceeding login attempts: Lock user for 1 minutes、User authentication timeout：600 seconds；2、通过返回信息确认用户连续错误登录3次锁定账户1分钟，用户登录连接超时时间限制为600秒。 |
| 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； | 1、经现场访谈网络管理员及核查其远程连接防火墙的方式，管理员在远程管理防火墙时采用SSH协议或HTTPS协议进行通信，防止鉴别信息在网络传输过程中被窃听；2、访谈网络管理员，Telnet协议默认为关闭状态，通过输入命令telnet server enable尝试启用Telnet协议，返回信息为Telnet is insecure because it transmits data in plaintext form，Telnet协议未启成功；3，通过在终端Telnet该防火墙，无法连接成功。 |
| 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。 | 经现场核查网络管理员远程登录防火墙方式，防火墙仅采用用户名、口令方式进行身份鉴别，未采用两种或两种以上组合的鉴别技术对用户进行身份鉴别。 |
| 访问控制 | a）应对登录的用户分配账户和权限； | 1、经现场核查防火墙中用户信息，通过输入display local-user命令，返回信息中显示防火墙中存在security、tulei、xuweilai、ylops等用户，其中security的 user role list：level-1，network-operator；tulei、xuweilai、ylops的 user role list：network-admin,network-operator。 |
| b）应重命名或删除默认账户，修改默认账户的默认口令； | 1、经现场核查防火墙中用户信息，通过输入display local-user命令，返回信息中显示防火墙中存在security、tulei、xuweilai、ylops等用户,不存在默认账户，2、经核查防火墙配置，输入display password-control命令，返回信息为 Password aging:Enabled (90 days) Password length: Enabled (10 characters) Password composition:Enabled (3 types, 1 characters per type) Password history: Enabled (max history records：3、用户口令已按照复杂度策略更改。 |
| 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； | 经现场核查防火墙中用户信息，通过输入display local-user命令，返回信息中显示防火墙中存在security、tulei、xuweilai、ylops等用户,经访谈网络管理员，其中tulei、xuweilai为两位网络管理员账号，ylops为网络主管账户，security为安全管理账号，不存在多余、过期、共享账户。 |
| 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； | 经现场核查防火墙中用户信息，通过输入display local-user命令，返回信息中显示防火墙中存在security、tulei、xuweilai、ylops等用户，经访谈网络管理员，防火墙中未单独创建审计管理员账户，并且网络管理员权限为超管用户权限，未实现管理用户权限最小化及权限分离。 |
| e）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； | 经核查配置文件及访谈，防火墙中由网络管理员角色账户为管理用户配置相应账号，并按照用户角色级别赋予管理用户操作权限。 |
| f）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； | 经核查配置文件及访谈，防火墙中访问控制策略为管理用户的防火墙中配置文件等进行配置管理及访问管理等，访问控制粒度达到主体为用户级、客体为文件级。 |
| g）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。 | 经核查配置文件及访谈，防火墙未对重要主体和客体设置安全标记。 |
| 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； | 经现场访谈网络管理员及核查防火墙配置，输入命令display logbuffer reverse，返回信息为logbuffer:enable；确认防火墙中其中安全审计功能，通过查看审计记录内容，确认审计记录中包含设备运行记录及用户操作行为审计记录等。 |
| 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； | 经现场核查防火墙中审计记录内容，攻击日志包括：时间、严重级别、攻击类型、动作类型、入安全域名称、目的地址、源地址等；用户操作日志包括：日期、时间、协议类型、IP地址、用户、命令详情等。 |
| 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、经访谈网络管理员，防火墙中所有用户均无权限对审计记录进行删除或修改，并且管理员在备份服务器（10.33.110.160）中添加审计记录下载脚本（python脚本），实时将防火墙中审计记录下载至备份服务器中进行备份；2、经现场核查备份服务器（10.33.110.160）中/home/network\_backup目录中存在审计记录备份文件，备份文件宿主为root，权限为744，其他用户仅拥有读权限。 |
| d）应对审计进程进行保护，防止未经授权的中断。 | 经现场访谈网络管理员，防火墙中审计进程受系统进程保护，所有用户均无权限将审计进程单独中断。 |
| 入侵防范 | a）应遵循最小安装的原则，仅安装需要的组件和应用程序； | 经访谈及核查配置文件，防火墙为厂商提供独立封装系统，不允许安装其他组件及应用程序，遵循最小安装原则。 |
| b）应关闭不需要的系统服务、默认共享和高危端口； | 经现场访谈网络管理员及核查防火墙配置，输入display current-fonfiguration，返回信息HTTP、Telnet协议均已关闭，防火墙中未启用不需要的系统服务、默认共享及高危端口。 |
| c）应通过设定终端接入方式或网络地址范围对通过网络进行管理的管理终端进行限制； | 经访谈网络管理员，在防火墙中添加访问控制策略，仅允许管理用户通过堡垒机远程管理网络设备、安全设备及服务器等，经核查防火墙中访问控制策略，具备堡垒机地址-设备管理网段（10.33.0.0）的访问控制策略。 |
| d）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； | 该测评项测评对象为业务应用系统、中间件和系统管理软件，故将该项调整为不适用。 |
| e）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； | 1、经访谈网络管理员，会定期对官方网站通报的安全漏洞进行评估，然后从官方网站下载安全补丁，经过综合评估测试后对防火墙系统进行补丁修复，避免系统中存在安全漏洞，2、经现场漏洞扫描，未发现防火墙中存在安全漏洞。 |
| f）应能够检测到对重要节点进行入侵的行为，并在发生严重入侵事件时提供报警。 | 经现场访谈及核查防火墙配置策略，防火墙中具备安全防护功能，在防火墙导航菜单栏中安全防护菜单中启用攻击防护策略，能够对从外部发起的攻击行为进行监测，发现外部攻击行为及时报警。 |
| 可信验证 | a）可基于可信根对计算设备的系统引导程序、系统程序、重要配置参数和应用程序等进行可信验证，并在应用程序的关键执行环节进行动态可信验证，在检测到其可信性受到破坏后进行报警，并将验证结果形成审计记录送至安全管理中心。 | 未基于可信根对计算设备提供可信验证。 |
| 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； | 经现场访谈网络管理员及对防火墙配置，防火墙中关闭Telnet协议，采用SSH协议或HTTPS协议进行通信，保证重要数据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。 | 经访谈网络管理员及核查H3C SecPath F1000系列防火墙产品文档，文件中目录05-参考指南--05文件系统管理命令中包含：“防火墙中文件系统通常使用摘要算法（SHA-256）对文件计算摘要值，用于验证文件的正确性和完整性”。 |
| 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； | 经现场访谈网络管理员及对防火墙配置，防火墙中关闭Telnet协议，采用SSH协议或HTTPS协议进行通信，保证重要数据在传输过程中的保密性。 |
| b）应采用密码技术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个人信息等。 | 经访谈网管理员，管理员在设置用户口令时添加simple参数，经核查H3C SecPath F1000系列防火墙产品文档，在文档05-参考指南--03-登录设备命令--1、登录设备--1.1等设备命令--1.1.28 set authentication password中正对simple参数进行说明：“simple：以明文方式设置密码，该密码将以密文方式存储。 |
| 数据备份恢复 | a）应提供重要数据的本地数据备份与恢复功能； | 经现场访谈网络管理员及核查相应配置，在备份服务器中配置python脚本，并设置每天凌晨4点将防火墙中配置文件下载至备份服务器中进行备份，管理员每周对备份文件进行巡检，确保配置文件完整备份至备份服务器中。 |
| b）应提供异地实时备份功能，利用通信网络将重要数据实时备份至备份场地； | 1、经现场访谈网络管理员，管理员添加了数据同步策略，每天将备份服务器中备份文件拷贝至阿里公共云备份服务器中进行备份；2、经核查阿里公共云备份服务器（10.30.19.10）中备份目录/data/network-backup中具备网络设备配置备份文件；3、综上，因世纪互联IDC机房及阿里云公共云均在上海市，未实现异地实时备份功能。 |
| c）应提供重要数据处理系统的热冗余，保证系统的高可用性。 | 经访谈访问管理员及核查网络拓扑图，重要数据处理系统中采用双机冗余部署，保证系统的高可用性。 |

4.1.2.18. 分拨中心出口防火墙4

|  |  |  |
| --- | --- | --- |
| **安全控制点** | **测评指标** | **结果记录** |
| 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、经现场访谈网络管理员，防火墙采用用户名、口令进行身份标识及身份鉴别；2、经核查防火墙配置，输入display password-control命令，返回信息为 Password aging:Enabled (90 days) Password length: Enabled (10 characters) Password composition:Enabled (3 types, 1 characters per type) Password history: Enabled (max history records:4)，通过返回信息确认：用户口令长度为至少10位，包含数字、字母、字符三种类型，用户口令更改周期为90天；3、通过现场在防火墙中创建与网络管理员ylops同名账户时，防火墙中会提示用户名已存在，无法创重名用户，确认用户标识具备唯一性。 |
| 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、经现场核查防火墙配置策略，输入display password-control命令，返回信息为 Maximum login attempts: 3，Action for exceeding login attempts: Lock user for 1 minutes、User authentication timeout：600 seconds；2、通过返回信息确认用户连续错误登录3次锁定账户1分钟，用户登录连接超时时间限制为600秒。 |
| 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； | 1、经现场访谈网络管理员及核查其远程连接防火墙的方式，管理员在远程管理防火墙时采用SSH协议或HTTPS协议进行通信，防止鉴别信息在网络传输过程中被窃听；2、访谈网络管理员，Telnet协议默认为关闭状态，通过输入命令telnet server enable尝试启用Telnet协议，返回信息为Telnet is insecure because it transmits data in plaintext form，Telnet协议未启成功；3，通过在终端Telnet该防火墙，无法连接成功。 |
| 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。 | 经现场核查网络管理员远程登录防火墙方式，防火墙仅采用用户名、口令方式进行身份鉴别，未采用两种或两种以上组合的鉴别技术对用户进行身份鉴别。 |
| 访问控制 | a）应对登录的用户分配账户和权限； | 1、经现场核查防火墙中用户信息，通过输入display local-user命令，返回信息中显示防火墙中存在security、tulei、xuweilai、ylops等用户，其中security的 user role list：level-1，network-operator；tulei、xuweilai、ylops的 user role list：network-admin,network-operator。 |
| b）应重命名或删除默认账户，修改默认账户的默认口令； | 1、经现场核查防火墙中用户信息，通过输入display local-user命令，返回信息中显示防火墙中存在security、tulei、xuweilai、ylops等用户,不存在默认账户，2、经核查防火墙配置，输入display password-control命令，返回信息为 Password aging:Enabled (90 days) Password length: Enabled (10 characters) Password composition:Enabled (3 types, 1 characters per type) Password history: Enabled (max history records：3、用户口令已按照复杂度策略更改。 |
| 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； | 经现场核查防火墙中用户信息，通过输入display local-user命令，返回信息中显示防火墙中存在security、tulei、xuweilai、ylops等用户,经访谈网络管理员，其中tulei、xuweilai为两位网络管理员账号，ylops为网络主管账户，security为安全管理账号，不存在多余、过期、共享账户。 |
| 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； | 经现场核查防火墙中用户信息，通过输入display local-user命令，返回信息中显示防火墙中存在security、tulei、xuweilai、ylops等用户，经访谈网络管理员，防火墙中未单独创建审计管理员账户，并且网络管理员权限为超管用户权限，未实现管理用户权限最小化及权限分离。 |
| e）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； | 经核查配置文件及访谈，防火墙中由网络管理员角色账户为管理用户配置相应账号，并按照用户角色级别赋予管理用户操作权限。 |
| f）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； | 经核查配置文件及访谈，防火墙中访问控制策略为管理用户的防火墙中配置文件等进行配置管理及访问管理等，访问控制粒度达到主体为用户级、客体为文件级。 |
| g）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。 | 经核查配置文件及访谈，防火墙未对重要主体和客体设置安全标记。 |
| 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； | 经现场访谈网络管理员及核查防火墙配置，输入命令display logbuffer reverse，返回信息为logbuffer:enable；确认防火墙中其中安全审计功能，通过查看审计记录内容，确认审计记录中包含设备运行记录及用户操作行为审计记录等。 |
| 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； | 经现场核查防火墙中审计记录内容，攻击日志包括：时间、严重级别、攻击类型、动作类型、入安全域名称、目的地址、源地址等；用户操作日志包括：日期、时间、协议类型、IP地址、用户、命令详情等。 |
| 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、经访谈网络管理员，防火墙中所有用户均无权限对审计记录进行删除或修改，并且管理员在备份服务器（10.33.110.160）中添加审计记录下载脚本（python脚本），实时将防火墙中审计记录下载至备份服务器中进行备份；2、经现场核查备份服务器（10.33.110.160）中/home/network\_backup目录中存在审计记录备份文件，备份文件宿主为root，权限为744，其他用户仅拥有读权限。 |
| d）应对审计进程进行保护，防止未经授权的中断。 | 经现场访谈网络管理员，防火墙中审计进程受系统进程保护，所有用户均无权限将审计进程单独中断。 |
| 入侵防范 | a）应遵循最小安装的原则，仅安装需要的组件和应用程序； | 经访谈及核查配置文件，防火墙为厂商提供独立封装系统，不允许安装其他组件及应用程序，遵循最小安装原则。 |
| b）应关闭不需要的系统服务、默认共享和高危端口； | 经现场访谈网络管理员及核查防火墙配置，输入display current-fonfiguration，返回信息HTTP、Telnet协议均已关闭，防火墙中未启用不需要的系统服务、默认共享及高危端口。 |
| c）应通过设定终端接入方式或网络地址范围对通过网络进行管理的管理终端进行限制； | 经访谈网络管理员，在防火墙中添加访问控制策略，仅允许管理用户通过堡垒机远程管理网络设备、安全设备及服务器等，经核查防火墙中访问控制策略，具备堡垒机地址-设备管理网段（10.33.0.0）的访问控制策略。 |
| d）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； | 该测评项测评对象为业务应用系统、中间件和系统管理软件，故将该项调整为不适用。 |
| e）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； | 1、经访谈网络管理员，会定期对官方网站通报的安全漏洞进行评估，然后从官方网站下载安全补丁，经过综合评估测试后对防火墙系统进行补丁修复，避免系统中存在安全漏洞，2、经现场漏洞扫描，未发现防火墙中存在安全漏洞。 |
| f）应能够检测到对重要节点进行入侵的行为，并在发生严重入侵事件时提供报警。 | 经现场访谈及核查防火墙配置策略，防火墙中具备安全防护功能，在防火墙导航菜单栏中安全防护菜单中启用攻击防护策略，能够对从外部发起的攻击行为进行监测，发现外部攻击行为及时报警。 |
| 可信验证 | a）可基于可信根对计算设备的系统引导程序、系统程序、重要配置参数和应用程序等进行可信验证，并在应用程序的关键执行环节进行动态可信验证，在检测到其可信性受到破坏后进行报警，并将验证结果形成审计记录送至安全管理中心。 | 未基于可信根对计算设备提供可信验证。 |
| 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； | 经现场访谈网络管理员及对防火墙配置，防火墙中关闭Telnet协议，采用SSH协议或HTTPS协议进行通信，保证重要数据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。 | 经访谈网络管理员及核查H3C SecPath F1000系列防火墙产品文档，文件中目录05-参考指南--05文件系统管理命令中包含：“防火墙中文件系统通常使用摘要算法（SHA-256）对文件计算摘要值，用于验证文件的正确性和完整性”。 |
| 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； | 经现场访谈网络管理员及对防火墙配置，防火墙中关闭Telnet协议，采用SSH协议或HTTPS协议进行通信，保证重要数据在传输过程中的保密性。 |
| b）应采用密码技术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个人信息等。 | 经访谈网管理员，管理员在设置用户口令时添加simple参数，经核查H3C SecPath F1000系列防火墙产品文档，在文档05-参考指南--03-登录设备命令--1、登录设备--1.1等设备命令--1.1.28 set authentication password中正对simple参数进行说明：“simple：以明文方式设置密码，该密码将以密文方式存储。 |
| 数据备份恢复 | a）应提供重要数据的本地数据备份与恢复功能； | 经现场访谈网络管理员及核查相应配置，在备份服务器中配置python脚本，并设置每天凌晨4点将防火墙中配置文件下载至备份服务器中进行备份，管理员每周对备份文件进行巡检，确保配置文件完整备份至备份服务器中。 |
| b）应提供异地实时备份功能，利用通信网络将重要数据实时备份至备份场地； | 1、经现场访谈网络管理员，管理员添加了数据同步策略，每天将备份服务器中备份文件拷贝至阿里公共云备份服务器中进行备份；2、经核查阿里公共云备份服务器（10.30.19.10）中备份目录/data/network-backup中具备网络设备配置备份文件；3、综上，因世纪互联IDC机房及阿里云公共云均在上海市，未实现异地实时备份功能。 |
| c）应提供重要数据处理系统的热冗余，保证系统的高可用性。 | 经访谈访问管理员及核查网络拓扑图，重要数据处理系统中采用双机冗余部署，保证系统的高可用性。 |

4.1.2.19. 分拨中心出口防火墙5

|  |  |  |
| --- | --- | --- |
| **安全控制点** | **测评指标** | **结果记录** |
| 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、经现场访谈网络管理员，防火墙采用用户名、口令进行身份标识及身份鉴别；2、经核查防火墙配置，输入display password-control命令，返回信息为 Password aging:Enabled (90 days) Password length: Enabled (10 characters) Password composition:Enabled (3 types, 1 characters per type) Password history: Enabled (max history records:4)，通过返回信息确认：用户口令长度为至少10位，包含数字、字母、字符三种类型，用户口令更改周期为90天；3、通过现场在防火墙中创建与网络管理员ylops同名账户时，防火墙中会提示用户名已存在，无法创重名用户，确认用户标识具备唯一性。 |
| 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、经现场核查防火墙配置策略，输入display password-control命令，返回信息为 Maximum login attempts: 3，Action for exceeding login attempts: Lock user for 1 minutes、User authentication timeout：600 seconds；2、通过返回信息确认用户连续错误登录3次锁定账户1分钟，用户登录连接超时时间限制为600秒。 |
| 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； | 1、经现场访谈网络管理员及核查其远程连接防火墙的方式，管理员在远程管理防火墙时采用SSH协议或HTTPS协议进行通信，防止鉴别信息在网络传输过程中被窃听；2、访谈网络管理员，Telnet协议默认为关闭状态，通过输入命令telnet server enable尝试启用Telnet协议，返回信息为Telnet is insecure because it transmits data in plaintext form，Telnet协议未启成功；3，通过在终端Telnet该防火墙，无法连接成功。 |
| 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。 | 经现场核查网络管理员远程登录防火墙方式，防火墙仅采用用户名、口令方式进行身份鉴别，未采用两种或两种以上组合的鉴别技术对用户进行身份鉴别。 |
| 访问控制 | a）应对登录的用户分配账户和权限； | 1、经现场核查防火墙中用户信息，通过输入display local-user命令，返回信息中显示防火墙中存在security、tulei、xuweilai、ylops等用户，其中security的 user role list：level-1，network-operator；tulei、xuweilai、ylops的 user role list：network-admin,network-operator。 |
| b）应重命名或删除默认账户，修改默认账户的默认口令； | 1、经现场核查防火墙中用户信息，通过输入display local-user命令，返回信息中显示防火墙中存在security、tulei、xuweilai、ylops等用户,不存在默认账户，2、经核查防火墙配置，输入display password-control命令，返回信息为 Password aging:Enabled (90 days) Password length: Enabled (10 characters) Password composition:Enabled (3 types, 1 characters per type) Password history: Enabled (max history records：3、用户口令已按照复杂度策略更改。 |
| 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； | 经现场核查防火墙中用户信息，通过输入display local-user命令，返回信息中显示防火墙中存在security、tulei、xuweilai、ylops等用户,经访谈网络管理员，其中tulei、xuweilai为两位网络管理员账号，ylops为网络主管账户，security为安全管理账号，不存在多余、过期、共享账户。 |
| 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； | 经现场核查防火墙中用户信息，通过输入display local-user命令，返回信息中显示防火墙中存在security、tulei、xuweilai、ylops等用户，经访谈网络管理员，防火墙中未单独创建审计管理员账户，并且网络管理员权限为超管用户权限，未实现管理用户权限最小化及权限分离。 |
| e）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； | 经核查配置文件及访谈，防火墙中由网络管理员角色账户为管理用户配置相应账号，并按照用户角色级别赋予管理用户操作权限。 |
| f）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； | 经核查配置文件及访谈，防火墙中访问控制策略为管理用户的防火墙中配置文件等进行配置管理及访问管理等，访问控制粒度达到主体为用户级、客体为文件级。 |
| g）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。 | 经核查配置文件及访谈，防火墙未对重要主体和客体设置安全标记。 |
| 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； | 经现场访谈网络管理员及核查防火墙配置，输入命令display logbuffer reverse，返回信息为logbuffer:enable；确认防火墙中其中安全审计功能，通过查看审计记录内容，确认审计记录中包含设备运行记录及用户操作行为审计记录等。 |
| 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； | 经现场核查防火墙中审计记录内容，攻击日志包括：时间、严重级别、攻击类型、动作类型、入安全域名称、目的地址、源地址等；用户操作日志包括：日期、时间、协议类型、IP地址、用户、命令详情等。 |
| 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、经访谈网络管理员，防火墙中所有用户均无权限对审计记录进行删除或修改，并且管理员在备份服务器（10.33.110.160）中添加审计记录下载脚本（python脚本），实时将防火墙中审计记录下载至备份服务器中进行备份；2、经现场核查备份服务器（10.33.110.160）中/home/network\_backup目录中存在审计记录备份文件，备份文件宿主为root，权限为744，其他用户仅拥有读权限。 |
| d）应对审计进程进行保护，防止未经授权的中断。 | 经现场访谈网络管理员，防火墙中审计进程受系统进程保护，所有用户均无权限将审计进程单独中断。 |
| 入侵防范 | a）应遵循最小安装的原则，仅安装需要的组件和应用程序； | 经访谈及核查配置文件，防火墙为厂商提供独立封装系统，不允许安装其他组件及应用程序，遵循最小安装原则。 |
| b）应关闭不需要的系统服务、默认共享和高危端口； | 经现场访谈网络管理员及核查防火墙配置，输入display current-fonfiguration，返回信息HTTP、Telnet协议均已关闭，防火墙中未启用不需要的系统服务、默认共享及高危端口。 |
| c）应通过设定终端接入方式或网络地址范围对通过网络进行管理的管理终端进行限制； | 经访谈网络管理员，在防火墙中添加访问控制策略，仅允许管理用户通过堡垒机远程管理网络设备、安全设备及服务器等，经核查防火墙中访问控制策略，具备堡垒机地址-设备管理网段（10.33.0.0）的访问控制策略。 |
| d）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； | 该测评项测评对象为业务应用系统、中间件和系统管理软件，故将该项调整为不适用。 |
| e）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； | 1、经访谈网络管理员，会定期对官方网站通报的安全漏洞进行评估，然后从官方网站下载安全补丁，经过综合评估测试后对防火墙系统进行补丁修复，避免系统中存在安全漏洞，2、经现场漏洞扫描，未发现防火墙中存在安全漏洞。 |
| f）应能够检测到对重要节点进行入侵的行为，并在发生严重入侵事件时提供报警。 | 经现场访谈及核查防火墙配置策略，防火墙中具备安全防护功能，在防火墙导航菜单栏中安全防护菜单中启用攻击防护策略，能够对从外部发起的攻击行为进行监测，发现外部攻击行为及时报警。 |
| 可信验证 | a）可基于可信根对计算设备的系统引导程序、系统程序、重要配置参数和应用程序等进行可信验证，并在应用程序的关键执行环节进行动态可信验证，在检测到其可信性受到破坏后进行报警，并将验证结果形成审计记录送至安全管理中心。 | 未基于可信根对计算设备提供可信验证。 |
| 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； | 经现场访谈网络管理员及对防火墙配置，防火墙中关闭Telnet协议，采用SSH协议或HTTPS协议进行通信，保证重要数据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。 | 经访谈网络管理员及核查H3C SecPath F1000系列防火墙产品文档，文件中目录05-参考指南--05文件系统管理命令中包含：“防火墙中文件系统通常使用摘要算法（SHA-256）对文件计算摘要值，用于验证文件的正确性和完整性”。 |
| 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； | 经现场访谈网络管理员及对防火墙配置，防火墙中关闭Telnet协议，采用SSH协议或HTTPS协议进行通信，保证重要数据在传输过程中的保密性。 |
| b）应采用密码技术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个人信息等。 | 经访谈网管理员，管理员在设置用户口令时添加simple参数，经核查H3C SecPath F1000系列防火墙产品文档，在文档05-参考指南--03-登录设备命令--1、登录设备--1.1等设备命令--1.1.28 set authentication password中正对simple参数进行说明：“simple：以明文方式设置密码，该密码将以密文方式存储。 |
| 数据备份恢复 | a）应提供重要数据的本地数据备份与恢复功能； | 经现场访谈网络管理员及核查相应配置，在备份服务器中配置python脚本，并设置每天凌晨4点将防火墙中配置文件下载至备份服务器中进行备份，管理员每周对备份文件进行巡检，确保配置文件完整备份至备份服务器中。 |
| b）应提供异地实时备份功能，利用通信网络将重要数据实时备份至备份场地； | 1、经现场访谈网络管理员，管理员添加了数据同步策略，每天将备份服务器中备份文件拷贝至阿里公共云备份服务器中进行备份；2、经核查阿里公共云备份服务器（10.30.19.10）中备份目录/data/network-backup中具备网络设备配置备份文件；3、综上，因世纪互联IDC机房及阿里云公共云均在上海市，未实现异地实时备份功能。 |
| c）应提供重要数据处理系统的热冗余，保证系统的高可用性。 | 经访谈访问管理员及核查网络拓扑图，重要数据处理系统中采用双机冗余部署，保证系统的高可用性。 |

4.1.2.20. 分拨中心出口防火墙6-20

|  |  |  |
| --- | --- | --- |
| **安全控制点** | **测评指标** | **结果记录** |
| 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、经现场访谈网络管理员，防火墙采用用户名、口令进行身份标识及身份鉴别；2、经核查防火墙配置，输入display password-control命令，返回信息为 Password aging:Enabled (90 days) Password length: Enabled (10 characters) Password composition:Enabled (3 types, 1 characters per type) Password history: Enabled (max history records:4)，通过返回信息确认：用户口令长度为至少10位，包含数字、字母、字符三种类型，用户口令更改周期为90天；3、通过现场在防火墙中创建与网络管理员ylops同名账户时，防火墙中会提示用户名已存在，无法创重名用户，确认用户标识具备唯一性。 |
| 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、经现场核查防火墙配置策略，输入display password-control命令，返回信息为 Maximum login attempts: 3，Action for exceeding login attempts: Lock user for 1 minutes、User authentication timeout：600 seconds；2、通过返回信息确认用户连续错误登录3次锁定账户1分钟，用户登录连接超时时间限制为600秒。 |
| 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； | 1、经现场访谈网络管理员及核查其远程连接防火墙的方式，管理员在远程管理防火墙时采用SSH协议或HTTPS协议进行通信，防止鉴别信息在网络传输过程中被窃听；2、访谈网络管理员，Telnet协议默认为关闭状态，通过输入命令telnet server enable尝试启用Telnet协议，返回信息为Telnet is insecure because it transmits data in plaintext form，Telnet协议未启成功；3，通过在终端Telnet该防火墙，无法连接成功。 |
| 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。 | 经现场核查网络管理员远程登录防火墙方式，防火墙仅采用用户名、口令方式进行身份鉴别，未采用两种或两种以上组合的鉴别技术对用户进行身份鉴别。 |
| 访问控制 | a）应对登录的用户分配账户和权限； | 1、经现场核查防火墙中用户信息，通过输入display local-user命令，返回信息中显示防火墙中存在security、tulei、xuweilai、ylops等用户，其中security的 user role list：level-1，network-operator；tulei、xuweilai、ylops的 user role list：network-admin,network-operator。 |
| b）应重命名或删除默认账户，修改默认账户的默认口令； | 1、经现场核查防火墙中用户信息，通过输入display local-user命令，返回信息中显示防火墙中存在security、tulei、xuweilai、ylops等用户,不存在默认账户，2、经核查防火墙配置，输入display password-control命令，返回信息为 Password aging:Enabled (90 days) Password length: Enabled (10 characters) Password composition:Enabled (3 types, 1 characters per type) Password history: Enabled (max history records：3、用户口令已按照复杂度策略更改。 |
| 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； | 经现场核查防火墙中用户信息，通过输入display local-user命令，返回信息中显示防火墙中存在security、tulei、xuweilai、ylops等用户,经访谈网络管理员，其中tulei、xuweilai为两位网络管理员账号，ylops为网络主管账户，security为安全管理账号，不存在多余、过期、共享账户。 |
| 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； | 经现场核查防火墙中用户信息，通过输入display local-user命令，返回信息中显示防火墙中存在security、tulei、xuweilai、ylops等用户，经访谈网络管理员，防火墙中未单独创建审计管理员账户，并且网络管理员权限为超管用户权限，未实现管理用户权限最小化及权限分离。 |
| e）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； | 经核查配置文件及访谈，防火墙中由网络管理员角色账户为管理用户配置相应账号，并按照用户角色级别赋予管理用户操作权限。 |
| f）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； | 经核查配置文件及访谈，防火墙中访问控制策略为管理用户的防火墙中配置文件等进行配置管理及访问管理等，访问控制粒度达到主体为用户级、客体为文件级。 |
| g）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。 | 经核查配置文件及访谈，防火墙未对重要主体和客体设置安全标记。 |
| 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； | 经现场访谈网络管理员及核查防火墙配置，输入命令display logbuffer reverse，返回信息为logbuffer:enable；确认防火墙中其中安全审计功能，通过查看审计记录内容，确认审计记录中包含设备运行记录及用户操作行为审计记录等。 |
| 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； | 经现场核查防火墙中审计记录内容，攻击日志包括：时间、严重级别、攻击类型、动作类型、入安全域名称、目的地址、源地址等；用户操作日志包括：日期、时间、协议类型、IP地址、用户、命令详情等。 |
| 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、经访谈网络管理员，防火墙中所有用户均无权限对审计记录进行删除或修改，并且管理员在备份服务器（10.33.110.160）中添加审计记录下载脚本（python脚本），实时将防火墙中审计记录下载至备份服务器中进行备份；2、经现场核查备份服务器（10.33.110.160）中/home/network\_backup目录中存在审计记录备份文件，备份文件宿主为root，权限为744，其他用户仅拥有读权限。 |
| d）应对审计进程进行保护，防止未经授权的中断。 | 经现场访谈网络管理员，防火墙中审计进程受系统进程保护，所有用户均无权限将审计进程单独中断。 |
| 入侵防范 | a）应遵循最小安装的原则，仅安装需要的组件和应用程序； | 经访谈及核查配置文件，防火墙为厂商提供独立封装系统，不允许安装其他组件及应用程序，遵循最小安装原则。 |
| b）应关闭不需要的系统服务、默认共享和高危端口； | 经现场访谈网络管理员及核查防火墙配置，输入display current-fonfiguration，返回信息HTTP、Telnet协议均已关闭，防火墙中未启用不需要的系统服务、默认共享及高危端口。 |
| c）应通过设定终端接入方式或网络地址范围对通过网络进行管理的管理终端进行限制； | 经访谈网络管理员，在防火墙中添加访问控制策略，仅允许管理用户通过堡垒机远程管理网络设备、安全设备及服务器等，经核查防火墙中访问控制策略，具备堡垒机地址-设备管理网段（10.33.0.0）的访问控制策略。 |
| d）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； | 该测评项测评对象为业务应用系统、中间件和系统管理软件，故将该项调整为不适用。 |
| e）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； | 1、经访谈网络管理员，会定期对官方网站通报的安全漏洞进行评估，然后从官方网站下载安全补丁，经过综合评估测试后对防火墙系统进行补丁修复，避免系统中存在安全漏洞，2、经现场漏洞扫描，未发现防火墙中存在安全漏洞。 |
| f）应能够检测到对重要节点进行入侵的行为，并在发生严重入侵事件时提供报警。 | 经现场访谈及核查防火墙配置策略，防火墙中具备安全防护功能，在防火墙导航菜单栏中安全防护菜单中启用攻击防护策略，能够对从外部发起的攻击行为进行监测，发现外部攻击行为及时报警。 |
| 可信验证 | a）可基于可信根对计算设备的系统引导程序、系统程序、重要配置参数和应用程序等进行可信验证，并在应用程序的关键执行环节进行动态可信验证，在检测到其可信性受到破坏后进行报警，并将验证结果形成审计记录送至安全管理中心。 | 未基于可信根对计算设备提供可信验证。 |
| 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； | 经现场访谈网络管理员及对防火墙配置，防火墙中关闭Telnet协议，采用SSH协议或HTTPS协议进行通信，保证重要数据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。 | 经访谈网络管理员及核查H3C SecPath F1000系列防火墙产品文档，文件中目录05-参考指南--05文件系统管理命令中包含：“防火墙中文件系统通常使用摘要算法（SHA-256）对文件计算摘要值，用于验证文件的正确性和完整性”。 |
| 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； | 经现场访谈网络管理员及对防火墙配置，防火墙中关闭Telnet协议，采用SSH协议或HTTPS协议进行通信，保证重要数据在传输过程中的保密性。 |
| b）应采用密码技术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个人信息等。 | 经访谈网管理员，管理员在设置用户口令时添加simple参数，经核查H3C SecPath F1000系列防火墙产品文档，在文档05-参考指南--03-登录设备命令--1、登录设备--1.1等设备命令--1.1.28 set authentication password中正对simple参数进行说明：“simple：以明文方式设置密码，该密码将以密文方式存储。 |
| 数据备份恢复 | a）应提供重要数据的本地数据备份与恢复功能； | 经现场访谈网络管理员及核查相应配置，在备份服务器中配置python脚本，并设置每天凌晨4点将防火墙中配置文件下载至备份服务器中进行备份，管理员每周对备份文件进行巡检，确保配置文件完整备份至备份服务器中。 |
| b）应提供异地实时备份功能，利用通信网络将重要数据实时备份至备份场地； | 1、经现场访谈网络管理员，管理员添加了数据同步策略，每天将备份服务器中备份文件拷贝至阿里公共云备份服务器中进行备份；2、经核查阿里公共云备份服务器（10.30.19.10）中备份目录/data/network-backup中具备网络设备配置备份文件；3、综上，因世纪互联IDC机房及阿里云公共云均在上海市，未实现异地实时备份功能。 |
| c）应提供重要数据处理系统的热冗余，保证系统的高可用性。 | 经访谈访问管理员及核查网络拓扑图，重要数据处理系统中采用双机冗余部署，保证系统的高可用性。 |

|  |  |  |  |
| --- | --- | --- | --- |
| **测评项目** |  | **测评对象** | 服务器和终端 |
| **测评单位** |  | | |
| **测评地点** |  | | |
| **测评人员** |  | **配合人员** | 刘亮 |
| **测评日期** | 2023.6.15 | | |
| **测评人员签字** |  | **配合人员签字** |  |

4.1.3. 服务器和终端

4.1.3.1. 应用服务器1

|  |  |  |
| --- | --- | --- |
| **安全控制点** | **测评指标** | **结果记录** |
| 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）操作系统时采用用户名+SSHKey公私钥进行身份鉴别鉴别信息具有复杂度要求；2）执行cat /etc/shadow命令，查看shadow文件系统内用户身份标识唯一，不存在同名用户，且不存在空口令账号；3）经访谈，SSHKey公私钥每半年进行更换；4）查看sshd\_config配置文件中配置PasswordAuthentication no，拒绝使用密码方式进行身份鉴别。 |
| 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； | 操作系统采用用户名+SSHKey公私钥进行身份鉴别，可以防止鉴别信息被暴力破解；但未配置用户连接超时退出策略。 |
| 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； | 1）经核查，管理人员采用SSH协议连接操作系统；2）执行netatat –tpln| grep 23命令查看操作系统远程管理端口，不存在Telnet端口，防止鉴别信息在网络传输过程中的被窃听。 |
| 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。 | 未采用两种或两种以上组合的鉴别技术对用户进行身份鉴别。 |
| 访问控制 | a）应对登录的用户分配账户和权限； | 1）经访谈，通过root账户为登录的用户创建账户、分配权限；2）执行ls -l命令查看关键文件权限，均已为账户分配了相应权限，相关文件权限设置为/etc/shadow：000、/etc/passwd：644、/etc/group：644、/etc/profile：644、/etc/crontab：644、/ etc/securetty：600、/etc/ssh/sshd\_config：600。 |
| b）应重命名或删除默认账户，修改默认账户的默认口令； | 1）执行cat /etc/shadow命令查看shadow文件，操作系统中adm、lp、sync、shutdown、halt、mail、uucp、operator、games、gopher等账户均为nologin状态，存在默认账户root；2）执行more /etc/ssh/sshd\_config命令，查看“PermitRootLogin”参数设置为“yes”，即允许root远程登录；3）经访谈，root用户需通过公私钥方式进行身份鉴别。 |
| 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； | 1）执行cat /etc/shadow命令查看shadow文件，发现操作系统存在root、ysup、yops、yluser等在用账户，不存在多余的、过期账户；2）存在多个堡垒机账户登录操作系统时共用一个账户的情况。 |
| 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； | root账户具有系统所有权限，未实现管理用户的权限分离。 |
| e）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； | 经访谈，由系统管理员root配置访问控制策略，如：/etc/passwd，/etc/profile宿主为root、权限设置为644，audit文件为700、message文件为600，其他文件权限为750，实现用户对文件的权限控制。 |
| f）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； | 由管理用户进行用户访问权限分配进行设置，依据访问控制策略,对各类文件进行访问，重要文件和目录权限均在合理范围内，用户可根据文件不同的权限进行操作。 |
| g）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。 | 执 行more /etc/selinux/config 命令，查看config文件显示 SELINUX参数为 DISABLED，即未开启强制访问控制模式。 |
| 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）执行ps -ef|grep rsyslog和ps -ef|grep auditd命令，显示rsyslog和auditd进程正在运行；2）more /etc/audit/audit.rules，显示审计内容包括：\*.info、authriv.\*、mail.\*、cron.\*、\*.emerg、uucp、news.crit、local7.\*等事件。 |
| 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； | 执行tail -20 /var/log/audit/audit.log命令，查看近20条审计日志，内容包括：时间、对象、路径、用户ID、相关的系统调用、用户执行命令等。 |
| 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）通过访问权限对审计记录进行保护，日志文件/var/log/messages、/var/log/secure、/var/log/audit/audit.log访问 权限均为600；2）审计记录本地保存，且实时备份至360本地安全大脑，保存时间满足180天以上。 |
| d）应对审计进程进行保护，防止未经授权的中断。 | 执行service auditd status命令，系统开启auditd审计保护进程，审计进程由root用户维护，经现场使用yluser用户通过service auditd stop命令尝试中断审计进程，无法将审计进程单独中断。 |
| 入侵防范 | a）应遵循最小安装的原则，仅安装需要的组件和应用程序； | 1）系统安装遵循最小化安装原则；2）执行yum list installed命令查看操作系统已安装的程序包，存在Java、SSH、天眼云镜agent等应用程序或组件，不存在与业务系统无关的组件和应用程序。 |
| b）应关闭不需要的系统服务、默认共享和高危端口； | 1）执行systemctl list-unit-files 命令，系统已关闭FTP、Telnet 等高危网络服务；2）执行netstat -pantu命令，系统关闭了135、445等高危端口，仅开启了22、8080等端口。 |
| c）应通过设定终端接入方式或网络地址范围对通过网络进行管理的管理终端进行限制； | 经核查，1）通过配置安全组策略限制仅允许通过堡垒机管理服务器；2）经核查防火墙中访问控制策略，具备堡垒机地址-服务器管理网段（10.33.0.0）的访问控制策略。 |
| d）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； | 根据GB∕T 28448-2019 《信息安全技术 网络安全等级保护测评要求》测评对象范围描述，服务器无该项要求，故判为“不适用”。 |
| e）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； | 1）经过漏洞扫描，服务器不存在高危安全漏洞；2）执行rpm -qa grep patch命令，查看系统补丁已更新至最新。 |
| f）应能够检测到对重要节点进行入侵的行为，并在发生严重入侵事件时提供报警。 | 经核查，服务器上安装有青藤云天眼云镜，对主机入侵行为进行检测，发现严重安全事件时通过钉钉告警。 |
| 恶意代码防范 | a）应采用免受恶意代码攻击的技术措施或主动免疫可信验证机制及时识别入侵和病毒行为，并将其有效阻断。 | 经核查，服务器上安装有青藤云天眼云镜，对主机恶意代码进行检测、清除，每天凌晨自动更新恶意代码特征库，经核查，具备恶意代码特征库更新记录。 |
| 可信验证 | a）可基于可信根对计算设备的系统引导程序、系统程序、重要配置参数和应用程序等进行可信验证，并在应用程序的关键执行环节进行动态可信验证，在检测到其可信性受到破坏后进行报警，并将验证结果形成审计记录送至安全管理中心。 | 未采用技术措施对计算设备的系统引导程序、系统程序、重要配置参数和通信应用程序等进行可信验证。 |
| 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； | 采用SSH协议连接操作系统，保证了鉴别信息以及管理数据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。 | 操作系统中对重要鉴别信息通过自身的加密及校验（SHA256），保证数据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； | 采用SSH协议连接操作系统，保证了鉴别信息以及管理数据在传输过程中的保密性。 |
| b）应采用密码技术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个人信息等。 | 通过系统自带的加密模块保证鉴别数据在存储过程中的保密性。 |
| 数据备份恢复 | a）应提供重要数据的本地数据备份与恢复功能； | 经核查，通过脚本每周将配置文件、代码仓库等数据备份至备份服务器中，依据需要验证备份数据的有效性。 |
| b）应提供异地实时备份功能，利用通信网络将重要数据实时备份至备份场地； | 系统无异地备份机制。 |
| c）应提供重要数据处理系统的热冗余，保证系统的高可用性。 | 服务器采用K8S容器部署，保证系统的高可用性。 |
| 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； | 操作系统提供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功能。 |
| 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。 | 操作系统提供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的功能。 |

4.1.3.2. 应用服务器2

|  |  |  |
| --- | --- | --- |
| **安全控制点** | **测评指标** | **结果记录** |
| 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）操作系统时采用用户名+SSHKey公私钥进行身份鉴别鉴别信息具有复杂度要求；2）执行cat /etc/shadow命令，查看shadow文件系统内用户身份标识唯一，不存在同名用户，且不存在空口令账号；3）经访谈，SSHKey公私钥每半年进行更换；4）查看sshd\_config配置文件中配置PasswordAuthentication no，拒绝使用密码方式进行身份鉴别。 |
| 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； | 操作系统采用用户名+SSHKey公私钥进行身份鉴别，可以防止鉴别信息被暴力破解；但未配置用户连接超时退出策略。 |
| 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； | 1）经核查，管理人员采用SSH协议连接操作系统；2）执行netatat –tpln| grep 23命令查看操作系统远程管理端口，不存在Telnet端口，防止鉴别信息在网络传输过程中的被窃听。 |
| 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。 | 未采用两种或两种以上组合的鉴别技术对用户进行身份鉴别。 |
| 访问控制 | a）应对登录的用户分配账户和权限； | 1）经访谈，通过root账户为登录的用户创建账户、分配权限；2）执行ls -l命令查看关键文件权限，均已为账户分配了相应权限，相关文件权限设置为/etc/shadow：000、/etc/passwd：644、/etc/group：644、/etc/profile：644、/etc/crontab：644、/ etc/securetty：600、/etc/ssh/sshd\_config：600。 |
| b）应重命名或删除默认账户，修改默认账户的默认口令； | 1）执行cat /etc/shadow命令查看shadow文件，操作系统中adm、lp、sync、shutdown、halt、mail、uucp、operator、games、gopher等账户均为nologin状态，存在默认账户root；2）执行more /etc/ssh/sshd\_config命令，查看“PermitRootLogin”参数设置为“yes”，即允许root远程登录；3）经访谈，root用户需通过公私钥方式进行身份鉴别。 |
| 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； | 1）执行cat /etc/shadow命令查看shadow文件，发现操作系统存在root、ysup、yops、yluser等在用账户，不存在多余的、过期账户；2）存在多个堡垒机账户登录操作系统时共用一个账户的情况。 |
| 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； | root账户具有系统所有权限，未实现管理用户的权限分离。 |
| e）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； | 经访谈，由系统管理员root配置访问控制策略，如：/etc/passwd，/etc/profile宿主为root、权限设置为644，audit文件为700、message文件为600，其他文件权限为750，实现用户对文件的权限控制。 |
| f）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； | 由管理用户进行用户访问权限分配进行设置，依据访问控制策略,对各类文件进行访问，重要文件和目录权限均在合理范围内，用户可根据文件不同的权限进行操作。 |
| g）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。 | 执 行more /etc/selinux/config 命令，查看config文件显示 SELINUX参数为 DISABLED，即未开启强制访问控制模式。 |
| 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）执行ps -ef|grep rsyslog和ps -ef|grep auditd命令，显示rsyslog和auditd进程正在运行；2）more /etc/audit/audit.rules，显示审计内容包括：\*.info、authriv.\*、mail.\*、cron.\*、\*.emerg、uucp、news.crit、local7.\*等事件。 |
| 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； | 执行tail -20 /var/log/audit/audit.log命令，查看近20条审计日志，内容包括：时间、对象、路径、用户ID、相关的系统调用、用户执行命令等。 |
| 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）通过访问权限对审计记录进行保护，日志文件/var/log/messages、/var/log/secure、/var/log/audit/audit.log访问 权限均为600；2）审计记录本地保存，且实时备份至360本地安全大脑，保存时间满足180天以上。 |
| d）应对审计进程进行保护，防止未经授权的中断。 | 执行service auditd status命令，系统开启auditd审计保护进程，审计进程由root用户维护，经现场使用yluser用户通过service auditd stop命令尝试中断审计进程，无法将审计进程单独中断。 |
| 入侵防范 | a）应遵循最小安装的原则，仅安装需要的组件和应用程序； | 1）系统安装遵循最小化安装原则；2）执行yum list installed命令查看操作系统已安装的程序包，存在Java、SSH、天眼云镜agent等应用程序或组件，不存在与业务系统无关的组件和应用程序。 |
| b）应关闭不需要的系统服务、默认共享和高危端口； | 1）执行systemctl list-unit-files 命令，系统已关闭FTP、Telnet 等高危网络服务；2）执行netstat -pantu命令，系统关闭了135、445等高危端口，仅开启了22、8080等端口。 |
| c）应通过设定终端接入方式或网络地址范围对通过网络进行管理的管理终端进行限制； | 经核查，1）通过配置安全组策略限制仅允许通过堡垒机管理服务器；2）经核查防火墙中访问控制策略，具备堡垒机地址-服务器管理网段（10.33.0.0）的访问控制策略。 |
| d）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； | 根据GB∕T 28448-2019 《信息安全技术 网络安全等级保护测评要求》测评对象范围描述，服务器无该项要求，故判为“不适用”。 |
| e）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； | 1）经过漏洞扫描，服务器不存在高危安全漏洞；2）执行rpm -qa grep patch命令，查看系统补丁已更新至最新。 |
| f）应能够检测到对重要节点进行入侵的行为，并在发生严重入侵事件时提供报警。 | 经核查，服务器上安装有青藤云天眼云镜，对主机入侵行为进行检测，发现严重安全事件时通过钉钉告警。 |
| 恶意代码防范 | a）应采用免受恶意代码攻击的技术措施或主动免疫可信验证机制及时识别入侵和病毒行为，并将其有效阻断。 | 经核查，服务器上安装有青藤云天眼云镜，对主机恶意代码进行检测、清除，每天凌晨自动更新恶意代码特征库，经核查，具备恶意代码特征库更新记录。 |
| 可信验证 | a）可基于可信根对计算设备的系统引导程序、系统程序、重要配置参数和应用程序等进行可信验证，并在应用程序的关键执行环节进行动态可信验证，在检测到其可信性受到破坏后进行报警，并将验证结果形成审计记录送至安全管理中心。 | 未采用技术措施对计算设备的系统引导程序、系统程序、重要配置参数和通信应用程序等进行可信验证。 |
| 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； | 采用SSH协议连接操作系统，保证了鉴别信息以及管理数据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。 | 操作系统中对重要鉴别信息通过自身的加密及校验（SHA256），保证数据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； | 采用SSH协议连接操作系统，保证了鉴别信息以及管理数据在传输过程中的保密性。 |
| b）应采用密码技术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个人信息等。 | 通过系统自带的加密模块保证鉴别数据在存储过程中的保密性。 |
| 数据备份恢复 | a）应提供重要数据的本地数据备份与恢复功能； | 经核查，通过脚本每周将配置文件、代码仓库等数据备份至备份服务器中，依据需要验证备份数据的有效性。 |
| b）应提供异地实时备份功能，利用通信网络将重要数据实时备份至备份场地； | 系统无异地备份机制。 |
| c）应提供重要数据处理系统的热冗余，保证系统的高可用性。 | 服务器采用K8S容器部署，保证系统的高可用性。 |
| 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； | 操作系统提供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功能。 |
| 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。 | 操作系统提供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的功能。 |

4.1.3.3. 应用服务器3

|  |  |  |
| --- | --- | --- |
| **安全控制点** | **测评指标** | **结果记录** |
| 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）操作系统时采用用户名+SSHKey公私钥进行身份鉴别鉴别信息具有复杂度要求；2）执行cat /etc/shadow命令，查看shadow文件系统内用户身份标识唯一，不存在同名用户，且不存在空口令账号；3）经访谈，SSHKey公私钥每半年进行更换；4）查看sshd\_config配置文件中配置PasswordAuthentication no，拒绝使用密码方式进行身份鉴别。 |
| 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； | 操作系统采用用户名+SSHKey公私钥进行身份鉴别，可以防止鉴别信息被暴力破解；但未配置用户连接超时退出策略。 |
| 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； | 1）经核查，管理人员采用SSH协议连接操作系统；2）执行netatat –tpln| grep 23命令查看操作系统远程管理端口，不存在Telnet端口，防止鉴别信息在网络传输过程中的被窃听。 |
| 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。 | 未采用两种或两种以上组合的鉴别技术对用户进行身份鉴别。 |
| 访问控制 | a）应对登录的用户分配账户和权限； | 1）经访谈，通过root账户为登录的用户创建账户、分配权限；2）执行ls -l命令查看关键文件权限，均已为账户分配了相应权限，相关文件权限设置为/etc/shadow：000、/etc/passwd：644、/etc/group：644、/etc/profile：644、/etc/crontab：644、/ etc/securetty：600、/etc/ssh/sshd\_config：600。 |
| b）应重命名或删除默认账户，修改默认账户的默认口令； | 1）执行cat /etc/shadow命令查看shadow文件，操作系统中adm、lp、sync、shutdown、halt、mail、uucp、operator、games、gopher等账户均为nologin状态，存在默认账户root；2）执行more /etc/ssh/sshd\_config命令，查看“PermitRootLogin”参数设置为“yes”，即允许root远程登录；3）经访谈，root用户需通过公私钥方式进行身份鉴别。 |
| 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； | 1）执行cat /etc/shadow命令查看shadow文件，发现操作系统存在root、ysup、yops、yluser等在用账户，不存在多余的、过期账户；2）存在多个堡垒机账户登录操作系统时共用一个账户的情况。 |
| 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； | root账户具有系统所有权限，未实现管理用户的权限分离。 |
| e）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； | 经访谈，由系统管理员root配置访问控制策略，如：/etc/passwd，/etc/profile宿主为root、权限设置为644，audit文件为700、message文件为600，其他文件权限为750，实现用户对文件的权限控制。 |
| f）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； | 由管理用户进行用户访问权限分配进行设置，依据访问控制策略,对各类文件进行访问，重要文件和目录权限均在合理范围内，用户可根据文件不同的权限进行操作。 |
| g）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。 | 执 行more /etc/selinux/config 命令，查看config文件显示 SELINUX参数为 DISABLED，即未开启强制访问控制模式。 |
| 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）执行ps -ef|grep rsyslog和ps -ef|grep auditd命令，显示rsyslog和auditd进程正在运行；2）more /etc/audit/audit.rules，显示审计内容包括：\*.info、authriv.\*、mail.\*、cron.\*、\*.emerg、uucp、news.crit、local7.\*等事件。 |
| 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； | 执行tail -20 /var/log/audit/audit.log命令，查看近20条审计日志，内容包括：时间、对象、路径、用户ID、相关的系统调用、用户执行命令等。 |
| 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）通过访问权限对审计记录进行保护，日志文件/var/log/messages、/var/log/secure、/var/log/audit/audit.log访问 权限均为600；2）审计记录本地保存，且实时备份至360本地安全大脑，保存时间满足180天以上。 |
| d）应对审计进程进行保护，防止未经授权的中断。 | 执行service auditd status命令，系统开启auditd审计保护进程，审计进程由root用户维护，经现场使用yluser用户通过service auditd stop命令尝试中断审计进程，无法将审计进程单独中断。 |
| 入侵防范 | a）应遵循最小安装的原则，仅安装需要的组件和应用程序； | 1）系统安装遵循最小化安装原则；2）执行yum list installed命令查看操作系统已安装的程序包，存在Java、SSH、天眼云镜agent等应用程序或组件，不存在与业务系统无关的组件和应用程序。 |
| b）应关闭不需要的系统服务、默认共享和高危端口； | 1）执行systemctl list-unit-files 命令，系统已关闭FTP、Telnet 等高危网络服务；2）执行netstat -pantu命令，系统关闭了135、445等高危端口，仅开启了22、8080等端口。 |
| c）应通过设定终端接入方式或网络地址范围对通过网络进行管理的管理终端进行限制； | 经核查，1）通过配置安全组策略限制仅允许通过堡垒机管理服务器；2）经核查防火墙中访问控制策略，具备堡垒机地址-服务器管理网段（10.33.0.0）的访问控制策略。 |
| d）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； | 根据GB∕T 28448-2019 《信息安全技术 网络安全等级保护测评要求》测评对象范围描述，服务器无该项要求，故判为“不适用”。 |
| e）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； | 1）经过漏洞扫描，服务器不存在高危安全漏洞；2）执行rpm -qa grep patch命令，查看系统补丁已更新至最新。 |
| f）应能够检测到对重要节点进行入侵的行为，并在发生严重入侵事件时提供报警。 | 经核查，服务器上安装有青藤云天眼云镜，对主机入侵行为进行检测，发现严重安全事件时通过钉钉告警。 |
| 恶意代码防范 | a）应采用免受恶意代码攻击的技术措施或主动免疫可信验证机制及时识别入侵和病毒行为，并将其有效阻断。 | 经核查，服务器上安装有青藤云天眼云镜，对主机恶意代码进行检测、清除，每天凌晨自动更新恶意代码特征库，经核查，具备恶意代码特征库更新记录。 |
| 可信验证 | a）可基于可信根对计算设备的系统引导程序、系统程序、重要配置参数和应用程序等进行可信验证，并在应用程序的关键执行环节进行动态可信验证，在检测到其可信性受到破坏后进行报警，并将验证结果形成审计记录送至安全管理中心。 | 未采用技术措施对计算设备的系统引导程序、系统程序、重要配置参数和通信应用程序等进行可信验证。 |
| 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； | 采用SSH协议连接操作系统，保证了鉴别信息以及管理数据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。 | 操作系统中对重要鉴别信息通过自身的加密及校验（SHA256），保证数据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； | 采用SSH协议连接操作系统，保证了鉴别信息以及管理数据在传输过程中的保密性。 |
| b）应采用密码技术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个人信息等。 | 通过系统自带的加密模块保证鉴别数据在存储过程中的保密性。 |
| 数据备份恢复 | a）应提供重要数据的本地数据备份与恢复功能； | 经核查，通过脚本每周将配置文件、代码仓库等数据备份至备份服务器中，依据需要验证备份数据的有效性。 |
| b）应提供异地实时备份功能，利用通信网络将重要数据实时备份至备份场地； | 系统无异地备份机制。 |
| c）应提供重要数据处理系统的热冗余，保证系统的高可用性。 | 服务器采用K8S容器部署，保证系统的高可用性。 |
| 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； | 操作系统提供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功能。 |
| 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。 | 操作系统提供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的功能。 |

4.1.3.4. 应用服务器6

|  |  |  |
| --- | --- | --- |
| **安全控制点** | **测评指标** | **结果记录** |
| 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）操作系统时采用用户名+SSHKey公私钥进行身份鉴别鉴别信息具有复杂度要求；2）执行cat /etc/shadow命令，查看shadow文件系统内用户身份标识唯一，不存在同名用户，且不存在空口令账号；3）经访谈，SSHKey公私钥每半年进行更换；4）查看sshd\_config配置文件中配置PasswordAuthentication no，拒绝使用密码方式进行身份鉴别。 |
| 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； | 操作系统采用用户名+SSHKey公私钥进行身份鉴别，可以防止鉴别信息被暴力破解；但未配置用户连接超时退出策略。 |
| 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； | 1）经核查，管理人员采用SSH协议连接操作系统；2）执行netatat –tpln| grep 23命令查看操作系统远程管理端口，不存在Telnet端口，防止鉴别信息在网络传输过程中的被窃听。 |
| 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。 | 未采用两种或两种以上组合的鉴别技术对用户进行身份鉴别。 |
| 访问控制 | a）应对登录的用户分配账户和权限； | 1）经访谈，通过root账户为登录的用户创建账户、分配权限；2）执行ls -l命令查看关键文件权限，均已为账户分配了相应权限，相关文件权限设置为/etc/shadow：000、/etc/passwd：644、/etc/group：644、/etc/profile：644、/etc/crontab：644、/ etc/securetty：600、/etc/ssh/sshd\_config：600。 |
| b）应重命名或删除默认账户，修改默认账户的默认口令； | 1）执行cat /etc/shadow命令查看shadow文件，操作系统中adm、lp、sync、shutdown、halt、mail、uucp、operator、games、gopher等账户均为nologin状态，存在默认账户root；2）执行more /etc/ssh/sshd\_config命令，查看“PermitRootLogin”参数设置为“yes”，即允许root远程登录；3）经访谈，root用户需通过公私钥方式进行身份鉴别。 |
| 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； | 1）执行cat /etc/shadow命令查看shadow文件，发现操作系统存在root、ysup、yops、yluser等在用账户，不存在多余的、过期账户；2）存在多个堡垒机账户登录操作系统时共用一个账户的情况。 |
| 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； | root账户具有系统所有权限，未实现管理用户的权限分离。 |
| e）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； | 经访谈，由系统管理员root配置访问控制策略，如：/etc/passwd，/etc/profile宿主为root、权限设置为644，audit文件为700、message文件为600，其他文件权限为750，实现用户对文件的权限控制。 |
| f）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； | 由管理用户进行用户访问权限分配进行设置，依据访问控制策略,对各类文件进行访问，重要文件和目录权限均在合理范围内，用户可根据文件不同的权限进行操作。 |
| g）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。 | 执 行more /etc/selinux/config 命令，查看config文件显示 SELINUX参数为 DISABLED，即未开启强制访问控制模式。 |
| 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）执行ps -ef|grep rsyslog和ps -ef|grep auditd命令，显示rsyslog和auditd进程正在运行；2）more /etc/audit/audit.rules，显示审计内容包括：\*.info、authriv.\*、mail.\*、cron.\*、\*.emerg、uucp、news.crit、local7.\*等事件。 |
| 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； | 执行tail -20 /var/log/audit/audit.log命令，查看近20条审计日志，内容包括：时间、对象、路径、用户ID、相关的系统调用、用户执行命令等。 |
| 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）通过访问权限对审计记录进行保护，日志文件/var/log/messages、/var/log/secure、/var/log/audit/audit.log访问 权限均为600；2）审计记录本地保存，且实时备份至360本地安全大脑，保存时间满足180天以上。 |
| d）应对审计进程进行保护，防止未经授权的中断。 | 执行service auditd status命令，系统开启auditd审计保护进程，审计进程由root用户维护，经现场使用yluser用户通过service auditd stop命令尝试中断审计进程，无法将审计进程单独中断。 |
| 入侵防范 | a）应遵循最小安装的原则，仅安装需要的组件和应用程序； | 1）系统安装遵循最小化安装原则；2）执行yum list installed命令查看操作系统已安装的程序包，存在Java、SSH、天眼云镜agent等应用程序或组件，不存在与业务系统无关的组件和应用程序。 |
| b）应关闭不需要的系统服务、默认共享和高危端口； | 1）执行systemctl list-unit-files 命令，系统已关闭FTP、Telnet 等高危网络服务；2）执行netstat -pantu命令，系统关闭了135、445等高危端口，仅开启了22、8080等端口。 |
| c）应通过设定终端接入方式或网络地址范围对通过网络进行管理的管理终端进行限制； | 经核查，1）通过配置安全组策略限制仅允许通过堡垒机管理服务器；2）经核查防火墙中访问控制策略，具备堡垒机地址-服务器管理网段（10.33.0.0）的访问控制策略。 |
| d）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； | 根据GB∕T 28448-2019 《信息安全技术 网络安全等级保护测评要求》测评对象范围描述，服务器无该项要求，故判为“不适用”。 |
| e）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； | 1）经过漏洞扫描，服务器不存在高危安全漏洞；2）执行rpm -qa grep patch命令，查看系统补丁已更新至最新。 |
| f）应能够检测到对重要节点进行入侵的行为，并在发生严重入侵事件时提供报警。 | 经核查，服务器上安装有青藤云天眼云镜，对主机入侵行为进行检测，发现严重安全事件时通过钉钉告警。 |
| 恶意代码防范 | a）应采用免受恶意代码攻击的技术措施或主动免疫可信验证机制及时识别入侵和病毒行为，并将其有效阻断。 | 经核查，服务器上安装有青藤云天眼云镜，对主机恶意代码进行检测、清除，每天凌晨自动更新恶意代码特征库，经核查，具备恶意代码特征库更新记录。 |
| 可信验证 | a）可基于可信根对计算设备的系统引导程序、系统程序、重要配置参数和应用程序等进行可信验证，并在应用程序的关键执行环节进行动态可信验证，在检测到其可信性受到破坏后进行报警，并将验证结果形成审计记录送至安全管理中心。 | 未采用技术措施对计算设备的系统引导程序、系统程序、重要配置参数和通信应用程序等进行可信验证。 |
| 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； | 采用SSH协议连接操作系统，保证了鉴别信息以及管理数据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。 | 操作系统中对重要鉴别信息通过自身的加密及校验（SHA256），保证数据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； | 采用SSH协议连接操作系统，保证了鉴别信息以及管理数据在传输过程中的保密性。 |
| b）应采用密码技术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个人信息等。 | 通过系统自带的加密模块保证鉴别数据在存储过程中的保密性。 |
| 数据备份恢复 | a）应提供重要数据的本地数据备份与恢复功能； | 经核查，通过脚本每周将配置文件、代码仓库等数据备份至备份服务器中，依据需要验证备份数据的有效性。 |
| b）应提供异地实时备份功能，利用通信网络将重要数据实时备份至备份场地； | 系统无异地备份机制。 |
| c）应提供重要数据处理系统的热冗余，保证系统的高可用性。 | 服务器采用K8S容器部署，保证系统的高可用性。 |
| 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； | 操作系统提供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功能。 |
| 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。 | 操作系统提供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的功能。 |

4.1.3.5. 应用服务器9

|  |  |  |
| --- | --- | --- |
| **安全控制点** | **测评指标** | **结果记录** |
| 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）操作系统时采用用户名+SSHKey公私钥进行身份鉴别鉴别信息具有复杂度要求；2）执行cat /etc/shadow命令，查看shadow文件系统内用户身份标识唯一，不存在同名用户，且不存在空口令账号；3）经访谈，SSHKey公私钥每半年进行更换；4）查看sshd\_config配置文件中配置PasswordAuthentication no，拒绝使用密码方式进行身份鉴别。 |
| 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； | 操作系统采用用户名+SSHKey公私钥进行身份鉴别，可以防止鉴别信息被暴力破解；但未配置用户连接超时退出策略。 |
| 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； | 1）经核查，管理人员采用SSH协议连接操作系统；2）执行netatat –tpln| grep 23命令查看操作系统远程管理端口，不存在Telnet端口，防止鉴别信息在网络传输过程中的被窃听。 |
| 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。 | 未采用两种或两种以上组合的鉴别技术对用户进行身份鉴别。 |
| 访问控制 | a）应对登录的用户分配账户和权限； | 1）经访谈，通过root账户为登录的用户创建账户、分配权限；2）执行ls -l命令查看关键文件权限，均已为账户分配了相应权限，相关文件权限设置为/etc/shadow：000、/etc/passwd：644、/etc/group：644、/etc/profile：644、/etc/crontab：644、/ etc/securetty：600、/etc/ssh/sshd\_config：600。 |
| b）应重命名或删除默认账户，修改默认账户的默认口令； | 1）执行cat /etc/shadow命令查看shadow文件，操作系统中adm、lp、sync、shutdown、halt、mail、uucp、operator、games、gopher等账户均为nologin状态，存在默认账户root；2）执行more /etc/ssh/sshd\_config命令，查看“PermitRootLogin”参数设置为“yes”，即允许root远程登录；3）经访谈，root用户需通过公私钥方式进行身份鉴别。 |
| 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； | 1）执行cat /etc/shadow命令查看shadow文件，发现操作系统存在root、ysup、yops、yluser等在用账户，不存在多余的、过期账户；2）存在多个堡垒机账户登录操作系统时共用一个账户的情况。 |
| 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； | root账户具有系统所有权限，未实现管理用户的权限分离。 |
| e）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； | 经访谈，由系统管理员root配置访问控制策略，如：/etc/passwd，/etc/profile宿主为root、权限设置为644，audit文件为700、message文件为600，其他文件权限为750，实现用户对文件的权限控制。 |
| f）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； | 由管理用户进行用户访问权限分配进行设置，依据访问控制策略,对各类文件进行访问，重要文件和目录权限均在合理范围内，用户可根据文件不同的权限进行操作。 |
| g）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。 | 执 行more /etc/selinux/config 命令，查看config文件显示 SELINUX参数为 DISABLED，即未开启强制访问控制模式。 |
| 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）执行ps -ef|grep rsyslog和ps -ef|grep auditd命令，显示rsyslog和auditd进程正在运行；2）more /etc/audit/audit.rules，显示审计内容包括：\*.info、authriv.\*、mail.\*、cron.\*、\*.emerg、uucp、news.crit、local7.\*等事件。 |
| 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； | 执行tail -20 /var/log/audit/audit.log命令，查看近20条审计日志，内容包括：时间、对象、路径、用户ID、相关的系统调用、用户执行命令等。 |
| 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）通过访问权限对审计记录进行保护，日志文件/var/log/messages、/var/log/secure、/var/log/audit/audit.log访问 权限均为600；2）审计记录本地保存，且实时备份至360本地安全大脑，保存时间满足180天以上。 |
| d）应对审计进程进行保护，防止未经授权的中断。 | 执行service auditd status命令，系统开启auditd审计保护进程，审计进程由root用户维护，经现场使用yluser用户通过service auditd stop命令尝试中断审计进程，无法将审计进程单独中断。 |
| 入侵防范 | a）应遵循最小安装的原则，仅安装需要的组件和应用程序； | 1）系统安装遵循最小化安装原则；2）执行yum list installed命令查看操作系统已安装的程序包，存在Java、SSH、天眼云镜agent等应用程序或组件，不存在与业务系统无关的组件和应用程序。 |
| b）应关闭不需要的系统服务、默认共享和高危端口； | 1）执行systemctl list-unit-files 命令，系统已关闭FTP、Telnet 等高危网络服务；2）执行netstat -pantu命令，系统关闭了135、445等高危端口，仅开启了22、8080等端口。 |
| c）应通过设定终端接入方式或网络地址范围对通过网络进行管理的管理终端进行限制； | 经核查，1）通过配置安全组策略限制仅允许通过堡垒机管理服务器；2）经核查防火墙中访问控制策略，具备堡垒机地址-服务器管理网段（10.33.0.0）的访问控制策略。 |
| d）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； | 根据GB∕T 28448-2019 《信息安全技术 网络安全等级保护测评要求》测评对象范围描述，服务器无该项要求，故判为“不适用”。 |
| e）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； | 1）经过漏洞扫描，服务器不存在高危安全漏洞；2）执行rpm -qa grep patch命令，查看系统补丁已更新至最新。 |
| f）应能够检测到对重要节点进行入侵的行为，并在发生严重入侵事件时提供报警。 | 经核查，服务器上安装有青藤云天眼云镜，对主机入侵行为进行检测，发现严重安全事件时通过钉钉告警。 |
| 恶意代码防范 | a）应采用免受恶意代码攻击的技术措施或主动免疫可信验证机制及时识别入侵和病毒行为，并将其有效阻断。 | 经核查，服务器上安装有青藤云天眼云镜，对主机恶意代码进行检测、清除，每天凌晨自动更新恶意代码特征库，经核查，具备恶意代码特征库更新记录。 |
| 可信验证 | a）可基于可信根对计算设备的系统引导程序、系统程序、重要配置参数和应用程序等进行可信验证，并在应用程序的关键执行环节进行动态可信验证，在检测到其可信性受到破坏后进行报警，并将验证结果形成审计记录送至安全管理中心。 | 未采用技术措施对计算设备的系统引导程序、系统程序、重要配置参数和通信应用程序等进行可信验证。 |
| 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； | 采用SSH协议连接操作系统，保证了鉴别信息以及管理数据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。 | 操作系统中对重要鉴别信息通过自身的加密及校验（SHA256），保证数据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； | 采用SSH协议连接操作系统，保证了鉴别信息以及管理数据在传输过程中的保密性。 |
| b）应采用密码技术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个人信息等。 | 通过系统自带的加密模块保证鉴别数据在存储过程中的保密性。 |
| 数据备份恢复 | a）应提供重要数据的本地数据备份与恢复功能； | 经核查，通过脚本每周将配置文件、代码仓库等数据备份至备份服务器中，依据需要验证备份数据的有效性。 |
| b）应提供异地实时备份功能，利用通信网络将重要数据实时备份至备份场地； | 系统无异地备份机制。 |
| c）应提供重要数据处理系统的热冗余，保证系统的高可用性。 | 服务器采用K8S容器部署，保证系统的高可用性。 |
| 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； | 操作系统提供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功能。 |
| 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。 | 操作系统提供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的功能。 |

4.1.3.6. 应用服务器10

|  |  |  |
| --- | --- | --- |
| **安全控制点** | **测评指标** | **结果记录** |
| 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）操作系统时采用用户名+SSHKey公私钥进行身份鉴别鉴别信息具有复杂度要求；2）执行cat /etc/shadow命令，查看shadow文件系统内用户身份标识唯一，不存在同名用户，且不存在空口令账号；3）经访谈，SSHKey公私钥每半年进行更换；4）查看sshd\_config配置文件中配置PasswordAuthentication no，拒绝使用密码方式进行身份鉴别。 |
| 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； | 操作系统采用用户名+SSHKey公私钥进行身份鉴别，可以防止鉴别信息被暴力破解；但未配置用户连接超时退出策略。 |
| 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； | 1）经核查，管理人员采用SSH协议连接操作系统；2）执行netatat –tpln| grep 23命令查看操作系统远程管理端口，不存在Telnet端口，防止鉴别信息在网络传输过程中的被窃听。 |
| 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。 | 未采用两种或两种以上组合的鉴别技术对用户进行身份鉴别。 |
| 访问控制 | a）应对登录的用户分配账户和权限； | 1）经访谈，通过root账户为登录的用户创建账户、分配权限；2）执行ls -l命令查看关键文件权限，均已为账户分配了相应权限，相关文件权限设置为/etc/shadow：000、/etc/passwd：644、/etc/group：644、/etc/profile：644、/etc/crontab：644、/ etc/securetty：600、/etc/ssh/sshd\_config：600。 |
| b）应重命名或删除默认账户，修改默认账户的默认口令； | 1）执行cat /etc/shadow命令查看shadow文件，操作系统中adm、lp、sync、shutdown、halt、mail、uucp、operator、games、gopher等账户均为nologin状态，存在默认账户root；2）执行more /etc/ssh/sshd\_config命令，查看“PermitRootLogin”参数设置为“yes”，即允许root远程登录；3）经访谈，root用户需通过公私钥方式进行身份鉴别。 |
| 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； | 1）执行cat /etc/shadow命令查看shadow文件，发现操作系统存在root、ysup、yops、yluser等在用账户，不存在多余的、过期账户；2）存在多个堡垒机账户登录操作系统时共用一个账户的情况。 |
| 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； | root账户具有系统所有权限，未实现管理用户的权限分离。 |
| e）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； | 经访谈，由系统管理员root配置访问控制策略，如：/etc/passwd，/etc/profile宿主为root、权限设置为644，audit文件为700、message文件为600，其他文件权限为750，实现用户对文件的权限控制。 |
| f）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； | 由管理用户进行用户访问权限分配进行设置，依据访问控制策略,对各类文件进行访问，重要文件和目录权限均在合理范围内，用户可根据文件不同的权限进行操作。 |
| g）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。 | 执 行more /etc/selinux/config 命令，查看config文件显示 SELINUX参数为 DISABLED，即未开启强制访问控制模式。 |
| 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）执行ps -ef|grep rsyslog和ps -ef|grep auditd命令，显示rsyslog和auditd进程正在运行；2）more /etc/audit/audit.rules，显示审计内容包括：\*.info、authriv.\*、mail.\*、cron.\*、\*.emerg、uucp、news.crit、local7.\*等事件。 |
| 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； | 执行tail -20 /var/log/audit/audit.log命令，查看近20条审计日志，内容包括：时间、对象、路径、用户ID、相关的系统调用、用户执行命令等。 |
| 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）通过访问权限对审计记录进行保护，日志文件/var/log/messages、/var/log/secure、/var/log/audit/audit.log访问 权限均为600；2）审计记录本地保存，且实时备份至360本地安全大脑，保存时间满足180天以上。 |
| d）应对审计进程进行保护，防止未经授权的中断。 | 执行service auditd status命令，系统开启auditd审计保护进程，审计进程由root用户维护，经现场使用yluser用户通过service auditd stop命令尝试中断审计进程，无法将审计进程单独中断。 |
| 入侵防范 | a）应遵循最小安装的原则，仅安装需要的组件和应用程序； | 1）系统安装遵循最小化安装原则；2）执行yum list installed命令查看操作系统已安装的程序包，存在Java、SSH、天眼云镜agent等应用程序或组件，不存在与业务系统无关的组件和应用程序。 |
| b）应关闭不需要的系统服务、默认共享和高危端口； | 1）执行systemctl list-unit-files 命令，系统已关闭FTP、Telnet 等高危网络服务；2）执行netstat -pantu命令，系统关闭了135、445等高危端口，仅开启了22、8080等端口。 |
| c）应通过设定终端接入方式或网络地址范围对通过网络进行管理的管理终端进行限制； | 经核查，1）通过配置安全组策略限制仅允许通过堡垒机管理服务器；2）经核查防火墙中访问控制策略，具备堡垒机地址-服务器管理网段（10.33.0.0）的访问控制策略。 |
| d）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； | 根据GB∕T 28448-2019 《信息安全技术 网络安全等级保护测评要求》测评对象范围描述，服务器无该项要求，故判为“不适用”。 |
| e）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； | 1）经过漏洞扫描，服务器不存在高危安全漏洞；2）执行rpm -qa grep patch命令，查看系统补丁已更新至最新。 |
| f）应能够检测到对重要节点进行入侵的行为，并在发生严重入侵事件时提供报警。 | 经核查，服务器上安装有青藤云天眼云镜，对主机入侵行为进行检测，发现严重安全事件时通过钉钉告警。 |
| 恶意代码防范 | a）应采用免受恶意代码攻击的技术措施或主动免疫可信验证机制及时识别入侵和病毒行为，并将其有效阻断。 | 经核查，服务器上安装有青藤云天眼云镜，对主机恶意代码进行检测、清除，每天凌晨自动更新恶意代码特征库，经核查，具备恶意代码特征库更新记录。 |
| 可信验证 | a）可基于可信根对计算设备的系统引导程序、系统程序、重要配置参数和应用程序等进行可信验证，并在应用程序的关键执行环节进行动态可信验证，在检测到其可信性受到破坏后进行报警，并将验证结果形成审计记录送至安全管理中心。 | 未采用技术措施对计算设备的系统引导程序、系统程序、重要配置参数和通信应用程序等进行可信验证。 |
| 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； | 采用SSH协议连接操作系统，保证了鉴别信息以及管理数据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。 | 操作系统中对重要鉴别信息通过自身的加密及校验（SHA256），保证数据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； | 采用SSH协议连接操作系统，保证了鉴别信息以及管理数据在传输过程中的保密性。 |
| b）应采用密码技术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个人信息等。 | 通过系统自带的加密模块保证鉴别数据在存储过程中的保密性。 |
| 数据备份恢复 | a）应提供重要数据的本地数据备份与恢复功能； | 经核查，通过脚本每周将配置文件、代码仓库等数据备份至备份服务器中，依据需要验证备份数据的有效性。 |
| b）应提供异地实时备份功能，利用通信网络将重要数据实时备份至备份场地； | 系统无异地备份机制。 |
| c）应提供重要数据处理系统的热冗余，保证系统的高可用性。 | 服务器采用K8S容器部署，保证系统的高可用性。 |
| 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； | 操作系统提供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功能。 |
| 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。 | 操作系统提供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的功能。 |

4.1.3.7. 应用服务器11

|  |  |  |
| --- | --- | --- |
| **安全控制点** | **测评指标** | **结果记录** |
| 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）操作系统时采用用户名+SSHKey公私钥进行身份鉴别鉴别信息具有复杂度要求；2）执行cat /etc/shadow命令，查看shadow文件系统内用户身份标识唯一，不存在同名用户，且不存在空口令账号；3）经访谈，SSHKey公私钥每半年进行更换；4）查看sshd\_config配置文件中配置PasswordAuthentication no，拒绝使用密码方式进行身份鉴别。 |
| 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； | 操作系统采用用户名+SSHKey公私钥进行身份鉴别，可以防止鉴别信息被暴力破解；但未配置用户连接超时退出策略。 |
| 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； | 1）经核查，管理人员采用SSH协议连接操作系统；2）执行netatat –tpln| grep 23命令查看操作系统远程管理端口，不存在Telnet端口，防止鉴别信息在网络传输过程中的被窃听。 |
| 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。 | 未采用两种或两种以上组合的鉴别技术对用户进行身份鉴别。 |
| 访问控制 | a）应对登录的用户分配账户和权限； | 1）经访谈，通过root账户为登录的用户创建账户、分配权限；2）执行ls -l命令查看关键文件权限，均已为账户分配了相应权限，相关文件权限设置为/etc/shadow：000、/etc/passwd：644、/etc/group：644、/etc/profile：644、/etc/crontab：644、/ etc/securetty：600、/etc/ssh/sshd\_config：600。 |
| b）应重命名或删除默认账户，修改默认账户的默认口令； | 1）执行cat /etc/shadow命令查看shadow文件，操作系统中adm、lp、sync、shutdown、halt、mail、uucp、operator、games、gopher等账户均为nologin状态，存在默认账户root；2）执行more /etc/ssh/sshd\_config命令，查看“PermitRootLogin”参数设置为“yes”，即允许root远程登录；3）经访谈，root用户需通过公私钥方式进行身份鉴别。 |
| 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； | 1）执行cat /etc/shadow命令查看shadow文件，发现操作系统存在root、ysup、yops、yluser等在用账户，不存在多余的、过期账户；2）存在多个堡垒机账户登录操作系统时共用一个账户的情况。 |
| 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； | root账户具有系统所有权限，未实现管理用户的权限分离。 |
| e）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； | 经访谈，由系统管理员root配置访问控制策略，如：/etc/passwd，/etc/profile宿主为root、权限设置为644，audit文件为700、message文件为600，其他文件权限为750，实现用户对文件的权限控制。 |
| f）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； | 由管理用户进行用户访问权限分配进行设置，依据访问控制策略,对各类文件进行访问，重要文件和目录权限均在合理范围内，用户可根据文件不同的权限进行操作。 |
| g）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。 | 执 行more /etc/selinux/config 命令，查看config文件显示 SELINUX参数为 DISABLED，即未开启强制访问控制模式。 |
| 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）执行ps -ef|grep rsyslog和ps -ef|grep auditd命令，显示rsyslog和auditd进程正在运行；2）more /etc/audit/audit.rules，显示审计内容包括：\*.info、authriv.\*、mail.\*、cron.\*、\*.emerg、uucp、news.crit、local7.\*等事件。 |
| 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； | 执行tail -20 /var/log/audit/audit.log命令，查看近20条审计日志，内容包括：时间、对象、路径、用户ID、相关的系统调用、用户执行命令等。 |
| 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）通过访问权限对审计记录进行保护，日志文件/var/log/messages、/var/log/secure、/var/log/audit/audit.log访问 权限均为600；2）审计记录本地保存，且实时备份至360本地安全大脑，保存时间满足180天以上。 |
| d）应对审计进程进行保护，防止未经授权的中断。 | 执行service auditd status命令，系统开启auditd审计保护进程，审计进程由root用户维护，经现场使用yluser用户通过service auditd stop命令尝试中断审计进程，无法将审计进程单独中断。 |
| 入侵防范 | a）应遵循最小安装的原则，仅安装需要的组件和应用程序； | 1）系统安装遵循最小化安装原则；2）执行yum list installed命令查看操作系统已安装的程序包，存在Java、SSH、天眼云镜agent等应用程序或组件，不存在与业务系统无关的组件和应用程序。 |
| b）应关闭不需要的系统服务、默认共享和高危端口； | 1）执行systemctl list-unit-files 命令，系统已关闭FTP、Telnet 等高危网络服务；2）执行netstat -pantu命令，系统关闭了135、445等高危端口，仅开启了22、8080等端口。 |
| c）应通过设定终端接入方式或网络地址范围对通过网络进行管理的管理终端进行限制； | 经核查，1）通过配置安全组策略限制仅允许通过堡垒机管理服务器；2）经核查防火墙中访问控制策略，具备堡垒机地址-服务器管理网段（10.33.0.0）的访问控制策略。 |
| d）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； | 根据GB∕T 28448-2019 《信息安全技术 网络安全等级保护测评要求》测评对象范围描述，服务器无该项要求，故判为“不适用”。 |
| e）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； | 1）经过漏洞扫描，服务器不存在高危安全漏洞；2）执行rpm -qa grep patch命令，查看系统补丁已更新至最新。 |
| f）应能够检测到对重要节点进行入侵的行为，并在发生严重入侵事件时提供报警。 | 经核查，服务器上安装有青藤云天眼云镜，对主机入侵行为进行检测，发现严重安全事件时通过钉钉告警。 |
| 恶意代码防范 | a）应采用免受恶意代码攻击的技术措施或主动免疫可信验证机制及时识别入侵和病毒行为，并将其有效阻断。 | 经核查，服务器上安装有青藤云天眼云镜，对主机恶意代码进行检测、清除，每天凌晨自动更新恶意代码特征库，经核查，具备恶意代码特征库更新记录。 |
| 可信验证 | a）可基于可信根对计算设备的系统引导程序、系统程序、重要配置参数和应用程序等进行可信验证，并在应用程序的关键执行环节进行动态可信验证，在检测到其可信性受到破坏后进行报警，并将验证结果形成审计记录送至安全管理中心。 | 未采用技术措施对计算设备的系统引导程序、系统程序、重要配置参数和通信应用程序等进行可信验证。 |
| 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； | 采用SSH协议连接操作系统，保证了鉴别信息以及管理数据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。 | 操作系统中对重要鉴别信息通过自身的加密及校验（SHA256），保证数据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； | 采用SSH协议连接操作系统，保证了鉴别信息以及管理数据在传输过程中的保密性。 |
| b）应采用密码技术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个人信息等。 | 通过系统自带的加密模块保证鉴别数据在存储过程中的保密性。 |
| 数据备份恢复 | a）应提供重要数据的本地数据备份与恢复功能； | 经核查，通过脚本每周将配置文件、代码仓库等数据备份至备份服务器中，依据需要验证备份数据的有效性。 |
| b）应提供异地实时备份功能，利用通信网络将重要数据实时备份至备份场地； | 系统无异地备份机制。 |
| c）应提供重要数据处理系统的热冗余，保证系统的高可用性。 | 服务器采用K8S容器部署，保证系统的高可用性。 |
| 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； | 操作系统提供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功能。 |
| 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。 | 操作系统提供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的功能。 |

4.1.3.8. 应用服务器14

|  |  |  |
| --- | --- | --- |
| **安全控制点** | **测评指标** | **结果记录** |
| 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）操作系统时采用用户名+SSHKey公私钥进行身份鉴别鉴别信息具有复杂度要求；2）执行cat /etc/shadow命令，查看shadow文件系统内用户身份标识唯一，不存在同名用户，且不存在空口令账号；3）经访谈，SSHKey公私钥每半年进行更换；4）查看sshd\_config配置文件中配置PasswordAuthentication no，拒绝使用密码方式进行身份鉴别。 |
| 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； | 操作系统采用用户名+SSHKey公私钥进行身份鉴别，可以防止鉴别信息被暴力破解；但未配置用户连接超时退出策略。 |
| 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； | 1）经核查，管理人员采用SSH协议连接操作系统；2）执行netatat –tpln| grep 23命令查看操作系统远程管理端口，不存在Telnet端口，防止鉴别信息在网络传输过程中的被窃听。 |
| 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。 | 未采用两种或两种以上组合的鉴别技术对用户进行身份鉴别。 |
| 访问控制 | a）应对登录的用户分配账户和权限； | 1）经访谈，通过root账户为登录的用户创建账户、分配权限；2）执行ls -l命令查看关键文件权限，均已为账户分配了相应权限，相关文件权限设置为/etc/shadow：000、/etc/passwd：644、/etc/group：644、/etc/profile：644、/etc/crontab：644、/ etc/securetty：600、/etc/ssh/sshd\_config：600。 |
| b）应重命名或删除默认账户，修改默认账户的默认口令； | 1）执行cat /etc/shadow命令查看shadow文件，操作系统中adm、lp、sync、shutdown、halt、mail、uucp、operator、games、gopher等账户均为nologin状态，存在默认账户root；2）执行more /etc/ssh/sshd\_config命令，查看“PermitRootLogin”参数设置为“yes”，即允许root远程登录；3）经访谈，root用户需通过公私钥方式进行身份鉴别。 |
| 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； | 1）执行cat /etc/shadow命令查看shadow文件，发现操作系统存在root、ysup、yops、yluser等在用账户，不存在多余的、过期账户；2）存在多个堡垒机账户登录操作系统时共用一个账户的情况。 |
| 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； | root账户具有系统所有权限，未实现管理用户的权限分离。 |
| e）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； | 经访谈，由系统管理员root配置访问控制策略，如：/etc/passwd，/etc/profile宿主为root、权限设置为644，audit文件为700、message文件为600，其他文件权限为750，实现用户对文件的权限控制。 |
| f）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； | 由管理用户进行用户访问权限分配进行设置，依据访问控制策略,对各类文件进行访问，重要文件和目录权限均在合理范围内，用户可根据文件不同的权限进行操作。 |
| g）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。 | 执 行more /etc/selinux/config 命令，查看config文件显示 SELINUX参数为 DISABLED，即未开启强制访问控制模式。 |
| 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）执行ps -ef|grep rsyslog和ps -ef|grep auditd命令，显示rsyslog和auditd进程正在运行；2）more /etc/audit/audit.rules，显示审计内容包括：\*.info、authriv.\*、mail.\*、cron.\*、\*.emerg、uucp、news.crit、local7.\*等事件。 |
| 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； | 执行tail -20 /var/log/audit/audit.log命令，查看近20条审计日志，内容包括：时间、对象、路径、用户ID、相关的系统调用、用户执行命令等。 |
| 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）通过访问权限对审计记录进行保护，日志文件/var/log/messages、/var/log/secure、/var/log/audit/audit.log访问 权限均为600；2）审计记录本地保存，且实时备份至360本地安全大脑，保存时间满足180天以上。 |
| d）应对审计进程进行保护，防止未经授权的中断。 | 执行service auditd status命令，系统开启auditd审计保护进程，审计进程由root用户维护，经现场使用yluser用户通过service auditd stop命令尝试中断审计进程，无法将审计进程单独中断。 |
| 入侵防范 | a）应遵循最小安装的原则，仅安装需要的组件和应用程序； | 1）系统安装遵循最小化安装原则；2）执行yum list installed命令查看操作系统已安装的程序包，存在Java、SSH、天眼云镜agent等应用程序或组件，不存在与业务系统无关的组件和应用程序。 |
| b）应关闭不需要的系统服务、默认共享和高危端口； | 1）执行systemctl list-unit-files 命令，系统已关闭FTP、Telnet 等高危网络服务；2）执行netstat -pantu命令，系统关闭了135、445等高危端口，仅开启了22、8080等端口。 |
| c）应通过设定终端接入方式或网络地址范围对通过网络进行管理的管理终端进行限制； | 经核查，1）通过配置安全组策略限制仅允许通过堡垒机管理服务器；2）经核查防火墙中访问控制策略，具备堡垒机地址-服务器管理网段（10.33.0.0）的访问控制策略。 |
| d）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； | 根据GB∕T 28448-2019 《信息安全技术 网络安全等级保护测评要求》测评对象范围描述，服务器无该项要求，故判为“不适用”。 |
| e）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； | 1）经过漏洞扫描，服务器不存在高危安全漏洞；2）执行rpm -qa grep patch命令，查看系统补丁已更新至最新。 |
| f）应能够检测到对重要节点进行入侵的行为，并在发生严重入侵事件时提供报警。 | 经核查，服务器上安装有青藤云天眼云镜，对主机入侵行为进行检测，发现严重安全事件时通过钉钉告警。 |
| 恶意代码防范 | a）应采用免受恶意代码攻击的技术措施或主动免疫可信验证机制及时识别入侵和病毒行为，并将其有效阻断。 | 经核查，服务器上安装有青藤云天眼云镜，对主机恶意代码进行检测、清除，每天凌晨自动更新恶意代码特征库，经核查，具备恶意代码特征库更新记录。 |
| 可信验证 | a）可基于可信根对计算设备的系统引导程序、系统程序、重要配置参数和应用程序等进行可信验证，并在应用程序的关键执行环节进行动态可信验证，在检测到其可信性受到破坏后进行报警，并将验证结果形成审计记录送至安全管理中心。 | 未采用技术措施对计算设备的系统引导程序、系统程序、重要配置参数和通信应用程序等进行可信验证。 |
| 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； | 采用SSH协议连接操作系统，保证了鉴别信息以及管理数据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。 | 操作系统中对重要鉴别信息通过自身的加密及校验（SHA256），保证数据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； | 采用SSH协议连接操作系统，保证了鉴别信息以及管理数据在传输过程中的保密性。 |
| b）应采用密码技术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个人信息等。 | 通过系统自带的加密模块保证鉴别数据在存储过程中的保密性。 |
| 数据备份恢复 | a）应提供重要数据的本地数据备份与恢复功能； | 经核查，通过脚本每周将配置文件、代码仓库等数据备份至备份服务器中，依据需要验证备份数据的有效性。 |
| b）应提供异地实时备份功能，利用通信网络将重要数据实时备份至备份场地； | 系统无异地备份机制。 |
| c）应提供重要数据处理系统的热冗余，保证系统的高可用性。 | 服务器采用K8S容器部署，保证系统的高可用性。 |
| 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； | 操作系统提供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功能。 |
| 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。 | 操作系统提供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的功能。 |

4.1.3.9. 应用服务器19

|  |  |  |
| --- | --- | --- |
| **安全控制点** | **测评指标** | **结果记录** |
| 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）操作系统时采用用户名+SSHKey公私钥进行身份鉴别鉴别信息具有复杂度要求；2）执行cat /etc/shadow命令，查看shadow文件系统内用户身份标识唯一，不存在同名用户，且不存在空口令账号；3）经访谈，SSHKey公私钥每半年进行更换；4）查看sshd\_config配置文件中配置PasswordAuthentication no，拒绝使用密码方式进行身份鉴别。 |
| 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； | 操作系统采用用户名+SSHKey公私钥进行身份鉴别，可以防止鉴别信息被暴力破解；但未配置用户连接超时退出策略。 |
| 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； | 1）经核查，管理人员采用SSH协议连接操作系统；2）执行netatat –tpln| grep 23命令查看操作系统远程管理端口，不存在Telnet端口，防止鉴别信息在网络传输过程中的被窃听。 |
| 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。 | 未采用两种或两种以上组合的鉴别技术对用户进行身份鉴别。 |
| 访问控制 | a）应对登录的用户分配账户和权限； | 1）经访谈，通过root账户为登录的用户创建账户、分配权限；2）执行ls -l命令查看关键文件权限，均已为账户分配了相应权限，相关文件权限设置为/etc/shadow：000、/etc/passwd：644、/etc/group：644、/etc/profile：644、/etc/crontab：644、/ etc/securetty：600、/etc/ssh/sshd\_config：600。 |
| b）应重命名或删除默认账户，修改默认账户的默认口令； | 1）执行cat /etc/shadow命令查看shadow文件，操作系统中adm、lp、sync、shutdown、halt、mail、uucp、operator、games、gopher等账户均为nologin状态，存在默认账户root；2）执行more /etc/ssh/sshd\_config命令，查看“PermitRootLogin”参数设置为“yes”，即允许root远程登录；3）经访谈，root用户需通过公私钥方式进行身份鉴别。 |
| 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； | 1）执行cat /etc/shadow命令查看shadow文件，发现操作系统存在root、ysup、yops、yluser等在用账户，不存在多余的、过期账户；2）存在多个堡垒机账户登录操作系统时共用一个账户的情况。 |
| 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； | root账户具有系统所有权限，未实现管理用户的权限分离。 |
| e）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； | 经访谈，由系统管理员root配置访问控制策略，如：/etc/passwd，/etc/profile宿主为root、权限设置为644，audit文件为700、message文件为600，其他文件权限为750，实现用户对文件的权限控制。 |
| f）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； | 由管理用户进行用户访问权限分配进行设置，依据访问控制策略,对各类文件进行访问，重要文件和目录权限均在合理范围内，用户可根据文件不同的权限进行操作。 |
| g）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。 | 执 行more /etc/selinux/config 命令，查看config文件显示 SELINUX参数为 DISABLED，即未开启强制访问控制模式。 |
| 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）执行ps -ef|grep rsyslog和ps -ef|grep auditd命令，显示rsyslog和auditd进程正在运行；2）more /etc/audit/audit.rules，显示审计内容包括：\*.info、authriv.\*、mail.\*、cron.\*、\*.emerg、uucp、news.crit、local7.\*等事件。 |
| 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； | 执行tail -20 /var/log/audit/audit.log命令，查看近20条审计日志，内容包括：时间、对象、路径、用户ID、相关的系统调用、用户执行命令等。 |
| 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）通过访问权限对审计记录进行保护，日志文件/var/log/messages、/var/log/secure、/var/log/audit/audit.log访问 权限均为600；2）审计记录本地保存，且实时备份至360本地安全大脑，保存时间满足180天以上。 |
| d）应对审计进程进行保护，防止未经授权的中断。 | 执行service auditd status命令，系统开启auditd审计保护进程，审计进程由root用户维护，经现场使用yluser用户通过service auditd stop命令尝试中断审计进程，无法将审计进程单独中断。 |
| 入侵防范 | a）应遵循最小安装的原则，仅安装需要的组件和应用程序； | 1）系统安装遵循最小化安装原则；2）执行yum list installed命令查看操作系统已安装的程序包，存在Java、SSH、天眼云镜agent等应用程序或组件，不存在与业务系统无关的组件和应用程序。 |
| b）应关闭不需要的系统服务、默认共享和高危端口； | 1）执行systemctl list-unit-files 命令，系统已关闭FTP、Telnet 等高危网络服务；2）执行netstat -pantu命令，系统关闭了135、445等高危端口，仅开启了22、8080等端口。 |
| c）应通过设定终端接入方式或网络地址范围对通过网络进行管理的管理终端进行限制； | 经核查，1）通过配置安全组策略限制仅允许通过堡垒机管理服务器；2）经核查防火墙中访问控制策略，具备堡垒机地址-服务器管理网段（10.33.0.0）的访问控制策略。 |
| d）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； | 根据GB∕T 28448-2019 《信息安全技术 网络安全等级保护测评要求》测评对象范围描述，服务器无该项要求，故判为“不适用”。 |
| e）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； | 1）经过漏洞扫描，服务器不存在高危安全漏洞；2）执行rpm -qa grep patch命令，查看系统补丁已更新至最新。 |
| f）应能够检测到对重要节点进行入侵的行为，并在发生严重入侵事件时提供报警。 | 经核查，服务器上安装有青藤云天眼云镜，对主机入侵行为进行检测，发现严重安全事件时通过钉钉告警。 |
| 恶意代码防范 | a）应采用免受恶意代码攻击的技术措施或主动免疫可信验证机制及时识别入侵和病毒行为，并将其有效阻断。 | 经核查，服务器上安装有青藤云天眼云镜，对主机恶意代码进行检测、清除，每天凌晨自动更新恶意代码特征库，经核查，具备恶意代码特征库更新记录。 |
| 可信验证 | a）可基于可信根对计算设备的系统引导程序、系统程序、重要配置参数和应用程序等进行可信验证，并在应用程序的关键执行环节进行动态可信验证，在检测到其可信性受到破坏后进行报警，并将验证结果形成审计记录送至安全管理中心。 | 未采用技术措施对计算设备的系统引导程序、系统程序、重要配置参数和通信应用程序等进行可信验证。 |
| 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； | 采用SSH协议连接操作系统，保证了鉴别信息以及管理数据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。 | 操作系统中对重要鉴别信息通过自身的加密及校验（SHA256），保证数据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； | 采用SSH协议连接操作系统，保证了鉴别信息以及管理数据在传输过程中的保密性。 |
| b）应采用密码技术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个人信息等。 | 通过系统自带的加密模块保证鉴别数据在存储过程中的保密性。 |
| 数据备份恢复 | a）应提供重要数据的本地数据备份与恢复功能； | 经核查，通过脚本每周将配置文件、代码仓库等数据备份至备份服务器中，依据需要验证备份数据的有效性。 |
| b）应提供异地实时备份功能，利用通信网络将重要数据实时备份至备份场地； | 系统无异地备份机制。 |
| c）应提供重要数据处理系统的热冗余，保证系统的高可用性。 | 服务器采用K8S容器部署，保证系统的高可用性。 |
| 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； | 操作系统提供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功能。 |
| 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。 | 操作系统提供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的功能。 |

4.1.3.10. 应用服务器20

|  |  |  |
| --- | --- | --- |
| **安全控制点** | **测评指标** | **结果记录** |
| 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）操作系统时采用用户名+SSHKey公私钥进行身份鉴别鉴别信息具有复杂度要求；2）执行cat /etc/shadow命令，查看shadow文件系统内用户身份标识唯一，不存在同名用户，且不存在空口令账号；3）经访谈，SSHKey公私钥每半年进行更换；4）查看sshd\_config配置文件中配置PasswordAuthentication no，拒绝使用密码方式进行身份鉴别。 |
| 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； | 操作系统采用用户名+SSHKey公私钥进行身份鉴别，可以防止鉴别信息被暴力破解；但未配置用户连接超时退出策略。 |
| 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； | 1）经核查，管理人员采用SSH协议连接操作系统；2）执行netatat –tpln| grep 23命令查看操作系统远程管理端口，不存在Telnet端口，防止鉴别信息在网络传输过程中的被窃听。 |
| 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。 | 未采用两种或两种以上组合的鉴别技术对用户进行身份鉴别。 |
| 访问控制 | a）应对登录的用户分配账户和权限； | 1）经访谈，通过root账户为登录的用户创建账户、分配权限；2）执行ls -l命令查看关键文件权限，均已为账户分配了相应权限，相关文件权限设置为/etc/shadow：000、/etc/passwd：644、/etc/group：644、/etc/profile：644、/etc/crontab：644、/ etc/securetty：600、/etc/ssh/sshd\_config：600。 |
| b）应重命名或删除默认账户，修改默认账户的默认口令； | 1）执行cat /etc/shadow命令查看shadow文件，操作系统中adm、lp、sync、shutdown、halt、mail、uucp、operator、games、gopher等账户均为nologin状态，存在默认账户root；2）执行more /etc/ssh/sshd\_config命令，查看“PermitRootLogin”参数设置为“yes”，即允许root远程登录；3）经访谈，root用户需通过公私钥方式进行身份鉴别。 |
| 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； | 1）执行cat /etc/shadow命令查看shadow文件，发现操作系统存在root、ysup、yops、yluser等在用账户，不存在多余的、过期账户；2）存在多个堡垒机账户登录操作系统时共用一个账户的情况。 |
| 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； | root账户具有系统所有权限，未实现管理用户的权限分离。 |
| e）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； | 经访谈，由系统管理员root配置访问控制策略，如：/etc/passwd，/etc/profile宿主为root、权限设置为644，audit文件为700、message文件为600，其他文件权限为750，实现用户对文件的权限控制。 |
| f）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； | 由管理用户进行用户访问权限分配进行设置，依据访问控制策略,对各类文件进行访问，重要文件和目录权限均在合理范围内，用户可根据文件不同的权限进行操作。 |
| g）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。 | 执 行more /etc/selinux/config 命令，查看config文件显示 SELINUX参数为 DISABLED，即未开启强制访问控制模式。 |
| 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）执行ps -ef|grep rsyslog和ps -ef|grep auditd命令，显示rsyslog和auditd进程正在运行；2）more /etc/audit/audit.rules，显示审计内容包括：\*.info、authriv.\*、mail.\*、cron.\*、\*.emerg、uucp、news.crit、local7.\*等事件。 |
| 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； | 执行tail -20 /var/log/audit/audit.log命令，查看近20条审计日志，内容包括：时间、对象、路径、用户ID、相关的系统调用、用户执行命令等。 |
| 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）通过访问权限对审计记录进行保护，日志文件/var/log/messages、/var/log/secure、/var/log/audit/audit.log访问 权限均为600；2）审计记录本地保存，且实时备份至360本地安全大脑，保存时间满足180天以上。 |
| d）应对审计进程进行保护，防止未经授权的中断。 | 执行service auditd status命令，系统开启auditd审计保护进程，审计进程由root用户维护，经现场使用yluser用户通过service auditd stop命令尝试中断审计进程，无法将审计进程单独中断。 |
| 入侵防范 | a）应遵循最小安装的原则，仅安装需要的组件和应用程序； | 1）系统安装遵循最小化安装原则；2）执行yum list installed命令查看操作系统已安装的程序包，存在Java、SSH、天眼云镜agent等应用程序或组件，不存在与业务系统无关的组件和应用程序。 |
| b）应关闭不需要的系统服务、默认共享和高危端口； | 1）执行systemctl list-unit-files 命令，系统已关闭FTP、Telnet 等高危网络服务；2）执行netstat -pantu命令，系统关闭了135、445等高危端口，仅开启了22、8080等端口。 |
| c）应通过设定终端接入方式或网络地址范围对通过网络进行管理的管理终端进行限制； | 经核查，1）通过配置安全组策略限制仅允许通过堡垒机管理服务器；2）经核查防火墙中访问控制策略，具备堡垒机地址-服务器管理网段（10.33.0.0）的访问控制策略。 |
| d）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； | 根据GB∕T 28448-2019 《信息安全技术 网络安全等级保护测评要求》测评对象范围描述，服务器无该项要求，故判为“不适用”。 |
| e）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； | 1）经过漏洞扫描，服务器不存在高危安全漏洞；2）执行rpm -qa grep patch命令，查看系统补丁已更新至最新。 |
| f）应能够检测到对重要节点进行入侵的行为，并在发生严重入侵事件时提供报警。 | 经核查，服务器上安装有青藤云天眼云镜，对主机入侵行为进行检测，发现严重安全事件时通过钉钉告警。 |
| 恶意代码防范 | a）应采用免受恶意代码攻击的技术措施或主动免疫可信验证机制及时识别入侵和病毒行为，并将其有效阻断。 | 经核查，服务器上安装有青藤云天眼云镜，对主机恶意代码进行检测、清除，每天凌晨自动更新恶意代码特征库，经核查，具备恶意代码特征库更新记录。 |
| 可信验证 | a）可基于可信根对计算设备的系统引导程序、系统程序、重要配置参数和应用程序等进行可信验证，并在应用程序的关键执行环节进行动态可信验证，在检测到其可信性受到破坏后进行报警，并将验证结果形成审计记录送至安全管理中心。 | 未采用技术措施对计算设备的系统引导程序、系统程序、重要配置参数和通信应用程序等进行可信验证。 |
| 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； | 采用SSH协议连接操作系统，保证了鉴别信息以及管理数据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。 | 操作系统中对重要鉴别信息通过自身的加密及校验（SHA256），保证数据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； | 采用SSH协议连接操作系统，保证了鉴别信息以及管理数据在传输过程中的保密性。 |
| b）应采用密码技术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个人信息等。 | 通过系统自带的加密模块保证鉴别数据在存储过程中的保密性。 |
| 数据备份恢复 | a）应提供重要数据的本地数据备份与恢复功能； | 经核查，通过脚本每周将配置文件、代码仓库等数据备份至备份服务器中，依据需要验证备份数据的有效性。 |
| b）应提供异地实时备份功能，利用通信网络将重要数据实时备份至备份场地； | 系统无异地备份机制。 |
| c）应提供重要数据处理系统的热冗余，保证系统的高可用性。 | 服务器采用K8S容器部署，保证系统的高可用性。 |
| 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； | 操作系统提供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功能。 |
| 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。 | 操作系统提供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的功能。 |

4.1.3.11. 应用服务器21

|  |  |  |
| --- | --- | --- |
| **安全控制点** | **测评指标** | **结果记录** |
| 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）操作系统时采用用户名+SSHKey公私钥进行身份鉴别鉴别信息具有复杂度要求；2）执行cat /etc/shadow命令，查看shadow文件系统内用户身份标识唯一，不存在同名用户，且不存在空口令账号；3）经访谈，SSHKey公私钥每半年进行更换；4）查看sshd\_config配置文件中配置PasswordAuthentication no，拒绝使用密码方式进行身份鉴别。 |
| 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； | 操作系统采用用户名+SSHKey公私钥进行身份鉴别，可以防止鉴别信息被暴力破解；但未配置用户连接超时退出策略。 |
| 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； | 1）经核查，管理人员采用SSH协议连接操作系统；2）执行netatat –tpln| grep 23命令查看操作系统远程管理端口，不存在Telnet端口，防止鉴别信息在网络传输过程中的被窃听。 |
| 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。 | 未采用两种或两种以上组合的鉴别技术对用户进行身份鉴别。 |
| 访问控制 | a）应对登录的用户分配账户和权限； | 1）经访谈，通过root账户为登录的用户创建账户、分配权限；2）执行ls -l命令查看关键文件权限，均已为账户分配了相应权限，相关文件权限设置为/etc/shadow：000、/etc/passwd：644、/etc/group：644、/etc/profile：644、/etc/crontab：644、/ etc/securetty：600、/etc/ssh/sshd\_config：600。 |
| b）应重命名或删除默认账户，修改默认账户的默认口令； | 1）执行cat /etc/shadow命令查看shadow文件，操作系统中adm、lp、sync、shutdown、halt、mail、uucp、operator、games、gopher等账户均为nologin状态，存在默认账户root；2）执行more /etc/ssh/sshd\_config命令，查看“PermitRootLogin”参数设置为“yes”，即允许root远程登录；3）经访谈，root用户需通过公私钥方式进行身份鉴别。 |
| 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； | 1）执行cat /etc/shadow命令查看shadow文件，发现操作系统存在root、ysup、yops、yluser等在用账户，不存在多余的、过期账户；2）存在多个堡垒机账户登录操作系统时共用一个账户的情况。 |
| 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； | root账户具有系统所有权限，未实现管理用户的权限分离。 |
| e）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； | 经访谈，由系统管理员root配置访问控制策略，如：/etc/passwd，/etc/profile宿主为root、权限设置为644，audit文件为700、message文件为600，其他文件权限为750，实现用户对文件的权限控制。 |
| f）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； | 由管理用户进行用户访问权限分配进行设置，依据访问控制策略,对各类文件进行访问，重要文件和目录权限均在合理范围内，用户可根据文件不同的权限进行操作。 |
| g）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。 | 执 行more /etc/selinux/config 命令，查看config文件显示 SELINUX参数为 DISABLED，即未开启强制访问控制模式。 |
| 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）执行ps -ef|grep rsyslog和ps -ef|grep auditd命令，显示rsyslog和auditd进程正在运行；2）more /etc/audit/audit.rules，显示审计内容包括：\*.info、authriv.\*、mail.\*、cron.\*、\*.emerg、uucp、news.crit、local7.\*等事件。 |
| 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； | 执行tail -20 /var/log/audit/audit.log命令，查看近20条审计日志，内容包括：时间、对象、路径、用户ID、相关的系统调用、用户执行命令等。 |
| 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）通过访问权限对审计记录进行保护，日志文件/var/log/messages、/var/log/secure、/var/log/audit/audit.log访问 权限均为600；2）审计记录本地保存，且实时备份至360本地安全大脑，保存时间满足180天以上。 |
| d）应对审计进程进行保护，防止未经授权的中断。 | 执行service auditd status命令，系统开启auditd审计保护进程，审计进程由root用户维护，经现场使用yluser用户通过service auditd stop命令尝试中断审计进程，无法将审计进程单独中断。 |
| 入侵防范 | a）应遵循最小安装的原则，仅安装需要的组件和应用程序； | 1）系统安装遵循最小化安装原则；2）执行yum list installed命令查看操作系统已安装的程序包，存在Java、SSH、天眼云镜agent等应用程序或组件，不存在与业务系统无关的组件和应用程序。 |
| b）应关闭不需要的系统服务、默认共享和高危端口； | 1）执行systemctl list-unit-files 命令，系统已关闭FTP、Telnet 等高危网络服务；2）执行netstat -pantu命令，系统关闭了135、445等高危端口，仅开启了22、8080等端口。 |
| c）应通过设定终端接入方式或网络地址范围对通过网络进行管理的管理终端进行限制； | 经核查，1）通过配置安全组策略限制仅允许通过堡垒机管理服务器；2）经核查防火墙中访问控制策略，具备堡垒机地址-服务器管理网段（10.33.0.0）的访问控制策略。 |
| d）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； | 根据GB∕T 28448-2019 《信息安全技术 网络安全等级保护测评要求》测评对象范围描述，服务器无该项要求，故判为“不适用”。 |
| e）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； | 1）经过漏洞扫描，服务器不存在高危安全漏洞；2）执行rpm -qa grep patch命令，查看系统补丁已更新至最新。 |
| f）应能够检测到对重要节点进行入侵的行为，并在发生严重入侵事件时提供报警。 | 经核查，服务器上安装有青藤云天眼云镜，对主机入侵行为进行检测，发现严重安全事件时通过钉钉告警。 |
| 恶意代码防范 | a）应采用免受恶意代码攻击的技术措施或主动免疫可信验证机制及时识别入侵和病毒行为，并将其有效阻断。 | 经核查，服务器上安装有青藤云天眼云镜，对主机恶意代码进行检测、清除，每天凌晨自动更新恶意代码特征库，经核查，具备恶意代码特征库更新记录。 |
| 可信验证 | a）可基于可信根对计算设备的系统引导程序、系统程序、重要配置参数和应用程序等进行可信验证，并在应用程序的关键执行环节进行动态可信验证，在检测到其可信性受到破坏后进行报警，并将验证结果形成审计记录送至安全管理中心。 | 未采用技术措施对计算设备的系统引导程序、系统程序、重要配置参数和通信应用程序等进行可信验证。 |
| 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； | 采用SSH协议连接操作系统，保证了鉴别信息以及管理数据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。 | 操作系统中对重要鉴别信息通过自身的加密及校验（SHA256），保证数据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； | 采用SSH协议连接操作系统，保证了鉴别信息以及管理数据在传输过程中的保密性。 |
| b）应采用密码技术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个人信息等。 | 通过系统自带的加密模块保证鉴别数据在存储过程中的保密性。 |
| 数据备份恢复 | a）应提供重要数据的本地数据备份与恢复功能； | 经核查，通过脚本每周将配置文件、代码仓库等数据备份至备份服务器中，依据需要验证备份数据的有效性。 |
| b）应提供异地实时备份功能，利用通信网络将重要数据实时备份至备份场地； | 系统无异地备份机制。 |
| c）应提供重要数据处理系统的热冗余，保证系统的高可用性。 | 服务器采用K8S容器部署，保证系统的高可用性。 |
| 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； | 操作系统提供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功能。 |
| 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。 | 操作系统提供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的功能。 |

4.1.3.12. 应用服务器25

|  |  |  |
| --- | --- | --- |
| **安全控制点** | **测评指标** | **结果记录** |
| 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）操作系统时采用用户名+SSHKey公私钥进行身份鉴别鉴别信息具有复杂度要求；2）执行cat /etc/shadow命令，查看shadow文件系统内用户身份标识唯一，不存在同名用户，且不存在空口令账号；3）经访谈，SSHKey公私钥每半年进行更换；4）查看sshd\_config配置文件中配置PasswordAuthentication no，拒绝使用密码方式进行身份鉴别。 |
| 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； | 操作系统采用用户名+SSHKey公私钥进行身份鉴别，可以防止鉴别信息被暴力破解；但未配置用户连接超时退出策略。 |
| 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； | 1）经核查，管理人员采用SSH协议连接操作系统；2）执行netatat –tpln| grep 23命令查看操作系统远程管理端口，不存在Telnet端口，防止鉴别信息在网络传输过程中的被窃听。 |
| 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。 | 未采用两种或两种以上组合的鉴别技术对用户进行身份鉴别。 |
| 访问控制 | a）应对登录的用户分配账户和权限； | 1）经访谈，通过root账户为登录的用户创建账户、分配权限；2）执行ls -l命令查看关键文件权限，均已为账户分配了相应权限，相关文件权限设置为/etc/shadow：000、/etc/passwd：644、/etc/group：644、/etc/profile：644、/etc/crontab：644、/ etc/securetty：600、/etc/ssh/sshd\_config：600。 |
| b）应重命名或删除默认账户，修改默认账户的默认口令； | 1）执行cat /etc/shadow命令查看shadow文件，操作系统中adm、lp、sync、shutdown、halt、mail、uucp、operator、games、gopher等账户均为nologin状态，存在默认账户root；2）执行more /etc/ssh/sshd\_config命令，查看“PermitRootLogin”参数设置为“yes”，即允许root远程登录；3）经访谈，root用户需通过公私钥方式进行身份鉴别。 |
| 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； | 1）执行cat /etc/shadow命令查看shadow文件，发现操作系统存在root、ysup、yops、yluser等在用账户，不存在多余的、过期账户；2）存在多个堡垒机账户登录操作系统时共用一个账户的情况。 |
| 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； | root账户具有系统所有权限，未实现管理用户的权限分离。 |
| e）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； | 经访谈，由系统管理员root配置访问控制策略，如：/etc/passwd，/etc/profile宿主为root、权限设置为644，audit文件为700、message文件为600，其他文件权限为750，实现用户对文件的权限控制。 |
| f）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； | 由管理用户进行用户访问权限分配进行设置，依据访问控制策略,对各类文件进行访问，重要文件和目录权限均在合理范围内，用户可根据文件不同的权限进行操作。 |
| g）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。 | 执 行more /etc/selinux/config 命令，查看config文件显示 SELINUX参数为 DISABLED，即未开启强制访问控制模式。 |
| 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）执行ps -ef|grep rsyslog和ps -ef|grep auditd命令，显示rsyslog和auditd进程正在运行；2）more /etc/audit/audit.rules，显示审计内容包括：\*.info、authriv.\*、mail.\*、cron.\*、\*.emerg、uucp、news.crit、local7.\*等事件。 |
| 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； | 执行tail -20 /var/log/audit/audit.log命令，查看近20条审计日志，内容包括：时间、对象、路径、用户ID、相关的系统调用、用户执行命令等。 |
| 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）通过访问权限对审计记录进行保护，日志文件/var/log/messages、/var/log/secure、/var/log/audit/audit.log访问 权限均为600；2）审计记录本地保存，且实时备份至360本地安全大脑，保存时间满足180天以上。 |
| d）应对审计进程进行保护，防止未经授权的中断。 | 执行service auditd status命令，系统开启auditd审计保护进程，审计进程由root用户维护，经现场使用yluser用户通过service auditd stop命令尝试中断审计进程，无法将审计进程单独中断。 |
| 入侵防范 | a）应遵循最小安装的原则，仅安装需要的组件和应用程序； | 1）系统安装遵循最小化安装原则；2）执行yum list installed命令查看操作系统已安装的程序包，存在Java、SSH、天眼云镜agent等应用程序或组件，不存在与业务系统无关的组件和应用程序。 |
| b）应关闭不需要的系统服务、默认共享和高危端口； | 1）执行systemctl list-unit-files 命令，系统已关闭FTP、Telnet 等高危网络服务；2）执行netstat -pantu命令，系统关闭了135、445等高危端口，仅开启了22、8080等端口。 |
| c）应通过设定终端接入方式或网络地址范围对通过网络进行管理的管理终端进行限制； | 经核查，1）通过配置安全组策略限制仅允许通过堡垒机管理服务器；2）经核查防火墙中访问控制策略，具备堡垒机地址-服务器管理网段（10.33.0.0）的访问控制策略。 |
| d）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； | 根据GB∕T 28448-2019 《信息安全技术 网络安全等级保护测评要求》测评对象范围描述，服务器无该项要求，故判为“不适用”。 |
| e）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； | 1）经过漏洞扫描，服务器不存在高危安全漏洞；2）执行rpm -qa grep patch命令，查看系统补丁已更新至最新。 |
| f）应能够检测到对重要节点进行入侵的行为，并在发生严重入侵事件时提供报警。 | 经核查，服务器上安装有青藤云天眼云镜，对主机入侵行为进行检测，发现严重安全事件时通过钉钉告警。 |
| 恶意代码防范 | a）应采用免受恶意代码攻击的技术措施或主动免疫可信验证机制及时识别入侵和病毒行为，并将其有效阻断。 | 经核查，服务器上安装有青藤云天眼云镜，对主机恶意代码进行检测、清除，每天凌晨自动更新恶意代码特征库，经核查，具备恶意代码特征库更新记录。 |
| 可信验证 | a）可基于可信根对计算设备的系统引导程序、系统程序、重要配置参数和应用程序等进行可信验证，并在应用程序的关键执行环节进行动态可信验证，在检测到其可信性受到破坏后进行报警，并将验证结果形成审计记录送至安全管理中心。 | 未采用技术措施对计算设备的系统引导程序、系统程序、重要配置参数和通信应用程序等进行可信验证。 |
| 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； | 采用SSH协议连接操作系统，保证了鉴别信息以及管理数据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。 | 操作系统中对重要鉴别信息通过自身的加密及校验（SHA256），保证数据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； | 采用SSH协议连接操作系统，保证了鉴别信息以及管理数据在传输过程中的保密性。 |
| b）应采用密码技术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个人信息等。 | 通过系统自带的加密模块保证鉴别数据在存储过程中的保密性。 |
| 数据备份恢复 | a）应提供重要数据的本地数据备份与恢复功能； | 经核查，通过脚本每周将配置文件、代码仓库等数据备份至备份服务器中，依据需要验证备份数据的有效性。 |
| b）应提供异地实时备份功能，利用通信网络将重要数据实时备份至备份场地； | 系统无异地备份机制。 |
| c）应提供重要数据处理系统的热冗余，保证系统的高可用性。 | 服务器采用K8S容器部署，保证系统的高可用性。 |
| 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； | 操作系统提供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功能。 |
| 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。 | 操作系统提供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的功能。 |

4.1.3.13. 应用服务器26

|  |  |  |
| --- | --- | --- |
| **安全控制点** | **测评指标** | **结果记录** |
| 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）操作系统时采用用户名+SSHKey公私钥进行身份鉴别鉴别信息具有复杂度要求；2）执行cat /etc/shadow命令，查看shadow文件系统内用户身份标识唯一，不存在同名用户，且不存在空口令账号；3）经访谈，SSHKey公私钥每半年进行更换；4）查看sshd\_config配置文件中配置PasswordAuthentication no，拒绝使用密码方式进行身份鉴别。 |
| 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； | 操作系统采用用户名+SSHKey公私钥进行身份鉴别，可以防止鉴别信息被暴力破解；但未配置用户连接超时退出策略。 |
| 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； | 1）经核查，管理人员采用SSH协议连接操作系统；2）执行netatat –tpln| grep 23命令查看操作系统远程管理端口，不存在Telnet端口，防止鉴别信息在网络传输过程中的被窃听。 |
| 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。 | 未采用两种或两种以上组合的鉴别技术对用户进行身份鉴别。 |
| 访问控制 | a）应对登录的用户分配账户和权限； | 1）经访谈，通过root账户为登录的用户创建账户、分配权限；2）执行ls -l命令查看关键文件权限，均已为账户分配了相应权限，相关文件权限设置为/etc/shadow：000、/etc/passwd：644、/etc/group：644、/etc/profile：644、/etc/crontab：644、/ etc/securetty：600、/etc/ssh/sshd\_config：600。 |
| b）应重命名或删除默认账户，修改默认账户的默认口令； | 1）执行cat /etc/shadow命令查看shadow文件，操作系统中adm、lp、sync、shutdown、halt、mail、uucp、operator、games、gopher等账户均为nologin状态，存在默认账户root；2）执行more /etc/ssh/sshd\_config命令，查看“PermitRootLogin”参数设置为“yes”，即允许root远程登录；3）经访谈，root用户需通过公私钥方式进行身份鉴别。 |
| 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； | 1）执行cat /etc/shadow命令查看shadow文件，发现操作系统存在root、ysup、yops、yluser等在用账户，不存在多余的、过期账户；2）存在多个堡垒机账户登录操作系统时共用一个账户的情况。 |
| 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； | root账户具有系统所有权限，未实现管理用户的权限分离。 |
| e）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； | 经访谈，由系统管理员root配置访问控制策略，如：/etc/passwd，/etc/profile宿主为root、权限设置为644，audit文件为700、message文件为600，其他文件权限为750，实现用户对文件的权限控制。 |
| f）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； | 由管理用户进行用户访问权限分配进行设置，依据访问控制策略,对各类文件进行访问，重要文件和目录权限均在合理范围内，用户可根据文件不同的权限进行操作。 |
| g）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。 | 执 行more /etc/selinux/config 命令，查看config文件显示 SELINUX参数为 DISABLED，即未开启强制访问控制模式。 |
| 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）执行ps -ef|grep rsyslog和ps -ef|grep auditd命令，显示rsyslog和auditd进程正在运行；2）more /etc/audit/audit.rules，显示审计内容包括：\*.info、authriv.\*、mail.\*、cron.\*、\*.emerg、uucp、news.crit、local7.\*等事件。 |
| 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； | 执行tail -20 /var/log/audit/audit.log命令，查看近20条审计日志，内容包括：时间、对象、路径、用户ID、相关的系统调用、用户执行命令等。 |
| 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）通过访问权限对审计记录进行保护，日志文件/var/log/messages、/var/log/secure、/var/log/audit/audit.log访问 权限均为600；2）审计记录本地保存，且实时备份至360本地安全大脑，保存时间满足180天以上。 |
| d）应对审计进程进行保护，防止未经授权的中断。 | 执行service auditd status命令，系统开启auditd审计保护进程，审计进程由root用户维护，经现场使用yluser用户通过service auditd stop命令尝试中断审计进程，无法将审计进程单独中断。 |
| 入侵防范 | a）应遵循最小安装的原则，仅安装需要的组件和应用程序； | 1）系统安装遵循最小化安装原则；2）执行yum list installed命令查看操作系统已安装的程序包，存在Java、SSH、天眼云镜agent等应用程序或组件，不存在与业务系统无关的组件和应用程序。 |
| b）应关闭不需要的系统服务、默认共享和高危端口； | 1）执行systemctl list-unit-files 命令，系统已关闭FTP、Telnet 等高危网络服务；2）执行netstat -pantu命令，系统关闭了135、445等高危端口，仅开启了22、8080等端口。 |
| c）应通过设定终端接入方式或网络地址范围对通过网络进行管理的管理终端进行限制； | 经核查，1）通过配置安全组策略限制仅允许通过堡垒机管理服务器；2）经核查防火墙中访问控制策略，具备堡垒机地址-服务器管理网段（10.33.0.0）的访问控制策略。 |
| d）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； | 根据GB∕T 28448-2019 《信息安全技术 网络安全等级保护测评要求》测评对象范围描述，服务器无该项要求，故判为“不适用”。 |
| e）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； | 1）经过漏洞扫描，服务器不存在高危安全漏洞；2）执行rpm -qa grep patch命令，查看系统补丁已更新至最新。 |
| f）应能够检测到对重要节点进行入侵的行为，并在发生严重入侵事件时提供报警。 | 经核查，服务器上安装有青藤云天眼云镜，对主机入侵行为进行检测，发现严重安全事件时通过钉钉告警。 |
| 恶意代码防范 | a）应采用免受恶意代码攻击的技术措施或主动免疫可信验证机制及时识别入侵和病毒行为，并将其有效阻断。 | 经核查，服务器上安装有青藤云天眼云镜，对主机恶意代码进行检测、清除，每天凌晨自动更新恶意代码特征库，经核查，具备恶意代码特征库更新记录。 |
| 可信验证 | a）可基于可信根对计算设备的系统引导程序、系统程序、重要配置参数和应用程序等进行可信验证，并在应用程序的关键执行环节进行动态可信验证，在检测到其可信性受到破坏后进行报警，并将验证结果形成审计记录送至安全管理中心。 | 未采用技术措施对计算设备的系统引导程序、系统程序、重要配置参数和通信应用程序等进行可信验证。 |
| 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； | 采用SSH协议连接操作系统，保证了鉴别信息以及管理数据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。 | 操作系统中对重要鉴别信息通过自身的加密及校验（SHA256），保证数据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； | 采用SSH协议连接操作系统，保证了鉴别信息以及管理数据在传输过程中的保密性。 |
| b）应采用密码技术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个人信息等。 | 通过系统自带的加密模块保证鉴别数据在存储过程中的保密性。 |
| 数据备份恢复 | a）应提供重要数据的本地数据备份与恢复功能； | 经核查，通过脚本每周将配置文件、代码仓库等数据备份至备份服务器中，依据需要验证备份数据的有效性。 |
| b）应提供异地实时备份功能，利用通信网络将重要数据实时备份至备份场地； | 系统无异地备份机制。 |
| c）应提供重要数据处理系统的热冗余，保证系统的高可用性。 | 服务器采用K8S容器部署，保证系统的高可用性。 |
| 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； | 操作系统提供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功能。 |
| 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。 | 操作系统提供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的功能。 |

4.1.3.14. 应用服务器29

|  |  |  |
| --- | --- | --- |
| **安全控制点** | **测评指标** | **结果记录** |
| 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）操作系统时采用用户名+SSHKey公私钥进行身份鉴别鉴别信息具有复杂度要求；2）执行cat /etc/shadow命令，查看shadow文件系统内用户身份标识唯一，不存在同名用户，且不存在空口令账号；3）经访谈，SSHKey公私钥每半年进行更换；4）查看sshd\_config配置文件中配置PasswordAuthentication no，拒绝使用密码方式进行身份鉴别。 |
| 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； | 操作系统采用用户名+SSHKey公私钥进行身份鉴别，可以防止鉴别信息被暴力破解；但未配置用户连接超时退出策略。 |
| 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； | 1）经核查，管理人员采用SSH协议连接操作系统；2）执行netatat –tpln| grep 23命令查看操作系统远程管理端口，不存在Telnet端口，防止鉴别信息在网络传输过程中的被窃听。 |
| 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。 | 未采用两种或两种以上组合的鉴别技术对用户进行身份鉴别。 |
| 访问控制 | a）应对登录的用户分配账户和权限； | 1）经访谈，通过root账户为登录的用户创建账户、分配权限；2）执行ls -l命令查看关键文件权限，均已为账户分配了相应权限，相关文件权限设置为/etc/shadow：000、/etc/passwd：644、/etc/group：644、/etc/profile：644、/etc/crontab：644、/ etc/securetty：600、/etc/ssh/sshd\_config：600。 |
| b）应重命名或删除默认账户，修改默认账户的默认口令； | 1）执行cat /etc/shadow命令查看shadow文件，操作系统中adm、lp、sync、shutdown、halt、mail、uucp、operator、games、gopher等账户均为nologin状态，存在默认账户root；2）执行more /etc/ssh/sshd\_config命令，查看“PermitRootLogin”参数设置为“yes”，即允许root远程登录；3）经访谈，root用户需通过公私钥方式进行身份鉴别。 |
| 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； | 1）执行cat /etc/shadow命令查看shadow文件，发现操作系统存在root、ysup、yops、yluser等在用账户，不存在多余的、过期账户；2）存在多个堡垒机账户登录操作系统时共用一个账户的情况。 |
| 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； | root账户具有系统所有权限，未实现管理用户的权限分离。 |
| e）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； | 经访谈，由系统管理员root配置访问控制策略，如：/etc/passwd，/etc/profile宿主为root、权限设置为644，audit文件为700、message文件为600，其他文件权限为750，实现用户对文件的权限控制。 |
| f）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； | 由管理用户进行用户访问权限分配进行设置，依据访问控制策略,对各类文件进行访问，重要文件和目录权限均在合理范围内，用户可根据文件不同的权限进行操作。 |
| g）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。 | 执 行more /etc/selinux/config 命令，查看config文件显示 SELINUX参数为 DISABLED，即未开启强制访问控制模式。 |
| 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）执行ps -ef|grep rsyslog和ps -ef|grep auditd命令，显示rsyslog和auditd进程正在运行；2）more /etc/audit/audit.rules，显示审计内容包括：\*.info、authriv.\*、mail.\*、cron.\*、\*.emerg、uucp、news.crit、local7.\*等事件。 |
| 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； | 执行tail -20 /var/log/audit/audit.log命令，查看近20条审计日志，内容包括：时间、对象、路径、用户ID、相关的系统调用、用户执行命令等。 |
| 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）通过访问权限对审计记录进行保护，日志文件/var/log/messages、/var/log/secure、/var/log/audit/audit.log访问 权限均为600；2）审计记录本地保存，且实时备份至360本地安全大脑，保存时间满足180天以上。 |
| d）应对审计进程进行保护，防止未经授权的中断。 | 执行service auditd status命令，系统开启auditd审计保护进程，审计进程由root用户维护，经现场使用yluser用户通过service auditd stop命令尝试中断审计进程，无法将审计进程单独中断。 |
| 入侵防范 | a）应遵循最小安装的原则，仅安装需要的组件和应用程序； | 1）系统安装遵循最小化安装原则；2）执行yum list installed命令查看操作系统已安装的程序包，存在Java、SSH、天眼云镜agent等应用程序或组件，不存在与业务系统无关的组件和应用程序。 |
| b）应关闭不需要的系统服务、默认共享和高危端口； | 1）执行systemctl list-unit-files 命令，系统已关闭FTP、Telnet 等高危网络服务；2）执行netstat -pantu命令，系统关闭了135、445等高危端口，仅开启了22、8080等端口。 |
| c）应通过设定终端接入方式或网络地址范围对通过网络进行管理的管理终端进行限制； | 经核查，1）通过配置安全组策略限制仅允许通过堡垒机管理服务器；2）经核查防火墙中访问控制策略，具备堡垒机地址-服务器管理网段（10.33.0.0）的访问控制策略。 |
| d）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； | 根据GB∕T 28448-2019 《信息安全技术 网络安全等级保护测评要求》测评对象范围描述，服务器无该项要求，故判为“不适用”。 |
| e）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； | 1）经过漏洞扫描，服务器不存在高危安全漏洞；2）执行rpm -qa grep patch命令，查看系统补丁已更新至最新。 |
| f）应能够检测到对重要节点进行入侵的行为，并在发生严重入侵事件时提供报警。 | 经核查，服务器上安装有青藤云天眼云镜，对主机入侵行为进行检测，发现严重安全事件时通过钉钉告警。 |
| 恶意代码防范 | a）应采用免受恶意代码攻击的技术措施或主动免疫可信验证机制及时识别入侵和病毒行为，并将其有效阻断。 | 经核查，服务器上安装有青藤云天眼云镜，对主机恶意代码进行检测、清除，每天凌晨自动更新恶意代码特征库，经核查，具备恶意代码特征库更新记录。 |
| 可信验证 | a）可基于可信根对计算设备的系统引导程序、系统程序、重要配置参数和应用程序等进行可信验证，并在应用程序的关键执行环节进行动态可信验证，在检测到其可信性受到破坏后进行报警，并将验证结果形成审计记录送至安全管理中心。 | 未采用技术措施对计算设备的系统引导程序、系统程序、重要配置参数和通信应用程序等进行可信验证。 |
| 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； | 采用SSH协议连接操作系统，保证了鉴别信息以及管理数据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。 | 操作系统中对重要鉴别信息通过自身的加密及校验（SHA256），保证数据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； | 采用SSH协议连接操作系统，保证了鉴别信息以及管理数据在传输过程中的保密性。 |
| b）应采用密码技术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个人信息等。 | 通过系统自带的加密模块保证鉴别数据在存储过程中的保密性。 |
| 数据备份恢复 | a）应提供重要数据的本地数据备份与恢复功能； | 经核查，通过脚本每周将配置文件、代码仓库等数据备份至备份服务器中，依据需要验证备份数据的有效性。 |
| b）应提供异地实时备份功能，利用通信网络将重要数据实时备份至备份场地； | 系统无异地备份机制。 |
| c）应提供重要数据处理系统的热冗余，保证系统的高可用性。 | 服务器采用K8S容器部署，保证系统的高可用性。 |
| 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； | 操作系统提供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功能。 |
| 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。 | 操作系统提供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的功能。 |

4.1.3.15. 应用服务器32

|  |  |  |
| --- | --- | --- |
| **安全控制点** | **测评指标** | **结果记录** |
| 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）操作系统时采用用户名+SSHKey公私钥进行身份鉴别鉴别信息具有复杂度要求；2）执行cat /etc/shadow命令，查看shadow文件系统内用户身份标识唯一，不存在同名用户，且不存在空口令账号；3）经访谈，SSHKey公私钥每半年进行更换；4）查看sshd\_config配置文件中配置PasswordAuthentication no，拒绝使用密码方式进行身份鉴别。 |
| 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； | 操作系统采用用户名+SSHKey公私钥进行身份鉴别，可以防止鉴别信息被暴力破解；但未配置用户连接超时退出策略。 |
| 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； | 1）经核查，管理人员采用SSH协议连接操作系统；2）执行netatat –tpln| grep 23命令查看操作系统远程管理端口，不存在Telnet端口，防止鉴别信息在网络传输过程中的被窃听。 |
| 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。 | 未采用两种或两种以上组合的鉴别技术对用户进行身份鉴别。 |
| 访问控制 | a）应对登录的用户分配账户和权限； | 1）经访谈，通过root账户为登录的用户创建账户、分配权限；2）执行ls -l命令查看关键文件权限，均已为账户分配了相应权限，相关文件权限设置为/etc/shadow：000、/etc/passwd：644、/etc/group：644、/etc/profile：644、/etc/crontab：644、/ etc/securetty：600、/etc/ssh/sshd\_config：600。 |
| b）应重命名或删除默认账户，修改默认账户的默认口令； | 1）执行cat /etc/shadow命令查看shadow文件，操作系统中adm、lp、sync、shutdown、halt、mail、uucp、operator、games、gopher等账户均为nologin状态，存在默认账户root；2）执行more /etc/ssh/sshd\_config命令，查看“PermitRootLogin”参数设置为“yes”，即允许root远程登录；3）经访谈，root用户需通过公私钥方式进行身份鉴别。 |
| 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； | 1）执行cat /etc/shadow命令查看shadow文件，发现操作系统存在root、ysup、yops、yluser等在用账户，不存在多余的、过期账户；2）存在多个堡垒机账户登录操作系统时共用一个账户的情况。 |
| 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； | root账户具有系统所有权限，未实现管理用户的权限分离。 |
| e）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； | 经访谈，由系统管理员root配置访问控制策略，如：/etc/passwd，/etc/profile宿主为root、权限设置为644，audit文件为700、message文件为600，其他文件权限为750，实现用户对文件的权限控制。 |
| f）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； | 由管理用户进行用户访问权限分配进行设置，依据访问控制策略,对各类文件进行访问，重要文件和目录权限均在合理范围内，用户可根据文件不同的权限进行操作。 |
| g）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。 | 执 行more /etc/selinux/config 命令，查看config文件显示 SELINUX参数为 DISABLED，即未开启强制访问控制模式。 |
| 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）执行ps -ef|grep rsyslog和ps -ef|grep auditd命令，显示rsyslog和auditd进程正在运行；2）more /etc/audit/audit.rules，显示审计内容包括：\*.info、authriv.\*、mail.\*、cron.\*、\*.emerg、uucp、news.crit、local7.\*等事件。 |
| 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； | 执行tail -20 /var/log/audit/audit.log命令，查看近20条审计日志，内容包括：时间、对象、路径、用户ID、相关的系统调用、用户执行命令等。 |
| 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）通过访问权限对审计记录进行保护，日志文件/var/log/messages、/var/log/secure、/var/log/audit/audit.log访问 权限均为600；2）审计记录本地保存，且实时备份至360本地安全大脑，保存时间满足180天以上。 |
| d）应对审计进程进行保护，防止未经授权的中断。 | 执行service auditd status命令，系统开启auditd审计保护进程，审计进程由root用户维护，经现场使用yluser用户通过service auditd stop命令尝试中断审计进程，无法将审计进程单独中断。 |
| 入侵防范 | a）应遵循最小安装的原则，仅安装需要的组件和应用程序； | 1）系统安装遵循最小化安装原则；2）执行yum list installed命令查看操作系统已安装的程序包，存在Java、SSH、天眼云镜agent等应用程序或组件，不存在与业务系统无关的组件和应用程序。 |
| b）应关闭不需要的系统服务、默认共享和高危端口； | 1）执行systemctl list-unit-files 命令，系统已关闭FTP、Telnet 等高危网络服务；2）执行netstat -pantu命令，系统关闭了135、445等高危端口，仅开启了22、8080等端口。 |
| c）应通过设定终端接入方式或网络地址范围对通过网络进行管理的管理终端进行限制； | 经核查，1）通过配置安全组策略限制仅允许通过堡垒机管理服务器；2）经核查防火墙中访问控制策略，具备堡垒机地址-服务器管理网段（10.33.0.0）的访问控制策略。 |
| d）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； | 根据GB∕T 28448-2019 《信息安全技术 网络安全等级保护测评要求》测评对象范围描述，服务器无该项要求，故判为“不适用”。 |
| e）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； | 1）经过漏洞扫描，服务器不存在高危安全漏洞；2）执行rpm -qa grep patch命令，查看系统补丁已更新至最新。 |
| f）应能够检测到对重要节点进行入侵的行为，并在发生严重入侵事件时提供报警。 | 经核查，服务器上安装有青藤云天眼云镜，对主机入侵行为进行检测，发现严重安全事件时通过钉钉告警。 |
| 恶意代码防范 | a）应采用免受恶意代码攻击的技术措施或主动免疫可信验证机制及时识别入侵和病毒行为，并将其有效阻断。 | 经核查，服务器上安装有青藤云天眼云镜，对主机恶意代码进行检测、清除，每天凌晨自动更新恶意代码特征库，经核查，具备恶意代码特征库更新记录。 |
| 可信验证 | a）可基于可信根对计算设备的系统引导程序、系统程序、重要配置参数和应用程序等进行可信验证，并在应用程序的关键执行环节进行动态可信验证，在检测到其可信性受到破坏后进行报警，并将验证结果形成审计记录送至安全管理中心。 | 未采用技术措施对计算设备的系统引导程序、系统程序、重要配置参数和通信应用程序等进行可信验证。 |
| 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； | 采用SSH协议连接操作系统，保证了鉴别信息以及管理数据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。 | 操作系统中对重要鉴别信息通过自身的加密及校验（SHA256），保证数据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； | 采用SSH协议连接操作系统，保证了鉴别信息以及管理数据在传输过程中的保密性。 |
| b）应采用密码技术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个人信息等。 | 通过系统自带的加密模块保证鉴别数据在存储过程中的保密性。 |
| 数据备份恢复 | a）应提供重要数据的本地数据备份与恢复功能； | 经核查，通过脚本每周将配置文件、代码仓库等数据备份至备份服务器中，依据需要验证备份数据的有效性。 |
| b）应提供异地实时备份功能，利用通信网络将重要数据实时备份至备份场地； | 系统无异地备份机制。 |
| c）应提供重要数据处理系统的热冗余，保证系统的高可用性。 | 服务器采用K8S容器部署，保证系统的高可用性。 |
| 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； | 操作系统提供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功能。 |
| 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。 | 操作系统提供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的功能。 |

4.1.3.16. 应用服务器33

|  |  |  |
| --- | --- | --- |
| **安全控制点** | **测评指标** | **结果记录** |
| 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）操作系统时采用用户名+SSHKey公私钥进行身份鉴别鉴别信息具有复杂度要求；2）执行cat /etc/shadow命令，查看shadow文件系统内用户身份标识唯一，不存在同名用户，且不存在空口令账号；3）经访谈，SSHKey公私钥每半年进行更换；4）查看sshd\_config配置文件中配置PasswordAuthentication no，拒绝使用密码方式进行身份鉴别。 |
| 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； | 操作系统采用用户名+SSHKey公私钥进行身份鉴别，可以防止鉴别信息被暴力破解；但未配置用户连接超时退出策略。 |
| 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； | 1）经核查，管理人员采用SSH协议连接操作系统；2）执行netatat –tpln| grep 23命令查看操作系统远程管理端口，不存在Telnet端口，防止鉴别信息在网络传输过程中的被窃听。 |
| 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。 | 未采用两种或两种以上组合的鉴别技术对用户进行身份鉴别。 |
| 访问控制 | a）应对登录的用户分配账户和权限； | 1）经访谈，通过root账户为登录的用户创建账户、分配权限；2）执行ls -l命令查看关键文件权限，均已为账户分配了相应权限，相关文件权限设置为/etc/shadow：000、/etc/passwd：644、/etc/group：644、/etc/profile：644、/etc/crontab：644、/ etc/securetty：600、/etc/ssh/sshd\_config：600。 |
| b）应重命名或删除默认账户，修改默认账户的默认口令； | 1）执行cat /etc/shadow命令查看shadow文件，操作系统中adm、lp、sync、shutdown、halt、mail、uucp、operator、games、gopher等账户均为nologin状态，存在默认账户root；2）执行more /etc/ssh/sshd\_config命令，查看“PermitRootLogin”参数设置为“yes”，即允许root远程登录；3）经访谈，root用户需通过公私钥方式进行身份鉴别。 |
| 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； | 1）执行cat /etc/shadow命令查看shadow文件，发现操作系统存在root、ysup、yops、yluser等在用账户，不存在多余的、过期账户；2）存在多个堡垒机账户登录操作系统时共用一个账户的情况。 |
| 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； | root账户具有系统所有权限，未实现管理用户的权限分离。 |
| e）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； | 经访谈，由系统管理员root配置访问控制策略，如：/etc/passwd，/etc/profile宿主为root、权限设置为644，audit文件为700、message文件为600，其他文件权限为750，实现用户对文件的权限控制。 |
| f）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； | 由管理用户进行用户访问权限分配进行设置，依据访问控制策略,对各类文件进行访问，重要文件和目录权限均在合理范围内，用户可根据文件不同的权限进行操作。 |
| g）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。 | 执 行more /etc/selinux/config 命令，查看config文件显示 SELINUX参数为 DISABLED，即未开启强制访问控制模式。 |
| 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）执行ps -ef|grep rsyslog和ps -ef|grep auditd命令，显示rsyslog和auditd进程正在运行；2）more /etc/audit/audit.rules，显示审计内容包括：\*.info、authriv.\*、mail.\*、cron.\*、\*.emerg、uucp、news.crit、local7.\*等事件。 |
| 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； | 执行tail -20 /var/log/audit/audit.log命令，查看近20条审计日志，内容包括：时间、对象、路径、用户ID、相关的系统调用、用户执行命令等。 |
| 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）通过访问权限对审计记录进行保护，日志文件/var/log/messages、/var/log/secure、/var/log/audit/audit.log访问 权限均为600；2）审计记录本地保存，且实时备份至360本地安全大脑，保存时间满足180天以上。 |
| d）应对审计进程进行保护，防止未经授权的中断。 | 执行service auditd status命令，系统开启auditd审计保护进程，审计进程由root用户维护，经现场使用yluser用户通过service auditd stop命令尝试中断审计进程，无法将审计进程单独中断。 |
| 入侵防范 | a）应遵循最小安装的原则，仅安装需要的组件和应用程序； | 1）系统安装遵循最小化安装原则；2）执行yum list installed命令查看操作系统已安装的程序包，存在Java、SSH、天眼云镜agent等应用程序或组件，不存在与业务系统无关的组件和应用程序。 |
| b）应关闭不需要的系统服务、默认共享和高危端口； | 1）执行systemctl list-unit-files 命令，系统已关闭FTP、Telnet 等高危网络服务；2）执行netstat -pantu命令，系统关闭了135、445等高危端口，仅开启了22、8080等端口。 |
| c）应通过设定终端接入方式或网络地址范围对通过网络进行管理的管理终端进行限制； | 经核查，1）通过配置安全组策略限制仅允许通过堡垒机管理服务器；2）经核查防火墙中访问控制策略，具备堡垒机地址-服务器管理网段（10.33.0.0）的访问控制策略。 |
| d）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； | 根据GB∕T 28448-2019 《信息安全技术 网络安全等级保护测评要求》测评对象范围描述，服务器无该项要求，故判为“不适用”。 |
| e）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； | 1）经过漏洞扫描，服务器不存在高危安全漏洞；2）执行rpm -qa grep patch命令，查看系统补丁已更新至最新。 |
| f）应能够检测到对重要节点进行入侵的行为，并在发生严重入侵事件时提供报警。 | 经核查，服务器上安装有青藤云天眼云镜，对主机入侵行为进行检测，发现严重安全事件时通过钉钉告警。 |
| 恶意代码防范 | a）应采用免受恶意代码攻击的技术措施或主动免疫可信验证机制及时识别入侵和病毒行为，并将其有效阻断。 | 经核查，服务器上安装有青藤云天眼云镜，对主机恶意代码进行检测、清除，每天凌晨自动更新恶意代码特征库，经核查，具备恶意代码特征库更新记录。 |
| 可信验证 | a）可基于可信根对计算设备的系统引导程序、系统程序、重要配置参数和应用程序等进行可信验证，并在应用程序的关键执行环节进行动态可信验证，在检测到其可信性受到破坏后进行报警，并将验证结果形成审计记录送至安全管理中心。 | 未采用技术措施对计算设备的系统引导程序、系统程序、重要配置参数和通信应用程序等进行可信验证。 |
| 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； | 采用SSH协议连接操作系统，保证了鉴别信息以及管理数据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。 | 操作系统中对重要鉴别信息通过自身的加密及校验（SHA256），保证数据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； | 采用SSH协议连接操作系统，保证了鉴别信息以及管理数据在传输过程中的保密性。 |
| b）应采用密码技术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个人信息等。 | 通过系统自带的加密模块保证鉴别数据在存储过程中的保密性。 |
| 数据备份恢复 | a）应提供重要数据的本地数据备份与恢复功能； | 经核查，通过脚本每周将配置文件、代码仓库等数据备份至备份服务器中，依据需要验证备份数据的有效性。 |
| b）应提供异地实时备份功能，利用通信网络将重要数据实时备份至备份场地； | 系统无异地备份机制。 |
| c）应提供重要数据处理系统的热冗余，保证系统的高可用性。 | 服务器采用K8S容器部署，保证系统的高可用性。 |
| 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； | 操作系统提供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功能。 |
| 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。 | 操作系统提供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的功能。 |

4.1.3.17. 应用服务器34

|  |  |  |
| --- | --- | --- |
| **安全控制点** | **测评指标** | **结果记录** |
| 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）操作系统时采用用户名+SSHKey公私钥进行身份鉴别鉴别信息具有复杂度要求；2）执行cat /etc/shadow命令，查看shadow文件系统内用户身份标识唯一，不存在同名用户，且不存在空口令账号；3）经访谈，SSHKey公私钥每半年进行更换；4）查看sshd\_config配置文件中配置PasswordAuthentication no，拒绝使用密码方式进行身份鉴别。 |
| 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； | 操作系统采用用户名+SSHKey公私钥进行身份鉴别，可以防止鉴别信息被暴力破解；但未配置用户连接超时退出策略。 |
| 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； | 1）经核查，管理人员采用SSH协议连接操作系统；2）执行netatat –tpln| grep 23命令查看操作系统远程管理端口，不存在Telnet端口，防止鉴别信息在网络传输过程中的被窃听。 |
| 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。 | 未采用两种或两种以上组合的鉴别技术对用户进行身份鉴别。 |
| 访问控制 | a）应对登录的用户分配账户和权限； | 1）经访谈，通过root账户为登录的用户创建账户、分配权限；2）执行ls -l命令查看关键文件权限，均已为账户分配了相应权限，相关文件权限设置为/etc/shadow：000、/etc/passwd：644、/etc/group：644、/etc/profile：644、/etc/crontab：644、/ etc/securetty：600、/etc/ssh/sshd\_config：600。 |
| b）应重命名或删除默认账户，修改默认账户的默认口令； | 1）执行cat /etc/shadow命令查看shadow文件，操作系统中adm、lp、sync、shutdown、halt、mail、uucp、operator、games、gopher等账户均为nologin状态，存在默认账户root；2）执行more /etc/ssh/sshd\_config命令，查看“PermitRootLogin”参数设置为“yes”，即允许root远程登录；3）经访谈，root用户需通过公私钥方式进行身份鉴别。 |
| 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； | 1）执行cat /etc/shadow命令查看shadow文件，发现操作系统存在root、ysup、yops、yluser等在用账户，不存在多余的、过期账户；2）存在多个堡垒机账户登录操作系统时共用一个账户的情况。 |
| 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； | root账户具有系统所有权限，未实现管理用户的权限分离。 |
| e）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； | 经访谈，由系统管理员root配置访问控制策略，如：/etc/passwd，/etc/profile宿主为root、权限设置为644，audit文件为700、message文件为600，其他文件权限为750，实现用户对文件的权限控制。 |
| f）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； | 由管理用户进行用户访问权限分配进行设置，依据访问控制策略,对各类文件进行访问，重要文件和目录权限均在合理范围内，用户可根据文件不同的权限进行操作。 |
| g）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。 | 执 行more /etc/selinux/config 命令，查看config文件显示 SELINUX参数为 DISABLED，即未开启强制访问控制模式。 |
| 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）执行ps -ef|grep rsyslog和ps -ef|grep auditd命令，显示rsyslog和auditd进程正在运行；2）more /etc/audit/audit.rules，显示审计内容包括：\*.info、authriv.\*、mail.\*、cron.\*、\*.emerg、uucp、news.crit、local7.\*等事件。 |
| 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； | 执行tail -20 /var/log/audit/audit.log命令，查看近20条审计日志，内容包括：时间、对象、路径、用户ID、相关的系统调用、用户执行命令等。 |
| 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）通过访问权限对审计记录进行保护，日志文件/var/log/messages、/var/log/secure、/var/log/audit/audit.log访问 权限均为600；2）审计记录本地保存，且实时备份至360本地安全大脑，保存时间满足180天以上。 |
| d）应对审计进程进行保护，防止未经授权的中断。 | 执行service auditd status命令，系统开启auditd审计保护进程，审计进程由root用户维护，经现场使用yluser用户通过service auditd stop命令尝试中断审计进程，无法将审计进程单独中断。 |
| 入侵防范 | a）应遵循最小安装的原则，仅安装需要的组件和应用程序； | 1）系统安装遵循最小化安装原则；2）执行yum list installed命令查看操作系统已安装的程序包，存在Java、SSH、天眼云镜agent等应用程序或组件，不存在与业务系统无关的组件和应用程序。 |
| b）应关闭不需要的系统服务、默认共享和高危端口； | 1）执行systemctl list-unit-files 命令，系统已关闭FTP、Telnet 等高危网络服务；2）执行netstat -pantu命令，系统关闭了135、445等高危端口，仅开启了22、8080等端口。 |
| c）应通过设定终端接入方式或网络地址范围对通过网络进行管理的管理终端进行限制； | 经核查，1）通过配置安全组策略限制仅允许通过堡垒机管理服务器；2）经核查防火墙中访问控制策略，具备堡垒机地址-服务器管理网段（10.33.0.0）的访问控制策略。 |
| d）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； | 根据GB∕T 28448-2019 《信息安全技术 网络安全等级保护测评要求》测评对象范围描述，服务器无该项要求，故判为“不适用”。 |
| e）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； | 1）经过漏洞扫描，服务器不存在高危安全漏洞；2）执行rpm -qa grep patch命令，查看系统补丁已更新至最新。 |
| f）应能够检测到对重要节点进行入侵的行为，并在发生严重入侵事件时提供报警。 | 经核查，服务器上安装有青藤云天眼云镜，对主机入侵行为进行检测，发现严重安全事件时通过钉钉告警。 |
| 恶意代码防范 | a）应采用免受恶意代码攻击的技术措施或主动免疫可信验证机制及时识别入侵和病毒行为，并将其有效阻断。 | 经核查，服务器上安装有青藤云天眼云镜，对主机恶意代码进行检测、清除，每天凌晨自动更新恶意代码特征库，经核查，具备恶意代码特征库更新记录。 |
| 可信验证 | a）可基于可信根对计算设备的系统引导程序、系统程序、重要配置参数和应用程序等进行可信验证，并在应用程序的关键执行环节进行动态可信验证，在检测到其可信性受到破坏后进行报警，并将验证结果形成审计记录送至安全管理中心。 | 未采用技术措施对计算设备的系统引导程序、系统程序、重要配置参数和通信应用程序等进行可信验证。 |
| 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； | 采用SSH协议连接操作系统，保证了鉴别信息以及管理数据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。 | 操作系统中对重要鉴别信息通过自身的加密及校验（SHA256），保证数据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； | 采用SSH协议连接操作系统，保证了鉴别信息以及管理数据在传输过程中的保密性。 |
| b）应采用密码技术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个人信息等。 | 通过系统自带的加密模块保证鉴别数据在存储过程中的保密性。 |
| 数据备份恢复 | a）应提供重要数据的本地数据备份与恢复功能； | 经核查，通过脚本每周将配置文件、代码仓库等数据备份至备份服务器中，依据需要验证备份数据的有效性。 |
| b）应提供异地实时备份功能，利用通信网络将重要数据实时备份至备份场地； | 系统无异地备份机制。 |
| c）应提供重要数据处理系统的热冗余，保证系统的高可用性。 | 服务器采用K8S容器部署，保证系统的高可用性。 |
| 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； | 操作系统提供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功能。 |
| 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。 | 操作系统提供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的功能。 |

4.1.3.18. 应用服务器38

|  |  |  |
| --- | --- | --- |
| **安全控制点** | **测评指标** | **结果记录** |
| 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）操作系统时采用用户名+SSHKey公私钥进行身份鉴别鉴别信息具有复杂度要求；2）执行cat /etc/shadow命令，查看shadow文件系统内用户身份标识唯一，不存在同名用户，且不存在空口令账号；3）经访谈，SSHKey公私钥每半年进行更换；4）查看sshd\_config配置文件中配置PasswordAuthentication no，拒绝使用密码方式进行身份鉴别。 |
| 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； | 操作系统采用用户名+SSHKey公私钥进行身份鉴别，可以防止鉴别信息被暴力破解；但未配置用户连接超时退出策略。 |
| 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； | 1）经核查，管理人员采用SSH协议连接操作系统；2）执行netatat –tpln| grep 23命令查看操作系统远程管理端口，不存在Telnet端口，防止鉴别信息在网络传输过程中的被窃听。 |
| 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。 | 未采用两种或两种以上组合的鉴别技术对用户进行身份鉴别。 |
| 访问控制 | a）应对登录的用户分配账户和权限； | 1）经访谈，通过root账户为登录的用户创建账户、分配权限；2）执行ls -l命令查看关键文件权限，均已为账户分配了相应权限，相关文件权限设置为/etc/shadow：000、/etc/passwd：644、/etc/group：644、/etc/profile：644、/etc/crontab：644、/ etc/securetty：600、/etc/ssh/sshd\_config：600。 |
| b）应重命名或删除默认账户，修改默认账户的默认口令； | 1）执行cat /etc/shadow命令查看shadow文件，操作系统中adm、lp、sync、shutdown、halt、mail、uucp、operator、games、gopher等账户均为nologin状态，存在默认账户root；2）执行more /etc/ssh/sshd\_config命令，查看“PermitRootLogin”参数设置为“yes”，即允许root远程登录；3）经访谈，root用户需通过公私钥方式进行身份鉴别。 |
| 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； | 1）执行cat /etc/shadow命令查看shadow文件，发现操作系统存在root、ysup、yops、yluser等在用账户，不存在多余的、过期账户；2）存在多个堡垒机账户登录操作系统时共用一个账户的情况。 |
| 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； | root账户具有系统所有权限，未实现管理用户的权限分离。 |
| e）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； | 经访谈，由系统管理员root配置访问控制策略，如：/etc/passwd，/etc/profile宿主为root、权限设置为644，audit文件为700、message文件为600，其他文件权限为750，实现用户对文件的权限控制。 |
| f）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； | 由管理用户进行用户访问权限分配进行设置，依据访问控制策略,对各类文件进行访问，重要文件和目录权限均在合理范围内，用户可根据文件不同的权限进行操作。 |
| g）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。 | 执 行more /etc/selinux/config 命令，查看config文件显示 SELINUX参数为 DISABLED，即未开启强制访问控制模式。 |
| 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）执行ps -ef|grep rsyslog和ps -ef|grep auditd命令，显示rsyslog和auditd进程正在运行；2）more /etc/audit/audit.rules，显示审计内容包括：\*.info、authriv.\*、mail.\*、cron.\*、\*.emerg、uucp、news.crit、local7.\*等事件。 |
| 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； | 执行tail -20 /var/log/audit/audit.log命令，查看近20条审计日志，内容包括：时间、对象、路径、用户ID、相关的系统调用、用户执行命令等。 |
| 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）通过访问权限对审计记录进行保护，日志文件/var/log/messages、/var/log/secure、/var/log/audit/audit.log访问 权限均为600；2）审计记录本地保存，且实时备份至360本地安全大脑，保存时间满足180天以上。 |
| d）应对审计进程进行保护，防止未经授权的中断。 | 执行service auditd status命令，系统开启auditd审计保护进程，审计进程由root用户维护，经现场使用yluser用户通过service auditd stop命令尝试中断审计进程，无法将审计进程单独中断。 |
| 入侵防范 | a）应遵循最小安装的原则，仅安装需要的组件和应用程序； | 1）系统安装遵循最小化安装原则；2）执行yum list installed命令查看操作系统已安装的程序包，存在Java、SSH、天眼云镜agent等应用程序或组件，不存在与业务系统无关的组件和应用程序。 |
| b）应关闭不需要的系统服务、默认共享和高危端口； | 1）执行systemctl list-unit-files 命令，系统已关闭FTP、Telnet 等高危网络服务；2）执行netstat -pantu命令，系统关闭了135、445等高危端口，仅开启了22、8080等端口。 |
| c）应通过设定终端接入方式或网络地址范围对通过网络进行管理的管理终端进行限制； | 经核查，1）通过配置安全组策略限制仅允许通过堡垒机管理服务器；2）经核查防火墙中访问控制策略，具备堡垒机地址-服务器管理网段（10.33.0.0）的访问控制策略。 |
| d）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； | 根据GB∕T 28448-2019 《信息安全技术 网络安全等级保护测评要求》测评对象范围描述，服务器无该项要求，故判为“不适用”。 |
| e）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； | 1）经过漏洞扫描，服务器不存在高危安全漏洞；2）执行rpm -qa grep patch命令，查看系统补丁已更新至最新。 |
| f）应能够检测到对重要节点进行入侵的行为，并在发生严重入侵事件时提供报警。 | 经核查，服务器上安装有青藤云天眼云镜，对主机入侵行为进行检测，发现严重安全事件时通过钉钉告警。 |
| 恶意代码防范 | a）应采用免受恶意代码攻击的技术措施或主动免疫可信验证机制及时识别入侵和病毒行为，并将其有效阻断。 | 经核查，服务器上安装有青藤云天眼云镜，对主机恶意代码进行检测、清除，每天凌晨自动更新恶意代码特征库，经核查，具备恶意代码特征库更新记录。 |
| 可信验证 | a）可基于可信根对计算设备的系统引导程序、系统程序、重要配置参数和应用程序等进行可信验证，并在应用程序的关键执行环节进行动态可信验证，在检测到其可信性受到破坏后进行报警，并将验证结果形成审计记录送至安全管理中心。 | 未采用技术措施对计算设备的系统引导程序、系统程序、重要配置参数和通信应用程序等进行可信验证。 |
| 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； | 采用SSH协议连接操作系统，保证了鉴别信息以及管理数据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。 | 操作系统中对重要鉴别信息通过自身的加密及校验（SHA256），保证数据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； | 采用SSH协议连接操作系统，保证了鉴别信息以及管理数据在传输过程中的保密性。 |
| b）应采用密码技术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个人信息等。 | 通过系统自带的加密模块保证鉴别数据在存储过程中的保密性。 |
| 数据备份恢复 | a）应提供重要数据的本地数据备份与恢复功能； | 经核查，通过脚本每周将配置文件、代码仓库等数据备份至备份服务器中，依据需要验证备份数据的有效性。 |
| b）应提供异地实时备份功能，利用通信网络将重要数据实时备份至备份场地； | 系统无异地备份机制。 |
| c）应提供重要数据处理系统的热冗余，保证系统的高可用性。 | 服务器采用K8S容器部署，保证系统的高可用性。 |
| 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； | 操作系统提供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功能。 |
| 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。 | 操作系统提供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的功能。 |

4.1.3.19. 应用服务器39

|  |  |  |
| --- | --- | --- |
| **安全控制点** | **测评指标** | **结果记录** |
| 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）操作系统时采用用户名+SSHKey公私钥进行身份鉴别鉴别信息具有复杂度要求；2）执行cat /etc/shadow命令，查看shadow文件系统内用户身份标识唯一，不存在同名用户，且不存在空口令账号；3）经访谈，SSHKey公私钥每半年进行更换；4）查看sshd\_config配置文件中配置PasswordAuthentication no，拒绝使用密码方式进行身份鉴别。 |
| 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； | 操作系统采用用户名+SSHKey公私钥进行身份鉴别，可以防止鉴别信息被暴力破解；但未配置用户连接超时退出策略。 |
| 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； | 1）经核查，管理人员采用SSH协议连接操作系统；2）执行netatat –tpln| grep 23命令查看操作系统远程管理端口，不存在Telnet端口，防止鉴别信息在网络传输过程中的被窃听。 |
| 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。 | 未采用两种或两种以上组合的鉴别技术对用户进行身份鉴别。 |
| 访问控制 | a）应对登录的用户分配账户和权限； | 1）经访谈，通过root账户为登录的用户创建账户、分配权限；2）执行ls -l命令查看关键文件权限，均已为账户分配了相应权限，相关文件权限设置为/etc/shadow：000、/etc/passwd：644、/etc/group：644、/etc/profile：644、/etc/crontab：644、/ etc/securetty：600、/etc/ssh/sshd\_config：600。 |
| b）应重命名或删除默认账户，修改默认账户的默认口令； | 1）执行cat /etc/shadow命令查看shadow文件，操作系统中adm、lp、sync、shutdown、halt、mail、uucp、operator、games、gopher等账户均为nologin状态，存在默认账户root；2）执行more /etc/ssh/sshd\_config命令，查看“PermitRootLogin”参数设置为“yes”，即允许root远程登录；3）经访谈，root用户需通过公私钥方式进行身份鉴别。 |
| 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； | 1）执行cat /etc/shadow命令查看shadow文件，发现操作系统存在root、ysup、yops、yluser等在用账户，不存在多余的、过期账户；2）存在多个堡垒机账户登录操作系统时共用一个账户的情况。 |
| 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； | root账户具有系统所有权限，未实现管理用户的权限分离。 |
| e）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； | 经访谈，由系统管理员root配置访问控制策略，如：/etc/passwd，/etc/profile宿主为root、权限设置为644，audit文件为700、message文件为600，其他文件权限为750，实现用户对文件的权限控制。 |
| f）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； | 由管理用户进行用户访问权限分配进行设置，依据访问控制策略,对各类文件进行访问，重要文件和目录权限均在合理范围内，用户可根据文件不同的权限进行操作。 |
| g）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。 | 执 行more /etc/selinux/config 命令，查看config文件显示 SELINUX参数为 DISABLED，即未开启强制访问控制模式。 |
| 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）执行ps -ef|grep rsyslog和ps -ef|grep auditd命令，显示rsyslog和auditd进程正在运行；2）more /etc/audit/audit.rules，显示审计内容包括：\*.info、authriv.\*、mail.\*、cron.\*、\*.emerg、uucp、news.crit、local7.\*等事件。 |
| 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； | 执行tail -20 /var/log/audit/audit.log命令，查看近20条审计日志，内容包括：时间、对象、路径、用户ID、相关的系统调用、用户执行命令等。 |
| 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）通过访问权限对审计记录进行保护，日志文件/var/log/messages、/var/log/secure、/var/log/audit/audit.log访问 权限均为600；2）审计记录本地保存，且实时备份至360本地安全大脑，保存时间满足180天以上。 |
| d）应对审计进程进行保护，防止未经授权的中断。 | 执行service auditd status命令，系统开启auditd审计保护进程，审计进程由root用户维护，经现场使用yluser用户通过service auditd stop命令尝试中断审计进程，无法将审计进程单独中断。 |
| 入侵防范 | a）应遵循最小安装的原则，仅安装需要的组件和应用程序； | 1）系统安装遵循最小化安装原则；2）执行yum list installed命令查看操作系统已安装的程序包，存在Java、SSH、天眼云镜agent等应用程序或组件，不存在与业务系统无关的组件和应用程序。 |
| b）应关闭不需要的系统服务、默认共享和高危端口； | 1）执行systemctl list-unit-files 命令，系统已关闭FTP、Telnet 等高危网络服务；2）执行netstat -pantu命令，系统关闭了135、445等高危端口，仅开启了22、8080等端口。 |
| c）应通过设定终端接入方式或网络地址范围对通过网络进行管理的管理终端进行限制； | 经核查，1）通过配置安全组策略限制仅允许通过堡垒机管理服务器；2）经核查防火墙中访问控制策略，具备堡垒机地址-服务器管理网段（10.33.0.0）的访问控制策略。 |
| d）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； | 根据GB∕T 28448-2019 《信息安全技术 网络安全等级保护测评要求》测评对象范围描述，服务器无该项要求，故判为“不适用”。 |
| e）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； | 1）经过漏洞扫描，服务器不存在高危安全漏洞；2）执行rpm -qa grep patch命令，查看系统补丁已更新至最新。 |
| f）应能够检测到对重要节点进行入侵的行为，并在发生严重入侵事件时提供报警。 | 经核查，服务器上安装有青藤云天眼云镜，对主机入侵行为进行检测，发现严重安全事件时通过钉钉告警。 |
| 恶意代码防范 | a）应采用免受恶意代码攻击的技术措施或主动免疫可信验证机制及时识别入侵和病毒行为，并将其有效阻断。 | 经核查，服务器上安装有青藤云天眼云镜，对主机恶意代码进行检测、清除，每天凌晨自动更新恶意代码特征库，经核查，具备恶意代码特征库更新记录。 |
| 可信验证 | a）可基于可信根对计算设备的系统引导程序、系统程序、重要配置参数和应用程序等进行可信验证，并在应用程序的关键执行环节进行动态可信验证，在检测到其可信性受到破坏后进行报警，并将验证结果形成审计记录送至安全管理中心。 | 未采用技术措施对计算设备的系统引导程序、系统程序、重要配置参数和通信应用程序等进行可信验证。 |
| 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； | 采用SSH协议连接操作系统，保证了鉴别信息以及管理数据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。 | 操作系统中对重要鉴别信息通过自身的加密及校验（SHA256），保证数据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； | 采用SSH协议连接操作系统，保证了鉴别信息以及管理数据在传输过程中的保密性。 |
| b）应采用密码技术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个人信息等。 | 通过系统自带的加密模块保证鉴别数据在存储过程中的保密性。 |
| 数据备份恢复 | a）应提供重要数据的本地数据备份与恢复功能； | 经核查，通过脚本每周将配置文件、代码仓库等数据备份至备份服务器中，依据需要验证备份数据的有效性。 |
| b）应提供异地实时备份功能，利用通信网络将重要数据实时备份至备份场地； | 系统无异地备份机制。 |
| c）应提供重要数据处理系统的热冗余，保证系统的高可用性。 | 服务器采用K8S容器部署，保证系统的高可用性。 |
| 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； | 操作系统提供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功能。 |
| 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。 | 操作系统提供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的功能。 |

4.1.3.20. 应用服务器40

|  |  |  |
| --- | --- | --- |
| **安全控制点** | **测评指标** | **结果记录** |
| 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）操作系统时采用用户名+SSHKey公私钥进行身份鉴别鉴别信息具有复杂度要求；2）执行cat /etc/shadow命令，查看shadow文件系统内用户身份标识唯一，不存在同名用户，且不存在空口令账号；3）经访谈，SSHKey公私钥每半年进行更换；4）查看sshd\_config配置文件中配置PasswordAuthentication no，拒绝使用密码方式进行身份鉴别。 |
| 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； | 操作系统采用用户名+SSHKey公私钥进行身份鉴别，可以防止鉴别信息被暴力破解；但未配置用户连接超时退出策略。 |
| 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； | 1）经核查，管理人员采用SSH协议连接操作系统；2）执行netatat –tpln| grep 23命令查看操作系统远程管理端口，不存在Telnet端口，防止鉴别信息在网络传输过程中的被窃听。 |
| 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。 | 未采用两种或两种以上组合的鉴别技术对用户进行身份鉴别。 |
| 访问控制 | a）应对登录的用户分配账户和权限； | 1）经访谈，通过root账户为登录的用户创建账户、分配权限；2）执行ls -l命令查看关键文件权限，均已为账户分配了相应权限，相关文件权限设置为/etc/shadow：000、/etc/passwd：644、/etc/group：644、/etc/profile：644、/etc/crontab：644、/ etc/securetty：600、/etc/ssh/sshd\_config：600。 |
| b）应重命名或删除默认账户，修改默认账户的默认口令； | 1）执行cat /etc/shadow命令查看shadow文件，操作系统中adm、lp、sync、shutdown、halt、mail、uucp、operator、games、gopher等账户均为nologin状态，存在默认账户root；2）执行more /etc/ssh/sshd\_config命令，查看“PermitRootLogin”参数设置为“yes”，即允许root远程登录；3）经访谈，root用户需通过公私钥方式进行身份鉴别。 |
| 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； | 1）执行cat /etc/shadow命令查看shadow文件，发现操作系统存在root、ysup、yops、yluser等在用账户，不存在多余的、过期账户；2）存在多个堡垒机账户登录操作系统时共用一个账户的情况。 |
| 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； | root账户具有系统所有权限，未实现管理用户的权限分离。 |
| e）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； | 经访谈，由系统管理员root配置访问控制策略，如：/etc/passwd，/etc/profile宿主为root、权限设置为644，audit文件为700、message文件为600，其他文件权限为750，实现用户对文件的权限控制。 |
| f）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； | 由管理用户进行用户访问权限分配进行设置，依据访问控制策略,对各类文件进行访问，重要文件和目录权限均在合理范围内，用户可根据文件不同的权限进行操作。 |
| g）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。 | 执 行more /etc/selinux/config 命令，查看config文件显示 SELINUX参数为 DISABLED，即未开启强制访问控制模式。 |
| 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）执行ps -ef|grep rsyslog和ps -ef|grep auditd命令，显示rsyslog和auditd进程正在运行；2）more /etc/audit/audit.rules，显示审计内容包括：\*.info、authriv.\*、mail.\*、cron.\*、\*.emerg、uucp、news.crit、local7.\*等事件。 |
| 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； | 执行tail -20 /var/log/audit/audit.log命令，查看近20条审计日志，内容包括：时间、对象、路径、用户ID、相关的系统调用、用户执行命令等。 |
| 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）通过访问权限对审计记录进行保护，日志文件/var/log/messages、/var/log/secure、/var/log/audit/audit.log访问 权限均为600；2）审计记录本地保存，且实时备份至360本地安全大脑，保存时间满足180天以上。 |
| d）应对审计进程进行保护，防止未经授权的中断。 | 执行service auditd status命令，系统开启auditd审计保护进程，审计进程由root用户维护，经现场使用yluser用户通过service auditd stop命令尝试中断审计进程，无法将审计进程单独中断。 |
| 入侵防范 | a）应遵循最小安装的原则，仅安装需要的组件和应用程序； | 1）系统安装遵循最小化安装原则；2）执行yum list installed命令查看操作系统已安装的程序包，存在Java、SSH、天眼云镜agent等应用程序或组件，不存在与业务系统无关的组件和应用程序。 |
| b）应关闭不需要的系统服务、默认共享和高危端口； | 1）执行systemctl list-unit-files 命令，系统已关闭FTP、Telnet 等高危网络服务；2）执行netstat -pantu命令，系统关闭了135、445等高危端口，仅开启了22、8080等端口。 |
| c）应通过设定终端接入方式或网络地址范围对通过网络进行管理的管理终端进行限制； | 经核查，1）通过配置安全组策略限制仅允许通过堡垒机管理服务器；2）经核查防火墙中访问控制策略，具备堡垒机地址-服务器管理网段（10.33.0.0）的访问控制策略。 |
| d）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； | 根据GB∕T 28448-2019 《信息安全技术 网络安全等级保护测评要求》测评对象范围描述，服务器无该项要求，故判为“不适用”。 |
| e）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； | 1）经过漏洞扫描，服务器不存在高危安全漏洞；2）执行rpm -qa grep patch命令，查看系统补丁已更新至最新。 |
| f）应能够检测到对重要节点进行入侵的行为，并在发生严重入侵事件时提供报警。 | 经核查，服务器上安装有青藤云天眼云镜，对主机入侵行为进行检测，发现严重安全事件时通过钉钉告警。 |
| 恶意代码防范 | a）应采用免受恶意代码攻击的技术措施或主动免疫可信验证机制及时识别入侵和病毒行为，并将其有效阻断。 | 经核查，服务器上安装有青藤云天眼云镜，对主机恶意代码进行检测、清除，每天凌晨自动更新恶意代码特征库，经核查，具备恶意代码特征库更新记录。 |
| 可信验证 | a）可基于可信根对计算设备的系统引导程序、系统程序、重要配置参数和应用程序等进行可信验证，并在应用程序的关键执行环节进行动态可信验证，在检测到其可信性受到破坏后进行报警，并将验证结果形成审计记录送至安全管理中心。 | 未采用技术措施对计算设备的系统引导程序、系统程序、重要配置参数和通信应用程序等进行可信验证。 |
| 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； | 采用SSH协议连接操作系统，保证了鉴别信息以及管理数据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。 | 操作系统中对重要鉴别信息通过自身的加密及校验（SHA256），保证数据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； | 采用SSH协议连接操作系统，保证了鉴别信息以及管理数据在传输过程中的保密性。 |
| b）应采用密码技术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个人信息等。 | 通过系统自带的加密模块保证鉴别数据在存储过程中的保密性。 |
| 数据备份恢复 | a）应提供重要数据的本地数据备份与恢复功能； | 经核查，通过脚本每周将配置文件、代码仓库等数据备份至备份服务器中，依据需要验证备份数据的有效性。 |
| b）应提供异地实时备份功能，利用通信网络将重要数据实时备份至备份场地； | 系统无异地备份机制。 |
| c）应提供重要数据处理系统的热冗余，保证系统的高可用性。 | 服务器采用K8S容器部署，保证系统的高可用性。 |
| 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； | 操作系统提供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功能。 |
| 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。 | 操作系统提供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的功能。 |

4.1.3.21. 应用服务器46

|  |  |  |
| --- | --- | --- |
| **安全控制点** | **测评指标** | **结果记录** |
| 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）操作系统时采用用户名+SSHKey公私钥进行身份鉴别鉴别信息具有复杂度要求；2）执行cat /etc/shadow命令，查看shadow文件系统内用户身份标识唯一，不存在同名用户，且不存在空口令账号；3）经访谈，SSHKey公私钥每半年进行更换；4）查看sshd\_config配置文件中配置PasswordAuthentication no，拒绝使用密码方式进行身份鉴别。 |
| 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； | 操作系统采用用户名+SSHKey公私钥进行身份鉴别，可以防止鉴别信息被暴力破解；但未配置用户连接超时退出策略。 |
| 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； | 1）经核查，管理人员采用SSH协议连接操作系统；2）执行netatat –tpln| grep 23命令查看操作系统远程管理端口，不存在Telnet端口，防止鉴别信息在网络传输过程中的被窃听。 |
| 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。 | 未采用两种或两种以上组合的鉴别技术对用户进行身份鉴别。 |
| 访问控制 | a）应对登录的用户分配账户和权限； | 1）经访谈，通过root账户为登录的用户创建账户、分配权限；2）执行ls -l命令查看关键文件权限，均已为账户分配了相应权限，相关文件权限设置为/etc/shadow：000、/etc/passwd：644、/etc/group：644、/etc/profile：644、/etc/crontab：644、/ etc/securetty：600、/etc/ssh/sshd\_config：600。 |
| b）应重命名或删除默认账户，修改默认账户的默认口令； | 1）执行cat /etc/shadow命令查看shadow文件，操作系统中adm、lp、sync、shutdown、halt、mail、uucp、operator、games、gopher等账户均为nologin状态，存在默认账户root；2）执行more /etc/ssh/sshd\_config命令，查看“PermitRootLogin”参数设置为“yes”，即允许root远程登录；3）经访谈，root用户需通过公私钥方式进行身份鉴别。 |
| 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； | 1）执行cat /etc/shadow命令查看shadow文件，发现操作系统存在root、ysup、yops、yluser等在用账户，不存在多余的、过期账户；2）存在多个堡垒机账户登录操作系统时共用一个账户的情况。 |
| 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； | root账户具有系统所有权限，未实现管理用户的权限分离。 |
| e）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； | 经访谈，由系统管理员root配置访问控制策略，如：/etc/passwd，/etc/profile宿主为root、权限设置为644，audit文件为700、message文件为600，其他文件权限为750，实现用户对文件的权限控制。 |
| f）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； | 由管理用户进行用户访问权限分配进行设置，依据访问控制策略,对各类文件进行访问，重要文件和目录权限均在合理范围内，用户可根据文件不同的权限进行操作。 |
| g）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。 | 执 行more /etc/selinux/config 命令，查看config文件显示 SELINUX参数为 DISABLED，即未开启强制访问控制模式。 |
| 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）执行ps -ef|grep rsyslog和ps -ef|grep auditd命令，显示rsyslog和auditd进程正在运行；2）more /etc/audit/audit.rules，显示审计内容包括：\*.info、authriv.\*、mail.\*、cron.\*、\*.emerg、uucp、news.crit、local7.\*等事件。 |
| 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； | 执行tail -20 /var/log/audit/audit.log命令，查看近20条审计日志，内容包括：时间、对象、路径、用户ID、相关的系统调用、用户执行命令等。 |
| 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）通过访问权限对审计记录进行保护，日志文件/var/log/messages、/var/log/secure、/var/log/audit/audit.log访问 权限均为600；2）审计记录本地保存，且实时备份至360本地安全大脑，保存时间满足180天以上。 |
| d）应对审计进程进行保护，防止未经授权的中断。 | 执行service auditd status命令，系统开启auditd审计保护进程，审计进程由root用户维护，经现场使用yluser用户通过service auditd stop命令尝试中断审计进程，无法将审计进程单独中断。 |
| 入侵防范 | a）应遵循最小安装的原则，仅安装需要的组件和应用程序； | 1）系统安装遵循最小化安装原则；2）执行yum list installed命令查看操作系统已安装的程序包，存在Java、SSH、天眼云镜agent等应用程序或组件，不存在与业务系统无关的组件和应用程序。 |
| b）应关闭不需要的系统服务、默认共享和高危端口； | 1）执行systemctl list-unit-files 命令，系统已关闭FTP、Telnet 等高危网络服务；2）执行netstat -pantu命令，系统关闭了135、445等高危端口，仅开启了22、8080等端口。 |
| c）应通过设定终端接入方式或网络地址范围对通过网络进行管理的管理终端进行限制； | 经核查，1）通过配置安全组策略限制仅允许通过堡垒机管理服务器；2）经核查防火墙中访问控制策略，具备堡垒机地址-服务器管理网段（10.33.0.0）的访问控制策略。 |
| d）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； | 根据GB∕T 28448-2019 《信息安全技术 网络安全等级保护测评要求》测评对象范围描述，服务器无该项要求，故判为“不适用”。 |
| e）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； | 1）经过漏洞扫描，服务器不存在高危安全漏洞；2）执行rpm -qa grep patch命令，查看系统补丁已更新至最新。 |
| f）应能够检测到对重要节点进行入侵的行为，并在发生严重入侵事件时提供报警。 | 经核查，服务器上安装有青藤云天眼云镜，对主机入侵行为进行检测，发现严重安全事件时通过钉钉告警。 |
| 恶意代码防范 | a）应采用免受恶意代码攻击的技术措施或主动免疫可信验证机制及时识别入侵和病毒行为，并将其有效阻断。 | 经核查，服务器上安装有青藤云天眼云镜，对主机恶意代码进行检测、清除，每天凌晨自动更新恶意代码特征库，经核查，具备恶意代码特征库更新记录。 |
| 可信验证 | a）可基于可信根对计算设备的系统引导程序、系统程序、重要配置参数和应用程序等进行可信验证，并在应用程序的关键执行环节进行动态可信验证，在检测到其可信性受到破坏后进行报警，并将验证结果形成审计记录送至安全管理中心。 | 未采用技术措施对计算设备的系统引导程序、系统程序、重要配置参数和通信应用程序等进行可信验证。 |
| 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； | 采用SSH协议连接操作系统，保证了鉴别信息以及管理数据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。 | 操作系统中对重要鉴别信息通过自身的加密及校验（SHA256），保证数据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； | 采用SSH协议连接操作系统，保证了鉴别信息以及管理数据在传输过程中的保密性。 |
| b）应采用密码技术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个人信息等。 | 通过系统自带的加密模块保证鉴别数据在存储过程中的保密性。 |
| 数据备份恢复 | a）应提供重要数据的本地数据备份与恢复功能； | 经核查，通过脚本每周将配置文件、代码仓库等数据备份至备份服务器中，依据需要验证备份数据的有效性。 |
| b）应提供异地实时备份功能，利用通信网络将重要数据实时备份至备份场地； | 系统无异地备份机制。 |
| c）应提供重要数据处理系统的热冗余，保证系统的高可用性。 | 服务器采用K8S容器部署，保证系统的高可用性。 |
| 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； | 操作系统提供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功能。 |
| 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。 | 操作系统提供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的功能。 |

4.1.3.22. 应用服务器47

|  |  |  |
| --- | --- | --- |
| **安全控制点** | **测评指标** | **结果记录** |
| 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）操作系统时采用用户名+SSHKey公私钥进行身份鉴别鉴别信息具有复杂度要求；2）执行cat /etc/shadow命令，查看shadow文件系统内用户身份标识唯一，不存在同名用户，且不存在空口令账号；3）经访谈，SSHKey公私钥每半年进行更换；4）查看sshd\_config配置文件中配置PasswordAuthentication no，拒绝使用密码方式进行身份鉴别。 |
| 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； | 操作系统采用用户名+SSHKey公私钥进行身份鉴别，可以防止鉴别信息被暴力破解；但未配置用户连接超时退出策略。 |
| 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； | 1）经核查，管理人员采用SSH协议连接操作系统；2）执行netatat –tpln| grep 23命令查看操作系统远程管理端口，不存在Telnet端口，防止鉴别信息在网络传输过程中的被窃听。 |
| 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。 | 未采用两种或两种以上组合的鉴别技术对用户进行身份鉴别。 |
| 访问控制 | a）应对登录的用户分配账户和权限； | 1）经访谈，通过root账户为登录的用户创建账户、分配权限；2）执行ls -l命令查看关键文件权限，均已为账户分配了相应权限，相关文件权限设置为/etc/shadow：000、/etc/passwd：644、/etc/group：644、/etc/profile：644、/etc/crontab：644、/ etc/securetty：600、/etc/ssh/sshd\_config：600。 |
| b）应重命名或删除默认账户，修改默认账户的默认口令； | 1）执行cat /etc/shadow命令查看shadow文件，操作系统中adm、lp、sync、shutdown、halt、mail、uucp、operator、games、gopher等账户均为nologin状态，存在默认账户root；2）执行more /etc/ssh/sshd\_config命令，查看“PermitRootLogin”参数设置为“yes”，即允许root远程登录；3）经访谈，root用户需通过公私钥方式进行身份鉴别。 |
| 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； | 1）执行cat /etc/shadow命令查看shadow文件，发现操作系统存在root、ysup、yops、yluser等在用账户，不存在多余的、过期账户；2）存在多个堡垒机账户登录操作系统时共用一个账户的情况。 |
| 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； | root账户具有系统所有权限，未实现管理用户的权限分离。 |
| e）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； | 经访谈，由系统管理员root配置访问控制策略，如：/etc/passwd，/etc/profile宿主为root、权限设置为644，audit文件为700、message文件为600，其他文件权限为750，实现用户对文件的权限控制。 |
| f）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； | 由管理用户进行用户访问权限分配进行设置，依据访问控制策略,对各类文件进行访问，重要文件和目录权限均在合理范围内，用户可根据文件不同的权限进行操作。 |
| g）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。 | 执 行more /etc/selinux/config 命令，查看config文件显示 SELINUX参数为 DISABLED，即未开启强制访问控制模式。 |
| 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）执行ps -ef|grep rsyslog和ps -ef|grep auditd命令，显示rsyslog和auditd进程正在运行；2）more /etc/audit/audit.rules，显示审计内容包括：\*.info、authriv.\*、mail.\*、cron.\*、\*.emerg、uucp、news.crit、local7.\*等事件。 |
| 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； | 执行tail -20 /var/log/audit/audit.log命令，查看近20条审计日志，内容包括：时间、对象、路径、用户ID、相关的系统调用、用户执行命令等。 |
| 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）通过访问权限对审计记录进行保护，日志文件/var/log/messages、/var/log/secure、/var/log/audit/audit.log访问 权限均为600；2）审计记录本地保存，且实时备份至360本地安全大脑，保存时间满足180天以上。 |
| d）应对审计进程进行保护，防止未经授权的中断。 | 执行service auditd status命令，系统开启auditd审计保护进程，审计进程由root用户维护，经现场使用yluser用户通过service auditd stop命令尝试中断审计进程，无法将审计进程单独中断。 |
| 入侵防范 | a）应遵循最小安装的原则，仅安装需要的组件和应用程序； | 1）系统安装遵循最小化安装原则；2）执行yum list installed命令查看操作系统已安装的程序包，存在Java、SSH、天眼云镜agent等应用程序或组件，不存在与业务系统无关的组件和应用程序。 |
| b）应关闭不需要的系统服务、默认共享和高危端口； | 1）执行systemctl list-unit-files 命令，系统已关闭FTP、Telnet 等高危网络服务；2）执行netstat -pantu命令，系统关闭了135、445等高危端口，仅开启了22、8080等端口。 |
| c）应通过设定终端接入方式或网络地址范围对通过网络进行管理的管理终端进行限制； | 经核查，1）通过配置安全组策略限制仅允许通过堡垒机管理服务器；2）经核查防火墙中访问控制策略，具备堡垒机地址-服务器管理网段（10.33.0.0）的访问控制策略。 |
| d）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； | 根据GB∕T 28448-2019 《信息安全技术 网络安全等级保护测评要求》测评对象范围描述，服务器无该项要求，故判为“不适用”。 |
| e）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； | 1）经过漏洞扫描，服务器不存在高危安全漏洞；2）执行rpm -qa grep patch命令，查看系统补丁已更新至最新。 |
| f）应能够检测到对重要节点进行入侵的行为，并在发生严重入侵事件时提供报警。 | 经核查，服务器上安装有青藤云天眼云镜，对主机入侵行为进行检测，发现严重安全事件时通过钉钉告警。 |
| 恶意代码防范 | a）应采用免受恶意代码攻击的技术措施或主动免疫可信验证机制及时识别入侵和病毒行为，并将其有效阻断。 | 经核查，服务器上安装有青藤云天眼云镜，对主机恶意代码进行检测、清除，每天凌晨自动更新恶意代码特征库，经核查，具备恶意代码特征库更新记录。 |
| 可信验证 | a）可基于可信根对计算设备的系统引导程序、系统程序、重要配置参数和应用程序等进行可信验证，并在应用程序的关键执行环节进行动态可信验证，在检测到其可信性受到破坏后进行报警，并将验证结果形成审计记录送至安全管理中心。 | 未采用技术措施对计算设备的系统引导程序、系统程序、重要配置参数和通信应用程序等进行可信验证。 |
| 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； | 采用SSH协议连接操作系统，保证了鉴别信息以及管理数据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。 | 操作系统中对重要鉴别信息通过自身的加密及校验（SHA256），保证数据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； | 采用SSH协议连接操作系统，保证了鉴别信息以及管理数据在传输过程中的保密性。 |
| b）应采用密码技术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个人信息等。 | 通过系统自带的加密模块保证鉴别数据在存储过程中的保密性。 |
| 数据备份恢复 | a）应提供重要数据的本地数据备份与恢复功能； | 经核查，通过脚本每周将配置文件、代码仓库等数据备份至备份服务器中，依据需要验证备份数据的有效性。 |
| b）应提供异地实时备份功能，利用通信网络将重要数据实时备份至备份场地； | 系统无异地备份机制。 |
| c）应提供重要数据处理系统的热冗余，保证系统的高可用性。 | 服务器采用K8S容器部署，保证系统的高可用性。 |
| 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； | 操作系统提供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功能。 |
| 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。 | 操作系统提供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的功能。 |

4.1.3.23. 应用服务器48

|  |  |  |
| --- | --- | --- |
| **安全控制点** | **测评指标** | **结果记录** |
| 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）操作系统时采用用户名+SSHKey公私钥进行身份鉴别鉴别信息具有复杂度要求；2）执行cat /etc/shadow命令，查看shadow文件系统内用户身份标识唯一，不存在同名用户，且不存在空口令账号；3）经访谈，SSHKey公私钥每半年进行更换；4）查看sshd\_config配置文件中配置PasswordAuthentication no，拒绝使用密码方式进行身份鉴别。 |
| 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； | 操作系统采用用户名+SSHKey公私钥进行身份鉴别，可以防止鉴别信息被暴力破解；但未配置用户连接超时退出策略。 |
| 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； | 1）经核查，管理人员采用SSH协议连接操作系统；2）执行netatat –tpln| grep 23命令查看操作系统远程管理端口，不存在Telnet端口，防止鉴别信息在网络传输过程中的被窃听。 |
| 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。 | 未采用两种或两种以上组合的鉴别技术对用户进行身份鉴别。 |
| 访问控制 | a）应对登录的用户分配账户和权限； | 1）经访谈，通过root账户为登录的用户创建账户、分配权限；2）执行ls -l命令查看关键文件权限，均已为账户分配了相应权限，相关文件权限设置为/etc/shadow：000、/etc/passwd：644、/etc/group：644、/etc/profile：644、/etc/crontab：644、/ etc/securetty：600、/etc/ssh/sshd\_config：600。 |
| b）应重命名或删除默认账户，修改默认账户的默认口令； | 1）执行cat /etc/shadow命令查看shadow文件，操作系统中adm、lp、sync、shutdown、halt、mail、uucp、operator、games、gopher等账户均为nologin状态，存在默认账户root；2）执行more /etc/ssh/sshd\_config命令，查看“PermitRootLogin”参数设置为“yes”，即允许root远程登录；3）经访谈，root用户需通过公私钥方式进行身份鉴别。 |
| 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； | 1）执行cat /etc/shadow命令查看shadow文件，发现操作系统存在root、ysup、yops、yluser等在用账户，不存在多余的、过期账户；2）存在多个堡垒机账户登录操作系统时共用一个账户的情况。 |
| 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； | root账户具有系统所有权限，未实现管理用户的权限分离。 |
| e）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； | 经访谈，由系统管理员root配置访问控制策略，如：/etc/passwd，/etc/profile宿主为root、权限设置为644，audit文件为700、message文件为600，其他文件权限为750，实现用户对文件的权限控制。 |
| f）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； | 由管理用户进行用户访问权限分配进行设置，依据访问控制策略,对各类文件进行访问，重要文件和目录权限均在合理范围内，用户可根据文件不同的权限进行操作。 |
| g）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。 | 执 行more /etc/selinux/config 命令，查看config文件显示 SELINUX参数为 DISABLED，即未开启强制访问控制模式。 |
| 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）执行ps -ef|grep rsyslog和ps -ef|grep auditd命令，显示rsyslog和auditd进程正在运行；2）more /etc/audit/audit.rules，显示审计内容包括：\*.info、authriv.\*、mail.\*、cron.\*、\*.emerg、uucp、news.crit、local7.\*等事件。 |
| 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； | 执行tail -20 /var/log/audit/audit.log命令，查看近20条审计日志，内容包括：时间、对象、路径、用户ID、相关的系统调用、用户执行命令等。 |
| 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）通过访问权限对审计记录进行保护，日志文件/var/log/messages、/var/log/secure、/var/log/audit/audit.log访问 权限均为600；2）审计记录本地保存，且实时备份至360本地安全大脑，保存时间满足180天以上。 |
| d）应对审计进程进行保护，防止未经授权的中断。 | 执行service auditd status命令，系统开启auditd审计保护进程，审计进程由root用户维护，经现场使用yluser用户通过service auditd stop命令尝试中断审计进程，无法将审计进程单独中断。 |
| 入侵防范 | a）应遵循最小安装的原则，仅安装需要的组件和应用程序； | 1）系统安装遵循最小化安装原则；2）执行yum list installed命令查看操作系统已安装的程序包，存在Java、SSH、天眼云镜agent等应用程序或组件，不存在与业务系统无关的组件和应用程序。 |
| b）应关闭不需要的系统服务、默认共享和高危端口； | 1）执行systemctl list-unit-files 命令，系统已关闭FTP、Telnet 等高危网络服务；2）执行netstat -pantu命令，系统关闭了135、445等高危端口，仅开启了22、8080等端口。 |
| c）应通过设定终端接入方式或网络地址范围对通过网络进行管理的管理终端进行限制； | 经核查，1）通过配置安全组策略限制仅允许通过堡垒机管理服务器；2）经核查防火墙中访问控制策略，具备堡垒机地址-服务器管理网段（10.33.0.0）的访问控制策略。 |
| d）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； | 根据GB∕T 28448-2019 《信息安全技术 网络安全等级保护测评要求》测评对象范围描述，服务器无该项要求，故判为“不适用”。 |
| e）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； | 1）经过漏洞扫描，服务器不存在高危安全漏洞；2）执行rpm -qa grep patch命令，查看系统补丁已更新至最新。 |
| f）应能够检测到对重要节点进行入侵的行为，并在发生严重入侵事件时提供报警。 | 经核查，服务器上安装有青藤云天眼云镜，对主机入侵行为进行检测，发现严重安全事件时通过钉钉告警。 |
| 恶意代码防范 | a）应采用免受恶意代码攻击的技术措施或主动免疫可信验证机制及时识别入侵和病毒行为，并将其有效阻断。 | 经核查，服务器上安装有青藤云天眼云镜，对主机恶意代码进行检测、清除，每天凌晨自动更新恶意代码特征库，经核查，具备恶意代码特征库更新记录。 |
| 可信验证 | a）可基于可信根对计算设备的系统引导程序、系统程序、重要配置参数和应用程序等进行可信验证，并在应用程序的关键执行环节进行动态可信验证，在检测到其可信性受到破坏后进行报警，并将验证结果形成审计记录送至安全管理中心。 | 未采用技术措施对计算设备的系统引导程序、系统程序、重要配置参数和通信应用程序等进行可信验证。 |
| 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； | 采用SSH协议连接操作系统，保证了鉴别信息以及管理数据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。 | 操作系统中对重要鉴别信息通过自身的加密及校验（SHA256），保证数据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； | 采用SSH协议连接操作系统，保证了鉴别信息以及管理数据在传输过程中的保密性。 |
| b）应采用密码技术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个人信息等。 | 通过系统自带的加密模块保证鉴别数据在存储过程中的保密性。 |
| 数据备份恢复 | a）应提供重要数据的本地数据备份与恢复功能； | 经核查，通过脚本每周将配置文件、代码仓库等数据备份至备份服务器中，依据需要验证备份数据的有效性。 |
| b）应提供异地实时备份功能，利用通信网络将重要数据实时备份至备份场地； | 系统无异地备份机制。 |
| c）应提供重要数据处理系统的热冗余，保证系统的高可用性。 | 服务器采用K8S容器部署，保证系统的高可用性。 |
| 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； | 操作系统提供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功能。 |
| 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。 | 操作系统提供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的功能。 |

4.1.3.24. 应用服务器49

|  |  |  |
| --- | --- | --- |
| **安全控制点** | **测评指标** | **结果记录** |
| 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）操作系统时采用用户名+SSHKey公私钥进行身份鉴别鉴别信息具有复杂度要求；2）执行cat /etc/shadow命令，查看shadow文件系统内用户身份标识唯一，不存在同名用户，且不存在空口令账号；3）经访谈，SSHKey公私钥每半年进行更换；4）查看sshd\_config配置文件中配置PasswordAuthentication no，拒绝使用密码方式进行身份鉴别。 |
| 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； | 操作系统采用用户名+SSHKey公私钥进行身份鉴别，可以防止鉴别信息被暴力破解；但未配置用户连接超时退出策略。 |
| 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； | 1）经核查，管理人员采用SSH协议连接操作系统；2）执行netatat –tpln| grep 23命令查看操作系统远程管理端口，不存在Telnet端口，防止鉴别信息在网络传输过程中的被窃听。 |
| 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。 | 未采用两种或两种以上组合的鉴别技术对用户进行身份鉴别。 |
| 访问控制 | a）应对登录的用户分配账户和权限； | 1）经访谈，通过root账户为登录的用户创建账户、分配权限；2）执行ls -l命令查看关键文件权限，均已为账户分配了相应权限，相关文件权限设置为/etc/shadow：000、/etc/passwd：644、/etc/group：644、/etc/profile：644、/etc/crontab：644、/ etc/securetty：600、/etc/ssh/sshd\_config：600。 |
| b）应重命名或删除默认账户，修改默认账户的默认口令； | 1）执行cat /etc/shadow命令查看shadow文件，操作系统中adm、lp、sync、shutdown、halt、mail、uucp、operator、games、gopher等账户均为nologin状态，存在默认账户root；2）执行more /etc/ssh/sshd\_config命令，查看“PermitRootLogin”参数设置为“yes”，即允许root远程登录；3）经访谈，root用户需通过公私钥方式进行身份鉴别。 |
| 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； | 1）执行cat /etc/shadow命令查看shadow文件，发现操作系统存在root、ysup、yops、yluser等在用账户，不存在多余的、过期账户；2）存在多个堡垒机账户登录操作系统时共用一个账户的情况。 |
| 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； | root账户具有系统所有权限，未实现管理用户的权限分离。 |
| e）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； | 经访谈，由系统管理员root配置访问控制策略，如：/etc/passwd，/etc/profile宿主为root、权限设置为644，audit文件为700、message文件为600，其他文件权限为750，实现用户对文件的权限控制。 |
| f）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； | 由管理用户进行用户访问权限分配进行设置，依据访问控制策略,对各类文件进行访问，重要文件和目录权限均在合理范围内，用户可根据文件不同的权限进行操作。 |
| g）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。 | 执 行more /etc/selinux/config 命令，查看config文件显示 SELINUX参数为 DISABLED，即未开启强制访问控制模式。 |
| 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）执行ps -ef|grep rsyslog和ps -ef|grep auditd命令，显示rsyslog和auditd进程正在运行；2）more /etc/audit/audit.rules，显示审计内容包括：\*.info、authriv.\*、mail.\*、cron.\*、\*.emerg、uucp、news.crit、local7.\*等事件。 |
| 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； | 执行tail -20 /var/log/audit/audit.log命令，查看近20条审计日志，内容包括：时间、对象、路径、用户ID、相关的系统调用、用户执行命令等。 |
| 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）通过访问权限对审计记录进行保护，日志文件/var/log/messages、/var/log/secure、/var/log/audit/audit.log访问 权限均为600；2）审计记录本地保存，且实时备份至360本地安全大脑，保存时间满足180天以上。 |
| d）应对审计进程进行保护，防止未经授权的中断。 | 执行service auditd status命令，系统开启auditd审计保护进程，审计进程由root用户维护，经现场使用yluser用户通过service auditd stop命令尝试中断审计进程，无法将审计进程单独中断。 |
| 入侵防范 | a）应遵循最小安装的原则，仅安装需要的组件和应用程序； | 1）系统安装遵循最小化安装原则；2）执行yum list installed命令查看操作系统已安装的程序包，存在Java、SSH、天眼云镜agent等应用程序或组件，不存在与业务系统无关的组件和应用程序。 |
| b）应关闭不需要的系统服务、默认共享和高危端口； | 1）执行systemctl list-unit-files 命令，系统已关闭FTP、Telnet 等高危网络服务；2）执行netstat -pantu命令，系统关闭了135、445等高危端口，仅开启了22、8080等端口。 |
| c）应通过设定终端接入方式或网络地址范围对通过网络进行管理的管理终端进行限制； | 经核查，1）通过配置安全组策略限制仅允许通过堡垒机管理服务器；2）经核查防火墙中访问控制策略，具备堡垒机地址-服务器管理网段（10.33.0.0）的访问控制策略。 |
| d）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； | 根据GB∕T 28448-2019 《信息安全技术 网络安全等级保护测评要求》测评对象范围描述，服务器无该项要求，故判为“不适用”。 |
| e）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； | 1）经过漏洞扫描，服务器不存在高危安全漏洞；2）执行rpm -qa grep patch命令，查看系统补丁已更新至最新。 |
| f）应能够检测到对重要节点进行入侵的行为，并在发生严重入侵事件时提供报警。 | 经核查，服务器上安装有青藤云天眼云镜，对主机入侵行为进行检测，发现严重安全事件时通过钉钉告警。 |
| 恶意代码防范 | a）应采用免受恶意代码攻击的技术措施或主动免疫可信验证机制及时识别入侵和病毒行为，并将其有效阻断。 | 经核查，服务器上安装有青藤云天眼云镜，对主机恶意代码进行检测、清除，每天凌晨自动更新恶意代码特征库，经核查，具备恶意代码特征库更新记录。 |
| 可信验证 | a）可基于可信根对计算设备的系统引导程序、系统程序、重要配置参数和应用程序等进行可信验证，并在应用程序的关键执行环节进行动态可信验证，在检测到其可信性受到破坏后进行报警，并将验证结果形成审计记录送至安全管理中心。 | 未采用技术措施对计算设备的系统引导程序、系统程序、重要配置参数和通信应用程序等进行可信验证。 |
| 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； | 采用SSH协议连接操作系统，保证了鉴别信息以及管理数据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。 | 操作系统中对重要鉴别信息通过自身的加密及校验（SHA256），保证数据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； | 采用SSH协议连接操作系统，保证了鉴别信息以及管理数据在传输过程中的保密性。 |
| b）应采用密码技术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个人信息等。 | 通过系统自带的加密模块保证鉴别数据在存储过程中的保密性。 |
| 数据备份恢复 | a）应提供重要数据的本地数据备份与恢复功能； | 经核查，通过脚本每周将配置文件、代码仓库等数据备份至备份服务器中，依据需要验证备份数据的有效性。 |
| b）应提供异地实时备份功能，利用通信网络将重要数据实时备份至备份场地； | 系统无异地备份机制。 |
| c）应提供重要数据处理系统的热冗余，保证系统的高可用性。 | 服务器采用K8S容器部署，保证系统的高可用性。 |
| 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； | 操作系统提供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功能。 |
| 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。 | 操作系统提供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的功能。 |

4.1.3.25. 应用服务器50

|  |  |  |
| --- | --- | --- |
| **安全控制点** | **测评指标** | **结果记录** |
| 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）操作系统时采用用户名+SSHKey公私钥进行身份鉴别鉴别信息具有复杂度要求；2）执行cat /etc/shadow命令，查看shadow文件系统内用户身份标识唯一，不存在同名用户，且不存在空口令账号；3）经访谈，SSHKey公私钥每半年进行更换；4）查看sshd\_config配置文件中配置PasswordAuthentication no，拒绝使用密码方式进行身份鉴别。 |
| 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； | 操作系统采用用户名+SSHKey公私钥进行身份鉴别，可以防止鉴别信息被暴力破解；但未配置用户连接超时退出策略。 |
| 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； | 1）经核查，管理人员采用SSH协议连接操作系统；2）执行netatat –tpln| grep 23命令查看操作系统远程管理端口，不存在Telnet端口，防止鉴别信息在网络传输过程中的被窃听。 |
| 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。 | 未采用两种或两种以上组合的鉴别技术对用户进行身份鉴别。 |
| 访问控制 | a）应对登录的用户分配账户和权限； | 1）经访谈，通过root账户为登录的用户创建账户、分配权限；2）执行ls -l命令查看关键文件权限，均已为账户分配了相应权限，相关文件权限设置为/etc/shadow：000、/etc/passwd：644、/etc/group：644、/etc/profile：644、/etc/crontab：644、/ etc/securetty：600、/etc/ssh/sshd\_config：600。 |
| b）应重命名或删除默认账户，修改默认账户的默认口令； | 1）执行cat /etc/shadow命令查看shadow文件，操作系统中adm、lp、sync、shutdown、halt、mail、uucp、operator、games、gopher等账户均为nologin状态，存在默认账户root；2）执行more /etc/ssh/sshd\_config命令，查看“PermitRootLogin”参数设置为“yes”，即允许root远程登录；3）经访谈，root用户需通过公私钥方式进行身份鉴别。 |
| 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； | 1）执行cat /etc/shadow命令查看shadow文件，发现操作系统存在root、ysup、yops、yluser等在用账户，不存在多余的、过期账户；2）存在多个堡垒机账户登录操作系统时共用一个账户的情况。 |
| 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； | root账户具有系统所有权限，未实现管理用户的权限分离。 |
| e）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； | 经访谈，由系统管理员root配置访问控制策略，如：/etc/passwd，/etc/profile宿主为root、权限设置为644，audit文件为700、message文件为600，其他文件权限为750，实现用户对文件的权限控制。 |
| f）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； | 由管理用户进行用户访问权限分配进行设置，依据访问控制策略,对各类文件进行访问，重要文件和目录权限均在合理范围内，用户可根据文件不同的权限进行操作。 |
| g）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。 | 执 行more /etc/selinux/config 命令，查看config文件显示 SELINUX参数为 DISABLED，即未开启强制访问控制模式。 |
| 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）执行ps -ef|grep rsyslog和ps -ef|grep auditd命令，显示rsyslog和auditd进程正在运行；2）more /etc/audit/audit.rules，显示审计内容包括：\*.info、authriv.\*、mail.\*、cron.\*、\*.emerg、uucp、news.crit、local7.\*等事件。 |
| 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； | 执行tail -20 /var/log/audit/audit.log命令，查看近20条审计日志，内容包括：时间、对象、路径、用户ID、相关的系统调用、用户执行命令等。 |
| 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）通过访问权限对审计记录进行保护，日志文件/var/log/messages、/var/log/secure、/var/log/audit/audit.log访问 权限均为600；2）审计记录本地保存，且实时备份至360本地安全大脑，保存时间满足180天以上。 |
| d）应对审计进程进行保护，防止未经授权的中断。 | 执行service auditd status命令，系统开启auditd审计保护进程，审计进程由root用户维护，经现场使用yluser用户通过service auditd stop命令尝试中断审计进程，无法将审计进程单独中断。 |
| 入侵防范 | a）应遵循最小安装的原则，仅安装需要的组件和应用程序； | 1）系统安装遵循最小化安装原则；2）执行yum list installed命令查看操作系统已安装的程序包，存在Java、SSH、天眼云镜agent等应用程序或组件，不存在与业务系统无关的组件和应用程序。 |
| b）应关闭不需要的系统服务、默认共享和高危端口； | 1）执行systemctl list-unit-files 命令，系统已关闭FTP、Telnet 等高危网络服务；2）执行netstat -pantu命令，系统关闭了135、445等高危端口，仅开启了22、8080等端口。 |
| c）应通过设定终端接入方式或网络地址范围对通过网络进行管理的管理终端进行限制； | 经核查，1）通过配置安全组策略限制仅允许通过堡垒机管理服务器；2）经核查防火墙中访问控制策略，具备堡垒机地址-服务器管理网段（10.33.0.0）的访问控制策略。 |
| d）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； | 根据GB∕T 28448-2019 《信息安全技术 网络安全等级保护测评要求》测评对象范围描述，服务器无该项要求，故判为“不适用”。 |
| e）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； | 1）经过漏洞扫描，服务器不存在高危安全漏洞；2）执行rpm -qa grep patch命令，查看系统补丁已更新至最新。 |
| f）应能够检测到对重要节点进行入侵的行为，并在发生严重入侵事件时提供报警。 | 经核查，服务器上安装有青藤云天眼云镜，对主机入侵行为进行检测，发现严重安全事件时通过钉钉告警。 |
| 恶意代码防范 | a）应采用免受恶意代码攻击的技术措施或主动免疫可信验证机制及时识别入侵和病毒行为，并将其有效阻断。 | 经核查，服务器上安装有青藤云天眼云镜，对主机恶意代码进行检测、清除，每天凌晨自动更新恶意代码特征库，经核查，具备恶意代码特征库更新记录。 |
| 可信验证 | a）可基于可信根对计算设备的系统引导程序、系统程序、重要配置参数和应用程序等进行可信验证，并在应用程序的关键执行环节进行动态可信验证，在检测到其可信性受到破坏后进行报警，并将验证结果形成审计记录送至安全管理中心。 | 未采用技术措施对计算设备的系统引导程序、系统程序、重要配置参数和通信应用程序等进行可信验证。 |
| 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； | 采用SSH协议连接操作系统，保证了鉴别信息以及管理数据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。 | 操作系统中对重要鉴别信息通过自身的加密及校验（SHA256），保证数据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； | 采用SSH协议连接操作系统，保证了鉴别信息以及管理数据在传输过程中的保密性。 |
| b）应采用密码技术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个人信息等。 | 通过系统自带的加密模块保证鉴别数据在存储过程中的保密性。 |
| 数据备份恢复 | a）应提供重要数据的本地数据备份与恢复功能； | 经核查，通过脚本每周将配置文件、代码仓库等数据备份至备份服务器中，依据需要验证备份数据的有效性。 |
| b）应提供异地实时备份功能，利用通信网络将重要数据实时备份至备份场地； | 系统无异地备份机制。 |
| c）应提供重要数据处理系统的热冗余，保证系统的高可用性。 | 服务器采用K8S容器部署，保证系统的高可用性。 |
| 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； | 操作系统提供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功能。 |
| 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。 | 操作系统提供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的功能。 |

4.1.3.26. 应用服务器55

|  |  |  |
| --- | --- | --- |
| **安全控制点** | **测评指标** | **结果记录** |
| 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）操作系统时采用用户名+SSHKey公私钥进行身份鉴别鉴别信息具有复杂度要求；2）执行cat /etc/shadow命令，查看shadow文件系统内用户身份标识唯一，不存在同名用户，且不存在空口令账号；3）经访谈，SSHKey公私钥每半年进行更换；4）查看sshd\_config配置文件中配置PasswordAuthentication no，拒绝使用密码方式进行身份鉴别。 |
| 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； | 操作系统采用用户名+SSHKey公私钥进行身份鉴别，可以防止鉴别信息被暴力破解；但未配置用户连接超时退出策略。 |
| 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； | 1）经核查，管理人员采用SSH协议连接操作系统；2）执行netatat –tpln| grep 23命令查看操作系统远程管理端口，不存在Telnet端口，防止鉴别信息在网络传输过程中的被窃听。 |
| 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。 | 未采用两种或两种以上组合的鉴别技术对用户进行身份鉴别。 |
| 访问控制 | a）应对登录的用户分配账户和权限； | 1）经访谈，通过root账户为登录的用户创建账户、分配权限；2）执行ls -l命令查看关键文件权限，均已为账户分配了相应权限，相关文件权限设置为/etc/shadow：000、/etc/passwd：644、/etc/group：644、/etc/profile：644、/etc/crontab：644、/ etc/securetty：600、/etc/ssh/sshd\_config：600。 |
| b）应重命名或删除默认账户，修改默认账户的默认口令； | 1）执行cat /etc/shadow命令查看shadow文件，操作系统中adm、lp、sync、shutdown、halt、mail、uucp、operator、games、gopher等账户均为nologin状态，存在默认账户root；2）执行more /etc/ssh/sshd\_config命令，查看“PermitRootLogin”参数设置为“yes”，即允许root远程登录；3）经访谈，root用户需通过公私钥方式进行身份鉴别。 |
| 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； | 1）执行cat /etc/shadow命令查看shadow文件，发现操作系统存在root、ysup、yops、yluser等在用账户，不存在多余的、过期账户；2）存在多个堡垒机账户登录操作系统时共用一个账户的情况。 |
| 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； | root账户具有系统所有权限，未实现管理用户的权限分离。 |
| e）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； | 经访谈，由系统管理员root配置访问控制策略，如：/etc/passwd，/etc/profile宿主为root、权限设置为644，audit文件为700、message文件为600，其他文件权限为750，实现用户对文件的权限控制。 |
| f）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； | 由管理用户进行用户访问权限分配进行设置，依据访问控制策略,对各类文件进行访问，重要文件和目录权限均在合理范围内，用户可根据文件不同的权限进行操作。 |
| g）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。 | 执 行more /etc/selinux/config 命令，查看config文件显示 SELINUX参数为 DISABLED，即未开启强制访问控制模式。 |
| 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）执行ps -ef|grep rsyslog和ps -ef|grep auditd命令，显示rsyslog和auditd进程正在运行；2）more /etc/audit/audit.rules，显示审计内容包括：\*.info、authriv.\*、mail.\*、cron.\*、\*.emerg、uucp、news.crit、local7.\*等事件。 |
| 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； | 执行tail -20 /var/log/audit/audit.log命令，查看近20条审计日志，内容包括：时间、对象、路径、用户ID、相关的系统调用、用户执行命令等。 |
| 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）通过访问权限对审计记录进行保护，日志文件/var/log/messages、/var/log/secure、/var/log/audit/audit.log访问 权限均为600；2）审计记录本地保存，且实时备份至360本地安全大脑，保存时间满足180天以上。 |
| d）应对审计进程进行保护，防止未经授权的中断。 | 执行service auditd status命令，系统开启auditd审计保护进程，审计进程由root用户维护，经现场使用yluser用户通过service auditd stop命令尝试中断审计进程，无法将审计进程单独中断。 |
| 入侵防范 | a）应遵循最小安装的原则，仅安装需要的组件和应用程序； | 1）系统安装遵循最小化安装原则；2）执行yum list installed命令查看操作系统已安装的程序包，存在Java、SSH、天眼云镜agent等应用程序或组件，不存在与业务系统无关的组件和应用程序。 |
| b）应关闭不需要的系统服务、默认共享和高危端口； | 1）执行systemctl list-unit-files 命令，系统已关闭FTP、Telnet 等高危网络服务；2）执行netstat -pantu命令，系统关闭了135、445等高危端口，仅开启了22、8080等端口。 |
| c）应通过设定终端接入方式或网络地址范围对通过网络进行管理的管理终端进行限制； | 经核查，1）通过配置安全组策略限制仅允许通过堡垒机管理服务器；2）经核查防火墙中访问控制策略，具备堡垒机地址-服务器管理网段（10.33.0.0）的访问控制策略。 |
| d）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； | 根据GB∕T 28448-2019 《信息安全技术 网络安全等级保护测评要求》测评对象范围描述，服务器无该项要求，故判为“不适用”。 |
| e）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； | 1）经过漏洞扫描，服务器不存在高危安全漏洞；2）执行rpm -qa grep patch命令，查看系统补丁已更新至最新。 |
| f）应能够检测到对重要节点进行入侵的行为，并在发生严重入侵事件时提供报警。 | 经核查，服务器上安装有青藤云天眼云镜，对主机入侵行为进行检测，发现严重安全事件时通过钉钉告警。 |
| 恶意代码防范 | a）应采用免受恶意代码攻击的技术措施或主动免疫可信验证机制及时识别入侵和病毒行为，并将其有效阻断。 | 经核查，服务器上安装有青藤云天眼云镜，对主机恶意代码进行检测、清除，每天凌晨自动更新恶意代码特征库，经核查，具备恶意代码特征库更新记录。 |
| 可信验证 | a）可基于可信根对计算设备的系统引导程序、系统程序、重要配置参数和应用程序等进行可信验证，并在应用程序的关键执行环节进行动态可信验证，在检测到其可信性受到破坏后进行报警，并将验证结果形成审计记录送至安全管理中心。 | 未采用技术措施对计算设备的系统引导程序、系统程序、重要配置参数和通信应用程序等进行可信验证。 |
| 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； | 采用SSH协议连接操作系统，保证了鉴别信息以及管理数据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。 | 操作系统中对重要鉴别信息通过自身的加密及校验（SHA256），保证数据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； | 采用SSH协议连接操作系统，保证了鉴别信息以及管理数据在传输过程中的保密性。 |
| b）应采用密码技术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个人信息等。 | 通过系统自带的加密模块保证鉴别数据在存储过程中的保密性。 |
| 数据备份恢复 | a）应提供重要数据的本地数据备份与恢复功能； | 经核查，通过脚本每周将配置文件、代码仓库等数据备份至备份服务器中，依据需要验证备份数据的有效性。 |
| b）应提供异地实时备份功能，利用通信网络将重要数据实时备份至备份场地； | 系统无异地备份机制。 |
| c）应提供重要数据处理系统的热冗余，保证系统的高可用性。 | 服务器采用K8S容器部署，保证系统的高可用性。 |
| 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； | 操作系统提供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功能。 |
| 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。 | 操作系统提供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的功能。 |

4.1.3.27. 应用服务器56

|  |  |  |
| --- | --- | --- |
| **安全控制点** | **测评指标** | **结果记录** |
| 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）操作系统时采用用户名+SSHKey公私钥进行身份鉴别鉴别信息具有复杂度要求；2）执行cat /etc/shadow命令，查看shadow文件系统内用户身份标识唯一，不存在同名用户，且不存在空口令账号；3）经访谈，SSHKey公私钥每半年进行更换；4）查看sshd\_config配置文件中配置PasswordAuthentication no，拒绝使用密码方式进行身份鉴别。 |
| 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； | 操作系统采用用户名+SSHKey公私钥进行身份鉴别，可以防止鉴别信息被暴力破解；但未配置用户连接超时退出策略。 |
| 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； | 1）经核查，管理人员采用SSH协议连接操作系统；2）执行netatat –tpln| grep 23命令查看操作系统远程管理端口，不存在Telnet端口，防止鉴别信息在网络传输过程中的被窃听。 |
| 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。 | 未采用两种或两种以上组合的鉴别技术对用户进行身份鉴别。 |
| 访问控制 | a）应对登录的用户分配账户和权限； | 1）经访谈，通过root账户为登录的用户创建账户、分配权限；2）执行ls -l命令查看关键文件权限，均已为账户分配了相应权限，相关文件权限设置为/etc/shadow：000、/etc/passwd：644、/etc/group：644、/etc/profile：644、/etc/crontab：644、/ etc/securetty：600、/etc/ssh/sshd\_config：600。 |
| b）应重命名或删除默认账户，修改默认账户的默认口令； | 1）执行cat /etc/shadow命令查看shadow文件，操作系统中adm、lp、sync、shutdown、halt、mail、uucp、operator、games、gopher等账户均为nologin状态，存在默认账户root；2）执行more /etc/ssh/sshd\_config命令，查看“PermitRootLogin”参数设置为“yes”，即允许root远程登录；3）经访谈，root用户需通过公私钥方式进行身份鉴别。 |
| 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； | 1）执行cat /etc/shadow命令查看shadow文件，发现操作系统存在root、ysup、yops、yluser等在用账户，不存在多余的、过期账户；2）存在多个堡垒机账户登录操作系统时共用一个账户的情况。 |
| 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； | root账户具有系统所有权限，未实现管理用户的权限分离。 |
| e）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； | 经访谈，由系统管理员root配置访问控制策略，如：/etc/passwd，/etc/profile宿主为root、权限设置为644，audit文件为700、message文件为600，其他文件权限为750，实现用户对文件的权限控制。 |
| f）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； | 由管理用户进行用户访问权限分配进行设置，依据访问控制策略,对各类文件进行访问，重要文件和目录权限均在合理范围内，用户可根据文件不同的权限进行操作。 |
| g）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。 | 执 行more /etc/selinux/config 命令，查看config文件显示 SELINUX参数为 DISABLED，即未开启强制访问控制模式。 |
| 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）执行ps -ef|grep rsyslog和ps -ef|grep auditd命令，显示rsyslog和auditd进程正在运行；2）more /etc/audit/audit.rules，显示审计内容包括：\*.info、authriv.\*、mail.\*、cron.\*、\*.emerg、uucp、news.crit、local7.\*等事件。 |
| 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； | 执行tail -20 /var/log/audit/audit.log命令，查看近20条审计日志，内容包括：时间、对象、路径、用户ID、相关的系统调用、用户执行命令等。 |
| 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）通过访问权限对审计记录进行保护，日志文件/var/log/messages、/var/log/secure、/var/log/audit/audit.log访问 权限均为600；2）审计记录本地保存，且实时备份至360本地安全大脑，保存时间满足180天以上。 |
| d）应对审计进程进行保护，防止未经授权的中断。 | 执行service auditd status命令，系统开启auditd审计保护进程，审计进程由root用户维护，经现场使用yluser用户通过service auditd stop命令尝试中断审计进程，无法将审计进程单独中断。 |
| 入侵防范 | a）应遵循最小安装的原则，仅安装需要的组件和应用程序； | 1）系统安装遵循最小化安装原则；2）执行yum list installed命令查看操作系统已安装的程序包，存在Java、SSH、天眼云镜agent等应用程序或组件，不存在与业务系统无关的组件和应用程序。 |
| b）应关闭不需要的系统服务、默认共享和高危端口； | 1）执行systemctl list-unit-files 命令，系统已关闭FTP、Telnet 等高危网络服务；2）执行netstat -pantu命令，系统关闭了135、445等高危端口，仅开启了22、8080等端口。 |
| c）应通过设定终端接入方式或网络地址范围对通过网络进行管理的管理终端进行限制； | 经核查，1）通过配置安全组策略限制仅允许通过堡垒机管理服务器；2）经核查防火墙中访问控制策略，具备堡垒机地址-服务器管理网段（10.33.0.0）的访问控制策略。 |
| d）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； | 根据GB∕T 28448-2019 《信息安全技术 网络安全等级保护测评要求》测评对象范围描述，服务器无该项要求，故判为“不适用”。 |
| e）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； | 1）经过漏洞扫描，服务器不存在高危安全漏洞；2）执行rpm -qa grep patch命令，查看系统补丁已更新至最新。 |
| f）应能够检测到对重要节点进行入侵的行为，并在发生严重入侵事件时提供报警。 | 经核查，服务器上安装有青藤云天眼云镜，对主机入侵行为进行检测，发现严重安全事件时通过钉钉告警。 |
| 恶意代码防范 | a）应采用免受恶意代码攻击的技术措施或主动免疫可信验证机制及时识别入侵和病毒行为，并将其有效阻断。 | 经核查，服务器上安装有青藤云天眼云镜，对主机恶意代码进行检测、清除，每天凌晨自动更新恶意代码特征库，经核查，具备恶意代码特征库更新记录。 |
| 可信验证 | a）可基于可信根对计算设备的系统引导程序、系统程序、重要配置参数和应用程序等进行可信验证，并在应用程序的关键执行环节进行动态可信验证，在检测到其可信性受到破坏后进行报警，并将验证结果形成审计记录送至安全管理中心。 | 未采用技术措施对计算设备的系统引导程序、系统程序、重要配置参数和通信应用程序等进行可信验证。 |
| 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； | 采用SSH协议连接操作系统，保证了鉴别信息以及管理数据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。 | 操作系统中对重要鉴别信息通过自身的加密及校验（SHA256），保证数据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； | 采用SSH协议连接操作系统，保证了鉴别信息以及管理数据在传输过程中的保密性。 |
| b）应采用密码技术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个人信息等。 | 通过系统自带的加密模块保证鉴别数据在存储过程中的保密性。 |
| 数据备份恢复 | a）应提供重要数据的本地数据备份与恢复功能； | 经核查，通过脚本每周将配置文件、代码仓库等数据备份至备份服务器中，依据需要验证备份数据的有效性。 |
| b）应提供异地实时备份功能，利用通信网络将重要数据实时备份至备份场地； | 系统无异地备份机制。 |
| c）应提供重要数据处理系统的热冗余，保证系统的高可用性。 | 服务器采用K8S容器部署，保证系统的高可用性。 |
| 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； | 操作系统提供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功能。 |
| 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。 | 操作系统提供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的功能。 |

4.1.3.28. 应用服务器61

|  |  |  |
| --- | --- | --- |
| **安全控制点** | **测评指标** | **结果记录** |
| 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）操作系统时采用用户名+SSHKey公私钥进行身份鉴别鉴别信息具有复杂度要求；2）执行cat /etc/shadow命令，查看shadow文件系统内用户身份标识唯一，不存在同名用户，且不存在空口令账号；3）经访谈，SSHKey公私钥每半年进行更换；4）查看sshd\_config配置文件中配置PasswordAuthentication no，拒绝使用密码方式进行身份鉴别。 |
| 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； | 操作系统采用用户名+SSHKey公私钥进行身份鉴别，可以防止鉴别信息被暴力破解；但未配置用户连接超时退出策略。 |
| 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； | 1）经核查，管理人员采用SSH协议连接操作系统；2）执行netatat –tpln| grep 23命令查看操作系统远程管理端口，不存在Telnet端口，防止鉴别信息在网络传输过程中的被窃听。 |
| 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。 | 未采用两种或两种以上组合的鉴别技术对用户进行身份鉴别。 |
| 访问控制 | a）应对登录的用户分配账户和权限； | 1）经访谈，通过root账户为登录的用户创建账户、分配权限；2）执行ls -l命令查看关键文件权限，均已为账户分配了相应权限，相关文件权限设置为/etc/shadow：000、/etc/passwd：644、/etc/group：644、/etc/profile：644、/etc/crontab：644、/ etc/securetty：600、/etc/ssh/sshd\_config：600。 |
| b）应重命名或删除默认账户，修改默认账户的默认口令； | 1）执行cat /etc/shadow命令查看shadow文件，操作系统中adm、lp、sync、shutdown、halt、mail、uucp、operator、games、gopher等账户均为nologin状态，存在默认账户root；2）执行more /etc/ssh/sshd\_config命令，查看“PermitRootLogin”参数设置为“yes”，即允许root远程登录；3）经访谈，root用户需通过公私钥方式进行身份鉴别。 |
| 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； | 1）执行cat /etc/shadow命令查看shadow文件，发现操作系统存在root、ysup、yops、yluser等在用账户，不存在多余的、过期账户；2）存在多个堡垒机账户登录操作系统时共用一个账户的情况。 |
| 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； | root账户具有系统所有权限，未实现管理用户的权限分离。 |
| e）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； | 经访谈，由系统管理员root配置访问控制策略，如：/etc/passwd，/etc/profile宿主为root、权限设置为644，audit文件为700、message文件为600，其他文件权限为750，实现用户对文件的权限控制。 |
| f）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； | 由管理用户进行用户访问权限分配进行设置，依据访问控制策略,对各类文件进行访问，重要文件和目录权限均在合理范围内，用户可根据文件不同的权限进行操作。 |
| g）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。 | 执 行more /etc/selinux/config 命令，查看config文件显示 SELINUX参数为 DISABLED，即未开启强制访问控制模式。 |
| 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）执行ps -ef|grep rsyslog和ps -ef|grep auditd命令，显示rsyslog和auditd进程正在运行；2）more /etc/audit/audit.rules，显示审计内容包括：\*.info、authriv.\*、mail.\*、cron.\*、\*.emerg、uucp、news.crit、local7.\*等事件。 |
| 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； | 执行tail -20 /var/log/audit/audit.log命令，查看近20条审计日志，内容包括：时间、对象、路径、用户ID、相关的系统调用、用户执行命令等。 |
| 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）通过访问权限对审计记录进行保护，日志文件/var/log/messages、/var/log/secure、/var/log/audit/audit.log访问 权限均为600；2）审计记录本地保存，且实时备份至360本地安全大脑，保存时间满足180天以上。 |
| d）应对审计进程进行保护，防止未经授权的中断。 | 执行service auditd status命令，系统开启auditd审计保护进程，审计进程由root用户维护，经现场使用yluser用户通过service auditd stop命令尝试中断审计进程，无法将审计进程单独中断。 |
| 入侵防范 | a）应遵循最小安装的原则，仅安装需要的组件和应用程序； | 1）系统安装遵循最小化安装原则；2）执行yum list installed命令查看操作系统已安装的程序包，存在Java、SSH、天眼云镜agent等应用程序或组件，不存在与业务系统无关的组件和应用程序。 |
| b）应关闭不需要的系统服务、默认共享和高危端口； | 1）执行systemctl list-unit-files 命令，系统已关闭FTP、Telnet 等高危网络服务；2）执行netstat -pantu命令，系统关闭了135、445等高危端口，仅开启了22、8080等端口。 |
| c）应通过设定终端接入方式或网络地址范围对通过网络进行管理的管理终端进行限制； | 经核查，1）通过配置安全组策略限制仅允许通过堡垒机管理服务器；2）经核查防火墙中访问控制策略，具备堡垒机地址-服务器管理网段（10.33.0.0）的访问控制策略。 |
| d）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； | 根据GB∕T 28448-2019 《信息安全技术 网络安全等级保护测评要求》测评对象范围描述，服务器无该项要求，故判为“不适用”。 |
| e）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； | 1）经过漏洞扫描，服务器不存在高危安全漏洞；2）执行rpm -qa grep patch命令，查看系统补丁已更新至最新。 |
| f）应能够检测到对重要节点进行入侵的行为，并在发生严重入侵事件时提供报警。 | 经核查，服务器上安装有青藤云天眼云镜，对主机入侵行为进行检测，发现严重安全事件时通过钉钉告警。 |
| 恶意代码防范 | a）应采用免受恶意代码攻击的技术措施或主动免疫可信验证机制及时识别入侵和病毒行为，并将其有效阻断。 | 经核查，服务器上安装有青藤云天眼云镜，对主机恶意代码进行检测、清除，每天凌晨自动更新恶意代码特征库，经核查，具备恶意代码特征库更新记录。 |
| 可信验证 | a）可基于可信根对计算设备的系统引导程序、系统程序、重要配置参数和应用程序等进行可信验证，并在应用程序的关键执行环节进行动态可信验证，在检测到其可信性受到破坏后进行报警，并将验证结果形成审计记录送至安全管理中心。 | 未采用技术措施对计算设备的系统引导程序、系统程序、重要配置参数和通信应用程序等进行可信验证。 |
| 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； | 采用SSH协议连接操作系统，保证了鉴别信息以及管理数据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。 | 操作系统中对重要鉴别信息通过自身的加密及校验（SHA256），保证数据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； | 采用SSH协议连接操作系统，保证了鉴别信息以及管理数据在传输过程中的保密性。 |
| b）应采用密码技术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个人信息等。 | 通过系统自带的加密模块保证鉴别数据在存储过程中的保密性。 |
| 数据备份恢复 | a）应提供重要数据的本地数据备份与恢复功能； | 经核查，通过脚本每周将配置文件、代码仓库等数据备份至备份服务器中，依据需要验证备份数据的有效性。 |
| b）应提供异地实时备份功能，利用通信网络将重要数据实时备份至备份场地； | 系统无异地备份机制。 |
| c）应提供重要数据处理系统的热冗余，保证系统的高可用性。 | 服务器采用K8S容器部署，保证系统的高可用性。 |
| 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； | 操作系统提供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功能。 |
| 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。 | 操作系统提供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的功能。 |

4.1.3.29. 应用服务器66

|  |  |  |
| --- | --- | --- |
| **安全控制点** | **测评指标** | **结果记录** |
| 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）操作系统时采用用户名+SSHKey公私钥进行身份鉴别鉴别信息具有复杂度要求；2）执行cat /etc/shadow命令，查看shadow文件系统内用户身份标识唯一，不存在同名用户，且不存在空口令账号；3）经访谈，SSHKey公私钥每半年进行更换；4）查看sshd\_config配置文件中配置PasswordAuthentication no，拒绝使用密码方式进行身份鉴别。 |
| 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； | 操作系统采用用户名+SSHKey公私钥进行身份鉴别，可以防止鉴别信息被暴力破解；但未配置用户连接超时退出策略。 |
| 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； | 1）经核查，管理人员采用SSH协议连接操作系统；2）执行netatat –tpln| grep 23命令查看操作系统远程管理端口，不存在Telnet端口，防止鉴别信息在网络传输过程中的被窃听。 |
| 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。 | 未采用两种或两种以上组合的鉴别技术对用户进行身份鉴别。 |
| 访问控制 | a）应对登录的用户分配账户和权限； | 1）经访谈，通过root账户为登录的用户创建账户、分配权限；2）执行ls -l命令查看关键文件权限，均已为账户分配了相应权限，相关文件权限设置为/etc/shadow：000、/etc/passwd：644、/etc/group：644、/etc/profile：644、/etc/crontab：644、/ etc/securetty：600、/etc/ssh/sshd\_config：600。 |
| b）应重命名或删除默认账户，修改默认账户的默认口令； | 1）执行cat /etc/shadow命令查看shadow文件，操作系统中adm、lp、sync、shutdown、halt、mail、uucp、operator、games、gopher等账户均为nologin状态，存在默认账户root；2）执行more /etc/ssh/sshd\_config命令，查看“PermitRootLogin”参数设置为“yes”，即允许root远程登录；3）经访谈，root用户需通过公私钥方式进行身份鉴别。 |
| 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； | 1）执行cat /etc/shadow命令查看shadow文件，发现操作系统存在root、ysup、yops、yluser等在用账户，不存在多余的、过期账户；2）存在多个堡垒机账户登录操作系统时共用一个账户的情况。 |
| 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； | root账户具有系统所有权限，未实现管理用户的权限分离。 |
| e）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； | 经访谈，由系统管理员root配置访问控制策略，如：/etc/passwd，/etc/profile宿主为root、权限设置为644，audit文件为700、message文件为600，其他文件权限为750，实现用户对文件的权限控制。 |
| f）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； | 由管理用户进行用户访问权限分配进行设置，依据访问控制策略,对各类文件进行访问，重要文件和目录权限均在合理范围内，用户可根据文件不同的权限进行操作。 |
| g）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。 | 执 行more /etc/selinux/config 命令，查看config文件显示 SELINUX参数为 DISABLED，即未开启强制访问控制模式。 |
| 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）执行ps -ef|grep rsyslog和ps -ef|grep auditd命令，显示rsyslog和auditd进程正在运行；2）more /etc/audit/audit.rules，显示审计内容包括：\*.info、authriv.\*、mail.\*、cron.\*、\*.emerg、uucp、news.crit、local7.\*等事件。 |
| 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； | 执行tail -20 /var/log/audit/audit.log命令，查看近20条审计日志，内容包括：时间、对象、路径、用户ID、相关的系统调用、用户执行命令等。 |
| 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）通过访问权限对审计记录进行保护，日志文件/var/log/messages、/var/log/secure、/var/log/audit/audit.log访问 权限均为600；2）审计记录本地保存，且实时备份至360本地安全大脑，保存时间满足180天以上。 |
| d）应对审计进程进行保护，防止未经授权的中断。 | 执行service auditd status命令，系统开启auditd审计保护进程，审计进程由root用户维护，经现场使用yluser用户通过service auditd stop命令尝试中断审计进程，无法将审计进程单独中断。 |
| 入侵防范 | a）应遵循最小安装的原则，仅安装需要的组件和应用程序； | 1）系统安装遵循最小化安装原则；2）执行yum list installed命令查看操作系统已安装的程序包，存在Java、SSH、天眼云镜agent等应用程序或组件，不存在与业务系统无关的组件和应用程序。 |
| b）应关闭不需要的系统服务、默认共享和高危端口； | 1）执行systemctl list-unit-files 命令，系统已关闭FTP、Telnet 等高危网络服务；2）执行netstat -pantu命令，系统关闭了135、445等高危端口，仅开启了22、8080等端口。 |
| c）应通过设定终端接入方式或网络地址范围对通过网络进行管理的管理终端进行限制； | 经核查，1）通过配置安全组策略限制仅允许通过堡垒机管理服务器；2）经核查防火墙中访问控制策略，具备堡垒机地址-服务器管理网段（10.33.0.0）的访问控制策略。 |
| d）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； | 根据GB∕T 28448-2019 《信息安全技术 网络安全等级保护测评要求》测评对象范围描述，服务器无该项要求，故判为“不适用”。 |
| e）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； | 1）经过漏洞扫描，服务器不存在高危安全漏洞；2）执行rpm -qa grep patch命令，查看系统补丁已更新至最新。 |
| f）应能够检测到对重要节点进行入侵的行为，并在发生严重入侵事件时提供报警。 | 经核查，服务器上安装有青藤云天眼云镜，对主机入侵行为进行检测，发现严重安全事件时通过钉钉告警。 |
| 恶意代码防范 | a）应采用免受恶意代码攻击的技术措施或主动免疫可信验证机制及时识别入侵和病毒行为，并将其有效阻断。 | 经核查，服务器上安装有青藤云天眼云镜，对主机恶意代码进行检测、清除，每天凌晨自动更新恶意代码特征库，经核查，具备恶意代码特征库更新记录。 |
| 可信验证 | a）可基于可信根对计算设备的系统引导程序、系统程序、重要配置参数和应用程序等进行可信验证，并在应用程序的关键执行环节进行动态可信验证，在检测到其可信性受到破坏后进行报警，并将验证结果形成审计记录送至安全管理中心。 | 未采用技术措施对计算设备的系统引导程序、系统程序、重要配置参数和通信应用程序等进行可信验证。 |
| 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； | 采用SSH协议连接操作系统，保证了鉴别信息以及管理数据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。 | 操作系统中对重要鉴别信息通过自身的加密及校验（SHA256），保证数据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； | 采用SSH协议连接操作系统，保证了鉴别信息以及管理数据在传输过程中的保密性。 |
| b）应采用密码技术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个人信息等。 | 通过系统自带的加密模块保证鉴别数据在存储过程中的保密性。 |
| 数据备份恢复 | a）应提供重要数据的本地数据备份与恢复功能； | 经核查，通过脚本每周将配置文件、代码仓库等数据备份至备份服务器中，依据需要验证备份数据的有效性。 |
| b）应提供异地实时备份功能，利用通信网络将重要数据实时备份至备份场地； | 系统无异地备份机制。 |
| c）应提供重要数据处理系统的热冗余，保证系统的高可用性。 | 服务器采用K8S容器部署，保证系统的高可用性。 |
| 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； | 操作系统提供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功能。 |
| 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。 | 操作系统提供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的功能。 |

4.1.3.30. 应用服务器67

|  |  |  |
| --- | --- | --- |
| **安全控制点** | **测评指标** | **结果记录** |
| 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）操作系统时采用用户名+SSHKey公私钥进行身份鉴别鉴别信息具有复杂度要求；2）执行cat /etc/shadow命令，查看shadow文件系统内用户身份标识唯一，不存在同名用户，且不存在空口令账号；3）经访谈，SSHKey公私钥每半年进行更换；4）查看sshd\_config配置文件中配置PasswordAuthentication no，拒绝使用密码方式进行身份鉴别。 |
| 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； | 操作系统采用用户名+SSHKey公私钥进行身份鉴别，可以防止鉴别信息被暴力破解；但未配置用户连接超时退出策略。 |
| 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； | 1）经核查，管理人员采用SSH协议连接操作系统；2）执行netatat –tpln| grep 23命令查看操作系统远程管理端口，不存在Telnet端口，防止鉴别信息在网络传输过程中的被窃听。 |
| 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。 | 未采用两种或两种以上组合的鉴别技术对用户进行身份鉴别。 |
| 访问控制 | a）应对登录的用户分配账户和权限； | 1）经访谈，通过root账户为登录的用户创建账户、分配权限；2）执行ls -l命令查看关键文件权限，均已为账户分配了相应权限，相关文件权限设置为/etc/shadow：000、/etc/passwd：644、/etc/group：644、/etc/profile：644、/etc/crontab：644、/ etc/securetty：600、/etc/ssh/sshd\_config：600。 |
| b）应重命名或删除默认账户，修改默认账户的默认口令； | 1）执行cat /etc/shadow命令查看shadow文件，操作系统中adm、lp、sync、shutdown、halt、mail、uucp、operator、games、gopher等账户均为nologin状态，存在默认账户root；2）执行more /etc/ssh/sshd\_config命令，查看“PermitRootLogin”参数设置为“yes”，即允许root远程登录；3）经访谈，root用户需通过公私钥方式进行身份鉴别。 |
| 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； | 1）执行cat /etc/shadow命令查看shadow文件，发现操作系统存在root、ysup、yops、yluser等在用账户，不存在多余的、过期账户；2）存在多个堡垒机账户登录操作系统时共用一个账户的情况。 |
| 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； | root账户具有系统所有权限，未实现管理用户的权限分离。 |
| e）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； | 经访谈，由系统管理员root配置访问控制策略，如：/etc/passwd，/etc/profile宿主为root、权限设置为644，audit文件为700、message文件为600，其他文件权限为750，实现用户对文件的权限控制。 |
| f）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； | 由管理用户进行用户访问权限分配进行设置，依据访问控制策略,对各类文件进行访问，重要文件和目录权限均在合理范围内，用户可根据文件不同的权限进行操作。 |
| g）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。 | 执 行more /etc/selinux/config 命令，查看config文件显示 SELINUX参数为 DISABLED，即未开启强制访问控制模式。 |
| 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）执行ps -ef|grep rsyslog和ps -ef|grep auditd命令，显示rsyslog和auditd进程正在运行；2）more /etc/audit/audit.rules，显示审计内容包括：\*.info、authriv.\*、mail.\*、cron.\*、\*.emerg、uucp、news.crit、local7.\*等事件。 |
| 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； | 执行tail -20 /var/log/audit/audit.log命令，查看近20条审计日志，内容包括：时间、对象、路径、用户ID、相关的系统调用、用户执行命令等。 |
| 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）通过访问权限对审计记录进行保护，日志文件/var/log/messages、/var/log/secure、/var/log/audit/audit.log访问 权限均为600；2）审计记录本地保存，且实时备份至360本地安全大脑，保存时间满足180天以上。 |
| d）应对审计进程进行保护，防止未经授权的中断。 | 执行service auditd status命令，系统开启auditd审计保护进程，审计进程由root用户维护，经现场使用yluser用户通过service auditd stop命令尝试中断审计进程，无法将审计进程单独中断。 |
| 入侵防范 | a）应遵循最小安装的原则，仅安装需要的组件和应用程序； | 1）系统安装遵循最小化安装原则；2）执行yum list installed命令查看操作系统已安装的程序包，存在Java、SSH、天眼云镜agent等应用程序或组件，不存在与业务系统无关的组件和应用程序。 |
| b）应关闭不需要的系统服务、默认共享和高危端口； | 1）执行systemctl list-unit-files 命令，系统已关闭FTP、Telnet 等高危网络服务；2）执行netstat -pantu命令，系统关闭了135、445等高危端口，仅开启了22、8080等端口。 |
| c）应通过设定终端接入方式或网络地址范围对通过网络进行管理的管理终端进行限制； | 经核查，1）通过配置安全组策略限制仅允许通过堡垒机管理服务器；2）经核查防火墙中访问控制策略，具备堡垒机地址-服务器管理网段（10.33.0.0）的访问控制策略。 |
| d）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； | 根据GB∕T 28448-2019 《信息安全技术 网络安全等级保护测评要求》测评对象范围描述，服务器无该项要求，故判为“不适用”。 |
| e）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； | 1）经过漏洞扫描，服务器不存在高危安全漏洞；2）执行rpm -qa grep patch命令，查看系统补丁已更新至最新。 |
| f）应能够检测到对重要节点进行入侵的行为，并在发生严重入侵事件时提供报警。 | 经核查，服务器上安装有青藤云天眼云镜，对主机入侵行为进行检测，发现严重安全事件时通过钉钉告警。 |
| 恶意代码防范 | a）应采用免受恶意代码攻击的技术措施或主动免疫可信验证机制及时识别入侵和病毒行为，并将其有效阻断。 | 经核查，服务器上安装有青藤云天眼云镜，对主机恶意代码进行检测、清除，每天凌晨自动更新恶意代码特征库，经核查，具备恶意代码特征库更新记录。 |
| 可信验证 | a）可基于可信根对计算设备的系统引导程序、系统程序、重要配置参数和应用程序等进行可信验证，并在应用程序的关键执行环节进行动态可信验证，在检测到其可信性受到破坏后进行报警，并将验证结果形成审计记录送至安全管理中心。 | 未采用技术措施对计算设备的系统引导程序、系统程序、重要配置参数和通信应用程序等进行可信验证。 |
| 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； | 采用SSH协议连接操作系统，保证了鉴别信息以及管理数据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。 | 操作系统中对重要鉴别信息通过自身的加密及校验（SHA256），保证数据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； | 采用SSH协议连接操作系统，保证了鉴别信息以及管理数据在传输过程中的保密性。 |
| b）应采用密码技术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个人信息等。 | 通过系统自带的加密模块保证鉴别数据在存储过程中的保密性。 |
| 数据备份恢复 | a）应提供重要数据的本地数据备份与恢复功能； | 经核查，通过脚本每周将配置文件、代码仓库等数据备份至备份服务器中，依据需要验证备份数据的有效性。 |
| b）应提供异地实时备份功能，利用通信网络将重要数据实时备份至备份场地； | 系统无异地备份机制。 |
| c）应提供重要数据处理系统的热冗余，保证系统的高可用性。 | 服务器采用K8S容器部署，保证系统的高可用性。 |
| 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； | 操作系统提供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功能。 |
| 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。 | 操作系统提供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的功能。 |

4.1.3.31. 应用服务器72

|  |  |  |
| --- | --- | --- |
| **安全控制点** | **测评指标** | **结果记录** |
| 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）操作系统时采用用户名+SSHKey公私钥进行身份鉴别鉴别信息具有复杂度要求；2）执行cat /etc/shadow命令，查看shadow文件系统内用户身份标识唯一，不存在同名用户，且不存在空口令账号；3）经访谈，SSHKey公私钥每半年进行更换；4）查看sshd\_config配置文件中配置PasswordAuthentication no，拒绝使用密码方式进行身份鉴别。 |
| 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； | 操作系统采用用户名+SSHKey公私钥进行身份鉴别，可以防止鉴别信息被暴力破解；但未配置用户连接超时退出策略。 |
| 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； | 1）经核查，管理人员采用SSH协议连接操作系统；2）执行netatat –tpln| grep 23命令查看操作系统远程管理端口，不存在Telnet端口，防止鉴别信息在网络传输过程中的被窃听。 |
| 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。 | 未采用两种或两种以上组合的鉴别技术对用户进行身份鉴别。 |
| 访问控制 | a）应对登录的用户分配账户和权限； | 1）经访谈，通过root账户为登录的用户创建账户、分配权限；2）执行ls -l命令查看关键文件权限，均已为账户分配了相应权限，相关文件权限设置为/etc/shadow：000、/etc/passwd：644、/etc/group：644、/etc/profile：644、/etc/crontab：644、/ etc/securetty：600、/etc/ssh/sshd\_config：600。 |
| b）应重命名或删除默认账户，修改默认账户的默认口令； | 1）执行cat /etc/shadow命令查看shadow文件，操作系统中adm、lp、sync、shutdown、halt、mail、uucp、operator、games、gopher等账户均为nologin状态，存在默认账户root；2）执行more /etc/ssh/sshd\_config命令，查看“PermitRootLogin”参数设置为“yes”，即允许root远程登录；3）经访谈，root用户需通过公私钥方式进行身份鉴别。 |
| 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； | 1）执行cat /etc/shadow命令查看shadow文件，发现操作系统存在root、ysup、yops、yluser等在用账户，不存在多余的、过期账户；2）存在多个堡垒机账户登录操作系统时共用一个账户的情况。 |
| 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； | root账户具有系统所有权限，未实现管理用户的权限分离。 |
| e）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； | 经访谈，由系统管理员root配置访问控制策略，如：/etc/passwd，/etc/profile宿主为root、权限设置为644，audit文件为700、message文件为600，其他文件权限为750，实现用户对文件的权限控制。 |
| f）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； | 由管理用户进行用户访问权限分配进行设置，依据访问控制策略,对各类文件进行访问，重要文件和目录权限均在合理范围内，用户可根据文件不同的权限进行操作。 |
| g）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。 | 执 行more /etc/selinux/config 命令，查看config文件显示 SELINUX参数为 DISABLED，即未开启强制访问控制模式。 |
| 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）执行ps -ef|grep rsyslog和ps -ef|grep auditd命令，显示rsyslog和auditd进程正在运行；2）more /etc/audit/audit.rules，显示审计内容包括：\*.info、authriv.\*、mail.\*、cron.\*、\*.emerg、uucp、news.crit、local7.\*等事件。 |
| 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； | 执行tail -20 /var/log/audit/audit.log命令，查看近20条审计日志，内容包括：时间、对象、路径、用户ID、相关的系统调用、用户执行命令等。 |
| 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）通过访问权限对审计记录进行保护，日志文件/var/log/messages、/var/log/secure、/var/log/audit/audit.log访问 权限均为600；2）审计记录本地保存，且实时备份至360本地安全大脑，保存时间满足180天以上。 |
| d）应对审计进程进行保护，防止未经授权的中断。 | 执行service auditd status命令，系统开启auditd审计保护进程，审计进程由root用户维护，经现场使用yluser用户通过service auditd stop命令尝试中断审计进程，无法将审计进程单独中断。 |
| 入侵防范 | a）应遵循最小安装的原则，仅安装需要的组件和应用程序； | 1）系统安装遵循最小化安装原则；2）执行yum list installed命令查看操作系统已安装的程序包，存在Java、SSH、天眼云镜agent等应用程序或组件，不存在与业务系统无关的组件和应用程序。 |
| b）应关闭不需要的系统服务、默认共享和高危端口； | 1）执行systemctl list-unit-files 命令，系统已关闭FTP、Telnet 等高危网络服务；2）执行netstat -pantu命令，系统关闭了135、445等高危端口，仅开启了22、8080等端口。 |
| c）应通过设定终端接入方式或网络地址范围对通过网络进行管理的管理终端进行限制； | 经核查，1）通过配置安全组策略限制仅允许通过堡垒机管理服务器；2）经核查防火墙中访问控制策略，具备堡垒机地址-服务器管理网段（10.33.0.0）的访问控制策略。 |
| d）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； | 根据GB∕T 28448-2019 《信息安全技术 网络安全等级保护测评要求》测评对象范围描述，服务器无该项要求，故判为“不适用”。 |
| e）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； | 1）经过漏洞扫描，服务器不存在高危安全漏洞；2）执行rpm -qa grep patch命令，查看系统补丁已更新至最新。 |
| f）应能够检测到对重要节点进行入侵的行为，并在发生严重入侵事件时提供报警。 | 经核查，服务器上安装有青藤云天眼云镜，对主机入侵行为进行检测，发现严重安全事件时通过钉钉告警。 |
| 恶意代码防范 | a）应采用免受恶意代码攻击的技术措施或主动免疫可信验证机制及时识别入侵和病毒行为，并将其有效阻断。 | 经核查，服务器上安装有青藤云天眼云镜，对主机恶意代码进行检测、清除，每天凌晨自动更新恶意代码特征库，经核查，具备恶意代码特征库更新记录。 |
| 可信验证 | a）可基于可信根对计算设备的系统引导程序、系统程序、重要配置参数和应用程序等进行可信验证，并在应用程序的关键执行环节进行动态可信验证，在检测到其可信性受到破坏后进行报警，并将验证结果形成审计记录送至安全管理中心。 | 未采用技术措施对计算设备的系统引导程序、系统程序、重要配置参数和通信应用程序等进行可信验证。 |
| 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； | 采用SSH协议连接操作系统，保证了鉴别信息以及管理数据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。 | 操作系统中对重要鉴别信息通过自身的加密及校验（SHA256），保证数据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； | 采用SSH协议连接操作系统，保证了鉴别信息以及管理数据在传输过程中的保密性。 |
| b）应采用密码技术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个人信息等。 | 通过系统自带的加密模块保证鉴别数据在存储过程中的保密性。 |
| 数据备份恢复 | a）应提供重要数据的本地数据备份与恢复功能； | 经核查，通过脚本每周将配置文件、代码仓库等数据备份至备份服务器中，依据需要验证备份数据的有效性。 |
| b）应提供异地实时备份功能，利用通信网络将重要数据实时备份至备份场地； | 系统无异地备份机制。 |
| c）应提供重要数据处理系统的热冗余，保证系统的高可用性。 | 服务器采用K8S容器部署，保证系统的高可用性。 |
| 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； | 操作系统提供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功能。 |
| 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。 | 操作系统提供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的功能。 |

4.1.3.32. 应用服务器77

|  |  |  |
| --- | --- | --- |
| **安全控制点** | **测评指标** | **结果记录** |
| 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）操作系统时采用用户名+SSHKey公私钥进行身份鉴别鉴别信息具有复杂度要求；2）执行cat /etc/shadow命令，查看shadow文件系统内用户身份标识唯一，不存在同名用户，且不存在空口令账号；3）经访谈，SSHKey公私钥每半年进行更换；4）查看sshd\_config配置文件中配置PasswordAuthentication no，拒绝使用密码方式进行身份鉴别。 |
| 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； | 操作系统采用用户名+SSHKey公私钥进行身份鉴别，可以防止鉴别信息被暴力破解；但未配置用户连接超时退出策略。 |
| 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； | 1）经核查，管理人员采用SSH协议连接操作系统；2）执行netatat –tpln| grep 23命令查看操作系统远程管理端口，不存在Telnet端口，防止鉴别信息在网络传输过程中的被窃听。 |
| 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。 | 未采用两种或两种以上组合的鉴别技术对用户进行身份鉴别。 |
| 访问控制 | a）应对登录的用户分配账户和权限； | 1）经访谈，通过root账户为登录的用户创建账户、分配权限；2）执行ls -l命令查看关键文件权限，均已为账户分配了相应权限，相关文件权限设置为/etc/shadow：000、/etc/passwd：644、/etc/group：644、/etc/profile：644、/etc/crontab：644、/ etc/securetty：600、/etc/ssh/sshd\_config：600。 |
| b）应重命名或删除默认账户，修改默认账户的默认口令； | 1）执行cat /etc/shadow命令查看shadow文件，操作系统中adm、lp、sync、shutdown、halt、mail、uucp、operator、games、gopher等账户均为nologin状态，存在默认账户root；2）执行more /etc/ssh/sshd\_config命令，查看“PermitRootLogin”参数设置为“yes”，即允许root远程登录；3）经访谈，root用户需通过公私钥方式进行身份鉴别。 |
| 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； | 1）执行cat /etc/shadow命令查看shadow文件，发现操作系统存在root、ysup、yops、yluser等在用账户，不存在多余的、过期账户；2）存在多个堡垒机账户登录操作系统时共用一个账户的情况。 |
| 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； | root账户具有系统所有权限，未实现管理用户的权限分离。 |
| e）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； | 经访谈，由系统管理员root配置访问控制策略，如：/etc/passwd，/etc/profile宿主为root、权限设置为644，audit文件为700、message文件为600，其他文件权限为750，实现用户对文件的权限控制。 |
| f）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； | 由管理用户进行用户访问权限分配进行设置，依据访问控制策略,对各类文件进行访问，重要文件和目录权限均在合理范围内，用户可根据文件不同的权限进行操作。 |
| g）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。 | 执 行more /etc/selinux/config 命令，查看config文件显示 SELINUX参数为 DISABLED，即未开启强制访问控制模式。 |
| 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）执行ps -ef|grep rsyslog和ps -ef|grep auditd命令，显示rsyslog和auditd进程正在运行；2）more /etc/audit/audit.rules，显示审计内容包括：\*.info、authriv.\*、mail.\*、cron.\*、\*.emerg、uucp、news.crit、local7.\*等事件。 |
| 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； | 执行tail -20 /var/log/audit/audit.log命令，查看近20条审计日志，内容包括：时间、对象、路径、用户ID、相关的系统调用、用户执行命令等。 |
| 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）通过访问权限对审计记录进行保护，日志文件/var/log/messages、/var/log/secure、/var/log/audit/audit.log访问 权限均为600；2）审计记录本地保存，且实时备份至360本地安全大脑，保存时间满足180天以上。 |
| d）应对审计进程进行保护，防止未经授权的中断。 | 执行service auditd status命令，系统开启auditd审计保护进程，审计进程由root用户维护，经现场使用yluser用户通过service auditd stop命令尝试中断审计进程，无法将审计进程单独中断。 |
| 入侵防范 | a）应遵循最小安装的原则，仅安装需要的组件和应用程序； | 1）系统安装遵循最小化安装原则；2）执行yum list installed命令查看操作系统已安装的程序包，存在Java、SSH、天眼云镜agent等应用程序或组件，不存在与业务系统无关的组件和应用程序。 |
| b）应关闭不需要的系统服务、默认共享和高危端口； | 1）执行systemctl list-unit-files 命令，系统已关闭FTP、Telnet 等高危网络服务；2）执行netstat -pantu命令，系统关闭了135、445等高危端口，仅开启了22、8080等端口。 |
| c）应通过设定终端接入方式或网络地址范围对通过网络进行管理的管理终端进行限制； | 经核查，1）通过配置安全组策略限制仅允许通过堡垒机管理服务器；2）经核查防火墙中访问控制策略，具备堡垒机地址-服务器管理网段（10.33.0.0）的访问控制策略。 |
| d）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； | 根据GB∕T 28448-2019 《信息安全技术 网络安全等级保护测评要求》测评对象范围描述，服务器无该项要求，故判为“不适用”。 |
| e）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； | 1）经过漏洞扫描，服务器不存在高危安全漏洞；2）执行rpm -qa grep patch命令，查看系统补丁已更新至最新。 |
| f）应能够检测到对重要节点进行入侵的行为，并在发生严重入侵事件时提供报警。 | 经核查，服务器上安装有青藤云天眼云镜，对主机入侵行为进行检测，发现严重安全事件时通过钉钉告警。 |
| 恶意代码防范 | a）应采用免受恶意代码攻击的技术措施或主动免疫可信验证机制及时识别入侵和病毒行为，并将其有效阻断。 | 经核查，服务器上安装有青藤云天眼云镜，对主机恶意代码进行检测、清除，每天凌晨自动更新恶意代码特征库，经核查，具备恶意代码特征库更新记录。 |
| 可信验证 | a）可基于可信根对计算设备的系统引导程序、系统程序、重要配置参数和应用程序等进行可信验证，并在应用程序的关键执行环节进行动态可信验证，在检测到其可信性受到破坏后进行报警，并将验证结果形成审计记录送至安全管理中心。 | 未采用技术措施对计算设备的系统引导程序、系统程序、重要配置参数和通信应用程序等进行可信验证。 |
| 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； | 采用SSH协议连接操作系统，保证了鉴别信息以及管理数据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。 | 操作系统中对重要鉴别信息通过自身的加密及校验（SHA256），保证数据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； | 采用SSH协议连接操作系统，保证了鉴别信息以及管理数据在传输过程中的保密性。 |
| b）应采用密码技术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个人信息等。 | 通过系统自带的加密模块保证鉴别数据在存储过程中的保密性。 |
| 数据备份恢复 | a）应提供重要数据的本地数据备份与恢复功能； | 经核查，通过脚本每周将配置文件、代码仓库等数据备份至备份服务器中，依据需要验证备份数据的有效性。 |
| b）应提供异地实时备份功能，利用通信网络将重要数据实时备份至备份场地； | 系统无异地备份机制。 |
| c）应提供重要数据处理系统的热冗余，保证系统的高可用性。 | 服务器采用K8S容器部署，保证系统的高可用性。 |
| 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； | 操作系统提供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功能。 |
| 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。 | 操作系统提供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的功能。 |

4.1.3.33. 应用服务器78

|  |  |  |
| --- | --- | --- |
| **安全控制点** | **测评指标** | **结果记录** |
| 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）操作系统时采用用户名+SSHKey公私钥进行身份鉴别鉴别信息具有复杂度要求；2）执行cat /etc/shadow命令，查看shadow文件系统内用户身份标识唯一，不存在同名用户，且不存在空口令账号；3）经访谈，SSHKey公私钥每半年进行更换；4）查看sshd\_config配置文件中配置PasswordAuthentication no，拒绝使用密码方式进行身份鉴别。 |
| 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； | 操作系统采用用户名+SSHKey公私钥进行身份鉴别，可以防止鉴别信息被暴力破解；但未配置用户连接超时退出策略。 |
| 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； | 1）经核查，管理人员采用SSH协议连接操作系统；2）执行netatat –tpln| grep 23命令查看操作系统远程管理端口，不存在Telnet端口，防止鉴别信息在网络传输过程中的被窃听。 |
| 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。 | 未采用两种或两种以上组合的鉴别技术对用户进行身份鉴别。 |
| 访问控制 | a）应对登录的用户分配账户和权限； | 1）经访谈，通过root账户为登录的用户创建账户、分配权限；2）执行ls -l命令查看关键文件权限，均已为账户分配了相应权限，相关文件权限设置为/etc/shadow：000、/etc/passwd：644、/etc/group：644、/etc/profile：644、/etc/crontab：644、/ etc/securetty：600、/etc/ssh/sshd\_config：600。 |
| b）应重命名或删除默认账户，修改默认账户的默认口令； | 1）执行cat /etc/shadow命令查看shadow文件，操作系统中adm、lp、sync、shutdown、halt、mail、uucp、operator、games、gopher等账户均为nologin状态，存在默认账户root；2）执行more /etc/ssh/sshd\_config命令，查看“PermitRootLogin”参数设置为“yes”，即允许root远程登录；3）经访谈，root用户需通过公私钥方式进行身份鉴别。 |
| 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； | 1）执行cat /etc/shadow命令查看shadow文件，发现操作系统存在root、ysup、yops、yluser等在用账户，不存在多余的、过期账户；2）存在多个堡垒机账户登录操作系统时共用一个账户的情况。 |
| 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； | root账户具有系统所有权限，未实现管理用户的权限分离。 |
| e）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； | 经访谈，由系统管理员root配置访问控制策略，如：/etc/passwd，/etc/profile宿主为root、权限设置为644，audit文件为700、message文件为600，其他文件权限为750，实现用户对文件的权限控制。 |
| f）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； | 由管理用户进行用户访问权限分配进行设置，依据访问控制策略,对各类文件进行访问，重要文件和目录权限均在合理范围内，用户可根据文件不同的权限进行操作。 |
| g）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。 | 执 行more /etc/selinux/config 命令，查看config文件显示 SELINUX参数为 DISABLED，即未开启强制访问控制模式。 |
| 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）执行ps -ef|grep rsyslog和ps -ef|grep auditd命令，显示rsyslog和auditd进程正在运行；2）more /etc/audit/audit.rules，显示审计内容包括：\*.info、authriv.\*、mail.\*、cron.\*、\*.emerg、uucp、news.crit、local7.\*等事件。 |
| 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； | 执行tail -20 /var/log/audit/audit.log命令，查看近20条审计日志，内容包括：时间、对象、路径、用户ID、相关的系统调用、用户执行命令等。 |
| 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）通过访问权限对审计记录进行保护，日志文件/var/log/messages、/var/log/secure、/var/log/audit/audit.log访问 权限均为600；2）审计记录本地保存，且实时备份至360本地安全大脑，保存时间满足180天以上。 |
| d）应对审计进程进行保护，防止未经授权的中断。 | 执行service auditd status命令，系统开启auditd审计保护进程，审计进程由root用户维护，经现场使用yluser用户通过service auditd stop命令尝试中断审计进程，无法将审计进程单独中断。 |
| 入侵防范 | a）应遵循最小安装的原则，仅安装需要的组件和应用程序； | 1）系统安装遵循最小化安装原则；2）执行yum list installed命令查看操作系统已安装的程序包，存在Java、SSH、天眼云镜agent等应用程序或组件，不存在与业务系统无关的组件和应用程序。 |
| b）应关闭不需要的系统服务、默认共享和高危端口； | 1）执行systemctl list-unit-files 命令，系统已关闭FTP、Telnet 等高危网络服务；2）执行netstat -pantu命令，系统关闭了135、445等高危端口，仅开启了22、8080等端口。 |
| c）应通过设定终端接入方式或网络地址范围对通过网络进行管理的管理终端进行限制； | 经核查，1）通过配置安全组策略限制仅允许通过堡垒机管理服务器；2）经核查防火墙中访问控制策略，具备堡垒机地址-服务器管理网段（10.33.0.0）的访问控制策略。 |
| d）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； | 根据GB∕T 28448-2019 《信息安全技术 网络安全等级保护测评要求》测评对象范围描述，服务器无该项要求，故判为“不适用”。 |
| e）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； | 1）经过漏洞扫描，服务器不存在高危安全漏洞；2）执行rpm -qa grep patch命令，查看系统补丁已更新至最新。 |
| f）应能够检测到对重要节点进行入侵的行为，并在发生严重入侵事件时提供报警。 | 经核查，服务器上安装有青藤云天眼云镜，对主机入侵行为进行检测，发现严重安全事件时通过钉钉告警。 |
| 恶意代码防范 | a）应采用免受恶意代码攻击的技术措施或主动免疫可信验证机制及时识别入侵和病毒行为，并将其有效阻断。 | 经核查，服务器上安装有青藤云天眼云镜，对主机恶意代码进行检测、清除，每天凌晨自动更新恶意代码特征库，经核查，具备恶意代码特征库更新记录。 |
| 可信验证 | a）可基于可信根对计算设备的系统引导程序、系统程序、重要配置参数和应用程序等进行可信验证，并在应用程序的关键执行环节进行动态可信验证，在检测到其可信性受到破坏后进行报警，并将验证结果形成审计记录送至安全管理中心。 | 未采用技术措施对计算设备的系统引导程序、系统程序、重要配置参数和通信应用程序等进行可信验证。 |
| 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； | 采用SSH协议连接操作系统，保证了鉴别信息以及管理数据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。 | 操作系统中对重要鉴别信息通过自身的加密及校验（SHA256），保证数据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； | 采用SSH协议连接操作系统，保证了鉴别信息以及管理数据在传输过程中的保密性。 |
| b）应采用密码技术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个人信息等。 | 通过系统自带的加密模块保证鉴别数据在存储过程中的保密性。 |
| 数据备份恢复 | a）应提供重要数据的本地数据备份与恢复功能； | 经核查，通过脚本每周将配置文件、代码仓库等数据备份至备份服务器中，依据需要验证备份数据的有效性。 |
| b）应提供异地实时备份功能，利用通信网络将重要数据实时备份至备份场地； | 系统无异地备份机制。 |
| c）应提供重要数据处理系统的热冗余，保证系统的高可用性。 | 服务器采用K8S容器部署，保证系统的高可用性。 |
| 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； | 操作系统提供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功能。 |
| 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。 | 操作系统提供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的功能。 |

4.1.3.34. 应用服务器81

|  |  |  |
| --- | --- | --- |
| **安全控制点** | **测评指标** | **结果记录** |
| 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）操作系统时采用用户名+SSHKey公私钥进行身份鉴别鉴别信息具有复杂度要求；2）执行cat /etc/shadow命令，查看shadow文件系统内用户身份标识唯一，不存在同名用户，且不存在空口令账号；3）经访谈，SSHKey公私钥每半年进行更换；4）查看sshd\_config配置文件中配置PasswordAuthentication no，拒绝使用密码方式进行身份鉴别。 |
| 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； | 操作系统采用用户名+SSHKey公私钥进行身份鉴别，可以防止鉴别信息被暴力破解；但未配置用户连接超时退出策略。 |
| 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； | 1）经核查，管理人员采用SSH协议连接操作系统；2）执行netatat –tpln| grep 23命令查看操作系统远程管理端口，不存在Telnet端口，防止鉴别信息在网络传输过程中的被窃听。 |
| 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。 | 未采用两种或两种以上组合的鉴别技术对用户进行身份鉴别。 |
| 访问控制 | a）应对登录的用户分配账户和权限； | 1）经访谈，通过root账户为登录的用户创建账户、分配权限；2）执行ls -l命令查看关键文件权限，均已为账户分配了相应权限，相关文件权限设置为/etc/shadow：000、/etc/passwd：644、/etc/group：644、/etc/profile：644、/etc/crontab：644、/ etc/securetty：600、/etc/ssh/sshd\_config：600。 |
| b）应重命名或删除默认账户，修改默认账户的默认口令； | 1）执行cat /etc/shadow命令查看shadow文件，操作系统中adm、lp、sync、shutdown、halt、mail、uucp、operator、games、gopher等账户均为nologin状态，存在默认账户root；2）执行more /etc/ssh/sshd\_config命令，查看“PermitRootLogin”参数设置为“yes”，即允许root远程登录；3）经访谈，root用户需通过公私钥方式进行身份鉴别。 |
| 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； | 1）执行cat /etc/shadow命令查看shadow文件，发现操作系统存在root、ysup、yops、yluser等在用账户，不存在多余的、过期账户；2）存在多个堡垒机账户登录操作系统时共用一个账户的情况。 |
| 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； | root账户具有系统所有权限，未实现管理用户的权限分离。 |
| e）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； | 经访谈，由系统管理员root配置访问控制策略，如：/etc/passwd，/etc/profile宿主为root、权限设置为644，audit文件为700、message文件为600，其他文件权限为750，实现用户对文件的权限控制。 |
| f）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； | 由管理用户进行用户访问权限分配进行设置，依据访问控制策略,对各类文件进行访问，重要文件和目录权限均在合理范围内，用户可根据文件不同的权限进行操作。 |
| g）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。 | 执 行more /etc/selinux/config 命令，查看config文件显示 SELINUX参数为 DISABLED，即未开启强制访问控制模式。 |
| 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）执行ps -ef|grep rsyslog和ps -ef|grep auditd命令，显示rsyslog和auditd进程正在运行；2）more /etc/audit/audit.rules，显示审计内容包括：\*.info、authriv.\*、mail.\*、cron.\*、\*.emerg、uucp、news.crit、local7.\*等事件。 |
| 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； | 执行tail -20 /var/log/audit/audit.log命令，查看近20条审计日志，内容包括：时间、对象、路径、用户ID、相关的系统调用、用户执行命令等。 |
| 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）通过访问权限对审计记录进行保护，日志文件/var/log/messages、/var/log/secure、/var/log/audit/audit.log访问 权限均为600；2）审计记录本地保存，且实时备份至360本地安全大脑，保存时间满足180天以上。 |
| d）应对审计进程进行保护，防止未经授权的中断。 | 执行service auditd status命令，系统开启auditd审计保护进程，审计进程由root用户维护，经现场使用yluser用户通过service auditd stop命令尝试中断审计进程，无法将审计进程单独中断。 |
| 入侵防范 | a）应遵循最小安装的原则，仅安装需要的组件和应用程序； | 1）系统安装遵循最小化安装原则；2）执行yum list installed命令查看操作系统已安装的程序包，存在Java、SSH、天眼云镜agent等应用程序或组件，不存在与业务系统无关的组件和应用程序。 |
| b）应关闭不需要的系统服务、默认共享和高危端口； | 1）执行systemctl list-unit-files 命令，系统已关闭FTP、Telnet 等高危网络服务；2）执行netstat -pantu命令，系统关闭了135、445等高危端口，仅开启了22、8080等端口。 |
| c）应通过设定终端接入方式或网络地址范围对通过网络进行管理的管理终端进行限制； | 经核查，1）通过配置安全组策略限制仅允许通过堡垒机管理服务器；2）经核查防火墙中访问控制策略，具备堡垒机地址-服务器管理网段（10.33.0.0）的访问控制策略。 |
| d）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； | 根据GB∕T 28448-2019 《信息安全技术 网络安全等级保护测评要求》测评对象范围描述，服务器无该项要求，故判为“不适用”。 |
| e）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； | 1）经过漏洞扫描，服务器不存在高危安全漏洞；2）执行rpm -qa grep patch命令，查看系统补丁已更新至最新。 |
| f）应能够检测到对重要节点进行入侵的行为，并在发生严重入侵事件时提供报警。 | 经核查，服务器上安装有青藤云天眼云镜，对主机入侵行为进行检测，发现严重安全事件时通过钉钉告警。 |
| 恶意代码防范 | a）应采用免受恶意代码攻击的技术措施或主动免疫可信验证机制及时识别入侵和病毒行为，并将其有效阻断。 | 经核查，服务器上安装有青藤云天眼云镜，对主机恶意代码进行检测、清除，每天凌晨自动更新恶意代码特征库，经核查，具备恶意代码特征库更新记录。 |
| 可信验证 | a）可基于可信根对计算设备的系统引导程序、系统程序、重要配置参数和应用程序等进行可信验证，并在应用程序的关键执行环节进行动态可信验证，在检测到其可信性受到破坏后进行报警，并将验证结果形成审计记录送至安全管理中心。 | 未采用技术措施对计算设备的系统引导程序、系统程序、重要配置参数和通信应用程序等进行可信验证。 |
| 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； | 采用SSH协议连接操作系统，保证了鉴别信息以及管理数据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。 | 操作系统中对重要鉴别信息通过自身的加密及校验（SHA256），保证数据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； | 采用SSH协议连接操作系统，保证了鉴别信息以及管理数据在传输过程中的保密性。 |
| b）应采用密码技术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个人信息等。 | 通过系统自带的加密模块保证鉴别数据在存储过程中的保密性。 |
| 数据备份恢复 | a）应提供重要数据的本地数据备份与恢复功能； | 经核查，通过脚本每周将配置文件、代码仓库等数据备份至备份服务器中，依据需要验证备份数据的有效性。 |
| b）应提供异地实时备份功能，利用通信网络将重要数据实时备份至备份场地； | 系统无异地备份机制。 |
| c）应提供重要数据处理系统的热冗余，保证系统的高可用性。 | 服务器采用K8S容器部署，保证系统的高可用性。 |
| 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； | 操作系统提供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功能。 |
| 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。 | 操作系统提供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的功能。 |

4.1.3.35. 应用服务器84

|  |  |  |
| --- | --- | --- |
| **安全控制点** | **测评指标** | **结果记录** |
| 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）操作系统时采用用户名+SSHKey公私钥进行身份鉴别鉴别信息具有复杂度要求；2）执行cat /etc/shadow命令，查看shadow文件系统内用户身份标识唯一，不存在同名用户，且不存在空口令账号；3）经访谈，SSHKey公私钥每半年进行更换；4）查看sshd\_config配置文件中配置PasswordAuthentication no，拒绝使用密码方式进行身份鉴别。 |
| 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； | 操作系统采用用户名+SSHKey公私钥进行身份鉴别，可以防止鉴别信息被暴力破解；但未配置用户连接超时退出策略。 |
| 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； | 1）经核查，管理人员采用SSH协议连接操作系统；2）执行netatat –tpln| grep 23命令查看操作系统远程管理端口，不存在Telnet端口，防止鉴别信息在网络传输过程中的被窃听。 |
| 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。 | 未采用两种或两种以上组合的鉴别技术对用户进行身份鉴别。 |
| 访问控制 | a）应对登录的用户分配账户和权限； | 1）经访谈，通过root账户为登录的用户创建账户、分配权限；2）执行ls -l命令查看关键文件权限，均已为账户分配了相应权限，相关文件权限设置为/etc/shadow：000、/etc/passwd：644、/etc/group：644、/etc/profile：644、/etc/crontab：644、/ etc/securetty：600、/etc/ssh/sshd\_config：600。 |
| b）应重命名或删除默认账户，修改默认账户的默认口令； | 1）执行cat /etc/shadow命令查看shadow文件，操作系统中adm、lp、sync、shutdown、halt、mail、uucp、operator、games、gopher等账户均为nologin状态，存在默认账户root；2）执行more /etc/ssh/sshd\_config命令，查看“PermitRootLogin”参数设置为“yes”，即允许root远程登录；3）经访谈，root用户需通过公私钥方式进行身份鉴别。 |
| 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； | 1）执行cat /etc/shadow命令查看shadow文件，发现操作系统存在root、ysup、yops、yluser等在用账户，不存在多余的、过期账户；2）存在多个堡垒机账户登录操作系统时共用一个账户的情况。 |
| 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； | root账户具有系统所有权限，未实现管理用户的权限分离。 |
| e）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； | 经访谈，由系统管理员root配置访问控制策略，如：/etc/passwd，/etc/profile宿主为root、权限设置为644，audit文件为700、message文件为600，其他文件权限为750，实现用户对文件的权限控制。 |
| f）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； | 由管理用户进行用户访问权限分配进行设置，依据访问控制策略,对各类文件进行访问，重要文件和目录权限均在合理范围内，用户可根据文件不同的权限进行操作。 |
| g）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。 | 执 行more /etc/selinux/config 命令，查看config文件显示 SELINUX参数为 DISABLED，即未开启强制访问控制模式。 |
| 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）执行ps -ef|grep rsyslog和ps -ef|grep auditd命令，显示rsyslog和auditd进程正在运行；2）more /etc/audit/audit.rules，显示审计内容包括：\*.info、authriv.\*、mail.\*、cron.\*、\*.emerg、uucp、news.crit、local7.\*等事件。 |
| 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； | 执行tail -20 /var/log/audit/audit.log命令，查看近20条审计日志，内容包括：时间、对象、路径、用户ID、相关的系统调用、用户执行命令等。 |
| 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）通过访问权限对审计记录进行保护，日志文件/var/log/messages、/var/log/secure、/var/log/audit/audit.log访问 权限均为600；2）审计记录本地保存，且实时备份至360本地安全大脑，保存时间满足180天以上。 |
| d）应对审计进程进行保护，防止未经授权的中断。 | 执行service auditd status命令，系统开启auditd审计保护进程，审计进程由root用户维护，经现场使用yluser用户通过service auditd stop命令尝试中断审计进程，无法将审计进程单独中断。 |
| 入侵防范 | a）应遵循最小安装的原则，仅安装需要的组件和应用程序； | 1）系统安装遵循最小化安装原则；2）执行yum list installed命令查看操作系统已安装的程序包，存在Java、SSH、天眼云镜agent等应用程序或组件，不存在与业务系统无关的组件和应用程序。 |
| b）应关闭不需要的系统服务、默认共享和高危端口； | 1）执行systemctl list-unit-files 命令，系统已关闭FTP、Telnet 等高危网络服务；2）执行netstat -pantu命令，系统关闭了135、445等高危端口，仅开启了22、8080等端口。 |
| c）应通过设定终端接入方式或网络地址范围对通过网络进行管理的管理终端进行限制； | 经核查，1）通过配置安全组策略限制仅允许通过堡垒机管理服务器；2）经核查防火墙中访问控制策略，具备堡垒机地址-服务器管理网段（10.33.0.0）的访问控制策略。 |
| d）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； | 根据GB∕T 28448-2019 《信息安全技术 网络安全等级保护测评要求》测评对象范围描述，服务器无该项要求，故判为“不适用”。 |
| e）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； | 1）经过漏洞扫描，服务器不存在高危安全漏洞；2）执行rpm -qa grep patch命令，查看系统补丁已更新至最新。 |
| f）应能够检测到对重要节点进行入侵的行为，并在发生严重入侵事件时提供报警。 | 经核查，服务器上安装有青藤云天眼云镜，对主机入侵行为进行检测，发现严重安全事件时通过钉钉告警。 |
| 恶意代码防范 | a）应采用免受恶意代码攻击的技术措施或主动免疫可信验证机制及时识别入侵和病毒行为，并将其有效阻断。 | 经核查，服务器上安装有青藤云天眼云镜，对主机恶意代码进行检测、清除，每天凌晨自动更新恶意代码特征库，经核查，具备恶意代码特征库更新记录。 |
| 可信验证 | a）可基于可信根对计算设备的系统引导程序、系统程序、重要配置参数和应用程序等进行可信验证，并在应用程序的关键执行环节进行动态可信验证，在检测到其可信性受到破坏后进行报警，并将验证结果形成审计记录送至安全管理中心。 | 未采用技术措施对计算设备的系统引导程序、系统程序、重要配置参数和通信应用程序等进行可信验证。 |
| 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； | 采用SSH协议连接操作系统，保证了鉴别信息以及管理数据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。 | 操作系统中对重要鉴别信息通过自身的加密及校验（SHA256），保证数据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； | 采用SSH协议连接操作系统，保证了鉴别信息以及管理数据在传输过程中的保密性。 |
| b）应采用密码技术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个人信息等。 | 通过系统自带的加密模块保证鉴别数据在存储过程中的保密性。 |
| 数据备份恢复 | a）应提供重要数据的本地数据备份与恢复功能； | 经核查，通过脚本每周将配置文件、代码仓库等数据备份至备份服务器中，依据需要验证备份数据的有效性。 |
| b）应提供异地实时备份功能，利用通信网络将重要数据实时备份至备份场地； | 系统无异地备份机制。 |
| c）应提供重要数据处理系统的热冗余，保证系统的高可用性。 | 服务器采用K8S容器部署，保证系统的高可用性。 |
| 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； | 操作系统提供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功能。 |
| 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。 | 操作系统提供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的功能。 |

4.1.3.36. 应用服务器90

|  |  |  |
| --- | --- | --- |
| **安全控制点** | **测评指标** | **结果记录** |
| 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）操作系统时采用用户名+SSHKey公私钥进行身份鉴别鉴别信息具有复杂度要求；2）执行cat /etc/shadow命令，查看shadow文件系统内用户身份标识唯一，不存在同名用户，且不存在空口令账号；3）经访谈，SSHKey公私钥每半年进行更换；4）查看sshd\_config配置文件中配置PasswordAuthentication no，拒绝使用密码方式进行身份鉴别。 |
| 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； | 操作系统采用用户名+SSHKey公私钥进行身份鉴别，可以防止鉴别信息被暴力破解；但未配置用户连接超时退出策略。 |
| 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； | 1）经核查，管理人员采用SSH协议连接操作系统；2）执行netatat –tpln| grep 23命令查看操作系统远程管理端口，不存在Telnet端口，防止鉴别信息在网络传输过程中的被窃听。 |
| 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。 | 未采用两种或两种以上组合的鉴别技术对用户进行身份鉴别。 |
| 访问控制 | a）应对登录的用户分配账户和权限； | 1）经访谈，通过root账户为登录的用户创建账户、分配权限；2）执行ls -l命令查看关键文件权限，均已为账户分配了相应权限，相关文件权限设置为/etc/shadow：000、/etc/passwd：644、/etc/group：644、/etc/profile：644、/etc/crontab：644、/ etc/securetty：600、/etc/ssh/sshd\_config：600。 |
| b）应重命名或删除默认账户，修改默认账户的默认口令； | 1）执行cat /etc/shadow命令查看shadow文件，操作系统中adm、lp、sync、shutdown、halt、mail、uucp、operator、games、gopher等账户均为nologin状态，存在默认账户root；2）执行more /etc/ssh/sshd\_config命令，查看“PermitRootLogin”参数设置为“yes”，即允许root远程登录；3）经访谈，root用户需通过公私钥方式进行身份鉴别。 |
| 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； | 1）执行cat /etc/shadow命令查看shadow文件，发现操作系统存在root、ysup、yops、yluser等在用账户，不存在多余的、过期账户；2）存在多个堡垒机账户登录操作系统时共用一个账户的情况。 |
| 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； | root账户具有系统所有权限，未实现管理用户的权限分离。 |
| e）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； | 经访谈，由系统管理员root配置访问控制策略，如：/etc/passwd，/etc/profile宿主为root、权限设置为644，audit文件为700、message文件为600，其他文件权限为750，实现用户对文件的权限控制。 |
| f）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； | 由管理用户进行用户访问权限分配进行设置，依据访问控制策略,对各类文件进行访问，重要文件和目录权限均在合理范围内，用户可根据文件不同的权限进行操作。 |
| g）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。 | 执 行more /etc/selinux/config 命令，查看config文件显示 SELINUX参数为 DISABLED，即未开启强制访问控制模式。 |
| 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）执行ps -ef|grep rsyslog和ps -ef|grep auditd命令，显示rsyslog和auditd进程正在运行；2）more /etc/audit/audit.rules，显示审计内容包括：\*.info、authriv.\*、mail.\*、cron.\*、\*.emerg、uucp、news.crit、local7.\*等事件。 |
| 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； | 执行tail -20 /var/log/audit/audit.log命令，查看近20条审计日志，内容包括：时间、对象、路径、用户ID、相关的系统调用、用户执行命令等。 |
| 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）通过访问权限对审计记录进行保护，日志文件/var/log/messages、/var/log/secure、/var/log/audit/audit.log访问 权限均为600；2）审计记录本地保存，且实时备份至360本地安全大脑，保存时间满足180天以上。 |
| d）应对审计进程进行保护，防止未经授权的中断。 | 执行service auditd status命令，系统开启auditd审计保护进程，审计进程由root用户维护，经现场使用yluser用户通过service auditd stop命令尝试中断审计进程，无法将审计进程单独中断。 |
| 入侵防范 | a）应遵循最小安装的原则，仅安装需要的组件和应用程序； | 1）系统安装遵循最小化安装原则；2）执行yum list installed命令查看操作系统已安装的程序包，存在Java、SSH、天眼云镜agent等应用程序或组件，不存在与业务系统无关的组件和应用程序。 |
| b）应关闭不需要的系统服务、默认共享和高危端口； | 1）执行systemctl list-unit-files 命令，系统已关闭FTP、Telnet 等高危网络服务；2）执行netstat -pantu命令，系统关闭了135、445等高危端口，仅开启了22、8080等端口。 |
| c）应通过设定终端接入方式或网络地址范围对通过网络进行管理的管理终端进行限制； | 经核查，1）通过配置安全组策略限制仅允许通过堡垒机管理服务器；2）经核查防火墙中访问控制策略，具备堡垒机地址-服务器管理网段（10.33.0.0）的访问控制策略。 |
| d）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； | 根据GB∕T 28448-2019 《信息安全技术 网络安全等级保护测评要求》测评对象范围描述，服务器无该项要求，故判为“不适用”。 |
| e）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； | 1）经过漏洞扫描，服务器不存在高危安全漏洞；2）执行rpm -qa grep patch命令，查看系统补丁已更新至最新。 |
| f）应能够检测到对重要节点进行入侵的行为，并在发生严重入侵事件时提供报警。 | 经核查，服务器上安装有青藤云天眼云镜，对主机入侵行为进行检测，发现严重安全事件时通过钉钉告警。 |
| 恶意代码防范 | a）应采用免受恶意代码攻击的技术措施或主动免疫可信验证机制及时识别入侵和病毒行为，并将其有效阻断。 | 经核查，服务器上安装有青藤云天眼云镜，对主机恶意代码进行检测、清除，每天凌晨自动更新恶意代码特征库，经核查，具备恶意代码特征库更新记录。 |
| 可信验证 | a）可基于可信根对计算设备的系统引导程序、系统程序、重要配置参数和应用程序等进行可信验证，并在应用程序的关键执行环节进行动态可信验证，在检测到其可信性受到破坏后进行报警，并将验证结果形成审计记录送至安全管理中心。 | 未采用技术措施对计算设备的系统引导程序、系统程序、重要配置参数和通信应用程序等进行可信验证。 |
| 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； | 采用SSH协议连接操作系统，保证了鉴别信息以及管理数据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。 | 操作系统中对重要鉴别信息通过自身的加密及校验（SHA256），保证数据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； | 采用SSH协议连接操作系统，保证了鉴别信息以及管理数据在传输过程中的保密性。 |
| b）应采用密码技术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个人信息等。 | 通过系统自带的加密模块保证鉴别数据在存储过程中的保密性。 |
| 数据备份恢复 | a）应提供重要数据的本地数据备份与恢复功能； | 经核查，通过脚本每周将配置文件、代码仓库等数据备份至备份服务器中，依据需要验证备份数据的有效性。 |
| b）应提供异地实时备份功能，利用通信网络将重要数据实时备份至备份场地； | 系统无异地备份机制。 |
| c）应提供重要数据处理系统的热冗余，保证系统的高可用性。 | 服务器采用K8S容器部署，保证系统的高可用性。 |
| 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； | 操作系统提供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功能。 |
| 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。 | 操作系统提供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的功能。 |

4.1.3.37. 应用服务器91

|  |  |  |
| --- | --- | --- |
| **安全控制点** | **测评指标** | **结果记录** |
| 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）操作系统时采用用户名+SSHKey公私钥进行身份鉴别鉴别信息具有复杂度要求；2）执行cat /etc/shadow命令，查看shadow文件系统内用户身份标识唯一，不存在同名用户，且不存在空口令账号；3）经访谈，SSHKey公私钥每半年进行更换；4）查看sshd\_config配置文件中配置PasswordAuthentication no，拒绝使用密码方式进行身份鉴别。 |
| 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； | 操作系统采用用户名+SSHKey公私钥进行身份鉴别，可以防止鉴别信息被暴力破解；但未配置用户连接超时退出策略。 |
| 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； | 1）经核查，管理人员采用SSH协议连接操作系统；2）执行netatat –tpln| grep 23命令查看操作系统远程管理端口，不存在Telnet端口，防止鉴别信息在网络传输过程中的被窃听。 |
| 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。 | 未采用两种或两种以上组合的鉴别技术对用户进行身份鉴别。 |
| 访问控制 | a）应对登录的用户分配账户和权限； | 1）经访谈，通过root账户为登录的用户创建账户、分配权限；2）执行ls -l命令查看关键文件权限，均已为账户分配了相应权限，相关文件权限设置为/etc/shadow：000、/etc/passwd：644、/etc/group：644、/etc/profile：644、/etc/crontab：644、/ etc/securetty：600、/etc/ssh/sshd\_config：600。 |
| b）应重命名或删除默认账户，修改默认账户的默认口令； | 1）执行cat /etc/shadow命令查看shadow文件，操作系统中adm、lp、sync、shutdown、halt、mail、uucp、operator、games、gopher等账户均为nologin状态，存在默认账户root；2）执行more /etc/ssh/sshd\_config命令，查看“PermitRootLogin”参数设置为“yes”，即允许root远程登录；3）经访谈，root用户需通过公私钥方式进行身份鉴别。 |
| 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； | 1）执行cat /etc/shadow命令查看shadow文件，发现操作系统存在root、ysup、yops、yluser等在用账户，不存在多余的、过期账户；2）存在多个堡垒机账户登录操作系统时共用一个账户的情况。 |
| 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； | root账户具有系统所有权限，未实现管理用户的权限分离。 |
| e）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； | 经访谈，由系统管理员root配置访问控制策略，如：/etc/passwd，/etc/profile宿主为root、权限设置为644，audit文件为700、message文件为600，其他文件权限为750，实现用户对文件的权限控制。 |
| f）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； | 由管理用户进行用户访问权限分配进行设置，依据访问控制策略,对各类文件进行访问，重要文件和目录权限均在合理范围内，用户可根据文件不同的权限进行操作。 |
| g）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。 | 执 行more /etc/selinux/config 命令，查看config文件显示 SELINUX参数为 DISABLED，即未开启强制访问控制模式。 |
| 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）执行ps -ef|grep rsyslog和ps -ef|grep auditd命令，显示rsyslog和auditd进程正在运行；2）more /etc/audit/audit.rules，显示审计内容包括：\*.info、authriv.\*、mail.\*、cron.\*、\*.emerg、uucp、news.crit、local7.\*等事件。 |
| 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； | 执行tail -20 /var/log/audit/audit.log命令，查看近20条审计日志，内容包括：时间、对象、路径、用户ID、相关的系统调用、用户执行命令等。 |
| 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）通过访问权限对审计记录进行保护，日志文件/var/log/messages、/var/log/secure、/var/log/audit/audit.log访问 权限均为600；2）审计记录本地保存，且实时备份至360本地安全大脑，保存时间满足180天以上。 |
| d）应对审计进程进行保护，防止未经授权的中断。 | 执行service auditd status命令，系统开启auditd审计保护进程，审计进程由root用户维护，经现场使用yluser用户通过service auditd stop命令尝试中断审计进程，无法将审计进程单独中断。 |
| 入侵防范 | a）应遵循最小安装的原则，仅安装需要的组件和应用程序； | 1）系统安装遵循最小化安装原则；2）执行yum list installed命令查看操作系统已安装的程序包，存在Java、SSH、天眼云镜agent等应用程序或组件，不存在与业务系统无关的组件和应用程序。 |
| b）应关闭不需要的系统服务、默认共享和高危端口； | 1）执行systemctl list-unit-files 命令，系统已关闭FTP、Telnet 等高危网络服务；2）执行netstat -pantu命令，系统关闭了135、445等高危端口，仅开启了22、8080等端口。 |
| c）应通过设定终端接入方式或网络地址范围对通过网络进行管理的管理终端进行限制； | 经核查，1）通过配置安全组策略限制仅允许通过堡垒机管理服务器；2）经核查防火墙中访问控制策略，具备堡垒机地址-服务器管理网段（10.33.0.0）的访问控制策略。 |
| d）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； | 根据GB∕T 28448-2019 《信息安全技术 网络安全等级保护测评要求》测评对象范围描述，服务器无该项要求，故判为“不适用”。 |
| e）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； | 1）经过漏洞扫描，服务器不存在高危安全漏洞；2）执行rpm -qa grep patch命令，查看系统补丁已更新至最新。 |
| f）应能够检测到对重要节点进行入侵的行为，并在发生严重入侵事件时提供报警。 | 经核查，服务器上安装有青藤云天眼云镜，对主机入侵行为进行检测，发现严重安全事件时通过钉钉告警。 |
| 恶意代码防范 | a）应采用免受恶意代码攻击的技术措施或主动免疫可信验证机制及时识别入侵和病毒行为，并将其有效阻断。 | 经核查，服务器上安装有青藤云天眼云镜，对主机恶意代码进行检测、清除，每天凌晨自动更新恶意代码特征库，经核查，具备恶意代码特征库更新记录。 |
| 可信验证 | a）可基于可信根对计算设备的系统引导程序、系统程序、重要配置参数和应用程序等进行可信验证，并在应用程序的关键执行环节进行动态可信验证，在检测到其可信性受到破坏后进行报警，并将验证结果形成审计记录送至安全管理中心。 | 未采用技术措施对计算设备的系统引导程序、系统程序、重要配置参数和通信应用程序等进行可信验证。 |
| 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； | 采用SSH协议连接操作系统，保证了鉴别信息以及管理数据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。 | 操作系统中对重要鉴别信息通过自身的加密及校验（SHA256），保证数据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； | 采用SSH协议连接操作系统，保证了鉴别信息以及管理数据在传输过程中的保密性。 |
| b）应采用密码技术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个人信息等。 | 通过系统自带的加密模块保证鉴别数据在存储过程中的保密性。 |
| 数据备份恢复 | a）应提供重要数据的本地数据备份与恢复功能； | 经核查，通过脚本每周将配置文件、代码仓库等数据备份至备份服务器中，依据需要验证备份数据的有效性。 |
| b）应提供异地实时备份功能，利用通信网络将重要数据实时备份至备份场地； | 系统无异地备份机制。 |
| c）应提供重要数据处理系统的热冗余，保证系统的高可用性。 | 服务器采用K8S容器部署，保证系统的高可用性。 |
| 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； | 操作系统提供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功能。 |
| 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。 | 操作系统提供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的功能。 |

4.1.3.38. 应用服务器94

|  |  |  |
| --- | --- | --- |
| **安全控制点** | **测评指标** | **结果记录** |
| 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）操作系统时采用用户名+SSHKey公私钥进行身份鉴别鉴别信息具有复杂度要求；2）执行cat /etc/shadow命令，查看shadow文件系统内用户身份标识唯一，不存在同名用户，且不存在空口令账号；3）经访谈，SSHKey公私钥每半年进行更换；4）查看sshd\_config配置文件中配置PasswordAuthentication no，拒绝使用密码方式进行身份鉴别。 |
| 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； | 操作系统采用用户名+SSHKey公私钥进行身份鉴别，可以防止鉴别信息被暴力破解；但未配置用户连接超时退出策略。 |
| 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； | 1）经核查，管理人员采用SSH协议连接操作系统；2）执行netatat –tpln| grep 23命令查看操作系统远程管理端口，不存在Telnet端口，防止鉴别信息在网络传输过程中的被窃听。 |
| 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。 | 未采用两种或两种以上组合的鉴别技术对用户进行身份鉴别。 |
| 访问控制 | a）应对登录的用户分配账户和权限； | 1）经访谈，通过root账户为登录的用户创建账户、分配权限；2）执行ls -l命令查看关键文件权限，均已为账户分配了相应权限，相关文件权限设置为/etc/shadow：000、/etc/passwd：644、/etc/group：644、/etc/profile：644、/etc/crontab：644、/ etc/securetty：600、/etc/ssh/sshd\_config：600。 |
| b）应重命名或删除默认账户，修改默认账户的默认口令； | 1）执行cat /etc/shadow命令查看shadow文件，操作系统中adm、lp、sync、shutdown、halt、mail、uucp、operator、games、gopher等账户均为nologin状态，存在默认账户root；2）执行more /etc/ssh/sshd\_config命令，查看“PermitRootLogin”参数设置为“yes”，即允许root远程登录；3）经访谈，root用户需通过公私钥方式进行身份鉴别。 |
| 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； | 1）执行cat /etc/shadow命令查看shadow文件，发现操作系统存在root、ysup、yops、yluser等在用账户，不存在多余的、过期账户；2）存在多个堡垒机账户登录操作系统时共用一个账户的情况。 |
| 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； | root账户具有系统所有权限，未实现管理用户的权限分离。 |
| e）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； | 经访谈，由系统管理员root配置访问控制策略，如：/etc/passwd，/etc/profile宿主为root、权限设置为644，audit文件为700、message文件为600，其他文件权限为750，实现用户对文件的权限控制。 |
| f）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； | 由管理用户进行用户访问权限分配进行设置，依据访问控制策略,对各类文件进行访问，重要文件和目录权限均在合理范围内，用户可根据文件不同的权限进行操作。 |
| g）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。 | 执 行more /etc/selinux/config 命令，查看config文件显示 SELINUX参数为 DISABLED，即未开启强制访问控制模式。 |
| 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）执行ps -ef|grep rsyslog和ps -ef|grep auditd命令，显示rsyslog和auditd进程正在运行；2）more /etc/audit/audit.rules，显示审计内容包括：\*.info、authriv.\*、mail.\*、cron.\*、\*.emerg、uucp、news.crit、local7.\*等事件。 |
| 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； | 执行tail -20 /var/log/audit/audit.log命令，查看近20条审计日志，内容包括：时间、对象、路径、用户ID、相关的系统调用、用户执行命令等。 |
| 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）通过访问权限对审计记录进行保护，日志文件/var/log/messages、/var/log/secure、/var/log/audit/audit.log访问 权限均为600；2）审计记录本地保存，且实时备份至360本地安全大脑，保存时间满足180天以上。 |
| d）应对审计进程进行保护，防止未经授权的中断。 | 执行service auditd status命令，系统开启auditd审计保护进程，审计进程由root用户维护，经现场使用yluser用户通过service auditd stop命令尝试中断审计进程，无法将审计进程单独中断。 |
| 入侵防范 | a）应遵循最小安装的原则，仅安装需要的组件和应用程序； | 1）系统安装遵循最小化安装原则；2）执行yum list installed命令查看操作系统已安装的程序包，存在Java、SSH、天眼云镜agent等应用程序或组件，不存在与业务系统无关的组件和应用程序。 |
| b）应关闭不需要的系统服务、默认共享和高危端口； | 1）执行systemctl list-unit-files 命令，系统已关闭FTP、Telnet 等高危网络服务；2）执行netstat -pantu命令，系统关闭了135、445等高危端口，仅开启了22、8080等端口。 |
| c）应通过设定终端接入方式或网络地址范围对通过网络进行管理的管理终端进行限制； | 经核查，1）通过配置安全组策略限制仅允许通过堡垒机管理服务器；2）经核查防火墙中访问控制策略，具备堡垒机地址-服务器管理网段（10.33.0.0）的访问控制策略。 |
| d）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； | 根据GB∕T 28448-2019 《信息安全技术 网络安全等级保护测评要求》测评对象范围描述，服务器无该项要求，故判为“不适用”。 |
| e）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； | 1）经过漏洞扫描，服务器不存在高危安全漏洞；2）执行rpm -qa grep patch命令，查看系统补丁已更新至最新。 |
| f）应能够检测到对重要节点进行入侵的行为，并在发生严重入侵事件时提供报警。 | 经核查，服务器上安装有青藤云天眼云镜，对主机入侵行为进行检测，发现严重安全事件时通过钉钉告警。 |
| 恶意代码防范 | a）应采用免受恶意代码攻击的技术措施或主动免疫可信验证机制及时识别入侵和病毒行为，并将其有效阻断。 | 经核查，服务器上安装有青藤云天眼云镜，对主机恶意代码进行检测、清除，每天凌晨自动更新恶意代码特征库，经核查，具备恶意代码特征库更新记录。 |
| 可信验证 | a）可基于可信根对计算设备的系统引导程序、系统程序、重要配置参数和应用程序等进行可信验证，并在应用程序的关键执行环节进行动态可信验证，在检测到其可信性受到破坏后进行报警，并将验证结果形成审计记录送至安全管理中心。 | 未采用技术措施对计算设备的系统引导程序、系统程序、重要配置参数和通信应用程序等进行可信验证。 |
| 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； | 采用SSH协议连接操作系统，保证了鉴别信息以及管理数据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。 | 操作系统中对重要鉴别信息通过自身的加密及校验（SHA256），保证数据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； | 采用SSH协议连接操作系统，保证了鉴别信息以及管理数据在传输过程中的保密性。 |
| b）应采用密码技术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个人信息等。 | 通过系统自带的加密模块保证鉴别数据在存储过程中的保密性。 |
| 数据备份恢复 | a）应提供重要数据的本地数据备份与恢复功能； | 经核查，通过脚本每周将配置文件、代码仓库等数据备份至备份服务器中，依据需要验证备份数据的有效性。 |
| b）应提供异地实时备份功能，利用通信网络将重要数据实时备份至备份场地； | 系统无异地备份机制。 |
| c）应提供重要数据处理系统的热冗余，保证系统的高可用性。 | 服务器采用K8S容器部署，保证系统的高可用性。 |
| 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； | 操作系统提供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功能。 |
| 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。 | 操作系统提供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的功能。 |

4.1.3.39. 应用服务器98

|  |  |  |
| --- | --- | --- |
| **安全控制点** | **测评指标** | **结果记录** |
| 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）操作系统时采用用户名+SSHKey公私钥进行身份鉴别鉴别信息具有复杂度要求；2）执行cat /etc/shadow命令，查看shadow文件系统内用户身份标识唯一，不存在同名用户，且不存在空口令账号；3）经访谈，SSHKey公私钥每半年进行更换；4）查看sshd\_config配置文件中配置PasswordAuthentication no，拒绝使用密码方式进行身份鉴别。 |
| 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； | 操作系统采用用户名+SSHKey公私钥进行身份鉴别，可以防止鉴别信息被暴力破解；但未配置用户连接超时退出策略。 |
| 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； | 1）经核查，管理人员采用SSH协议连接操作系统；2）执行netatat –tpln| grep 23命令查看操作系统远程管理端口，不存在Telnet端口，防止鉴别信息在网络传输过程中的被窃听。 |
| 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。 | 未采用两种或两种以上组合的鉴别技术对用户进行身份鉴别。 |
| 访问控制 | a）应对登录的用户分配账户和权限； | 1）经访谈，通过root账户为登录的用户创建账户、分配权限；2）执行ls -l命令查看关键文件权限，均已为账户分配了相应权限，相关文件权限设置为/etc/shadow：000、/etc/passwd：644、/etc/group：644、/etc/profile：644、/etc/crontab：644、/ etc/securetty：600、/etc/ssh/sshd\_config：600。 |
| b）应重命名或删除默认账户，修改默认账户的默认口令； | 1）执行cat /etc/shadow命令查看shadow文件，操作系统中adm、lp、sync、shutdown、halt、mail、uucp、operator、games、gopher等账户均为nologin状态，存在默认账户root；2）执行more /etc/ssh/sshd\_config命令，查看“PermitRootLogin”参数设置为“yes”，即允许root远程登录；3）经访谈，root用户需通过公私钥方式进行身份鉴别。 |
| 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； | 1）执行cat /etc/shadow命令查看shadow文件，发现操作系统存在root、ysup、yops、yluser等在用账户，不存在多余的、过期账户；2）存在多个堡垒机账户登录操作系统时共用一个账户的情况。 |
| 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； | root账户具有系统所有权限，未实现管理用户的权限分离。 |
| e）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； | 经访谈，由系统管理员root配置访问控制策略，如：/etc/passwd，/etc/profile宿主为root、权限设置为644，audit文件为700、message文件为600，其他文件权限为750，实现用户对文件的权限控制。 |
| f）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； | 由管理用户进行用户访问权限分配进行设置，依据访问控制策略,对各类文件进行访问，重要文件和目录权限均在合理范围内，用户可根据文件不同的权限进行操作。 |
| g）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。 | 执 行more /etc/selinux/config 命令，查看config文件显示 SELINUX参数为 DISABLED，即未开启强制访问控制模式。 |
| 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）执行ps -ef|grep rsyslog和ps -ef|grep auditd命令，显示rsyslog和auditd进程正在运行；2）more /etc/audit/audit.rules，显示审计内容包括：\*.info、authriv.\*、mail.\*、cron.\*、\*.emerg、uucp、news.crit、local7.\*等事件。 |
| 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； | 执行tail -20 /var/log/audit/audit.log命令，查看近20条审计日志，内容包括：时间、对象、路径、用户ID、相关的系统调用、用户执行命令等。 |
| 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）通过访问权限对审计记录进行保护，日志文件/var/log/messages、/var/log/secure、/var/log/audit/audit.log访问 权限均为600；2）审计记录本地保存，且实时备份至360本地安全大脑，保存时间满足180天以上。 |
| d）应对审计进程进行保护，防止未经授权的中断。 | 执行service auditd status命令，系统开启auditd审计保护进程，审计进程由root用户维护，经现场使用yluser用户通过service auditd stop命令尝试中断审计进程，无法将审计进程单独中断。 |
| 入侵防范 | a）应遵循最小安装的原则，仅安装需要的组件和应用程序； | 1）系统安装遵循最小化安装原则；2）执行yum list installed命令查看操作系统已安装的程序包，存在Java、SSH、天眼云镜agent等应用程序或组件，不存在与业务系统无关的组件和应用程序。 |
| b）应关闭不需要的系统服务、默认共享和高危端口； | 1）执行systemctl list-unit-files 命令，系统已关闭FTP、Telnet 等高危网络服务；2）执行netstat -pantu命令，系统关闭了135、445等高危端口，仅开启了22、8080等端口。 |
| c）应通过设定终端接入方式或网络地址范围对通过网络进行管理的管理终端进行限制； | 经核查，1）通过配置安全组策略限制仅允许通过堡垒机管理服务器；2）经核查防火墙中访问控制策略，具备堡垒机地址-服务器管理网段（10.33.0.0）的访问控制策略。 |
| d）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； | 根据GB∕T 28448-2019 《信息安全技术 网络安全等级保护测评要求》测评对象范围描述，服务器无该项要求，故判为“不适用”。 |
| e）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； | 1）经过漏洞扫描，服务器不存在高危安全漏洞；2）执行rpm -qa grep patch命令，查看系统补丁已更新至最新。 |
| f）应能够检测到对重要节点进行入侵的行为，并在发生严重入侵事件时提供报警。 | 经核查，服务器上安装有青藤云天眼云镜，对主机入侵行为进行检测，发现严重安全事件时通过钉钉告警。 |
| 恶意代码防范 | a）应采用免受恶意代码攻击的技术措施或主动免疫可信验证机制及时识别入侵和病毒行为，并将其有效阻断。 | 经核查，服务器上安装有青藤云天眼云镜，对主机恶意代码进行检测、清除，每天凌晨自动更新恶意代码特征库，经核查，具备恶意代码特征库更新记录。 |
| 可信验证 | a）可基于可信根对计算设备的系统引导程序、系统程序、重要配置参数和应用程序等进行可信验证，并在应用程序的关键执行环节进行动态可信验证，在检测到其可信性受到破坏后进行报警，并将验证结果形成审计记录送至安全管理中心。 | 未采用技术措施对计算设备的系统引导程序、系统程序、重要配置参数和通信应用程序等进行可信验证。 |
| 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； | 采用SSH协议连接操作系统，保证了鉴别信息以及管理数据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。 | 操作系统中对重要鉴别信息通过自身的加密及校验（SHA256），保证数据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； | 采用SSH协议连接操作系统，保证了鉴别信息以及管理数据在传输过程中的保密性。 |
| b）应采用密码技术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个人信息等。 | 通过系统自带的加密模块保证鉴别数据在存储过程中的保密性。 |
| 数据备份恢复 | a）应提供重要数据的本地数据备份与恢复功能； | 经核查，通过脚本每周将配置文件、代码仓库等数据备份至备份服务器中，依据需要验证备份数据的有效性。 |
| b）应提供异地实时备份功能，利用通信网络将重要数据实时备份至备份场地； | 系统无异地备份机制。 |
| c）应提供重要数据处理系统的热冗余，保证系统的高可用性。 | 服务器采用K8S容器部署，保证系统的高可用性。 |
| 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； | 操作系统提供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功能。 |
| 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。 | 操作系统提供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的功能。 |

4.1.3.40. 应用服务器99

|  |  |  |
| --- | --- | --- |
| **安全控制点** | **测评指标** | **结果记录** |
| 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）操作系统时采用用户名+SSHKey公私钥进行身份鉴别鉴别信息具有复杂度要求；2）执行cat /etc/shadow命令，查看shadow文件系统内用户身份标识唯一，不存在同名用户，且不存在空口令账号；3）经访谈，SSHKey公私钥每半年进行更换；4）查看sshd\_config配置文件中配置PasswordAuthentication no，拒绝使用密码方式进行身份鉴别。 |
| 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； | 操作系统采用用户名+SSHKey公私钥进行身份鉴别，可以防止鉴别信息被暴力破解；但未配置用户连接超时退出策略。 |
| 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； | 1）经核查，管理人员采用SSH协议连接操作系统；2）执行netatat –tpln| grep 23命令查看操作系统远程管理端口，不存在Telnet端口，防止鉴别信息在网络传输过程中的被窃听。 |
| 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。 | 未采用两种或两种以上组合的鉴别技术对用户进行身份鉴别。 |
| 访问控制 | a）应对登录的用户分配账户和权限； | 1）经访谈，通过root账户为登录的用户创建账户、分配权限；2）执行ls -l命令查看关键文件权限，均已为账户分配了相应权限，相关文件权限设置为/etc/shadow：000、/etc/passwd：644、/etc/group：644、/etc/profile：644、/etc/crontab：644、/ etc/securetty：600、/etc/ssh/sshd\_config：600。 |
| b）应重命名或删除默认账户，修改默认账户的默认口令； | 1）执行cat /etc/shadow命令查看shadow文件，操作系统中adm、lp、sync、shutdown、halt、mail、uucp、operator、games、gopher等账户均为nologin状态，存在默认账户root；2）执行more /etc/ssh/sshd\_config命令，查看“PermitRootLogin”参数设置为“yes”，即允许root远程登录；3）经访谈，root用户需通过公私钥方式进行身份鉴别。 |
| 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； | 1）执行cat /etc/shadow命令查看shadow文件，发现操作系统存在root、ysup、yops、yluser等在用账户，不存在多余的、过期账户；2）存在多个堡垒机账户登录操作系统时共用一个账户的情况。 |
| 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； | root账户具有系统所有权限，未实现管理用户的权限分离。 |
| e）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； | 经访谈，由系统管理员root配置访问控制策略，如：/etc/passwd，/etc/profile宿主为root、权限设置为644，audit文件为700、message文件为600，其他文件权限为750，实现用户对文件的权限控制。 |
| f）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； | 由管理用户进行用户访问权限分配进行设置，依据访问控制策略,对各类文件进行访问，重要文件和目录权限均在合理范围内，用户可根据文件不同的权限进行操作。 |
| g）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。 | 执 行more /etc/selinux/config 命令，查看config文件显示 SELINUX参数为 DISABLED，即未开启强制访问控制模式。 |
| 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）执行ps -ef|grep rsyslog和ps -ef|grep auditd命令，显示rsyslog和auditd进程正在运行；2）more /etc/audit/audit.rules，显示审计内容包括：\*.info、authriv.\*、mail.\*、cron.\*、\*.emerg、uucp、news.crit、local7.\*等事件。 |
| 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； | 执行tail -20 /var/log/audit/audit.log命令，查看近20条审计日志，内容包括：时间、对象、路径、用户ID、相关的系统调用、用户执行命令等。 |
| 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）通过访问权限对审计记录进行保护，日志文件/var/log/messages、/var/log/secure、/var/log/audit/audit.log访问 权限均为600；2）审计记录本地保存，且实时备份至360本地安全大脑，保存时间满足180天以上。 |
| d）应对审计进程进行保护，防止未经授权的中断。 | 执行service auditd status命令，系统开启auditd审计保护进程，审计进程由root用户维护，经现场使用yluser用户通过service auditd stop命令尝试中断审计进程，无法将审计进程单独中断。 |
| 入侵防范 | a）应遵循最小安装的原则，仅安装需要的组件和应用程序； | 1）系统安装遵循最小化安装原则；2）执行yum list installed命令查看操作系统已安装的程序包，存在Java、SSH、天眼云镜agent等应用程序或组件，不存在与业务系统无关的组件和应用程序。 |
| b）应关闭不需要的系统服务、默认共享和高危端口； | 1）执行systemctl list-unit-files 命令，系统已关闭FTP、Telnet 等高危网络服务；2）执行netstat -pantu命令，系统关闭了135、445等高危端口，仅开启了22、8080等端口。 |
| c）应通过设定终端接入方式或网络地址范围对通过网络进行管理的管理终端进行限制； | 经核查，1）通过配置安全组策略限制仅允许通过堡垒机管理服务器；2）经核查防火墙中访问控制策略，具备堡垒机地址-服务器管理网段（10.33.0.0）的访问控制策略。 |
| d）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； | 根据GB∕T 28448-2019 《信息安全技术 网络安全等级保护测评要求》测评对象范围描述，服务器无该项要求，故判为“不适用”。 |
| e）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； | 1）经过漏洞扫描，服务器不存在高危安全漏洞；2）执行rpm -qa grep patch命令，查看系统补丁已更新至最新。 |
| f）应能够检测到对重要节点进行入侵的行为，并在发生严重入侵事件时提供报警。 | 经核查，服务器上安装有青藤云天眼云镜，对主机入侵行为进行检测，发现严重安全事件时通过钉钉告警。 |
| 恶意代码防范 | a）应采用免受恶意代码攻击的技术措施或主动免疫可信验证机制及时识别入侵和病毒行为，并将其有效阻断。 | 经核查，服务器上安装有青藤云天眼云镜，对主机恶意代码进行检测、清除，每天凌晨自动更新恶意代码特征库，经核查，具备恶意代码特征库更新记录。 |
| 可信验证 | a）可基于可信根对计算设备的系统引导程序、系统程序、重要配置参数和应用程序等进行可信验证，并在应用程序的关键执行环节进行动态可信验证，在检测到其可信性受到破坏后进行报警，并将验证结果形成审计记录送至安全管理中心。 | 未采用技术措施对计算设备的系统引导程序、系统程序、重要配置参数和通信应用程序等进行可信验证。 |
| 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； | 采用SSH协议连接操作系统，保证了鉴别信息以及管理数据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。 | 操作系统中对重要鉴别信息通过自身的加密及校验（SHA256），保证数据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； | 采用SSH协议连接操作系统，保证了鉴别信息以及管理数据在传输过程中的保密性。 |
| b）应采用密码技术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个人信息等。 | 通过系统自带的加密模块保证鉴别数据在存储过程中的保密性。 |
| 数据备份恢复 | a）应提供重要数据的本地数据备份与恢复功能； | 经核查，通过脚本每周将配置文件、代码仓库等数据备份至备份服务器中，依据需要验证备份数据的有效性。 |
| b）应提供异地实时备份功能，利用通信网络将重要数据实时备份至备份场地； | 系统无异地备份机制。 |
| c）应提供重要数据处理系统的热冗余，保证系统的高可用性。 | 服务器采用K8S容器部署，保证系统的高可用性。 |
| 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； | 操作系统提供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功能。 |
| 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。 | 操作系统提供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的功能。 |

4.1.3.41. 应用服务器100

|  |  |  |
| --- | --- | --- |
| **安全控制点** | **测评指标** | **结果记录** |
| 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）操作系统时采用用户名+SSHKey公私钥进行身份鉴别鉴别信息具有复杂度要求；2）执行cat /etc/shadow命令，查看shadow文件系统内用户身份标识唯一，不存在同名用户，且不存在空口令账号；3）经访谈，SSHKey公私钥每半年进行更换；4）查看sshd\_config配置文件中配置PasswordAuthentication no，拒绝使用密码方式进行身份鉴别。 |
| 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； | 操作系统采用用户名+SSHKey公私钥进行身份鉴别，可以防止鉴别信息被暴力破解；但未配置用户连接超时退出策略。 |
| 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； | 1）经核查，管理人员采用SSH协议连接操作系统；2）执行netatat –tpln| grep 23命令查看操作系统远程管理端口，不存在Telnet端口，防止鉴别信息在网络传输过程中的被窃听。 |
| 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。 | 未采用两种或两种以上组合的鉴别技术对用户进行身份鉴别。 |
| 访问控制 | a）应对登录的用户分配账户和权限； | 1）经访谈，通过root账户为登录的用户创建账户、分配权限；2）执行ls -l命令查看关键文件权限，均已为账户分配了相应权限，相关文件权限设置为/etc/shadow：000、/etc/passwd：644、/etc/group：644、/etc/profile：644、/etc/crontab：644、/ etc/securetty：600、/etc/ssh/sshd\_config：600。 |
| b）应重命名或删除默认账户，修改默认账户的默认口令； | 1）执行cat /etc/shadow命令查看shadow文件，操作系统中adm、lp、sync、shutdown、halt、mail、uucp、operator、games、gopher等账户均为nologin状态，存在默认账户root；2）执行more /etc/ssh/sshd\_config命令，查看“PermitRootLogin”参数设置为“yes”，即允许root远程登录；3）经访谈，root用户需通过公私钥方式进行身份鉴别。 |
| 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； | 1）执行cat /etc/shadow命令查看shadow文件，发现操作系统存在root、ysup、yops、yluser等在用账户，不存在多余的、过期账户；2）存在多个堡垒机账户登录操作系统时共用一个账户的情况。 |
| 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； | root账户具有系统所有权限，未实现管理用户的权限分离。 |
| e）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； | 经访谈，由系统管理员root配置访问控制策略，如：/etc/passwd，/etc/profile宿主为root、权限设置为644，audit文件为700、message文件为600，其他文件权限为750，实现用户对文件的权限控制。 |
| f）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； | 由管理用户进行用户访问权限分配进行设置，依据访问控制策略,对各类文件进行访问，重要文件和目录权限均在合理范围内，用户可根据文件不同的权限进行操作。 |
| g）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。 | 执 行more /etc/selinux/config 命令，查看config文件显示 SELINUX参数为 DISABLED，即未开启强制访问控制模式。 |
| 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）执行ps -ef|grep rsyslog和ps -ef|grep auditd命令，显示rsyslog和auditd进程正在运行；2）more /etc/audit/audit.rules，显示审计内容包括：\*.info、authriv.\*、mail.\*、cron.\*、\*.emerg、uucp、news.crit、local7.\*等事件。 |
| 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； | 执行tail -20 /var/log/audit/audit.log命令，查看近20条审计日志，内容包括：时间、对象、路径、用户ID、相关的系统调用、用户执行命令等。 |
| 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）通过访问权限对审计记录进行保护，日志文件/var/log/messages、/var/log/secure、/var/log/audit/audit.log访问 权限均为600；2）审计记录本地保存，且实时备份至360本地安全大脑，保存时间满足180天以上。 |
| d）应对审计进程进行保护，防止未经授权的中断。 | 执行service auditd status命令，系统开启auditd审计保护进程，审计进程由root用户维护，经现场使用yluser用户通过service auditd stop命令尝试中断审计进程，无法将审计进程单独中断。 |
| 入侵防范 | a）应遵循最小安装的原则，仅安装需要的组件和应用程序； | 1）系统安装遵循最小化安装原则；2）执行yum list installed命令查看操作系统已安装的程序包，存在Java、SSH、天眼云镜agent等应用程序或组件，不存在与业务系统无关的组件和应用程序。 |
| b）应关闭不需要的系统服务、默认共享和高危端口； | 1）执行systemctl list-unit-files 命令，系统已关闭FTP、Telnet 等高危网络服务；2）执行netstat -pantu命令，系统关闭了135、445等高危端口，仅开启了22、8080等端口。 |
| c）应通过设定终端接入方式或网络地址范围对通过网络进行管理的管理终端进行限制； | 经核查，1）通过配置安全组策略限制仅允许通过堡垒机管理服务器；2）经核查防火墙中访问控制策略，具备堡垒机地址-服务器管理网段（10.33.0.0）的访问控制策略。 |
| d）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； | 根据GB∕T 28448-2019 《信息安全技术 网络安全等级保护测评要求》测评对象范围描述，服务器无该项要求，故判为“不适用”。 |
| e）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； | 1）经过漏洞扫描，服务器不存在高危安全漏洞；2）执行rpm -qa grep patch命令，查看系统补丁已更新至最新。 |
| f）应能够检测到对重要节点进行入侵的行为，并在发生严重入侵事件时提供报警。 | 经核查，服务器上安装有青藤云天眼云镜，对主机入侵行为进行检测，发现严重安全事件时通过钉钉告警。 |
| 恶意代码防范 | a）应采用免受恶意代码攻击的技术措施或主动免疫可信验证机制及时识别入侵和病毒行为，并将其有效阻断。 | 经核查，服务器上安装有青藤云天眼云镜，对主机恶意代码进行检测、清除，每天凌晨自动更新恶意代码特征库，经核查，具备恶意代码特征库更新记录。 |
| 可信验证 | a）可基于可信根对计算设备的系统引导程序、系统程序、重要配置参数和应用程序等进行可信验证，并在应用程序的关键执行环节进行动态可信验证，在检测到其可信性受到破坏后进行报警，并将验证结果形成审计记录送至安全管理中心。 | 未采用技术措施对计算设备的系统引导程序、系统程序、重要配置参数和通信应用程序等进行可信验证。 |
| 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； | 采用SSH协议连接操作系统，保证了鉴别信息以及管理数据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。 | 操作系统中对重要鉴别信息通过自身的加密及校验（SHA256），保证数据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； | 采用SSH协议连接操作系统，保证了鉴别信息以及管理数据在传输过程中的保密性。 |
| b）应采用密码技术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个人信息等。 | 通过系统自带的加密模块保证鉴别数据在存储过程中的保密性。 |
| 数据备份恢复 | a）应提供重要数据的本地数据备份与恢复功能； | 经核查，通过脚本每周将配置文件、代码仓库等数据备份至备份服务器中，依据需要验证备份数据的有效性。 |
| b）应提供异地实时备份功能，利用通信网络将重要数据实时备份至备份场地； | 系统无异地备份机制。 |
| c）应提供重要数据处理系统的热冗余，保证系统的高可用性。 | 服务器采用K8S容器部署，保证系统的高可用性。 |
| 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； | 操作系统提供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功能。 |
| 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。 | 操作系统提供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的功能。 |

4.1.3.42. 应用服务器103

|  |  |  |
| --- | --- | --- |
| **安全控制点** | **测评指标** | **结果记录** |
| 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）操作系统时采用用户名+SSHKey公私钥进行身份鉴别鉴别信息具有复杂度要求；2）执行cat /etc/shadow命令，查看shadow文件系统内用户身份标识唯一，不存在同名用户，且不存在空口令账号；3）经访谈，SSHKey公私钥每半年进行更换；4）查看sshd\_config配置文件中配置PasswordAuthentication no，拒绝使用密码方式进行身份鉴别。 |
| 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； | 操作系统采用用户名+SSHKey公私钥进行身份鉴别，可以防止鉴别信息被暴力破解；但未配置用户连接超时退出策略。 |
| 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； | 1）经核查，管理人员采用SSH协议连接操作系统；2）执行netatat –tpln| grep 23命令查看操作系统远程管理端口，不存在Telnet端口，防止鉴别信息在网络传输过程中的被窃听。 |
| 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。 | 未采用两种或两种以上组合的鉴别技术对用户进行身份鉴别。 |
| 访问控制 | a）应对登录的用户分配账户和权限； | 1）经访谈，通过root账户为登录的用户创建账户、分配权限；2）执行ls -l命令查看关键文件权限，均已为账户分配了相应权限，相关文件权限设置为/etc/shadow：000、/etc/passwd：644、/etc/group：644、/etc/profile：644、/etc/crontab：644、/ etc/securetty：600、/etc/ssh/sshd\_config：600。 |
| b）应重命名或删除默认账户，修改默认账户的默认口令； | 1）执行cat /etc/shadow命令查看shadow文件，操作系统中adm、lp、sync、shutdown、halt、mail、uucp、operator、games、gopher等账户均为nologin状态，存在默认账户root；2）执行more /etc/ssh/sshd\_config命令，查看“PermitRootLogin”参数设置为“yes”，即允许root远程登录；3）经访谈，root用户需通过公私钥方式进行身份鉴别。 |
| 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； | 1）执行cat /etc/shadow命令查看shadow文件，发现操作系统存在root、ysup、yops、yluser等在用账户，不存在多余的、过期账户；2）存在多个堡垒机账户登录操作系统时共用一个账户的情况。 |
| 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； | root账户具有系统所有权限，未实现管理用户的权限分离。 |
| e）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； | 经访谈，由系统管理员root配置访问控制策略，如：/etc/passwd，/etc/profile宿主为root、权限设置为644，audit文件为700、message文件为600，其他文件权限为750，实现用户对文件的权限控制。 |
| f）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； | 由管理用户进行用户访问权限分配进行设置，依据访问控制策略,对各类文件进行访问，重要文件和目录权限均在合理范围内，用户可根据文件不同的权限进行操作。 |
| g）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。 | 执 行more /etc/selinux/config 命令，查看config文件显示 SELINUX参数为 DISABLED，即未开启强制访问控制模式。 |
| 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）执行ps -ef|grep rsyslog和ps -ef|grep auditd命令，显示rsyslog和auditd进程正在运行；2）more /etc/audit/audit.rules，显示审计内容包括：\*.info、authriv.\*、mail.\*、cron.\*、\*.emerg、uucp、news.crit、local7.\*等事件。 |
| 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； | 执行tail -20 /var/log/audit/audit.log命令，查看近20条审计日志，内容包括：时间、对象、路径、用户ID、相关的系统调用、用户执行命令等。 |
| 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）通过访问权限对审计记录进行保护，日志文件/var/log/messages、/var/log/secure、/var/log/audit/audit.log访问 权限均为600；2）审计记录本地保存，且实时备份至360本地安全大脑，保存时间满足180天以上。 |
| d）应对审计进程进行保护，防止未经授权的中断。 | 执行service auditd status命令，系统开启auditd审计保护进程，审计进程由root用户维护，经现场使用yluser用户通过service auditd stop命令尝试中断审计进程，无法将审计进程单独中断。 |
| 入侵防范 | a）应遵循最小安装的原则，仅安装需要的组件和应用程序； | 1）系统安装遵循最小化安装原则；2）执行yum list installed命令查看操作系统已安装的程序包，存在Java、SSH、天眼云镜agent等应用程序或组件，不存在与业务系统无关的组件和应用程序。 |
| b）应关闭不需要的系统服务、默认共享和高危端口； | 1）执行systemctl list-unit-files 命令，系统已关闭FTP、Telnet 等高危网络服务；2）执行netstat -pantu命令，系统关闭了135、445等高危端口，仅开启了22、8080等端口。 |
| c）应通过设定终端接入方式或网络地址范围对通过网络进行管理的管理终端进行限制； | 经核查，1）通过配置安全组策略限制仅允许通过堡垒机管理服务器；2）经核查防火墙中访问控制策略，具备堡垒机地址-服务器管理网段（10.33.0.0）的访问控制策略。 |
| d）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； | 根据GB∕T 28448-2019 《信息安全技术 网络安全等级保护测评要求》测评对象范围描述，服务器无该项要求，故判为“不适用”。 |
| e）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； | 1）经过漏洞扫描，服务器不存在高危安全漏洞；2）执行rpm -qa grep patch命令，查看系统补丁已更新至最新。 |
| f）应能够检测到对重要节点进行入侵的行为，并在发生严重入侵事件时提供报警。 | 经核查，服务器上安装有青藤云天眼云镜，对主机入侵行为进行检测，发现严重安全事件时通过钉钉告警。 |
| 恶意代码防范 | a）应采用免受恶意代码攻击的技术措施或主动免疫可信验证机制及时识别入侵和病毒行为，并将其有效阻断。 | 经核查，服务器上安装有青藤云天眼云镜，对主机恶意代码进行检测、清除，每天凌晨自动更新恶意代码特征库，经核查，具备恶意代码特征库更新记录。 |
| 可信验证 | a）可基于可信根对计算设备的系统引导程序、系统程序、重要配置参数和应用程序等进行可信验证，并在应用程序的关键执行环节进行动态可信验证，在检测到其可信性受到破坏后进行报警，并将验证结果形成审计记录送至安全管理中心。 | 未采用技术措施对计算设备的系统引导程序、系统程序、重要配置参数和通信应用程序等进行可信验证。 |
| 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； | 采用SSH协议连接操作系统，保证了鉴别信息以及管理数据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。 | 操作系统中对重要鉴别信息通过自身的加密及校验（SHA256），保证数据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； | 采用SSH协议连接操作系统，保证了鉴别信息以及管理数据在传输过程中的保密性。 |
| b）应采用密码技术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个人信息等。 | 通过系统自带的加密模块保证鉴别数据在存储过程中的保密性。 |
| 数据备份恢复 | a）应提供重要数据的本地数据备份与恢复功能； | 经核查，通过脚本每周将配置文件、代码仓库等数据备份至备份服务器中，依据需要验证备份数据的有效性。 |
| b）应提供异地实时备份功能，利用通信网络将重要数据实时备份至备份场地； | 系统无异地备份机制。 |
| c）应提供重要数据处理系统的热冗余，保证系统的高可用性。 | 服务器采用K8S容器部署，保证系统的高可用性。 |
| 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； | 操作系统提供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功能。 |
| 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。 | 操作系统提供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的功能。 |

4.1.3.43. 应用服务器106

|  |  |  |
| --- | --- | --- |
| **安全控制点** | **测评指标** | **结果记录** |
| 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）操作系统时采用用户名+SSHKey公私钥进行身份鉴别鉴别信息具有复杂度要求；2）执行cat /etc/shadow命令，查看shadow文件系统内用户身份标识唯一，不存在同名用户，且不存在空口令账号；3）经访谈，SSHKey公私钥每半年进行更换；4）查看sshd\_config配置文件中配置PasswordAuthentication no，拒绝使用密码方式进行身份鉴别。 |
| 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； | 操作系统采用用户名+SSHKey公私钥进行身份鉴别，可以防止鉴别信息被暴力破解；但未配置用户连接超时退出策略。 |
| 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； | 1）经核查，管理人员采用SSH协议连接操作系统；2）执行netatat –tpln| grep 23命令查看操作系统远程管理端口，不存在Telnet端口，防止鉴别信息在网络传输过程中的被窃听。 |
| 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。 | 未采用两种或两种以上组合的鉴别技术对用户进行身份鉴别。 |
| 访问控制 | a）应对登录的用户分配账户和权限； | 1）经访谈，通过root账户为登录的用户创建账户、分配权限；2）执行ls -l命令查看关键文件权限，均已为账户分配了相应权限，相关文件权限设置为/etc/shadow：000、/etc/passwd：644、/etc/group：644、/etc/profile：644、/etc/crontab：644、/ etc/securetty：600、/etc/ssh/sshd\_config：600。 |
| b）应重命名或删除默认账户，修改默认账户的默认口令； | 1）执行cat /etc/shadow命令查看shadow文件，操作系统中adm、lp、sync、shutdown、halt、mail、uucp、operator、games、gopher等账户均为nologin状态，存在默认账户root；2）执行more /etc/ssh/sshd\_config命令，查看“PermitRootLogin”参数设置为“yes”，即允许root远程登录；3）经访谈，root用户需通过公私钥方式进行身份鉴别。 |
| 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； | 1）执行cat /etc/shadow命令查看shadow文件，发现操作系统存在root、ysup、yops、yluser等在用账户，不存在多余的、过期账户；2）存在多个堡垒机账户登录操作系统时共用一个账户的情况。 |
| 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； | root账户具有系统所有权限，未实现管理用户的权限分离。 |
| e）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； | 经访谈，由系统管理员root配置访问控制策略，如：/etc/passwd，/etc/profile宿主为root、权限设置为644，audit文件为700、message文件为600，其他文件权限为750，实现用户对文件的权限控制。 |
| f）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； | 由管理用户进行用户访问权限分配进行设置，依据访问控制策略,对各类文件进行访问，重要文件和目录权限均在合理范围内，用户可根据文件不同的权限进行操作。 |
| g）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。 | 执 行more /etc/selinux/config 命令，查看config文件显示 SELINUX参数为 DISABLED，即未开启强制访问控制模式。 |
| 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）执行ps -ef|grep rsyslog和ps -ef|grep auditd命令，显示rsyslog和auditd进程正在运行；2）more /etc/audit/audit.rules，显示审计内容包括：\*.info、authriv.\*、mail.\*、cron.\*、\*.emerg、uucp、news.crit、local7.\*等事件。 |
| 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； | 执行tail -20 /var/log/audit/audit.log命令，查看近20条审计日志，内容包括：时间、对象、路径、用户ID、相关的系统调用、用户执行命令等。 |
| 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）通过访问权限对审计记录进行保护，日志文件/var/log/messages、/var/log/secure、/var/log/audit/audit.log访问 权限均为600；2）审计记录本地保存，且实时备份至360本地安全大脑，保存时间满足180天以上。 |
| d）应对审计进程进行保护，防止未经授权的中断。 | 执行service auditd status命令，系统开启auditd审计保护进程，审计进程由root用户维护，经现场使用yluser用户通过service auditd stop命令尝试中断审计进程，无法将审计进程单独中断。 |
| 入侵防范 | a）应遵循最小安装的原则，仅安装需要的组件和应用程序； | 1）系统安装遵循最小化安装原则；2）执行yum list installed命令查看操作系统已安装的程序包，存在Java、SSH、天眼云镜agent等应用程序或组件，不存在与业务系统无关的组件和应用程序。 |
| b）应关闭不需要的系统服务、默认共享和高危端口； | 1）执行systemctl list-unit-files 命令，系统已关闭FTP、Telnet 等高危网络服务；2）执行netstat -pantu命令，系统关闭了135、445等高危端口，仅开启了22、8080等端口。 |
| c）应通过设定终端接入方式或网络地址范围对通过网络进行管理的管理终端进行限制； | 经核查，1）通过配置安全组策略限制仅允许通过堡垒机管理服务器；2）经核查防火墙中访问控制策略，具备堡垒机地址-服务器管理网段（10.33.0.0）的访问控制策略。 |
| d）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； | 根据GB∕T 28448-2019 《信息安全技术 网络安全等级保护测评要求》测评对象范围描述，服务器无该项要求，故判为“不适用”。 |
| e）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； | 1）经过漏洞扫描，服务器不存在高危安全漏洞；2）执行rpm -qa grep patch命令，查看系统补丁已更新至最新。 |
| f）应能够检测到对重要节点进行入侵的行为，并在发生严重入侵事件时提供报警。 | 经核查，服务器上安装有青藤云天眼云镜，对主机入侵行为进行检测，发现严重安全事件时通过钉钉告警。 |
| 恶意代码防范 | a）应采用免受恶意代码攻击的技术措施或主动免疫可信验证机制及时识别入侵和病毒行为，并将其有效阻断。 | 经核查，服务器上安装有青藤云天眼云镜，对主机恶意代码进行检测、清除，每天凌晨自动更新恶意代码特征库，经核查，具备恶意代码特征库更新记录。 |
| 可信验证 | a）可基于可信根对计算设备的系统引导程序、系统程序、重要配置参数和应用程序等进行可信验证，并在应用程序的关键执行环节进行动态可信验证，在检测到其可信性受到破坏后进行报警，并将验证结果形成审计记录送至安全管理中心。 | 未采用技术措施对计算设备的系统引导程序、系统程序、重要配置参数和通信应用程序等进行可信验证。 |
| 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； | 采用SSH协议连接操作系统，保证了鉴别信息以及管理数据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。 | 操作系统中对重要鉴别信息通过自身的加密及校验（SHA256），保证数据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； | 采用SSH协议连接操作系统，保证了鉴别信息以及管理数据在传输过程中的保密性。 |
| b）应采用密码技术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个人信息等。 | 通过系统自带的加密模块保证鉴别数据在存储过程中的保密性。 |
| 数据备份恢复 | a）应提供重要数据的本地数据备份与恢复功能； | 经核查，通过脚本每周将配置文件、代码仓库等数据备份至备份服务器中，依据需要验证备份数据的有效性。 |
| b）应提供异地实时备份功能，利用通信网络将重要数据实时备份至备份场地； | 系统无异地备份机制。 |
| c）应提供重要数据处理系统的热冗余，保证系统的高可用性。 | 服务器采用K8S容器部署，保证系统的高可用性。 |
| 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； | 操作系统提供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功能。 |
| 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。 | 操作系统提供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的功能。 |

4.1.3.44. 应用服务器109

|  |  |  |
| --- | --- | --- |
| **安全控制点** | **测评指标** | **结果记录** |
| 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）操作系统时采用用户名+SSHKey公私钥进行身份鉴别鉴别信息具有复杂度要求；2）执行cat /etc/shadow命令，查看shadow文件系统内用户身份标识唯一，不存在同名用户，且不存在空口令账号；3）经访谈，SSHKey公私钥每半年进行更换；4）查看sshd\_config配置文件中配置PasswordAuthentication no，拒绝使用密码方式进行身份鉴别。 |
| 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； | 操作系统采用用户名+SSHKey公私钥进行身份鉴别，可以防止鉴别信息被暴力破解；但未配置用户连接超时退出策略。 |
| 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； | 1）经核查，管理人员采用SSH协议连接操作系统；2）执行netatat –tpln| grep 23命令查看操作系统远程管理端口，不存在Telnet端口，防止鉴别信息在网络传输过程中的被窃听。 |
| 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。 | 未采用两种或两种以上组合的鉴别技术对用户进行身份鉴别。 |
| 访问控制 | a）应对登录的用户分配账户和权限； | 1）经访谈，通过root账户为登录的用户创建账户、分配权限；2）执行ls -l命令查看关键文件权限，均已为账户分配了相应权限，相关文件权限设置为/etc/shadow：000、/etc/passwd：644、/etc/group：644、/etc/profile：644、/etc/crontab：644、/ etc/securetty：600、/etc/ssh/sshd\_config：600。 |
| b）应重命名或删除默认账户，修改默认账户的默认口令； | 1）执行cat /etc/shadow命令查看shadow文件，操作系统中adm、lp、sync、shutdown、halt、mail、uucp、operator、games、gopher等账户均为nologin状态，存在默认账户root；2）执行more /etc/ssh/sshd\_config命令，查看“PermitRootLogin”参数设置为“yes”，即允许root远程登录；3）经访谈，root用户需通过公私钥方式进行身份鉴别。 |
| 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； | 1）执行cat /etc/shadow命令查看shadow文件，发现操作系统存在root、ysup、yops、yluser等在用账户，不存在多余的、过期账户；2）存在多个堡垒机账户登录操作系统时共用一个账户的情况。 |
| 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； | root账户具有系统所有权限，未实现管理用户的权限分离。 |
| e）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； | 经访谈，由系统管理员root配置访问控制策略，如：/etc/passwd，/etc/profile宿主为root、权限设置为644，audit文件为700、message文件为600，其他文件权限为750，实现用户对文件的权限控制。 |
| f）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； | 由管理用户进行用户访问权限分配进行设置，依据访问控制策略,对各类文件进行访问，重要文件和目录权限均在合理范围内，用户可根据文件不同的权限进行操作。 |
| g）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。 | 执 行more /etc/selinux/config 命令，查看config文件显示 SELINUX参数为 DISABLED，即未开启强制访问控制模式。 |
| 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）执行ps -ef|grep rsyslog和ps -ef|grep auditd命令，显示rsyslog和auditd进程正在运行；2）more /etc/audit/audit.rules，显示审计内容包括：\*.info、authriv.\*、mail.\*、cron.\*、\*.emerg、uucp、news.crit、local7.\*等事件。 |
| 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； | 执行tail -20 /var/log/audit/audit.log命令，查看近20条审计日志，内容包括：时间、对象、路径、用户ID、相关的系统调用、用户执行命令等。 |
| 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）通过访问权限对审计记录进行保护，日志文件/var/log/messages、/var/log/secure、/var/log/audit/audit.log访问 权限均为600；2）审计记录本地保存，且实时备份至360本地安全大脑，保存时间满足180天以上。 |
| d）应对审计进程进行保护，防止未经授权的中断。 | 执行service auditd status命令，系统开启auditd审计保护进程，审计进程由root用户维护，经现场使用yluser用户通过service auditd stop命令尝试中断审计进程，无法将审计进程单独中断。 |
| 入侵防范 | a）应遵循最小安装的原则，仅安装需要的组件和应用程序； | 1）系统安装遵循最小化安装原则；2）执行yum list installed命令查看操作系统已安装的程序包，存在Java、SSH、天眼云镜agent等应用程序或组件，不存在与业务系统无关的组件和应用程序。 |
| b）应关闭不需要的系统服务、默认共享和高危端口； | 1）执行systemctl list-unit-files 命令，系统已关闭FTP、Telnet 等高危网络服务；2）执行netstat -pantu命令，系统关闭了135、445等高危端口，仅开启了22、8080等端口。 |
| c）应通过设定终端接入方式或网络地址范围对通过网络进行管理的管理终端进行限制； | 经核查，1）通过配置安全组策略限制仅允许通过堡垒机管理服务器；2）经核查防火墙中访问控制策略，具备堡垒机地址-服务器管理网段（10.33.0.0）的访问控制策略。 |
| d）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； | 根据GB∕T 28448-2019 《信息安全技术 网络安全等级保护测评要求》测评对象范围描述，服务器无该项要求，故判为“不适用”。 |
| e）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； | 1）经过漏洞扫描，服务器不存在高危安全漏洞；2）执行rpm -qa grep patch命令，查看系统补丁已更新至最新。 |
| f）应能够检测到对重要节点进行入侵的行为，并在发生严重入侵事件时提供报警。 | 经核查，服务器上安装有青藤云天眼云镜，对主机入侵行为进行检测，发现严重安全事件时通过钉钉告警。 |
| 恶意代码防范 | a）应采用免受恶意代码攻击的技术措施或主动免疫可信验证机制及时识别入侵和病毒行为，并将其有效阻断。 | 经核查，服务器上安装有青藤云天眼云镜，对主机恶意代码进行检测、清除，每天凌晨自动更新恶意代码特征库，经核查，具备恶意代码特征库更新记录。 |
| 可信验证 | a）可基于可信根对计算设备的系统引导程序、系统程序、重要配置参数和应用程序等进行可信验证，并在应用程序的关键执行环节进行动态可信验证，在检测到其可信性受到破坏后进行报警，并将验证结果形成审计记录送至安全管理中心。 | 未采用技术措施对计算设备的系统引导程序、系统程序、重要配置参数和通信应用程序等进行可信验证。 |
| 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； | 采用SSH协议连接操作系统，保证了鉴别信息以及管理数据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。 | 操作系统中对重要鉴别信息通过自身的加密及校验（SHA256），保证数据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； | 采用SSH协议连接操作系统，保证了鉴别信息以及管理数据在传输过程中的保密性。 |
| b）应采用密码技术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个人信息等。 | 通过系统自带的加密模块保证鉴别数据在存储过程中的保密性。 |
| 数据备份恢复 | a）应提供重要数据的本地数据备份与恢复功能； | 经核查，通过脚本每周将配置文件、代码仓库等数据备份至备份服务器中，依据需要验证备份数据的有效性。 |
| b）应提供异地实时备份功能，利用通信网络将重要数据实时备份至备份场地； | 系统无异地备份机制。 |
| c）应提供重要数据处理系统的热冗余，保证系统的高可用性。 | 服务器采用K8S容器部署，保证系统的高可用性。 |
| 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； | 操作系统提供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功能。 |
| 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。 | 操作系统提供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的功能。 |

4.1.3.45. 应用服务器110

|  |  |  |
| --- | --- | --- |
| **安全控制点** | **测评指标** | **结果记录** |
| 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）操作系统时采用用户名+SSHKey公私钥进行身份鉴别鉴别信息具有复杂度要求；2）执行cat /etc/shadow命令，查看shadow文件系统内用户身份标识唯一，不存在同名用户，且不存在空口令账号；3）经访谈，SSHKey公私钥每半年进行更换；4）查看sshd\_config配置文件中配置PasswordAuthentication no，拒绝使用密码方式进行身份鉴别。 |
| 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； | 操作系统采用用户名+SSHKey公私钥进行身份鉴别，可以防止鉴别信息被暴力破解；但未配置用户连接超时退出策略。 |
| 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； | 1）经核查，管理人员采用SSH协议连接操作系统；2）执行netatat –tpln| grep 23命令查看操作系统远程管理端口，不存在Telnet端口，防止鉴别信息在网络传输过程中的被窃听。 |
| 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。 | 未采用两种或两种以上组合的鉴别技术对用户进行身份鉴别。 |
| 访问控制 | a）应对登录的用户分配账户和权限； | 1）经访谈，通过root账户为登录的用户创建账户、分配权限；2）执行ls -l命令查看关键文件权限，均已为账户分配了相应权限，相关文件权限设置为/etc/shadow：000、/etc/passwd：644、/etc/group：644、/etc/profile：644、/etc/crontab：644、/ etc/securetty：600、/etc/ssh/sshd\_config：600。 |
| b）应重命名或删除默认账户，修改默认账户的默认口令； | 1）执行cat /etc/shadow命令查看shadow文件，操作系统中adm、lp、sync、shutdown、halt、mail、uucp、operator、games、gopher等账户均为nologin状态，存在默认账户root；2）执行more /etc/ssh/sshd\_config命令，查看“PermitRootLogin”参数设置为“yes”，即允许root远程登录；3）经访谈，root用户需通过公私钥方式进行身份鉴别。 |
| 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； | 1）执行cat /etc/shadow命令查看shadow文件，发现操作系统存在root、ysup、yops、yluser等在用账户，不存在多余的、过期账户；2）存在多个堡垒机账户登录操作系统时共用一个账户的情况。 |
| 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； | root账户具有系统所有权限，未实现管理用户的权限分离。 |
| e）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； | 经访谈，由系统管理员root配置访问控制策略，如：/etc/passwd，/etc/profile宿主为root、权限设置为644，audit文件为700、message文件为600，其他文件权限为750，实现用户对文件的权限控制。 |
| f）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； | 由管理用户进行用户访问权限分配进行设置，依据访问控制策略,对各类文件进行访问，重要文件和目录权限均在合理范围内，用户可根据文件不同的权限进行操作。 |
| g）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。 | 执 行more /etc/selinux/config 命令，查看config文件显示 SELINUX参数为 DISABLED，即未开启强制访问控制模式。 |
| 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）执行ps -ef|grep rsyslog和ps -ef|grep auditd命令，显示rsyslog和auditd进程正在运行；2）more /etc/audit/audit.rules，显示审计内容包括：\*.info、authriv.\*、mail.\*、cron.\*、\*.emerg、uucp、news.crit、local7.\*等事件。 |
| 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； | 执行tail -20 /var/log/audit/audit.log命令，查看近20条审计日志，内容包括：时间、对象、路径、用户ID、相关的系统调用、用户执行命令等。 |
| 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）通过访问权限对审计记录进行保护，日志文件/var/log/messages、/var/log/secure、/var/log/audit/audit.log访问 权限均为600；2）审计记录本地保存，且实时备份至360本地安全大脑，保存时间满足180天以上。 |
| d）应对审计进程进行保护，防止未经授权的中断。 | 执行service auditd status命令，系统开启auditd审计保护进程，审计进程由root用户维护，经现场使用yluser用户通过service auditd stop命令尝试中断审计进程，无法将审计进程单独中断。 |
| 入侵防范 | a）应遵循最小安装的原则，仅安装需要的组件和应用程序； | 1）系统安装遵循最小化安装原则；2）执行yum list installed命令查看操作系统已安装的程序包，存在Java、SSH、天眼云镜agent等应用程序或组件，不存在与业务系统无关的组件和应用程序。 |
| b）应关闭不需要的系统服务、默认共享和高危端口； | 1）执行systemctl list-unit-files 命令，系统已关闭FTP、Telnet 等高危网络服务；2）执行netstat -pantu命令，系统关闭了135、445等高危端口，仅开启了22、8080等端口。 |
| c）应通过设定终端接入方式或网络地址范围对通过网络进行管理的管理终端进行限制； | 经核查，1）通过配置安全组策略限制仅允许通过堡垒机管理服务器；2）经核查防火墙中访问控制策略，具备堡垒机地址-服务器管理网段（10.33.0.0）的访问控制策略。 |
| d）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； | 根据GB∕T 28448-2019 《信息安全技术 网络安全等级保护测评要求》测评对象范围描述，服务器无该项要求，故判为“不适用”。 |
| e）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； | 1）经过漏洞扫描，服务器不存在高危安全漏洞；2）执行rpm -qa grep patch命令，查看系统补丁已更新至最新。 |
| f）应能够检测到对重要节点进行入侵的行为，并在发生严重入侵事件时提供报警。 | 经核查，服务器上安装有青藤云天眼云镜，对主机入侵行为进行检测，发现严重安全事件时通过钉钉告警。 |
| 恶意代码防范 | a）应采用免受恶意代码攻击的技术措施或主动免疫可信验证机制及时识别入侵和病毒行为，并将其有效阻断。 | 经核查，服务器上安装有青藤云天眼云镜，对主机恶意代码进行检测、清除，每天凌晨自动更新恶意代码特征库，经核查，具备恶意代码特征库更新记录。 |
| 可信验证 | a）可基于可信根对计算设备的系统引导程序、系统程序、重要配置参数和应用程序等进行可信验证，并在应用程序的关键执行环节进行动态可信验证，在检测到其可信性受到破坏后进行报警，并将验证结果形成审计记录送至安全管理中心。 | 未采用技术措施对计算设备的系统引导程序、系统程序、重要配置参数和通信应用程序等进行可信验证。 |
| 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； | 采用SSH协议连接操作系统，保证了鉴别信息以及管理数据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。 | 操作系统中对重要鉴别信息通过自身的加密及校验（SHA256），保证数据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； | 采用SSH协议连接操作系统，保证了鉴别信息以及管理数据在传输过程中的保密性。 |
| b）应采用密码技术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个人信息等。 | 通过系统自带的加密模块保证鉴别数据在存储过程中的保密性。 |
| 数据备份恢复 | a）应提供重要数据的本地数据备份与恢复功能； | 经核查，通过脚本每周将配置文件、代码仓库等数据备份至备份服务器中，依据需要验证备份数据的有效性。 |
| b）应提供异地实时备份功能，利用通信网络将重要数据实时备份至备份场地； | 系统无异地备份机制。 |
| c）应提供重要数据处理系统的热冗余，保证系统的高可用性。 | 服务器采用K8S容器部署，保证系统的高可用性。 |
| 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； | 操作系统提供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功能。 |
| 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。 | 操作系统提供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的功能。 |

4.1.3.46. 应用服务器112

|  |  |  |
| --- | --- | --- |
| **安全控制点** | **测评指标** | **结果记录** |
| 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）操作系统时采用用户名+SSHKey公私钥进行身份鉴别鉴别信息具有复杂度要求；2）执行cat /etc/shadow命令，查看shadow文件系统内用户身份标识唯一，不存在同名用户，且不存在空口令账号；3）经访谈，SSHKey公私钥每半年进行更换；4）查看sshd\_config配置文件中配置PasswordAuthentication no，拒绝使用密码方式进行身份鉴别。 |
| 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； | 操作系统采用用户名+SSHKey公私钥进行身份鉴别，可以防止鉴别信息被暴力破解；但未配置用户连接超时退出策略。 |
| 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； | 1）经核查，管理人员采用SSH协议连接操作系统；2）执行netatat –tpln| grep 23命令查看操作系统远程管理端口，不存在Telnet端口，防止鉴别信息在网络传输过程中的被窃听。 |
| 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。 | 未采用两种或两种以上组合的鉴别技术对用户进行身份鉴别。 |
| 访问控制 | a）应对登录的用户分配账户和权限； | 1）经访谈，通过root账户为登录的用户创建账户、分配权限；2）执行ls -l命令查看关键文件权限，均已为账户分配了相应权限，相关文件权限设置为/etc/shadow：000、/etc/passwd：644、/etc/group：644、/etc/profile：644、/etc/crontab：644、/ etc/securetty：600、/etc/ssh/sshd\_config：600。 |
| b）应重命名或删除默认账户，修改默认账户的默认口令； | 1）执行cat /etc/shadow命令查看shadow文件，操作系统中adm、lp、sync、shutdown、halt、mail、uucp、operator、games、gopher等账户均为nologin状态，存在默认账户root；2）执行more /etc/ssh/sshd\_config命令，查看“PermitRootLogin”参数设置为“yes”，即允许root远程登录；3）经访谈，root用户需通过公私钥方式进行身份鉴别。 |
| 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； | 1）执行cat /etc/shadow命令查看shadow文件，发现操作系统存在root、ysup、yops、yluser等在用账户，不存在多余的、过期账户；2）存在多个堡垒机账户登录操作系统时共用一个账户的情况。 |
| 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； | root账户具有系统所有权限，未实现管理用户的权限分离。 |
| e）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； | 经访谈，由系统管理员root配置访问控制策略，如：/etc/passwd，/etc/profile宿主为root、权限设置为644，audit文件为700、message文件为600，其他文件权限为750，实现用户对文件的权限控制。 |
| f）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； | 由管理用户进行用户访问权限分配进行设置，依据访问控制策略,对各类文件进行访问，重要文件和目录权限均在合理范围内，用户可根据文件不同的权限进行操作。 |
| g）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。 | 执 行more /etc/selinux/config 命令，查看config文件显示 SELINUX参数为 DISABLED，即未开启强制访问控制模式。 |
| 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）执行ps -ef|grep rsyslog和ps -ef|grep auditd命令，显示rsyslog和auditd进程正在运行；2）more /etc/audit/audit.rules，显示审计内容包括：\*.info、authriv.\*、mail.\*、cron.\*、\*.emerg、uucp、news.crit、local7.\*等事件。 |
| 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； | 执行tail -20 /var/log/audit/audit.log命令，查看近20条审计日志，内容包括：时间、对象、路径、用户ID、相关的系统调用、用户执行命令等。 |
| 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）通过访问权限对审计记录进行保护，日志文件/var/log/messages、/var/log/secure、/var/log/audit/audit.log访问 权限均为600；2）审计记录本地保存，且实时备份至360本地安全大脑，保存时间满足180天以上。 |
| d）应对审计进程进行保护，防止未经授权的中断。 | 执行service auditd status命令，系统开启auditd审计保护进程，审计进程由root用户维护，经现场使用yluser用户通过service auditd stop命令尝试中断审计进程，无法将审计进程单独中断。 |
| 入侵防范 | a）应遵循最小安装的原则，仅安装需要的组件和应用程序； | 1）系统安装遵循最小化安装原则；2）执行yum list installed命令查看操作系统已安装的程序包，存在Java、SSH、天眼云镜agent等应用程序或组件，不存在与业务系统无关的组件和应用程序。 |
| b）应关闭不需要的系统服务、默认共享和高危端口； | 1）执行systemctl list-unit-files 命令，系统已关闭FTP、Telnet 等高危网络服务；2）执行netstat -pantu命令，系统关闭了135、445等高危端口，仅开启了22、8080等端口。 |
| c）应通过设定终端接入方式或网络地址范围对通过网络进行管理的管理终端进行限制； | 经核查，1）通过配置安全组策略限制仅允许通过堡垒机管理服务器；2）经核查防火墙中访问控制策略，具备堡垒机地址-服务器管理网段（10.33.0.0）的访问控制策略。 |
| d）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； | 根据GB∕T 28448-2019 《信息安全技术 网络安全等级保护测评要求》测评对象范围描述，服务器无该项要求，故判为“不适用”。 |
| e）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； | 1）经过漏洞扫描，服务器不存在高危安全漏洞；2）执行rpm -qa grep patch命令，查看系统补丁已更新至最新。 |
| f）应能够检测到对重要节点进行入侵的行为，并在发生严重入侵事件时提供报警。 | 经核查，服务器上安装有青藤云天眼云镜，对主机入侵行为进行检测，发现严重安全事件时通过钉钉告警。 |
| 恶意代码防范 | a）应采用免受恶意代码攻击的技术措施或主动免疫可信验证机制及时识别入侵和病毒行为，并将其有效阻断。 | 经核查，服务器上安装有青藤云天眼云镜，对主机恶意代码进行检测、清除，每天凌晨自动更新恶意代码特征库，经核查，具备恶意代码特征库更新记录。 |
| 可信验证 | a）可基于可信根对计算设备的系统引导程序、系统程序、重要配置参数和应用程序等进行可信验证，并在应用程序的关键执行环节进行动态可信验证，在检测到其可信性受到破坏后进行报警，并将验证结果形成审计记录送至安全管理中心。 | 未采用技术措施对计算设备的系统引导程序、系统程序、重要配置参数和通信应用程序等进行可信验证。 |
| 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； | 采用SSH协议连接操作系统，保证了鉴别信息以及管理数据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。 | 操作系统中对重要鉴别信息通过自身的加密及校验（SHA256），保证数据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； | 采用SSH协议连接操作系统，保证了鉴别信息以及管理数据在传输过程中的保密性。 |
| b）应采用密码技术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个人信息等。 | 通过系统自带的加密模块保证鉴别数据在存储过程中的保密性。 |
| 数据备份恢复 | a）应提供重要数据的本地数据备份与恢复功能； | 经核查，通过脚本每周将配置文件、代码仓库等数据备份至备份服务器中，依据需要验证备份数据的有效性。 |
| b）应提供异地实时备份功能，利用通信网络将重要数据实时备份至备份场地； | 系统无异地备份机制。 |
| c）应提供重要数据处理系统的热冗余，保证系统的高可用性。 | 服务器采用K8S容器部署，保证系统的高可用性。 |
| 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； | 操作系统提供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功能。 |
| 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。 | 操作系统提供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的功能。 |

4.1.3.47. 应用服务器117

|  |  |  |
| --- | --- | --- |
| **安全控制点** | **测评指标** | **结果记录** |
| 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）操作系统时采用用户名+SSHKey公私钥进行身份鉴别鉴别信息具有复杂度要求；2）执行cat /etc/shadow命令，查看shadow文件系统内用户身份标识唯一，不存在同名用户，且不存在空口令账号；3）经访谈，SSHKey公私钥每半年进行更换；4）查看sshd\_config配置文件中配置PasswordAuthentication no，拒绝使用密码方式进行身份鉴别。 |
| 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； | 操作系统采用用户名+SSHKey公私钥进行身份鉴别，可以防止鉴别信息被暴力破解；但未配置用户连接超时退出策略。 |
| 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； | 1）经核查，管理人员采用SSH协议连接操作系统；2）执行netatat –tpln| grep 23命令查看操作系统远程管理端口，不存在Telnet端口，防止鉴别信息在网络传输过程中的被窃听。 |
| 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。 | 未采用两种或两种以上组合的鉴别技术对用户进行身份鉴别。 |
| 访问控制 | a）应对登录的用户分配账户和权限； | 1）经访谈，通过root账户为登录的用户创建账户、分配权限；2）执行ls -l命令查看关键文件权限，均已为账户分配了相应权限，相关文件权限设置为/etc/shadow：000、/etc/passwd：644、/etc/group：644、/etc/profile：644、/etc/crontab：644、/ etc/securetty：600、/etc/ssh/sshd\_config：600。 |
| b）应重命名或删除默认账户，修改默认账户的默认口令； | 1）执行cat /etc/shadow命令查看shadow文件，操作系统中adm、lp、sync、shutdown、halt、mail、uucp、operator、games、gopher等账户均为nologin状态，存在默认账户root；2）执行more /etc/ssh/sshd\_config命令，查看“PermitRootLogin”参数设置为“yes”，即允许root远程登录；3）经访谈，root用户需通过公私钥方式进行身份鉴别。 |
| 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； | 1）执行cat /etc/shadow命令查看shadow文件，发现操作系统存在root、ysup、yops、yluser等在用账户，不存在多余的、过期账户；2）存在多个堡垒机账户登录操作系统时共用一个账户的情况。 |
| 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； | root账户具有系统所有权限，未实现管理用户的权限分离。 |
| e）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； | 经访谈，由系统管理员root配置访问控制策略，如：/etc/passwd，/etc/profile宿主为root、权限设置为644，audit文件为700、message文件为600，其他文件权限为750，实现用户对文件的权限控制。 |
| f）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； | 由管理用户进行用户访问权限分配进行设置，依据访问控制策略,对各类文件进行访问，重要文件和目录权限均在合理范围内，用户可根据文件不同的权限进行操作。 |
| g）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。 | 执 行more /etc/selinux/config 命令，查看config文件显示 SELINUX参数为 DISABLED，即未开启强制访问控制模式。 |
| 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）执行ps -ef|grep rsyslog和ps -ef|grep auditd命令，显示rsyslog和auditd进程正在运行；2）more /etc/audit/audit.rules，显示审计内容包括：\*.info、authriv.\*、mail.\*、cron.\*、\*.emerg、uucp、news.crit、local7.\*等事件。 |
| 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； | 执行tail -20 /var/log/audit/audit.log命令，查看近20条审计日志，内容包括：时间、对象、路径、用户ID、相关的系统调用、用户执行命令等。 |
| 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）通过访问权限对审计记录进行保护，日志文件/var/log/messages、/var/log/secure、/var/log/audit/audit.log访问 权限均为600；2）审计记录本地保存，且实时备份至360本地安全大脑，保存时间满足180天以上。 |
| d）应对审计进程进行保护，防止未经授权的中断。 | 执行service auditd status命令，系统开启auditd审计保护进程，审计进程由root用户维护，经现场使用yluser用户通过service auditd stop命令尝试中断审计进程，无法将审计进程单独中断。 |
| 入侵防范 | a）应遵循最小安装的原则，仅安装需要的组件和应用程序； | 1）系统安装遵循最小化安装原则；2）执行yum list installed命令查看操作系统已安装的程序包，存在Java、SSH、天眼云镜agent等应用程序或组件，不存在与业务系统无关的组件和应用程序。 |
| b）应关闭不需要的系统服务、默认共享和高危端口； | 1）执行systemctl list-unit-files 命令，系统已关闭FTP、Telnet 等高危网络服务；2）执行netstat -pantu命令，系统关闭了135、445等高危端口，仅开启了22、8080等端口。 |
| c）应通过设定终端接入方式或网络地址范围对通过网络进行管理的管理终端进行限制； | 经核查，1）通过配置安全组策略限制仅允许通过堡垒机管理服务器；2）经核查防火墙中访问控制策略，具备堡垒机地址-服务器管理网段（10.33.0.0）的访问控制策略。 |
| d）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； | 根据GB∕T 28448-2019 《信息安全技术 网络安全等级保护测评要求》测评对象范围描述，服务器无该项要求，故判为“不适用”。 |
| e）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； | 1）经过漏洞扫描，服务器不存在高危安全漏洞；2）执行rpm -qa grep patch命令，查看系统补丁已更新至最新。 |
| f）应能够检测到对重要节点进行入侵的行为，并在发生严重入侵事件时提供报警。 | 经核查，服务器上安装有青藤云天眼云镜，对主机入侵行为进行检测，发现严重安全事件时通过钉钉告警。 |
| 恶意代码防范 | a）应采用免受恶意代码攻击的技术措施或主动免疫可信验证机制及时识别入侵和病毒行为，并将其有效阻断。 | 经核查，服务器上安装有青藤云天眼云镜，对主机恶意代码进行检测、清除，每天凌晨自动更新恶意代码特征库，经核查，具备恶意代码特征库更新记录。 |
| 可信验证 | a）可基于可信根对计算设备的系统引导程序、系统程序、重要配置参数和应用程序等进行可信验证，并在应用程序的关键执行环节进行动态可信验证，在检测到其可信性受到破坏后进行报警，并将验证结果形成审计记录送至安全管理中心。 | 未采用技术措施对计算设备的系统引导程序、系统程序、重要配置参数和通信应用程序等进行可信验证。 |
| 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； | 采用SSH协议连接操作系统，保证了鉴别信息以及管理数据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。 | 操作系统中对重要鉴别信息通过自身的加密及校验（SHA256），保证数据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； | 采用SSH协议连接操作系统，保证了鉴别信息以及管理数据在传输过程中的保密性。 |
| b）应采用密码技术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个人信息等。 | 通过系统自带的加密模块保证鉴别数据在存储过程中的保密性。 |
| 数据备份恢复 | a）应提供重要数据的本地数据备份与恢复功能； | 经核查，通过脚本每周将配置文件、代码仓库等数据备份至备份服务器中，依据需要验证备份数据的有效性。 |
| b）应提供异地实时备份功能，利用通信网络将重要数据实时备份至备份场地； | 系统无异地备份机制。 |
| c）应提供重要数据处理系统的热冗余，保证系统的高可用性。 | 服务器采用K8S容器部署，保证系统的高可用性。 |
| 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； | 操作系统提供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功能。 |
| 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。 | 操作系统提供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的功能。 |

4.1.3.48. 应用服务器122

|  |  |  |
| --- | --- | --- |
| **安全控制点** | **测评指标** | **结果记录** |
| 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）操作系统时采用用户名+SSHKey公私钥进行身份鉴别鉴别信息具有复杂度要求；2）执行cat /etc/shadow命令，查看shadow文件系统内用户身份标识唯一，不存在同名用户，且不存在空口令账号；3）经访谈，SSHKey公私钥每半年进行更换；4）查看sshd\_config配置文件中配置PasswordAuthentication no，拒绝使用密码方式进行身份鉴别。 |
| 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； | 操作系统采用用户名+SSHKey公私钥进行身份鉴别，可以防止鉴别信息被暴力破解；但未配置用户连接超时退出策略。 |
| 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； | 1）经核查，管理人员采用SSH协议连接操作系统；2）执行netatat –tpln| grep 23命令查看操作系统远程管理端口，不存在Telnet端口，防止鉴别信息在网络传输过程中的被窃听。 |
| 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。 | 未采用两种或两种以上组合的鉴别技术对用户进行身份鉴别。 |
| 访问控制 | a）应对登录的用户分配账户和权限； | 1）经访谈，通过root账户为登录的用户创建账户、分配权限；2）执行ls -l命令查看关键文件权限，均已为账户分配了相应权限，相关文件权限设置为/etc/shadow：000、/etc/passwd：644、/etc/group：644、/etc/profile：644、/etc/crontab：644、/ etc/securetty：600、/etc/ssh/sshd\_config：600。 |
| b）应重命名或删除默认账户，修改默认账户的默认口令； | 1）执行cat /etc/shadow命令查看shadow文件，操作系统中adm、lp、sync、shutdown、halt、mail、uucp、operator、games、gopher等账户均为nologin状态，存在默认账户root；2）执行more /etc/ssh/sshd\_config命令，查看“PermitRootLogin”参数设置为“yes”，即允许root远程登录；3）经访谈，root用户需通过公私钥方式进行身份鉴别。 |
| 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； | 1）执行cat /etc/shadow命令查看shadow文件，发现操作系统存在root、ysup、yops、yluser等在用账户，不存在多余的、过期账户；2）存在多个堡垒机账户登录操作系统时共用一个账户的情况。 |
| 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； | root账户具有系统所有权限，未实现管理用户的权限分离。 |
| e）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； | 经访谈，由系统管理员root配置访问控制策略，如：/etc/passwd，/etc/profile宿主为root、权限设置为644，audit文件为700、message文件为600，其他文件权限为750，实现用户对文件的权限控制。 |
| f）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； | 由管理用户进行用户访问权限分配进行设置，依据访问控制策略,对各类文件进行访问，重要文件和目录权限均在合理范围内，用户可根据文件不同的权限进行操作。 |
| g）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。 | 执 行more /etc/selinux/config 命令，查看config文件显示 SELINUX参数为 DISABLED，即未开启强制访问控制模式。 |
| 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）执行ps -ef|grep rsyslog和ps -ef|grep auditd命令，显示rsyslog和auditd进程正在运行；2）more /etc/audit/audit.rules，显示审计内容包括：\*.info、authriv.\*、mail.\*、cron.\*、\*.emerg、uucp、news.crit、local7.\*等事件。 |
| 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； | 执行tail -20 /var/log/audit/audit.log命令，查看近20条审计日志，内容包括：时间、对象、路径、用户ID、相关的系统调用、用户执行命令等。 |
| 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）通过访问权限对审计记录进行保护，日志文件/var/log/messages、/var/log/secure、/var/log/audit/audit.log访问 权限均为600；2）审计记录本地保存，且实时备份至360本地安全大脑，保存时间满足180天以上。 |
| d）应对审计进程进行保护，防止未经授权的中断。 | 执行service auditd status命令，系统开启auditd审计保护进程，审计进程由root用户维护，经现场使用yluser用户通过service auditd stop命令尝试中断审计进程，无法将审计进程单独中断。 |
| 入侵防范 | a）应遵循最小安装的原则，仅安装需要的组件和应用程序； | 1）系统安装遵循最小化安装原则；2）执行yum list installed命令查看操作系统已安装的程序包，存在Java、SSH、天眼云镜agent等应用程序或组件，不存在与业务系统无关的组件和应用程序。 |
| b）应关闭不需要的系统服务、默认共享和高危端口； | 1）执行systemctl list-unit-files 命令，系统已关闭FTP、Telnet 等高危网络服务；2）执行netstat -pantu命令，系统关闭了135、445等高危端口，仅开启了22、8080等端口。 |
| c）应通过设定终端接入方式或网络地址范围对通过网络进行管理的管理终端进行限制； | 经核查，1）通过配置安全组策略限制仅允许通过堡垒机管理服务器；2）经核查防火墙中访问控制策略，具备堡垒机地址-服务器管理网段（10.33.0.0）的访问控制策略。 |
| d）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； | 根据GB∕T 28448-2019 《信息安全技术 网络安全等级保护测评要求》测评对象范围描述，服务器无该项要求，故判为“不适用”。 |
| e）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； | 1）经过漏洞扫描，服务器不存在高危安全漏洞；2）执行rpm -qa grep patch命令，查看系统补丁已更新至最新。 |
| f）应能够检测到对重要节点进行入侵的行为，并在发生严重入侵事件时提供报警。 | 经核查，服务器上安装有青藤云天眼云镜，对主机入侵行为进行检测，发现严重安全事件时通过钉钉告警。 |
| 恶意代码防范 | a）应采用免受恶意代码攻击的技术措施或主动免疫可信验证机制及时识别入侵和病毒行为，并将其有效阻断。 | 经核查，服务器上安装有青藤云天眼云镜，对主机恶意代码进行检测、清除，每天凌晨自动更新恶意代码特征库，经核查，具备恶意代码特征库更新记录。 |
| 可信验证 | a）可基于可信根对计算设备的系统引导程序、系统程序、重要配置参数和应用程序等进行可信验证，并在应用程序的关键执行环节进行动态可信验证，在检测到其可信性受到破坏后进行报警，并将验证结果形成审计记录送至安全管理中心。 | 未采用技术措施对计算设备的系统引导程序、系统程序、重要配置参数和通信应用程序等进行可信验证。 |
| 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； | 采用SSH协议连接操作系统，保证了鉴别信息以及管理数据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。 | 操作系统中对重要鉴别信息通过自身的加密及校验（SHA256），保证数据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； | 采用SSH协议连接操作系统，保证了鉴别信息以及管理数据在传输过程中的保密性。 |
| b）应采用密码技术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个人信息等。 | 通过系统自带的加密模块保证鉴别数据在存储过程中的保密性。 |
| 数据备份恢复 | a）应提供重要数据的本地数据备份与恢复功能； | 经核查，通过脚本每周将配置文件、代码仓库等数据备份至备份服务器中，依据需要验证备份数据的有效性。 |
| b）应提供异地实时备份功能，利用通信网络将重要数据实时备份至备份场地； | 系统无异地备份机制。 |
| c）应提供重要数据处理系统的热冗余，保证系统的高可用性。 | 服务器采用K8S容器部署，保证系统的高可用性。 |
| 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； | 操作系统提供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功能。 |
| 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。 | 操作系统提供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的功能。 |

4.1.3.49. 应用服务器127

|  |  |  |
| --- | --- | --- |
| **安全控制点** | **测评指标** | **结果记录** |
| 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）操作系统时采用用户名+SSHKey公私钥进行身份鉴别鉴别信息具有复杂度要求；2）执行cat /etc/shadow命令，查看shadow文件系统内用户身份标识唯一，不存在同名用户，且不存在空口令账号；3）经访谈，SSHKey公私钥每半年进行更换；4）查看sshd\_config配置文件中配置PasswordAuthentication no，拒绝使用密码方式进行身份鉴别。 |
| 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； | 操作系统采用用户名+SSHKey公私钥进行身份鉴别，可以防止鉴别信息被暴力破解；但未配置用户连接超时退出策略。 |
| 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； | 1）经核查，管理人员采用SSH协议连接操作系统；2）执行netatat –tpln| grep 23命令查看操作系统远程管理端口，不存在Telnet端口，防止鉴别信息在网络传输过程中的被窃听。 |
| 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。 | 未采用两种或两种以上组合的鉴别技术对用户进行身份鉴别。 |
| 访问控制 | a）应对登录的用户分配账户和权限； | 1）经访谈，通过root账户为登录的用户创建账户、分配权限；2）执行ls -l命令查看关键文件权限，均已为账户分配了相应权限，相关文件权限设置为/etc/shadow：000、/etc/passwd：644、/etc/group：644、/etc/profile：644、/etc/crontab：644、/ etc/securetty：600、/etc/ssh/sshd\_config：600。 |
| b）应重命名或删除默认账户，修改默认账户的默认口令； | 1）执行cat /etc/shadow命令查看shadow文件，操作系统中adm、lp、sync、shutdown、halt、mail、uucp、operator、games、gopher等账户均为nologin状态，存在默认账户root；2）执行more /etc/ssh/sshd\_config命令，查看“PermitRootLogin”参数设置为“yes”，即允许root远程登录；3）经访谈，root用户需通过公私钥方式进行身份鉴别。 |
| 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； | 1）执行cat /etc/shadow命令查看shadow文件，发现操作系统存在root、ysup、yops、yluser等在用账户，不存在多余的、过期账户；2）存在多个堡垒机账户登录操作系统时共用一个账户的情况。 |
| 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； | root账户具有系统所有权限，未实现管理用户的权限分离。 |
| e）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； | 经访谈，由系统管理员root配置访问控制策略，如：/etc/passwd，/etc/profile宿主为root、权限设置为644，audit文件为700、message文件为600，其他文件权限为750，实现用户对文件的权限控制。 |
| f）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； | 由管理用户进行用户访问权限分配进行设置，依据访问控制策略,对各类文件进行访问，重要文件和目录权限均在合理范围内，用户可根据文件不同的权限进行操作。 |
| g）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。 | 执 行more /etc/selinux/config 命令，查看config文件显示 SELINUX参数为 DISABLED，即未开启强制访问控制模式。 |
| 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）执行ps -ef|grep rsyslog和ps -ef|grep auditd命令，显示rsyslog和auditd进程正在运行；2）more /etc/audit/audit.rules，显示审计内容包括：\*.info、authriv.\*、mail.\*、cron.\*、\*.emerg、uucp、news.crit、local7.\*等事件。 |
| 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； | 执行tail -20 /var/log/audit/audit.log命令，查看近20条审计日志，内容包括：时间、对象、路径、用户ID、相关的系统调用、用户执行命令等。 |
| 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）通过访问权限对审计记录进行保护，日志文件/var/log/messages、/var/log/secure、/var/log/audit/audit.log访问 权限均为600；2）审计记录本地保存，且实时备份至360本地安全大脑，保存时间满足180天以上。 |
| d）应对审计进程进行保护，防止未经授权的中断。 | 执行service auditd status命令，系统开启auditd审计保护进程，审计进程由root用户维护，经现场使用yluser用户通过service auditd stop命令尝试中断审计进程，无法将审计进程单独中断。 |
| 入侵防范 | a）应遵循最小安装的原则，仅安装需要的组件和应用程序； | 1）系统安装遵循最小化安装原则；2）执行yum list installed命令查看操作系统已安装的程序包，存在Java、SSH、天眼云镜agent等应用程序或组件，不存在与业务系统无关的组件和应用程序。 |
| b）应关闭不需要的系统服务、默认共享和高危端口； | 1）执行systemctl list-unit-files 命令，系统已关闭FTP、Telnet 等高危网络服务；2）执行netstat -pantu命令，系统关闭了135、445等高危端口，仅开启了22、8080等端口。 |
| c）应通过设定终端接入方式或网络地址范围对通过网络进行管理的管理终端进行限制； | 经核查，1）通过配置安全组策略限制仅允许通过堡垒机管理服务器；2）经核查防火墙中访问控制策略，具备堡垒机地址-服务器管理网段（10.33.0.0）的访问控制策略。 |
| d）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； | 根据GB∕T 28448-2019 《信息安全技术 网络安全等级保护测评要求》测评对象范围描述，服务器无该项要求，故判为“不适用”。 |
| e）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； | 1）经过漏洞扫描，服务器不存在高危安全漏洞；2）执行rpm -qa grep patch命令，查看系统补丁已更新至最新。 |
| f）应能够检测到对重要节点进行入侵的行为，并在发生严重入侵事件时提供报警。 | 经核查，服务器上安装有青藤云天眼云镜，对主机入侵行为进行检测，发现严重安全事件时通过钉钉告警。 |
| 恶意代码防范 | a）应采用免受恶意代码攻击的技术措施或主动免疫可信验证机制及时识别入侵和病毒行为，并将其有效阻断。 | 经核查，服务器上安装有青藤云天眼云镜，对主机恶意代码进行检测、清除，每天凌晨自动更新恶意代码特征库，经核查，具备恶意代码特征库更新记录。 |
| 可信验证 | a）可基于可信根对计算设备的系统引导程序、系统程序、重要配置参数和应用程序等进行可信验证，并在应用程序的关键执行环节进行动态可信验证，在检测到其可信性受到破坏后进行报警，并将验证结果形成审计记录送至安全管理中心。 | 未采用技术措施对计算设备的系统引导程序、系统程序、重要配置参数和通信应用程序等进行可信验证。 |
| 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； | 采用SSH协议连接操作系统，保证了鉴别信息以及管理数据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。 | 操作系统中对重要鉴别信息通过自身的加密及校验（SHA256），保证数据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； | 采用SSH协议连接操作系统，保证了鉴别信息以及管理数据在传输过程中的保密性。 |
| b）应采用密码技术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个人信息等。 | 通过系统自带的加密模块保证鉴别数据在存储过程中的保密性。 |
| 数据备份恢复 | a）应提供重要数据的本地数据备份与恢复功能； | 经核查，通过脚本每周将配置文件、代码仓库等数据备份至备份服务器中，依据需要验证备份数据的有效性。 |
| b）应提供异地实时备份功能，利用通信网络将重要数据实时备份至备份场地； | 系统无异地备份机制。 |
| c）应提供重要数据处理系统的热冗余，保证系统的高可用性。 | 服务器采用K8S容器部署，保证系统的高可用性。 |
| 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； | 操作系统提供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功能。 |
| 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。 | 操作系统提供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的功能。 |

4.1.3.50. 应用服务器132

|  |  |  |
| --- | --- | --- |
| **安全控制点** | **测评指标** | **结果记录** |
| 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）操作系统时采用用户名+SSHKey公私钥进行身份鉴别鉴别信息具有复杂度要求；2）执行cat /etc/shadow命令，查看shadow文件系统内用户身份标识唯一，不存在同名用户，且不存在空口令账号；3）经访谈，SSHKey公私钥每半年进行更换；4）查看sshd\_config配置文件中配置PasswordAuthentication no，拒绝使用密码方式进行身份鉴别。 |
| 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； | 操作系统采用用户名+SSHKey公私钥进行身份鉴别，可以防止鉴别信息被暴力破解；但未配置用户连接超时退出策略。 |
| 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； | 1）经核查，管理人员采用SSH协议连接操作系统；2）执行netatat –tpln| grep 23命令查看操作系统远程管理端口，不存在Telnet端口，防止鉴别信息在网络传输过程中的被窃听。 |
| 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。 | 未采用两种或两种以上组合的鉴别技术对用户进行身份鉴别。 |
| 访问控制 | a）应对登录的用户分配账户和权限； | 1）经访谈，通过root账户为登录的用户创建账户、分配权限；2）执行ls -l命令查看关键文件权限，均已为账户分配了相应权限，相关文件权限设置为/etc/shadow：000、/etc/passwd：644、/etc/group：644、/etc/profile：644、/etc/crontab：644、/ etc/securetty：600、/etc/ssh/sshd\_config：600。 |
| b）应重命名或删除默认账户，修改默认账户的默认口令； | 1）执行cat /etc/shadow命令查看shadow文件，操作系统中adm、lp、sync、shutdown、halt、mail、uucp、operator、games、gopher等账户均为nologin状态，存在默认账户root；2）执行more /etc/ssh/sshd\_config命令，查看“PermitRootLogin”参数设置为“yes”，即允许root远程登录；3）经访谈，root用户需通过公私钥方式进行身份鉴别。 |
| 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； | 1）执行cat /etc/shadow命令查看shadow文件，发现操作系统存在root、ysup、yops、yluser等在用账户，不存在多余的、过期账户；2）存在多个堡垒机账户登录操作系统时共用一个账户的情况。 |
| 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； | root账户具有系统所有权限，未实现管理用户的权限分离。 |
| e）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； | 经访谈，由系统管理员root配置访问控制策略，如：/etc/passwd，/etc/profile宿主为root、权限设置为644，audit文件为700、message文件为600，其他文件权限为750，实现用户对文件的权限控制。 |
| f）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； | 由管理用户进行用户访问权限分配进行设置，依据访问控制策略,对各类文件进行访问，重要文件和目录权限均在合理范围内，用户可根据文件不同的权限进行操作。 |
| g）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。 | 执 行more /etc/selinux/config 命令，查看config文件显示 SELINUX参数为 DISABLED，即未开启强制访问控制模式。 |
| 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）执行ps -ef|grep rsyslog和ps -ef|grep auditd命令，显示rsyslog和auditd进程正在运行；2）more /etc/audit/audit.rules，显示审计内容包括：\*.info、authriv.\*、mail.\*、cron.\*、\*.emerg、uucp、news.crit、local7.\*等事件。 |
| 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； | 执行tail -20 /var/log/audit/audit.log命令，查看近20条审计日志，内容包括：时间、对象、路径、用户ID、相关的系统调用、用户执行命令等。 |
| 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）通过访问权限对审计记录进行保护，日志文件/var/log/messages、/var/log/secure、/var/log/audit/audit.log访问 权限均为600；2）审计记录本地保存，且实时备份至360本地安全大脑，保存时间满足180天以上。 |
| d）应对审计进程进行保护，防止未经授权的中断。 | 执行service auditd status命令，系统开启auditd审计保护进程，审计进程由root用户维护，经现场使用yluser用户通过service auditd stop命令尝试中断审计进程，无法将审计进程单独中断。 |
| 入侵防范 | a）应遵循最小安装的原则，仅安装需要的组件和应用程序； | 1）系统安装遵循最小化安装原则；2）执行yum list installed命令查看操作系统已安装的程序包，存在Java、SSH、天眼云镜agent等应用程序或组件，不存在与业务系统无关的组件和应用程序。 |
| b）应关闭不需要的系统服务、默认共享和高危端口； | 1）执行systemctl list-unit-files 命令，系统已关闭FTP、Telnet 等高危网络服务；2）执行netstat -pantu命令，系统关闭了135、445等高危端口，仅开启了22、8080等端口。 |
| c）应通过设定终端接入方式或网络地址范围对通过网络进行管理的管理终端进行限制； | 经核查，1）通过配置安全组策略限制仅允许通过堡垒机管理服务器；2）经核查防火墙中访问控制策略，具备堡垒机地址-服务器管理网段（10.33.0.0）的访问控制策略。 |
| d）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； | 根据GB∕T 28448-2019 《信息安全技术 网络安全等级保护测评要求》测评对象范围描述，服务器无该项要求，故判为“不适用”。 |
| e）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； | 1）经过漏洞扫描，服务器不存在高危安全漏洞；2）执行rpm -qa grep patch命令，查看系统补丁已更新至最新。 |
| f）应能够检测到对重要节点进行入侵的行为，并在发生严重入侵事件时提供报警。 | 经核查，服务器上安装有青藤云天眼云镜，对主机入侵行为进行检测，发现严重安全事件时通过钉钉告警。 |
| 恶意代码防范 | a）应采用免受恶意代码攻击的技术措施或主动免疫可信验证机制及时识别入侵和病毒行为，并将其有效阻断。 | 经核查，服务器上安装有青藤云天眼云镜，对主机恶意代码进行检测、清除，每天凌晨自动更新恶意代码特征库，经核查，具备恶意代码特征库更新记录。 |
| 可信验证 | a）可基于可信根对计算设备的系统引导程序、系统程序、重要配置参数和应用程序等进行可信验证，并在应用程序的关键执行环节进行动态可信验证，在检测到其可信性受到破坏后进行报警，并将验证结果形成审计记录送至安全管理中心。 | 未采用技术措施对计算设备的系统引导程序、系统程序、重要配置参数和通信应用程序等进行可信验证。 |
| 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； | 采用SSH协议连接操作系统，保证了鉴别信息以及管理数据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。 | 操作系统中对重要鉴别信息通过自身的加密及校验（SHA256），保证数据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； | 采用SSH协议连接操作系统，保证了鉴别信息以及管理数据在传输过程中的保密性。 |
| b）应采用密码技术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个人信息等。 | 通过系统自带的加密模块保证鉴别数据在存储过程中的保密性。 |
| 数据备份恢复 | a）应提供重要数据的本地数据备份与恢复功能； | 经核查，通过脚本每周将配置文件、代码仓库等数据备份至备份服务器中，依据需要验证备份数据的有效性。 |
| b）应提供异地实时备份功能，利用通信网络将重要数据实时备份至备份场地； | 系统无异地备份机制。 |
| c）应提供重要数据处理系统的热冗余，保证系统的高可用性。 | 服务器采用K8S容器部署，保证系统的高可用性。 |
| 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； | 操作系统提供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功能。 |
| 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。 | 操作系统提供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的功能。 |

4.1.3.51. 应用服务器133

|  |  |  |
| --- | --- | --- |
| **安全控制点** | **测评指标** | **结果记录** |
| 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）操作系统时采用用户名+SSHKey公私钥进行身份鉴别鉴别信息具有复杂度要求；2）执行cat /etc/shadow命令，查看shadow文件系统内用户身份标识唯一，不存在同名用户，且不存在空口令账号；3）经访谈，SSHKey公私钥每半年进行更换；4）查看sshd\_config配置文件中配置PasswordAuthentication no，拒绝使用密码方式进行身份鉴别。 |
| 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； | 操作系统采用用户名+SSHKey公私钥进行身份鉴别，可以防止鉴别信息被暴力破解；但未配置用户连接超时退出策略。 |
| 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； | 1）经核查，管理人员采用SSH协议连接操作系统；2）执行netatat –tpln| grep 23命令查看操作系统远程管理端口，不存在Telnet端口，防止鉴别信息在网络传输过程中的被窃听。 |
| 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。 | 未采用两种或两种以上组合的鉴别技术对用户进行身份鉴别。 |
| 访问控制 | a）应对登录的用户分配账户和权限； | 1）经访谈，通过root账户为登录的用户创建账户、分配权限；2）执行ls -l命令查看关键文件权限，均已为账户分配了相应权限，相关文件权限设置为/etc/shadow：000、/etc/passwd：644、/etc/group：644、/etc/profile：644、/etc/crontab：644、/ etc/securetty：600、/etc/ssh/sshd\_config：600。 |
| b）应重命名或删除默认账户，修改默认账户的默认口令； | 1）执行cat /etc/shadow命令查看shadow文件，操作系统中adm、lp、sync、shutdown、halt、mail、uucp、operator、games、gopher等账户均为nologin状态，存在默认账户root；2）执行more /etc/ssh/sshd\_config命令，查看“PermitRootLogin”参数设置为“yes”，即允许root远程登录；3）经访谈，root用户需通过公私钥方式进行身份鉴别。 |
| 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； | 1）执行cat /etc/shadow命令查看shadow文件，发现操作系统存在root、ysup、yops、yluser等在用账户，不存在多余的、过期账户；2）存在多个堡垒机账户登录操作系统时共用一个账户的情况。 |
| 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； | root账户具有系统所有权限，未实现管理用户的权限分离。 |
| e）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； | 经访谈，由系统管理员root配置访问控制策略，如：/etc/passwd，/etc/profile宿主为root、权限设置为644，audit文件为700、message文件为600，其他文件权限为750，实现用户对文件的权限控制。 |
| f）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； | 由管理用户进行用户访问权限分配进行设置，依据访问控制策略,对各类文件进行访问，重要文件和目录权限均在合理范围内，用户可根据文件不同的权限进行操作。 |
| g）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。 | 执 行more /etc/selinux/config 命令，查看config文件显示 SELINUX参数为 DISABLED，即未开启强制访问控制模式。 |
| 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）执行ps -ef|grep rsyslog和ps -ef|grep auditd命令，显示rsyslog和auditd进程正在运行；2）more /etc/audit/audit.rules，显示审计内容包括：\*.info、authriv.\*、mail.\*、cron.\*、\*.emerg、uucp、news.crit、local7.\*等事件。 |
| 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； | 执行tail -20 /var/log/audit/audit.log命令，查看近20条审计日志，内容包括：时间、对象、路径、用户ID、相关的系统调用、用户执行命令等。 |
| 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）通过访问权限对审计记录进行保护，日志文件/var/log/messages、/var/log/secure、/var/log/audit/audit.log访问 权限均为600；2）审计记录本地保存，且实时备份至360本地安全大脑，保存时间满足180天以上。 |
| d）应对审计进程进行保护，防止未经授权的中断。 | 执行service auditd status命令，系统开启auditd审计保护进程，审计进程由root用户维护，经现场使用yluser用户通过service auditd stop命令尝试中断审计进程，无法将审计进程单独中断。 |
| 入侵防范 | a）应遵循最小安装的原则，仅安装需要的组件和应用程序； | 1）系统安装遵循最小化安装原则；2）执行yum list installed命令查看操作系统已安装的程序包，存在Java、SSH、天眼云镜agent等应用程序或组件，不存在与业务系统无关的组件和应用程序。 |
| b）应关闭不需要的系统服务、默认共享和高危端口； | 1）执行systemctl list-unit-files 命令，系统已关闭FTP、Telnet 等高危网络服务；2）执行netstat -pantu命令，系统关闭了135、445等高危端口，仅开启了22、8080等端口。 |
| c）应通过设定终端接入方式或网络地址范围对通过网络进行管理的管理终端进行限制； | 经核查，1）通过配置安全组策略限制仅允许通过堡垒机管理服务器；2）经核查防火墙中访问控制策略，具备堡垒机地址-服务器管理网段（10.33.0.0）的访问控制策略。 |
| d）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； | 根据GB∕T 28448-2019 《信息安全技术 网络安全等级保护测评要求》测评对象范围描述，服务器无该项要求，故判为“不适用”。 |
| e）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； | 1）经过漏洞扫描，服务器不存在高危安全漏洞；2）执行rpm -qa grep patch命令，查看系统补丁已更新至最新。 |
| f）应能够检测到对重要节点进行入侵的行为，并在发生严重入侵事件时提供报警。 | 经核查，服务器上安装有青藤云天眼云镜，对主机入侵行为进行检测，发现严重安全事件时通过钉钉告警。 |
| 恶意代码防范 | a）应采用免受恶意代码攻击的技术措施或主动免疫可信验证机制及时识别入侵和病毒行为，并将其有效阻断。 | 经核查，服务器上安装有青藤云天眼云镜，对主机恶意代码进行检测、清除，每天凌晨自动更新恶意代码特征库，经核查，具备恶意代码特征库更新记录。 |
| 可信验证 | a）可基于可信根对计算设备的系统引导程序、系统程序、重要配置参数和应用程序等进行可信验证，并在应用程序的关键执行环节进行动态可信验证，在检测到其可信性受到破坏后进行报警，并将验证结果形成审计记录送至安全管理中心。 | 未采用技术措施对计算设备的系统引导程序、系统程序、重要配置参数和通信应用程序等进行可信验证。 |
| 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； | 采用SSH协议连接操作系统，保证了鉴别信息以及管理数据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。 | 操作系统中对重要鉴别信息通过自身的加密及校验（SHA256），保证数据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； | 采用SSH协议连接操作系统，保证了鉴别信息以及管理数据在传输过程中的保密性。 |
| b）应采用密码技术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个人信息等。 | 通过系统自带的加密模块保证鉴别数据在存储过程中的保密性。 |
| 数据备份恢复 | a）应提供重要数据的本地数据备份与恢复功能； | 经核查，通过脚本每周将配置文件、代码仓库等数据备份至备份服务器中，依据需要验证备份数据的有效性。 |
| b）应提供异地实时备份功能，利用通信网络将重要数据实时备份至备份场地； | 系统无异地备份机制。 |
| c）应提供重要数据处理系统的热冗余，保证系统的高可用性。 | 服务器采用K8S容器部署，保证系统的高可用性。 |
| 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； | 操作系统提供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功能。 |
| 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。 | 操作系统提供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的功能。 |

4.1.3.52. 应用服务器136

|  |  |  |
| --- | --- | --- |
| **安全控制点** | **测评指标** | **结果记录** |
| 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）操作系统时采用用户名+SSHKey公私钥进行身份鉴别鉴别信息具有复杂度要求；2）执行cat /etc/shadow命令，查看shadow文件系统内用户身份标识唯一，不存在同名用户，且不存在空口令账号；3）经访谈，SSHKey公私钥每半年进行更换；4）查看sshd\_config配置文件中配置PasswordAuthentication no，拒绝使用密码方式进行身份鉴别。 |
| 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； | 操作系统采用用户名+SSHKey公私钥进行身份鉴别，可以防止鉴别信息被暴力破解；但未配置用户连接超时退出策略。 |
| 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； | 1）经核查，管理人员采用SSH协议连接操作系统；2）执行netatat –tpln| grep 23命令查看操作系统远程管理端口，不存在Telnet端口，防止鉴别信息在网络传输过程中的被窃听。 |
| 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。 | 未采用两种或两种以上组合的鉴别技术对用户进行身份鉴别。 |
| 访问控制 | a）应对登录的用户分配账户和权限； | 1）经访谈，通过root账户为登录的用户创建账户、分配权限；2）执行ls -l命令查看关键文件权限，均已为账户分配了相应权限，相关文件权限设置为/etc/shadow：000、/etc/passwd：644、/etc/group：644、/etc/profile：644、/etc/crontab：644、/ etc/securetty：600、/etc/ssh/sshd\_config：600。 |
| b）应重命名或删除默认账户，修改默认账户的默认口令； | 1）执行cat /etc/shadow命令查看shadow文件，操作系统中adm、lp、sync、shutdown、halt、mail、uucp、operator、games、gopher等账户均为nologin状态，存在默认账户root；2）执行more /etc/ssh/sshd\_config命令，查看“PermitRootLogin”参数设置为“yes”，即允许root远程登录；3）经访谈，root用户需通过公私钥方式进行身份鉴别。 |
| 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； | 1）执行cat /etc/shadow命令查看shadow文件，发现操作系统存在root、ysup、yops、yluser等在用账户，不存在多余的、过期账户；2）存在多个堡垒机账户登录操作系统时共用一个账户的情况。 |
| 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； | root账户具有系统所有权限，未实现管理用户的权限分离。 |
| e）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； | 经访谈，由系统管理员root配置访问控制策略，如：/etc/passwd，/etc/profile宿主为root、权限设置为644，audit文件为700、message文件为600，其他文件权限为750，实现用户对文件的权限控制。 |
| f）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； | 由管理用户进行用户访问权限分配进行设置，依据访问控制策略,对各类文件进行访问，重要文件和目录权限均在合理范围内，用户可根据文件不同的权限进行操作。 |
| g）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。 | 执 行more /etc/selinux/config 命令，查看config文件显示 SELINUX参数为 DISABLED，即未开启强制访问控制模式。 |
| 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）执行ps -ef|grep rsyslog和ps -ef|grep auditd命令，显示rsyslog和auditd进程正在运行；2）more /etc/audit/audit.rules，显示审计内容包括：\*.info、authriv.\*、mail.\*、cron.\*、\*.emerg、uucp、news.crit、local7.\*等事件。 |
| 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； | 执行tail -20 /var/log/audit/audit.log命令，查看近20条审计日志，内容包括：时间、对象、路径、用户ID、相关的系统调用、用户执行命令等。 |
| 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）通过访问权限对审计记录进行保护，日志文件/var/log/messages、/var/log/secure、/var/log/audit/audit.log访问 权限均为600；2）审计记录本地保存，且实时备份至360本地安全大脑，保存时间满足180天以上。 |
| d）应对审计进程进行保护，防止未经授权的中断。 | 执行service auditd status命令，系统开启auditd审计保护进程，审计进程由root用户维护，经现场使用yluser用户通过service auditd stop命令尝试中断审计进程，无法将审计进程单独中断。 |
| 入侵防范 | a）应遵循最小安装的原则，仅安装需要的组件和应用程序； | 1）系统安装遵循最小化安装原则；2）执行yum list installed命令查看操作系统已安装的程序包，存在Java、SSH、天眼云镜agent等应用程序或组件，不存在与业务系统无关的组件和应用程序。 |
| b）应关闭不需要的系统服务、默认共享和高危端口； | 1）执行systemctl list-unit-files 命令，系统已关闭FTP、Telnet 等高危网络服务；2）执行netstat -pantu命令，系统关闭了135、445等高危端口，仅开启了22、8080等端口。 |
| c）应通过设定终端接入方式或网络地址范围对通过网络进行管理的管理终端进行限制； | 经核查，1）通过配置安全组策略限制仅允许通过堡垒机管理服务器；2）经核查防火墙中访问控制策略，具备堡垒机地址-服务器管理网段（10.33.0.0）的访问控制策略。 |
| d）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； | 根据GB∕T 28448-2019 《信息安全技术 网络安全等级保护测评要求》测评对象范围描述，服务器无该项要求，故判为“不适用”。 |
| e）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； | 1）经过漏洞扫描，服务器不存在高危安全漏洞；2）执行rpm -qa grep patch命令，查看系统补丁已更新至最新。 |
| f）应能够检测到对重要节点进行入侵的行为，并在发生严重入侵事件时提供报警。 | 经核查，服务器上安装有青藤云天眼云镜，对主机入侵行为进行检测，发现严重安全事件时通过钉钉告警。 |
| 恶意代码防范 | a）应采用免受恶意代码攻击的技术措施或主动免疫可信验证机制及时识别入侵和病毒行为，并将其有效阻断。 | 经核查，服务器上安装有青藤云天眼云镜，对主机恶意代码进行检测、清除，每天凌晨自动更新恶意代码特征库，经核查，具备恶意代码特征库更新记录。 |
| 可信验证 | a）可基于可信根对计算设备的系统引导程序、系统程序、重要配置参数和应用程序等进行可信验证，并在应用程序的关键执行环节进行动态可信验证，在检测到其可信性受到破坏后进行报警，并将验证结果形成审计记录送至安全管理中心。 | 未采用技术措施对计算设备的系统引导程序、系统程序、重要配置参数和通信应用程序等进行可信验证。 |
| 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； | 采用SSH协议连接操作系统，保证了鉴别信息以及管理数据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。 | 操作系统中对重要鉴别信息通过自身的加密及校验（SHA256），保证数据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； | 采用SSH协议连接操作系统，保证了鉴别信息以及管理数据在传输过程中的保密性。 |
| b）应采用密码技术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个人信息等。 | 通过系统自带的加密模块保证鉴别数据在存储过程中的保密性。 |
| 数据备份恢复 | a）应提供重要数据的本地数据备份与恢复功能； | 经核查，通过脚本每周将配置文件、代码仓库等数据备份至备份服务器中，依据需要验证备份数据的有效性。 |
| b）应提供异地实时备份功能，利用通信网络将重要数据实时备份至备份场地； | 系统无异地备份机制。 |
| c）应提供重要数据处理系统的热冗余，保证系统的高可用性。 | 服务器采用K8S容器部署，保证系统的高可用性。 |
| 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； | 操作系统提供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功能。 |
| 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。 | 操作系统提供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的功能。 |

4.1.3.53. 应用服务器140

|  |  |  |
| --- | --- | --- |
| **安全控制点** | **测评指标** | **结果记录** |
| 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）操作系统时采用用户名+SSHKey公私钥进行身份鉴别鉴别信息具有复杂度要求；2）执行cat /etc/shadow命令，查看shadow文件系统内用户身份标识唯一，不存在同名用户，且不存在空口令账号；3）经访谈，SSHKey公私钥每半年进行更换；4）查看sshd\_config配置文件中配置PasswordAuthentication no，拒绝使用密码方式进行身份鉴别。 |
| 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； | 操作系统采用用户名+SSHKey公私钥进行身份鉴别，可以防止鉴别信息被暴力破解；但未配置用户连接超时退出策略。 |
| 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； | 1）经核查，管理人员采用SSH协议连接操作系统；2）执行netatat –tpln| grep 23命令查看操作系统远程管理端口，不存在Telnet端口，防止鉴别信息在网络传输过程中的被窃听。 |
| 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。 | 未采用两种或两种以上组合的鉴别技术对用户进行身份鉴别。 |
| 访问控制 | a）应对登录的用户分配账户和权限； | 1）经访谈，通过root账户为登录的用户创建账户、分配权限；2）执行ls -l命令查看关键文件权限，均已为账户分配了相应权限，相关文件权限设置为/etc/shadow：000、/etc/passwd：644、/etc/group：644、/etc/profile：644、/etc/crontab：644、/ etc/securetty：600、/etc/ssh/sshd\_config：600。 |
| b）应重命名或删除默认账户，修改默认账户的默认口令； | 1）执行cat /etc/shadow命令查看shadow文件，操作系统中adm、lp、sync、shutdown、halt、mail、uucp、operator、games、gopher等账户均为nologin状态，存在默认账户root；2）执行more /etc/ssh/sshd\_config命令，查看“PermitRootLogin”参数设置为“yes”，即允许root远程登录；3）经访谈，root用户需通过公私钥方式进行身份鉴别。 |
| 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； | 1）执行cat /etc/shadow命令查看shadow文件，发现操作系统存在root、ysup、yops、yluser等在用账户，不存在多余的、过期账户；2）存在多个堡垒机账户登录操作系统时共用一个账户的情况。 |
| 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； | root账户具有系统所有权限，未实现管理用户的权限分离。 |
| e）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； | 经访谈，由系统管理员root配置访问控制策略，如：/etc/passwd，/etc/profile宿主为root、权限设置为644，audit文件为700、message文件为600，其他文件权限为750，实现用户对文件的权限控制。 |
| f）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； | 由管理用户进行用户访问权限分配进行设置，依据访问控制策略,对各类文件进行访问，重要文件和目录权限均在合理范围内，用户可根据文件不同的权限进行操作。 |
| g）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。 | 执 行more /etc/selinux/config 命令，查看config文件显示 SELINUX参数为 DISABLED，即未开启强制访问控制模式。 |
| 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）执行ps -ef|grep rsyslog和ps -ef|grep auditd命令，显示rsyslog和auditd进程正在运行；2）more /etc/audit/audit.rules，显示审计内容包括：\*.info、authriv.\*、mail.\*、cron.\*、\*.emerg、uucp、news.crit、local7.\*等事件。 |
| 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； | 执行tail -20 /var/log/audit/audit.log命令，查看近20条审计日志，内容包括：时间、对象、路径、用户ID、相关的系统调用、用户执行命令等。 |
| 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）通过访问权限对审计记录进行保护，日志文件/var/log/messages、/var/log/secure、/var/log/audit/audit.log访问 权限均为600；2）审计记录本地保存，且实时备份至360本地安全大脑，保存时间满足180天以上。 |
| d）应对审计进程进行保护，防止未经授权的中断。 | 执行service auditd status命令，系统开启auditd审计保护进程，审计进程由root用户维护，经现场使用yluser用户通过service auditd stop命令尝试中断审计进程，无法将审计进程单独中断。 |
| 入侵防范 | a）应遵循最小安装的原则，仅安装需要的组件和应用程序； | 1）系统安装遵循最小化安装原则；2）执行yum list installed命令查看操作系统已安装的程序包，存在Java、SSH、天眼云镜agent等应用程序或组件，不存在与业务系统无关的组件和应用程序。 |
| b）应关闭不需要的系统服务、默认共享和高危端口； | 1）执行systemctl list-unit-files 命令，系统已关闭FTP、Telnet 等高危网络服务；2）执行netstat -pantu命令，系统关闭了135、445等高危端口，仅开启了22、8080等端口。 |
| c）应通过设定终端接入方式或网络地址范围对通过网络进行管理的管理终端进行限制； | 经核查，1）通过配置安全组策略限制仅允许通过堡垒机管理服务器；2）经核查防火墙中访问控制策略，具备堡垒机地址-服务器管理网段（10.33.0.0）的访问控制策略。 |
| d）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； | 根据GB∕T 28448-2019 《信息安全技术 网络安全等级保护测评要求》测评对象范围描述，服务器无该项要求，故判为“不适用”。 |
| e）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； | 1）经过漏洞扫描，服务器不存在高危安全漏洞；2）执行rpm -qa grep patch命令，查看系统补丁已更新至最新。 |
| f）应能够检测到对重要节点进行入侵的行为，并在发生严重入侵事件时提供报警。 | 经核查，服务器上安装有青藤云天眼云镜，对主机入侵行为进行检测，发现严重安全事件时通过钉钉告警。 |
| 恶意代码防范 | a）应采用免受恶意代码攻击的技术措施或主动免疫可信验证机制及时识别入侵和病毒行为，并将其有效阻断。 | 经核查，服务器上安装有青藤云天眼云镜，对主机恶意代码进行检测、清除，每天凌晨自动更新恶意代码特征库，经核查，具备恶意代码特征库更新记录。 |
| 可信验证 | a）可基于可信根对计算设备的系统引导程序、系统程序、重要配置参数和应用程序等进行可信验证，并在应用程序的关键执行环节进行动态可信验证，在检测到其可信性受到破坏后进行报警，并将验证结果形成审计记录送至安全管理中心。 | 未采用技术措施对计算设备的系统引导程序、系统程序、重要配置参数和通信应用程序等进行可信验证。 |
| 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； | 采用SSH协议连接操作系统，保证了鉴别信息以及管理数据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。 | 操作系统中对重要鉴别信息通过自身的加密及校验（SHA256），保证数据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； | 采用SSH协议连接操作系统，保证了鉴别信息以及管理数据在传输过程中的保密性。 |
| b）应采用密码技术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个人信息等。 | 通过系统自带的加密模块保证鉴别数据在存储过程中的保密性。 |
| 数据备份恢复 | a）应提供重要数据的本地数据备份与恢复功能； | 经核查，通过脚本每周将配置文件、代码仓库等数据备份至备份服务器中，依据需要验证备份数据的有效性。 |
| b）应提供异地实时备份功能，利用通信网络将重要数据实时备份至备份场地； | 系统无异地备份机制。 |
| c）应提供重要数据处理系统的热冗余，保证系统的高可用性。 | 服务器采用K8S容器部署，保证系统的高可用性。 |
| 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； | 操作系统提供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功能。 |
| 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。 | 操作系统提供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的功能。 |

4.1.3.54. 应用服务器142

|  |  |  |
| --- | --- | --- |
| **安全控制点** | **测评指标** | **结果记录** |
| 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）操作系统时采用用户名+SSHKey公私钥进行身份鉴别鉴别信息具有复杂度要求；2）执行cat /etc/shadow命令，查看shadow文件系统内用户身份标识唯一，不存在同名用户，且不存在空口令账号；3）经访谈，SSHKey公私钥每半年进行更换；4）查看sshd\_config配置文件中配置PasswordAuthentication no，拒绝使用密码方式进行身份鉴别。 |
| 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； | 操作系统采用用户名+SSHKey公私钥进行身份鉴别，可以防止鉴别信息被暴力破解；但未配置用户连接超时退出策略。 |
| 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； | 1）经核查，管理人员采用SSH协议连接操作系统；2）执行netatat –tpln| grep 23命令查看操作系统远程管理端口，不存在Telnet端口，防止鉴别信息在网络传输过程中的被窃听。 |
| 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。 | 未采用两种或两种以上组合的鉴别技术对用户进行身份鉴别。 |
| 访问控制 | a）应对登录的用户分配账户和权限； | 1）经访谈，通过root账户为登录的用户创建账户、分配权限；2）执行ls -l命令查看关键文件权限，均已为账户分配了相应权限，相关文件权限设置为/etc/shadow：000、/etc/passwd：644、/etc/group：644、/etc/profile：644、/etc/crontab：644、/ etc/securetty：600、/etc/ssh/sshd\_config：600。 |
| b）应重命名或删除默认账户，修改默认账户的默认口令； | 1）执行cat /etc/shadow命令查看shadow文件，操作系统中adm、lp、sync、shutdown、halt、mail、uucp、operator、games、gopher等账户均为nologin状态，存在默认账户root；2）执行more /etc/ssh/sshd\_config命令，查看“PermitRootLogin”参数设置为“yes”，即允许root远程登录；3）经访谈，root用户需通过公私钥方式进行身份鉴别。 |
| 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； | 1）执行cat /etc/shadow命令查看shadow文件，发现操作系统存在root、ysup、yops、yluser等在用账户，不存在多余的、过期账户；2）存在多个堡垒机账户登录操作系统时共用一个账户的情况。 |
| 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； | root账户具有系统所有权限，未实现管理用户的权限分离。 |
| e）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； | 经访谈，由系统管理员root配置访问控制策略，如：/etc/passwd，/etc/profile宿主为root、权限设置为644，audit文件为700、message文件为600，其他文件权限为750，实现用户对文件的权限控制。 |
| f）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； | 由管理用户进行用户访问权限分配进行设置，依据访问控制策略,对各类文件进行访问，重要文件和目录权限均在合理范围内，用户可根据文件不同的权限进行操作。 |
| g）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。 | 执 行more /etc/selinux/config 命令，查看config文件显示 SELINUX参数为 DISABLED，即未开启强制访问控制模式。 |
| 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）执行ps -ef|grep rsyslog和ps -ef|grep auditd命令，显示rsyslog和auditd进程正在运行；2）more /etc/audit/audit.rules，显示审计内容包括：\*.info、authriv.\*、mail.\*、cron.\*、\*.emerg、uucp、news.crit、local7.\*等事件。 |
| 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； | 执行tail -20 /var/log/audit/audit.log命令，查看近20条审计日志，内容包括：时间、对象、路径、用户ID、相关的系统调用、用户执行命令等。 |
| 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）通过访问权限对审计记录进行保护，日志文件/var/log/messages、/var/log/secure、/var/log/audit/audit.log访问 权限均为600；2）审计记录本地保存，且实时备份至360本地安全大脑，保存时间满足180天以上。 |
| d）应对审计进程进行保护，防止未经授权的中断。 | 执行service auditd status命令，系统开启auditd审计保护进程，审计进程由root用户维护，经现场使用yluser用户通过service auditd stop命令尝试中断审计进程，无法将审计进程单独中断。 |
| 入侵防范 | a）应遵循最小安装的原则，仅安装需要的组件和应用程序； | 1）系统安装遵循最小化安装原则；2）执行yum list installed命令查看操作系统已安装的程序包，存在Java、SSH、天眼云镜agent等应用程序或组件，不存在与业务系统无关的组件和应用程序。 |
| b）应关闭不需要的系统服务、默认共享和高危端口； | 1）执行systemctl list-unit-files 命令，系统已关闭FTP、Telnet 等高危网络服务；2）执行netstat -pantu命令，系统关闭了135、445等高危端口，仅开启了22、8080等端口。 |
| c）应通过设定终端接入方式或网络地址范围对通过网络进行管理的管理终端进行限制； | 经核查，1）通过配置安全组策略限制仅允许通过堡垒机管理服务器；2）经核查防火墙中访问控制策略，具备堡垒机地址-服务器管理网段（10.33.0.0）的访问控制策略。 |
| d）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； | 根据GB∕T 28448-2019 《信息安全技术 网络安全等级保护测评要求》测评对象范围描述，服务器无该项要求，故判为“不适用”。 |
| e）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； | 1）经过漏洞扫描，服务器不存在高危安全漏洞；2）执行rpm -qa grep patch命令，查看系统补丁已更新至最新。 |
| f）应能够检测到对重要节点进行入侵的行为，并在发生严重入侵事件时提供报警。 | 经核查，服务器上安装有青藤云天眼云镜，对主机入侵行为进行检测，发现严重安全事件时通过钉钉告警。 |
| 恶意代码防范 | a）应采用免受恶意代码攻击的技术措施或主动免疫可信验证机制及时识别入侵和病毒行为，并将其有效阻断。 | 经核查，服务器上安装有青藤云天眼云镜，对主机恶意代码进行检测、清除，每天凌晨自动更新恶意代码特征库，经核查，具备恶意代码特征库更新记录。 |
| 可信验证 | a）可基于可信根对计算设备的系统引导程序、系统程序、重要配置参数和应用程序等进行可信验证，并在应用程序的关键执行环节进行动态可信验证，在检测到其可信性受到破坏后进行报警，并将验证结果形成审计记录送至安全管理中心。 | 未采用技术措施对计算设备的系统引导程序、系统程序、重要配置参数和通信应用程序等进行可信验证。 |
| 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； | 采用SSH协议连接操作系统，保证了鉴别信息以及管理数据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。 | 操作系统中对重要鉴别信息通过自身的加密及校验（SHA256），保证数据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； | 采用SSH协议连接操作系统，保证了鉴别信息以及管理数据在传输过程中的保密性。 |
| b）应采用密码技术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个人信息等。 | 通过系统自带的加密模块保证鉴别数据在存储过程中的保密性。 |
| 数据备份恢复 | a）应提供重要数据的本地数据备份与恢复功能； | 经核查，通过脚本每周将配置文件、代码仓库等数据备份至备份服务器中，依据需要验证备份数据的有效性。 |
| b）应提供异地实时备份功能，利用通信网络将重要数据实时备份至备份场地； | 系统无异地备份机制。 |
| c）应提供重要数据处理系统的热冗余，保证系统的高可用性。 | 服务器采用K8S容器部署，保证系统的高可用性。 |
| 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； | 操作系统提供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功能。 |
| 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。 | 操作系统提供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的功能。 |

4.1.3.55. 接入代理服务器1

|  |  |  |
| --- | --- | --- |
| **安全控制点** | **测评指标** | **结果记录** |
| 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）操作系统时采用用户名+SSHKey公私钥进行身份鉴别鉴别信息具有复杂度要求；2）执行cat /etc/shadow命令，查看shadow文件系统内用户身份标识唯一，不存在同名用户，且不存在空口令账号；3）经访谈，SSHKey公私钥每半年进行更换；4）查看sshd\_config配置文件中配置PasswordAuthentication no，拒绝使用密码方式进行身份鉴别。 |
| 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； | 操作系统采用用户名+SSHKey公私钥进行身份鉴别，可以防止鉴别信息被暴力破解；但未配置用户连接超时退出策略。 |
| 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； | 1）经核查，管理人员采用SSH协议连接操作系统；2）执行netatat –tpln| grep 23命令查看操作系统远程管理端口，不存在Telnet端口，防止鉴别信息在网络传输过程中的被窃听。 |
| 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。 | 未采用两种或两种以上组合的鉴别技术对用户进行身份鉴别。 |
| 访问控制 | a）应对登录的用户分配账户和权限； | 1）经访谈，通过root账户为登录的用户创建账户、分配权限；2）执行ls -l命令查看关键文件权限，均已为账户分配了相应权限，相关文件权限设置为/etc/shadow：000、/etc/passwd：644、/etc/group：644、/etc/profile：644、/etc/crontab：644、/ etc/securetty：600、/etc/ssh/sshd\_config：600。 |
| b）应重命名或删除默认账户，修改默认账户的默认口令； | 1）执行cat /etc/shadow命令查看shadow文件，操作系统中adm、lp、sync、shutdown、halt、mail、uucp、operator、games、gopher等账户均为nologin状态，存在默认账户root；2）执行more /etc/ssh/sshd\_config命令，查看“PermitRootLogin”参数设置为“yes”，即允许root远程登录；3）经访谈，root用户需通过公私钥方式进行身份鉴别。 |
| 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； | 1）执行cat /etc/shadow命令查看shadow文件，发现操作系统存在root、ysup、yops、yluser等在用账户，不存在多余的、过期账户；2）存在多个堡垒机账户登录操作系统时共用一个账户的情况。 |
| 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； | root账户具有系统所有权限，未实现管理用户的权限分离。 |
| e）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； | 经访谈，由系统管理员root配置访问控制策略，如：/etc/passwd，/etc/profile宿主为root、权限设置为644，audit文件为700、message文件为600，其他文件权限为750，实现用户对文件的权限控制。 |
| f）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； | 由管理用户进行用户访问权限分配进行设置，依据访问控制策略,对各类文件进行访问，重要文件和目录权限均在合理范围内，用户可根据文件不同的权限进行操作。 |
| g）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。 | 执 行more /etc/selinux/config 命令，查看config文件显示 SELINUX参数为 DISABLED，即未开启强制访问控制模式。 |
| 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）执行ps -ef|grep rsyslog和ps -ef|grep auditd命令，显示rsyslog和auditd进程正在运行；2）more /etc/audit/audit.rules，显示审计内容包括：\*.info、authriv.\*、mail.\*、cron.\*、\*.emerg、uucp、news.crit、local7.\*等事件。 |
| 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； | 执行tail -20 /var/log/audit/audit.log命令，查看近20条审计日志，内容包括：时间、对象、路径、用户ID、相关的系统调用、用户执行命令等。 |
| 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）通过访问权限对审计记录进行保护，日志文件/var/log/messages、/var/log/secure、/var/log/audit/audit.log访问 权限均为600；2）审计记录本地保存，且实时备份至360本地安全大脑，保存时间满足180天以上。 |
| d）应对审计进程进行保护，防止未经授权的中断。 | 执行service auditd status命令，系统开启auditd审计保护进程，审计进程由root用户维护，经现场使用yluser用户通过service auditd stop命令尝试中断审计进程，无法将审计进程单独中断。 |
| 入侵防范 | a）应遵循最小安装的原则，仅安装需要的组件和应用程序； | 1）系统安装遵循最小化安装原则；2）执行yum list installed命令查看操作系统已安装的程序包，存在Java、nginx、SSH、天眼云镜agent等应用程序或组件，不存在与业务系统无关的组件和应用程序。 |
| b）应关闭不需要的系统服务、默认共享和高危端口； | 1）执行systemctl list-unit-files 命令，系统已关闭FTP、Telnet 等高危网络服务；2）执行netstat -pantu命令，系统关闭了135、445等高危端口，仅开启了22、8080等端口。 |
| c）应通过设定终端接入方式或网络地址范围对通过网络进行管理的管理终端进行限制； | 经核查，1）通过配置安全组策略限制仅允许通过堡垒机管理服务器；2）经核查防火墙中访问控制策略，具备堡垒机地址-服务器管理网段（10.33.0.0）的访问控制策略。 |
| d）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； | 根据GB∕T 28448-2019 《信息安全技术 网络安全等级保护测评要求》测评对象范围描述，服务器无该项要求，故判为“不适用”。 |
| e）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； | 1）经过漏洞扫描，服务器不存在高危安全漏洞；2）执行rpm -qa grep patch命令，查看系统补丁已更新至最新。 |
| f）应能够检测到对重要节点进行入侵的行为，并在发生严重入侵事件时提供报警。 | 经核查，服务器上安装有青藤云天眼云镜，对主机入侵行为进行检测，发现严重安全事件时通过钉钉告警。 |
| 恶意代码防范 | a）应采用免受恶意代码攻击的技术措施或主动免疫可信验证机制及时识别入侵和病毒行为，并将其有效阻断。 | 经核查，服务器上安装有青藤云天眼云镜，对主机恶意代码进行检测、清除，每天凌晨自动更新恶意代码特征库，经核查，具备恶意代码特征库更新记录。 |
| 可信验证 | a）可基于可信根对计算设备的系统引导程序、系统程序、重要配置参数和应用程序等进行可信验证，并在应用程序的关键执行环节进行动态可信验证，在检测到其可信性受到破坏后进行报警，并将验证结果形成审计记录送至安全管理中心。 | 未采用技术措施对计算设备的系统引导程序、系统程序、重要配置参数和通信应用程序等进行可信验证。 |
| 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； | 采用SSH协议连接操作系统，保证了鉴别信息以及管理数据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。 | 操作系统中对重要鉴别信息通过自身的加密及校验（SHA256），保证数据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； | 采用SSH协议连接操作系统，保证了鉴别信息以及管理数据在传输过程中的保密性。 |
| b）应采用密码技术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个人信息等。 | 通过系统自带的加密模块保证鉴别数据在存储过程中的保密性。 |
| 数据备份恢复 | a）应提供重要数据的本地数据备份与恢复功能； | 经核查，通过脚本每周将配置文件、代码仓库等数据备份至备份服务器中，依据需要验证备份数据的有效性。 |
| b）应提供异地实时备份功能，利用通信网络将重要数据实时备份至备份场地； | 系统无异地备份机制。 |
| c）应提供重要数据处理系统的热冗余，保证系统的高可用性。 | 服务器采用K8S容器部署，保证系统的高可用性。 |
| 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； | 操作系统提供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功能。 |
| 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。 | 操作系统提供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的功能。 |

4.1.3.56. 接入代理服务器2

|  |  |  |
| --- | --- | --- |
| **安全控制点** | **测评指标** | **结果记录** |
| 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）操作系统时采用用户名+SSHKey公私钥进行身份鉴别鉴别信息具有复杂度要求；2）执行cat /etc/shadow命令，查看shadow文件系统内用户身份标识唯一，不存在同名用户，且不存在空口令账号；3）经访谈，SSHKey公私钥每半年进行更换；4）查看sshd\_config配置文件中配置PasswordAuthentication no，拒绝使用密码方式进行身份鉴别。 |
| 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； | 操作系统采用用户名+SSHKey公私钥进行身份鉴别，可以防止鉴别信息被暴力破解；但未配置用户连接超时退出策略。 |
| 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； | 1）经核查，管理人员采用SSH协议连接操作系统；2）执行netatat –tpln| grep 23命令查看操作系统远程管理端口，不存在Telnet端口，防止鉴别信息在网络传输过程中的被窃听。 |
| 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。 | 未采用两种或两种以上组合的鉴别技术对用户进行身份鉴别。 |
| 访问控制 | a）应对登录的用户分配账户和权限； | 1）经访谈，通过root账户为登录的用户创建账户、分配权限；2）执行ls -l命令查看关键文件权限，均已为账户分配了相应权限，相关文件权限设置为/etc/shadow：000、/etc/passwd：644、/etc/group：644、/etc/profile：644、/etc/crontab：644、/ etc/securetty：600、/etc/ssh/sshd\_config：600。 |
| b）应重命名或删除默认账户，修改默认账户的默认口令； | 1）执行cat /etc/shadow命令查看shadow文件，操作系统中adm、lp、sync、shutdown、halt、mail、uucp、operator、games、gopher等账户均为nologin状态，存在默认账户root；2）执行more /etc/ssh/sshd\_config命令，查看“PermitRootLogin”参数设置为“yes”，即允许root远程登录；3）经访谈，root用户需通过公私钥方式进行身份鉴别。 |
| 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； | 1）执行cat /etc/shadow命令查看shadow文件，发现操作系统存在root、ysup、yops、yluser等在用账户，不存在多余的、过期账户；2）存在多个堡垒机账户登录操作系统时共用一个账户的情况。 |
| 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； | root账户具有系统所有权限，未实现管理用户的权限分离。 |
| e）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； | 经访谈，由系统管理员root配置访问控制策略，如：/etc/passwd，/etc/profile宿主为root、权限设置为644，audit文件为700、message文件为600，其他文件权限为750，实现用户对文件的权限控制。 |
| f）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； | 由管理用户进行用户访问权限分配进行设置，依据访问控制策略,对各类文件进行访问，重要文件和目录权限均在合理范围内，用户可根据文件不同的权限进行操作。 |
| g）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。 | 执 行more /etc/selinux/config 命令，查看config文件显示 SELINUX参数为 DISABLED，即未开启强制访问控制模式。 |
| 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）执行ps -ef|grep rsyslog和ps -ef|grep auditd命令，显示rsyslog和auditd进程正在运行；2）more /etc/audit/audit.rules，显示审计内容包括：\*.info、authriv.\*、mail.\*、cron.\*、\*.emerg、uucp、news.crit、local7.\*等事件。 |
| 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； | 执行tail -20 /var/log/audit/audit.log命令，查看近20条审计日志，内容包括：时间、对象、路径、用户ID、相关的系统调用、用户执行命令等。 |
| 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）通过访问权限对审计记录进行保护，日志文件/var/log/messages、/var/log/secure、/var/log/audit/audit.log访问 权限均为600；2）审计记录本地保存，且实时备份至360本地安全大脑，保存时间满足180天以上。 |
| d）应对审计进程进行保护，防止未经授权的中断。 | 执行service auditd status命令，系统开启auditd审计保护进程，审计进程由root用户维护，经现场使用yluser用户通过service auditd stop命令尝试中断审计进程，无法将审计进程单独中断。 |
| 入侵防范 | a）应遵循最小安装的原则，仅安装需要的组件和应用程序； | 1）系统安装遵循最小化安装原则；2）执行yum list installed命令查看操作系统已安装的程序包，存在Java、nginx、SSH、天眼云镜agent等应用程序或组件，不存在与业务系统无关的组件和应用程序。 |
| b）应关闭不需要的系统服务、默认共享和高危端口； | 1）执行systemctl list-unit-files 命令，系统已关闭FTP、Telnet 等高危网络服务；2）执行netstat -pantu命令，系统关闭了135、445等高危端口，仅开启了22、8080等端口。 |
| c）应通过设定终端接入方式或网络地址范围对通过网络进行管理的管理终端进行限制； | 经核查，1）通过配置安全组策略限制仅允许通过堡垒机管理服务器；2）经核查防火墙中访问控制策略，具备堡垒机地址-服务器管理网段（10.33.0.0）的访问控制策略。 |
| d）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； | 根据GB∕T 28448-2019 《信息安全技术 网络安全等级保护测评要求》测评对象范围描述，服务器无该项要求，故判为“不适用”。 |
| e）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； | 1）经过漏洞扫描，服务器不存在高危安全漏洞；2）执行rpm -qa grep patch命令，查看系统补丁已更新至最新。 |
| f）应能够检测到对重要节点进行入侵的行为，并在发生严重入侵事件时提供报警。 | 经核查，服务器上安装有青藤云天眼云镜，对主机入侵行为进行检测，发现严重安全事件时通过钉钉告警。 |
| 恶意代码防范 | a）应采用免受恶意代码攻击的技术措施或主动免疫可信验证机制及时识别入侵和病毒行为，并将其有效阻断。 | 经核查，服务器上安装有青藤云天眼云镜，对主机恶意代码进行检测、清除，每天凌晨自动更新恶意代码特征库，经核查，具备恶意代码特征库更新记录。 |
| 可信验证 | a）可基于可信根对计算设备的系统引导程序、系统程序、重要配置参数和应用程序等进行可信验证，并在应用程序的关键执行环节进行动态可信验证，在检测到其可信性受到破坏后进行报警，并将验证结果形成审计记录送至安全管理中心。 | 未采用技术措施对计算设备的系统引导程序、系统程序、重要配置参数和通信应用程序等进行可信验证。 |
| 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； | 采用SSH协议连接操作系统，保证了鉴别信息以及管理数据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。 | 操作系统中对重要鉴别信息通过自身的加密及校验（SHA256），保证数据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； | 采用SSH协议连接操作系统，保证了鉴别信息以及管理数据在传输过程中的保密性。 |
| b）应采用密码技术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个人信息等。 | 通过系统自带的加密模块保证鉴别数据在存储过程中的保密性。 |
| 数据备份恢复 | a）应提供重要数据的本地数据备份与恢复功能； | 经核查，通过脚本每周将配置文件、代码仓库等数据备份至备份服务器中，依据需要验证备份数据的有效性。 |
| b）应提供异地实时备份功能，利用通信网络将重要数据实时备份至备份场地； | 系统无异地备份机制。 |
| c）应提供重要数据处理系统的热冗余，保证系统的高可用性。 | 服务器采用K8S容器部署，保证系统的高可用性。 |
| 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； | 操作系统提供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功能。 |
| 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。 | 操作系统提供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的功能。 |

4.1.3.57. 接入代理服务器4

|  |  |  |
| --- | --- | --- |
| **安全控制点** | **测评指标** | **结果记录** |
| 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）操作系统时采用用户名+SSHKey公私钥进行身份鉴别鉴别信息具有复杂度要求；2）执行cat /etc/shadow命令，查看shadow文件系统内用户身份标识唯一，不存在同名用户，且不存在空口令账号；3）经访谈，SSHKey公私钥每半年进行更换；4）查看sshd\_config配置文件中配置PasswordAuthentication no，拒绝使用密码方式进行身份鉴别。 |
| 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； | 操作系统采用用户名+SSHKey公私钥进行身份鉴别，可以防止鉴别信息被暴力破解；但未配置用户连接超时退出策略。 |
| 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； | 1）经核查，管理人员采用SSH协议连接操作系统；2）执行netatat –tpln| grep 23命令查看操作系统远程管理端口，不存在Telnet端口，防止鉴别信息在网络传输过程中的被窃听。 |
| 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。 | 未采用两种或两种以上组合的鉴别技术对用户进行身份鉴别。 |
| 访问控制 | a）应对登录的用户分配账户和权限； | 1）经访谈，通过root账户为登录的用户创建账户、分配权限；2）执行ls -l命令查看关键文件权限，均已为账户分配了相应权限，相关文件权限设置为/etc/shadow：000、/etc/passwd：644、/etc/group：644、/etc/profile：644、/etc/crontab：644、/ etc/securetty：600、/etc/ssh/sshd\_config：600。 |
| b）应重命名或删除默认账户，修改默认账户的默认口令； | 1）执行cat /etc/shadow命令查看shadow文件，操作系统中adm、lp、sync、shutdown、halt、mail、uucp、operator、games、gopher等账户均为nologin状态，存在默认账户root；2）执行more /etc/ssh/sshd\_config命令，查看“PermitRootLogin”参数设置为“yes”，即允许root远程登录；3）经访谈，root用户需通过公私钥方式进行身份鉴别。 |
| 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； | 1）执行cat /etc/shadow命令查看shadow文件，发现操作系统存在root、ysup、yops、yluser等在用账户，不存在多余的、过期账户；2）存在多个堡垒机账户登录操作系统时共用一个账户的情况。 |
| 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； | root账户具有系统所有权限，未实现管理用户的权限分离。 |
| e）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； | 经访谈，由系统管理员root配置访问控制策略，如：/etc/passwd，/etc/profile宿主为root、权限设置为644，audit文件为700、message文件为600，其他文件权限为750，实现用户对文件的权限控制。 |
| f）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； | 由管理用户进行用户访问权限分配进行设置，依据访问控制策略,对各类文件进行访问，重要文件和目录权限均在合理范围内，用户可根据文件不同的权限进行操作。 |
| g）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。 | 执 行more /etc/selinux/config 命令，查看config文件显示 SELINUX参数为 DISABLED，即未开启强制访问控制模式。 |
| 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）执行ps -ef|grep rsyslog和ps -ef|grep auditd命令，显示rsyslog和auditd进程正在运行；2）more /etc/audit/audit.rules，显示审计内容包括：\*.info、authriv.\*、mail.\*、cron.\*、\*.emerg、uucp、news.crit、local7.\*等事件。 |
| 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； | 执行tail -20 /var/log/audit/audit.log命令，查看近20条审计日志，内容包括：时间、对象、路径、用户ID、相关的系统调用、用户执行命令等。 |
| 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）通过访问权限对审计记录进行保护，日志文件/var/log/messages、/var/log/secure、/var/log/audit/audit.log访问 权限均为600；2）审计记录本地保存，且实时备份至360本地安全大脑，保存时间满足180天以上。 |
| d）应对审计进程进行保护，防止未经授权的中断。 | 执行service auditd status命令，系统开启auditd审计保护进程，审计进程由root用户维护，经现场使用yluser用户通过service auditd stop命令尝试中断审计进程，无法将审计进程单独中断。 |
| 入侵防范 | a）应遵循最小安装的原则，仅安装需要的组件和应用程序； | 1）系统安装遵循最小化安装原则；2）执行yum list installed命令查看操作系统已安装的程序包，存在Java、nginx、SSH、天眼云镜agent等应用程序或组件，不存在与业务系统无关的组件和应用程序。 |
| b）应关闭不需要的系统服务、默认共享和高危端口； | 1）执行systemctl list-unit-files 命令，系统已关闭FTP、Telnet 等高危网络服务；2）执行netstat -pantu命令，系统关闭了135、445等高危端口，仅开启了22、8080等端口。 |
| c）应通过设定终端接入方式或网络地址范围对通过网络进行管理的管理终端进行限制； | 经核查，1）通过配置安全组策略限制仅允许通过堡垒机管理服务器；2）经核查防火墙中访问控制策略，具备堡垒机地址-服务器管理网段（10.33.0.0）的访问控制策略。 |
| d）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； | 根据GB∕T 28448-2019 《信息安全技术 网络安全等级保护测评要求》测评对象范围描述，服务器无该项要求，故判为“不适用”。 |
| e）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； | 1）经过漏洞扫描，服务器不存在高危安全漏洞；2）执行rpm -qa grep patch命令，查看系统补丁已更新至最新。 |
| f）应能够检测到对重要节点进行入侵的行为，并在发生严重入侵事件时提供报警。 | 经核查，服务器上安装有青藤云天眼云镜，对主机入侵行为进行检测，发现严重安全事件时通过钉钉告警。 |
| 恶意代码防范 | a）应采用免受恶意代码攻击的技术措施或主动免疫可信验证机制及时识别入侵和病毒行为，并将其有效阻断。 | 经核查，服务器上安装有青藤云天眼云镜，对主机恶意代码进行检测、清除，每天凌晨自动更新恶意代码特征库，经核查，具备恶意代码特征库更新记录。 |
| 可信验证 | a）可基于可信根对计算设备的系统引导程序、系统程序、重要配置参数和应用程序等进行可信验证，并在应用程序的关键执行环节进行动态可信验证，在检测到其可信性受到破坏后进行报警，并将验证结果形成审计记录送至安全管理中心。 | 未采用技术措施对计算设备的系统引导程序、系统程序、重要配置参数和通信应用程序等进行可信验证。 |
| 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； | 采用SSH协议连接操作系统，保证了鉴别信息以及管理数据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。 | 操作系统中对重要鉴别信息通过自身的加密及校验（SHA256），保证数据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； | 采用SSH协议连接操作系统，保证了鉴别信息以及管理数据在传输过程中的保密性。 |
| b）应采用密码技术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个人信息等。 | 通过系统自带的加密模块保证鉴别数据在存储过程中的保密性。 |
| 数据备份恢复 | a）应提供重要数据的本地数据备份与恢复功能； | 经核查，通过脚本每周将配置文件、代码仓库等数据备份至备份服务器中，依据需要验证备份数据的有效性。 |
| b）应提供异地实时备份功能，利用通信网络将重要数据实时备份至备份场地； | 系统无异地备份机制。 |
| c）应提供重要数据处理系统的热冗余，保证系统的高可用性。 | 服务器采用K8S容器部署，保证系统的高可用性。 |
| 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； | 操作系统提供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功能。 |
| 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。 | 操作系统提供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的功能。 |

4.1.3.58. 接入代理服务器20

|  |  |  |
| --- | --- | --- |
| **安全控制点** | **测评指标** | **结果记录** |
| 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）操作系统时采用用户名+SSHKey公私钥进行身份鉴别鉴别信息具有复杂度要求；2）执行cat /etc/shadow命令，查看shadow文件系统内用户身份标识唯一，不存在同名用户，且不存在空口令账号；3）经访谈，SSHKey公私钥每半年进行更换；4）查看sshd\_config配置文件中配置PasswordAuthentication no，拒绝使用密码方式进行身份鉴别。 |
| 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； | 操作系统采用用户名+SSHKey公私钥进行身份鉴别，可以防止鉴别信息被暴力破解；但未配置用户连接超时退出策略。 |
| 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； | 1）经核查，管理人员采用SSH协议连接操作系统；2）执行netatat –tpln| grep 23命令查看操作系统远程管理端口，不存在Telnet端口，防止鉴别信息在网络传输过程中的被窃听。 |
| 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。 | 未采用两种或两种以上组合的鉴别技术对用户进行身份鉴别。 |
| 访问控制 | a）应对登录的用户分配账户和权限； | 1）经访谈，通过root账户为登录的用户创建账户、分配权限；2）执行ls -l命令查看关键文件权限，均已为账户分配了相应权限，相关文件权限设置为/etc/shadow：000、/etc/passwd：644、/etc/group：644、/etc/profile：644、/etc/crontab：644、/ etc/securetty：600、/etc/ssh/sshd\_config：600。 |
| b）应重命名或删除默认账户，修改默认账户的默认口令； | 1）执行cat /etc/shadow命令查看shadow文件，操作系统中adm、lp、sync、shutdown、halt、mail、uucp、operator、games、gopher等账户均为nologin状态，存在默认账户root；2）执行more /etc/ssh/sshd\_config命令，查看“PermitRootLogin”参数设置为“yes”，即允许root远程登录；3）经访谈，root用户需通过公私钥方式进行身份鉴别。 |
| 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； | 1）执行cat /etc/shadow命令查看shadow文件，发现操作系统存在root、ysup、yops、yluser等在用账户，不存在多余的、过期账户；2）存在多个堡垒机账户登录操作系统时共用一个账户的情况。 |
| 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； | root账户具有系统所有权限，未实现管理用户的权限分离。 |
| e）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； | 经访谈，由系统管理员root配置访问控制策略，如：/etc/passwd，/etc/profile宿主为root、权限设置为644，audit文件为700、message文件为600，其他文件权限为750，实现用户对文件的权限控制。 |
| f）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； | 由管理用户进行用户访问权限分配进行设置，依据访问控制策略,对各类文件进行访问，重要文件和目录权限均在合理范围内，用户可根据文件不同的权限进行操作。 |
| g）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。 | 执 行more /etc/selinux/config 命令，查看config文件显示 SELINUX参数为 DISABLED，即未开启强制访问控制模式。 |
| 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）执行ps -ef|grep rsyslog和ps -ef|grep auditd命令，显示rsyslog和auditd进程正在运行；2）more /etc/audit/audit.rules，显示审计内容包括：\*.info、authriv.\*、mail.\*、cron.\*、\*.emerg、uucp、news.crit、local7.\*等事件。 |
| 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； | 执行tail -20 /var/log/audit/audit.log命令，查看近20条审计日志，内容包括：时间、对象、路径、用户ID、相关的系统调用、用户执行命令等。 |
| 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）通过访问权限对审计记录进行保护，日志文件/var/log/messages、/var/log/secure、/var/log/audit/audit.log访问 权限均为600；2）审计记录本地保存，且实时备份至360本地安全大脑，保存时间满足180天以上。 |
| d）应对审计进程进行保护，防止未经授权的中断。 | 执行service auditd status命令，系统开启auditd审计保护进程，审计进程由root用户维护，经现场使用yluser用户通过service auditd stop命令尝试中断审计进程，无法将审计进程单独中断。 |
| 入侵防范 | a）应遵循最小安装的原则，仅安装需要的组件和应用程序； | 1）系统安装遵循最小化安装原则；2）执行yum list installed命令查看操作系统已安装的程序包，存在Java、nginx、SSH、天眼云镜agent等应用程序或组件，不存在与业务系统无关的组件和应用程序。 |
| b）应关闭不需要的系统服务、默认共享和高危端口； | 1）执行systemctl list-unit-files 命令，系统已关闭FTP、Telnet 等高危网络服务；2）执行netstat -pantu命令，系统关闭了135、445等高危端口，仅开启了22、8080等端口。 |
| c）应通过设定终端接入方式或网络地址范围对通过网络进行管理的管理终端进行限制； | 经核查，1）通过配置安全组策略限制仅允许通过堡垒机管理服务器；2）经核查防火墙中访问控制策略，具备堡垒机地址-服务器管理网段（10.33.0.0）的访问控制策略。 |
| d）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； | 根据GB∕T 28448-2019 《信息安全技术 网络安全等级保护测评要求》测评对象范围描述，服务器无该项要求，故判为“不适用”。 |
| e）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； | 1）经过漏洞扫描，服务器不存在高危安全漏洞；2）执行rpm -qa grep patch命令，查看系统补丁已更新至最新。 |
| f）应能够检测到对重要节点进行入侵的行为，并在发生严重入侵事件时提供报警。 | 经核查，服务器上安装有青藤云天眼云镜，对主机入侵行为进行检测，发现严重安全事件时通过钉钉告警。 |
| 恶意代码防范 | a）应采用免受恶意代码攻击的技术措施或主动免疫可信验证机制及时识别入侵和病毒行为，并将其有效阻断。 | 经核查，服务器上安装有青藤云天眼云镜，对主机恶意代码进行检测、清除，每天凌晨自动更新恶意代码特征库，经核查，具备恶意代码特征库更新记录。 |
| 可信验证 | a）可基于可信根对计算设备的系统引导程序、系统程序、重要配置参数和应用程序等进行可信验证，并在应用程序的关键执行环节进行动态可信验证，在检测到其可信性受到破坏后进行报警，并将验证结果形成审计记录送至安全管理中心。 | 未采用技术措施对计算设备的系统引导程序、系统程序、重要配置参数和通信应用程序等进行可信验证。 |
| 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； | 采用SSH协议连接操作系统，保证了鉴别信息以及管理数据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。 | 操作系统中对重要鉴别信息通过自身的加密及校验（SHA256），保证数据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； | 采用SSH协议连接操作系统，保证了鉴别信息以及管理数据在传输过程中的保密性。 |
| b）应采用密码技术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个人信息等。 | 通过系统自带的加密模块保证鉴别数据在存储过程中的保密性。 |
| 数据备份恢复 | a）应提供重要数据的本地数据备份与恢复功能； | 经核查，通过脚本每周将配置文件、代码仓库等数据备份至备份服务器中，依据需要验证备份数据的有效性。 |
| b）应提供异地实时备份功能，利用通信网络将重要数据实时备份至备份场地； | 系统无异地备份机制。 |
| c）应提供重要数据处理系统的热冗余，保证系统的高可用性。 | 服务器采用K8S容器部署，保证系统的高可用性。 |
| 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； | 操作系统提供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功能。 |
| 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。 | 操作系统提供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的功能。 |

4.1.3.59. 接入代理服务器21

|  |  |  |
| --- | --- | --- |
| **安全控制点** | **测评指标** | **结果记录** |
| 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）操作系统时采用用户名+SSHKey公私钥进行身份鉴别鉴别信息具有复杂度要求；2）执行cat /etc/shadow命令，查看shadow文件系统内用户身份标识唯一，不存在同名用户，且不存在空口令账号；3）经访谈，SSHKey公私钥每半年进行更换；4）查看sshd\_config配置文件中配置PasswordAuthentication no，拒绝使用密码方式进行身份鉴别。 |
| 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； | 操作系统采用用户名+SSHKey公私钥进行身份鉴别，可以防止鉴别信息被暴力破解；但未配置用户连接超时退出策略。 |
| 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； | 1）经核查，管理人员采用SSH协议连接操作系统；2）执行netatat –tpln| grep 23命令查看操作系统远程管理端口，不存在Telnet端口，防止鉴别信息在网络传输过程中的被窃听。 |
| 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。 | 未采用两种或两种以上组合的鉴别技术对用户进行身份鉴别。 |
| 访问控制 | a）应对登录的用户分配账户和权限； | 1）经访谈，通过root账户为登录的用户创建账户、分配权限；2）执行ls -l命令查看关键文件权限，均已为账户分配了相应权限，相关文件权限设置为/etc/shadow：000、/etc/passwd：644、/etc/group：644、/etc/profile：644、/etc/crontab：644、/ etc/securetty：600、/etc/ssh/sshd\_config：600。 |
| b）应重命名或删除默认账户，修改默认账户的默认口令； | 1）执行cat /etc/shadow命令查看shadow文件，操作系统中adm、lp、sync、shutdown、halt、mail、uucp、operator、games、gopher等账户均为nologin状态，存在默认账户root；2）执行more /etc/ssh/sshd\_config命令，查看“PermitRootLogin”参数设置为“yes”，即允许root远程登录；3）经访谈，root用户需通过公私钥方式进行身份鉴别。 |
| 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； | 1）执行cat /etc/shadow命令查看shadow文件，发现操作系统存在root、ysup、yops、yluser等在用账户，不存在多余的、过期账户；2）存在多个堡垒机账户登录操作系统时共用一个账户的情况。 |
| 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； | root账户具有系统所有权限，未实现管理用户的权限分离。 |
| e）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； | 经访谈，由系统管理员root配置访问控制策略，如：/etc/passwd，/etc/profile宿主为root、权限设置为644，audit文件为700、message文件为600，其他文件权限为750，实现用户对文件的权限控制。 |
| f）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； | 由管理用户进行用户访问权限分配进行设置，依据访问控制策略,对各类文件进行访问，重要文件和目录权限均在合理范围内，用户可根据文件不同的权限进行操作。 |
| g）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。 | 执 行more /etc/selinux/config 命令，查看config文件显示 SELINUX参数为 DISABLED，即未开启强制访问控制模式。 |
| 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）执行ps -ef|grep rsyslog和ps -ef|grep auditd命令，显示rsyslog和auditd进程正在运行；2）more /etc/audit/audit.rules，显示审计内容包括：\*.info、authriv.\*、mail.\*、cron.\*、\*.emerg、uucp、news.crit、local7.\*等事件。 |
| 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； | 执行tail -20 /var/log/audit/audit.log命令，查看近20条审计日志，内容包括：时间、对象、路径、用户ID、相关的系统调用、用户执行命令等。 |
| 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）通过访问权限对审计记录进行保护，日志文件/var/log/messages、/var/log/secure、/var/log/audit/audit.log访问 权限均为600；2）审计记录本地保存，且实时备份至360本地安全大脑，保存时间满足180天以上。 |
| d）应对审计进程进行保护，防止未经授权的中断。 | 执行service auditd status命令，系统开启auditd审计保护进程，审计进程由root用户维护，经现场使用yluser用户通过service auditd stop命令尝试中断审计进程，无法将审计进程单独中断。 |
| 入侵防范 | a）应遵循最小安装的原则，仅安装需要的组件和应用程序； | 1）系统安装遵循最小化安装原则；2）执行yum list installed命令查看操作系统已安装的程序包，存在Java、nginx、SSH、天眼云镜agent等应用程序或组件，不存在与业务系统无关的组件和应用程序。 |
| b）应关闭不需要的系统服务、默认共享和高危端口； | 1）执行systemctl list-unit-files 命令，系统已关闭FTP、Telnet 等高危网络服务；2）执行netstat -pantu命令，系统关闭了135、445等高危端口，仅开启了22、8080等端口。 |
| c）应通过设定终端接入方式或网络地址范围对通过网络进行管理的管理终端进行限制； | 经核查，1）通过配置安全组策略限制仅允许通过堡垒机管理服务器；2）经核查防火墙中访问控制策略，具备堡垒机地址-服务器管理网段（10.33.0.0）的访问控制策略。 |
| d）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； | 根据GB∕T 28448-2019 《信息安全技术 网络安全等级保护测评要求》测评对象范围描述，服务器无该项要求，故判为“不适用”。 |
| e）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； | 1）经过漏洞扫描，服务器不存在高危安全漏洞；2）执行rpm -qa grep patch命令，查看系统补丁已更新至最新。 |
| f）应能够检测到对重要节点进行入侵的行为，并在发生严重入侵事件时提供报警。 | 经核查，服务器上安装有青藤云天眼云镜，对主机入侵行为进行检测，发现严重安全事件时通过钉钉告警。 |
| 恶意代码防范 | a）应采用免受恶意代码攻击的技术措施或主动免疫可信验证机制及时识别入侵和病毒行为，并将其有效阻断。 | 经核查，服务器上安装有青藤云天眼云镜，对主机恶意代码进行检测、清除，每天凌晨自动更新恶意代码特征库，经核查，具备恶意代码特征库更新记录。 |
| 可信验证 | a）可基于可信根对计算设备的系统引导程序、系统程序、重要配置参数和应用程序等进行可信验证，并在应用程序的关键执行环节进行动态可信验证，在检测到其可信性受到破坏后进行报警，并将验证结果形成审计记录送至安全管理中心。 | 未采用技术措施对计算设备的系统引导程序、系统程序、重要配置参数和通信应用程序等进行可信验证。 |
| 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； | 采用SSH协议连接操作系统，保证了鉴别信息以及管理数据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。 | 操作系统中对重要鉴别信息通过自身的加密及校验（SHA256），保证数据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； | 采用SSH协议连接操作系统，保证了鉴别信息以及管理数据在传输过程中的保密性。 |
| b）应采用密码技术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个人信息等。 | 通过系统自带的加密模块保证鉴别数据在存储过程中的保密性。 |
| 数据备份恢复 | a）应提供重要数据的本地数据备份与恢复功能； | 经核查，通过脚本每周将配置文件、代码仓库等数据备份至备份服务器中，依据需要验证备份数据的有效性。 |
| b）应提供异地实时备份功能，利用通信网络将重要数据实时备份至备份场地； | 系统无异地备份机制。 |
| c）应提供重要数据处理系统的热冗余，保证系统的高可用性。 | 服务器采用K8S容器部署，保证系统的高可用性。 |
| 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； | 操作系统提供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功能。 |
| 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。 | 操作系统提供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的功能。 |

4.1.3.60. 堡垒机服务器1

|  |  |  |
| --- | --- | --- |
| **安全控制点** | **测评指标** | **结果记录** |
| 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）操作系统时采用用户名+SSHKey公私钥进行身份鉴别鉴别信息具有复杂度要求；2）执行cat /etc/shadow命令，查看shadow文件系统内用户身份标识唯一，不存在同名用户，且不存在空口令账号；3）经访谈，SSHKey公私钥每半年进行更换；4）查看sshd\_config配置文件中配置PasswordAuthentication no，拒绝使用密码方式进行身份鉴别。 |
| 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； | 操作系统采用用户名+SSHKey公私钥进行身份鉴别，可以防止鉴别信息被暴力破解；但未配置用户连接超时退出策略。 |
| 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； | 1）经核查，管理人员采用SSH协议连接操作系统；2）执行netatat –tpln| grep 23命令查看操作系统远程管理端口，不存在Telnet端口，防止鉴别信息在网络传输过程中的被窃听。 |
| 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。 | 未采用两种或两种以上组合的鉴别技术对用户进行身份鉴别。 |
| 访问控制 | a）应对登录的用户分配账户和权限； | 1）经访谈，通过root账户为登录的用户创建账户、分配权限；2）执行ls -l命令查看关键文件权限，均已为账户分配了相应权限，相关文件权限设置为/etc/shadow：000、/etc/passwd：644、/etc/group：644、/etc/profile：644、/etc/crontab：644、/ etc/securetty：600、/etc/ssh/sshd\_config：600。 |
| b）应重命名或删除默认账户，修改默认账户的默认口令； | 1）执行cat /etc/shadow命令查看shadow文件，操作系统中adm、lp、sync、shutdown、halt、mail、uucp、operator、games、gopher等账户均为nologin状态，存在默认账户root；2）执行more /etc/ssh/sshd\_config命令，查看“PermitRootLogin”参数设置为“yes”，即允许root远程登录；3）经访谈，root用户需通过公私钥方式进行身份鉴别。 |
| 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； | 1）执行cat /etc/shadow命令查看shadow文件，发现操作系统存在root、ysup、yops、yluser等在用账户，不存在多余的、过期账户；2）存在多个堡垒机账户登录操作系统时共用一个账户的情况。 |
| 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； | root账户具有系统所有权限，未实现管理用户的权限分离。 |
| e）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； | 经访谈，由系统管理员root配置访问控制策略，如：/etc/passwd，/etc/profile宿主为root、权限设置为644，audit文件为700、message文件为600，其他文件权限为750，实现用户对文件的权限控制。 |
| f）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； | 由管理用户进行用户访问权限分配进行设置，依据访问控制策略,对各类文件进行访问，重要文件和目录权限均在合理范围内，用户可根据文件不同的权限进行操作。 |
| g）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。 | 执 行more /etc/selinux/config 命令，查看config文件显示 SELINUX参数为 DISABLED，即未开启强制访问控制模式。 |
| 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）执行ps -ef|grep rsyslog和ps -ef|grep auditd命令，显示rsyslog和auditd进程正在运行；2）more /etc/audit/audit.rules，显示审计内容包括：\*.info、authriv.\*、mail.\*、cron.\*、\*.emerg、uucp、news.crit、local7.\*等事件。 |
| 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； | 执行tail -20 /var/log/audit/audit.log命令，查看近20条审计日志，内容包括：时间、对象、路径、用户ID、相关的系统调用、用户执行命令等。 |
| 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）通过访问权限对审计记录进行保护，日志文件/var/log/messages、/var/log/secure、/var/log/audit/audit.log访问 权限均为600；2）审计记录本地保存，且实时备份至360本地安全大脑，保存时间满足180天以上。 |
| d）应对审计进程进行保护，防止未经授权的中断。 | 执行service auditd status命令，系统开启auditd审计保护进程，审计进程由root用户维护，经现场使用yluser用户通过service auditd stop命令尝试中断审计进程，无法将审计进程单独中断。 |
| 入侵防范 | a）应遵循最小安装的原则，仅安装需要的组件和应用程序； | 1）系统安装遵循最小化安装原则；2）执行yum list installed命令查看操作系统已安装的程序包，存在Java、jumpserver、SSH、天眼云镜agent等应用程序或组件，不存在与业务系统无关的组件和应用程序。 |
| b）应关闭不需要的系统服务、默认共享和高危端口； | 1）执行systemctl list-unit-files 命令，系统已关闭FTP、Telnet 等高危网络服务；2）执行netstat -pantu命令，系统关闭了135、445等高危端口，仅开启了22、8080等端口。 |
| c）应通过设定终端接入方式或网络地址范围对通过网络进行管理的管理终端进行限制； | 经核查，1）通过配置安全组策略限制仅允许通过堡垒机管理服务器；2）经核查防火墙中访问控制策略，具备堡垒机地址-服务器管理网段（10.33.0.0）的访问控制策略。 |
| d）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； | 根据GB∕T 28448-2019 《信息安全技术 网络安全等级保护测评要求》测评对象范围描述，服务器无该项要求，故判为“不适用”。 |
| e）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； | 1）经过漏洞扫描，服务器不存在高危安全漏洞；2）执行rpm -qa grep patch命令，查看系统补丁已更新至最新。 |
| f）应能够检测到对重要节点进行入侵的行为，并在发生严重入侵事件时提供报警。 | 经核查，服务器上安装有青藤云天眼云镜，对主机入侵行为进行检测，发现严重安全事件时通过钉钉告警。 |
| 恶意代码防范 | a）应采用免受恶意代码攻击的技术措施或主动免疫可信验证机制及时识别入侵和病毒行为，并将其有效阻断。 | 经核查，服务器上安装有青藤云天眼云镜，对主机恶意代码进行检测、清除，每天凌晨自动更新恶意代码特征库，经核查，具备恶意代码特征库更新记录。 |
| 可信验证 | a）可基于可信根对计算设备的系统引导程序、系统程序、重要配置参数和应用程序等进行可信验证，并在应用程序的关键执行环节进行动态可信验证，在检测到其可信性受到破坏后进行报警，并将验证结果形成审计记录送至安全管理中心。 | 未采用技术措施对计算设备的系统引导程序、系统程序、重要配置参数和通信应用程序等进行可信验证。 |
| 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； | 采用SSH协议连接操作系统，保证了鉴别信息以及管理数据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。 | 操作系统中对重要鉴别信息通过自身的加密及校验（SHA256），保证数据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； | 采用SSH协议连接操作系统，保证了鉴别信息以及管理数据在传输过程中的保密性。 |
| b）应采用密码技术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个人信息等。 | 通过系统自带的加密模块保证鉴别数据在存储过程中的保密性。 |
| 数据备份恢复 | a）应提供重要数据的本地数据备份与恢复功能； | 经核查，通过脚本每周将配置文件、代码仓库等数据备份至备份服务器中，依据需要验证备份数据的有效性。 |
| b）应提供异地实时备份功能，利用通信网络将重要数据实时备份至备份场地； | 系统无异地备份机制。 |
| c）应提供重要数据处理系统的热冗余，保证系统的高可用性。 | 服务器采用K8S容器部署，保证系统的高可用性。 |
| 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； | 操作系统提供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功能。 |
| 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。 | 操作系统提供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的功能。 |

4.1.3.61. 堡垒机服务器2

|  |  |  |
| --- | --- | --- |
| **安全控制点** | **测评指标** | **结果记录** |
| 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）操作系统时采用用户名+SSHKey公私钥进行身份鉴别鉴别信息具有复杂度要求；2）执行cat /etc/shadow命令，查看shadow文件系统内用户身份标识唯一，不存在同名用户，且不存在空口令账号；3）经访谈，SSHKey公私钥每半年进行更换；4）查看sshd\_config配置文件中配置PasswordAuthentication no，拒绝使用密码方式进行身份鉴别。 |
| 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； | 操作系统采用用户名+SSHKey公私钥进行身份鉴别，可以防止鉴别信息被暴力破解；但未配置用户连接超时退出策略。 |
| 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； | 1）经核查，管理人员采用SSH协议连接操作系统；2）执行netatat –tpln| grep 23命令查看操作系统远程管理端口，不存在Telnet端口，防止鉴别信息在网络传输过程中的被窃听。 |
| 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。 | 未采用两种或两种以上组合的鉴别技术对用户进行身份鉴别。 |
| 访问控制 | a）应对登录的用户分配账户和权限； | 1）经访谈，通过root账户为登录的用户创建账户、分配权限；2）执行ls -l命令查看关键文件权限，均已为账户分配了相应权限，相关文件权限设置为/etc/shadow：000、/etc/passwd：644、/etc/group：644、/etc/profile：644、/etc/crontab：644、/ etc/securetty：600、/etc/ssh/sshd\_config：600。 |
| b）应重命名或删除默认账户，修改默认账户的默认口令； | 1）执行cat /etc/shadow命令查看shadow文件，操作系统中adm、lp、sync、shutdown、halt、mail、uucp、operator、games、gopher等账户均为nologin状态，存在默认账户root；2）执行more /etc/ssh/sshd\_config命令，查看“PermitRootLogin”参数设置为“yes”，即允许root远程登录；3）经访谈，root用户需通过公私钥方式进行身份鉴别。 |
| 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； | 1）执行cat /etc/shadow命令查看shadow文件，发现操作系统存在root、ysup、yops、yluser等在用账户，不存在多余的、过期账户；2）存在多个堡垒机账户登录操作系统时共用一个账户的情况。 |
| 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； | root账户具有系统所有权限，未实现管理用户的权限分离。 |
| e）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； | 经访谈，由系统管理员root配置访问控制策略，如：/etc/passwd，/etc/profile宿主为root、权限设置为644，audit文件为700、message文件为600，其他文件权限为750，实现用户对文件的权限控制。 |
| f）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； | 由管理用户进行用户访问权限分配进行设置，依据访问控制策略,对各类文件进行访问，重要文件和目录权限均在合理范围内，用户可根据文件不同的权限进行操作。 |
| g）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。 | 执 行more /etc/selinux/config 命令，查看config文件显示 SELINUX参数为 DISABLED，即未开启强制访问控制模式。 |
| 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）执行ps -ef|grep rsyslog和ps -ef|grep auditd命令，显示rsyslog和auditd进程正在运行；2）more /etc/audit/audit.rules，显示审计内容包括：\*.info、authriv.\*、mail.\*、cron.\*、\*.emerg、uucp、news.crit、local7.\*等事件。 |
| 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； | 执行tail -20 /var/log/audit/audit.log命令，查看近20条审计日志，内容包括：时间、对象、路径、用户ID、相关的系统调用、用户执行命令等。 |
| 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）通过访问权限对审计记录进行保护，日志文件/var/log/messages、/var/log/secure、/var/log/audit/audit.log访问 权限均为600；2）审计记录本地保存，且实时备份至360本地安全大脑，保存时间满足180天以上。 |
| d）应对审计进程进行保护，防止未经授权的中断。 | 执行service auditd status命令，系统开启auditd审计保护进程，审计进程由root用户维护，经现场使用yluser用户通过service auditd stop命令尝试中断审计进程，无法将审计进程单独中断。 |
| 入侵防范 | a）应遵循最小安装的原则，仅安装需要的组件和应用程序； | 1）系统安装遵循最小化安装原则；2）执行yum list installed命令查看操作系统已安装的程序包，存在Java、jumpserver、SSH、天眼云镜agent等应用程序或组件，不存在与业务系统无关的组件和应用程序。 |
| b）应关闭不需要的系统服务、默认共享和高危端口； | 1）执行systemctl list-unit-files 命令，系统已关闭FTP、Telnet 等高危网络服务；2）执行netstat -pantu命令，系统关闭了135、445等高危端口，仅开启了22、8080等端口。 |
| c）应通过设定终端接入方式或网络地址范围对通过网络进行管理的管理终端进行限制； | 经核查，1）通过配置安全组策略限制仅允许通过堡垒机管理服务器；2）经核查防火墙中访问控制策略，具备堡垒机地址-服务器管理网段（10.33.0.0）的访问控制策略。 |
| d）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； | 根据GB∕T 28448-2019 《信息安全技术 网络安全等级保护测评要求》测评对象范围描述，服务器无该项要求，故判为“不适用”。 |
| e）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； | 1）经过漏洞扫描，服务器不存在高危安全漏洞；2）执行rpm -qa grep patch命令，查看系统补丁已更新至最新。 |
| f）应能够检测到对重要节点进行入侵的行为，并在发生严重入侵事件时提供报警。 | 经核查，服务器上安装有青藤云天眼云镜，对主机入侵行为进行检测，发现严重安全事件时通过钉钉告警。 |
| 恶意代码防范 | a）应采用免受恶意代码攻击的技术措施或主动免疫可信验证机制及时识别入侵和病毒行为，并将其有效阻断。 | 经核查，服务器上安装有青藤云天眼云镜，对主机恶意代码进行检测、清除，每天凌晨自动更新恶意代码特征库，经核查，具备恶意代码特征库更新记录。 |
| 可信验证 | a）可基于可信根对计算设备的系统引导程序、系统程序、重要配置参数和应用程序等进行可信验证，并在应用程序的关键执行环节进行动态可信验证，在检测到其可信性受到破坏后进行报警，并将验证结果形成审计记录送至安全管理中心。 | 未采用技术措施对计算设备的系统引导程序、系统程序、重要配置参数和通信应用程序等进行可信验证。 |
| 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； | 采用SSH协议连接操作系统，保证了鉴别信息以及管理数据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。 | 操作系统中对重要鉴别信息通过自身的加密及校验（SHA256），保证数据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； | 采用SSH协议连接操作系统，保证了鉴别信息以及管理数据在传输过程中的保密性。 |
| b）应采用密码技术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个人信息等。 | 通过系统自带的加密模块保证鉴别数据在存储过程中的保密性。 |
| 数据备份恢复 | a）应提供重要数据的本地数据备份与恢复功能； | 经核查，通过脚本每周将配置文件、代码仓库等数据备份至备份服务器中，依据需要验证备份数据的有效性。 |
| b）应提供异地实时备份功能，利用通信网络将重要数据实时备份至备份场地； | 系统无异地备份机制。 |
| c）应提供重要数据处理系统的热冗余，保证系统的高可用性。 | 服务器采用K8S容器部署，保证系统的高可用性。 |
| 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； | 操作系统提供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功能。 |
| 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。 | 操作系统提供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的功能。 |

4.1.3.62. 数据索引服务器1

|  |  |  |
| --- | --- | --- |
| **安全控制点** | **测评指标** | **结果记录** |
| 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）操作系统时采用用户名+SSHKey公私钥进行身份鉴别鉴别信息具有复杂度要求；2）执行cat /etc/shadow命令，查看shadow文件系统内用户身份标识唯一，不存在同名用户，且不存在空口令账号；3）经访谈，SSHKey公私钥每半年进行更换；4）查看sshd\_config配置文件中配置PasswordAuthentication no，拒绝使用密码方式进行身份鉴别。 |
| 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； | 操作系统采用用户名+SSHKey公私钥进行身份鉴别，可以防止鉴别信息被暴力破解；但未配置用户连接超时退出策略。 |
| 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； | 1）经核查，管理人员采用SSH协议连接操作系统；2）执行netatat –tpln| grep 23命令查看操作系统远程管理端口，不存在Telnet端口，防止鉴别信息在网络传输过程中的被窃听。 |
| 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。 | 未采用两种或两种以上组合的鉴别技术对用户进行身份鉴别。 |
| 访问控制 | a）应对登录的用户分配账户和权限； | 1）经访谈，通过root账户为登录的用户创建账户、分配权限；2）执行ls -l命令查看关键文件权限，均已为账户分配了相应权限，相关文件权限设置为/etc/shadow：000、/etc/passwd：644、/etc/group：644、/etc/profile：644、/etc/crontab：644、/ etc/securetty：600、/etc/ssh/sshd\_config：600。 |
| b）应重命名或删除默认账户，修改默认账户的默认口令； | 1）执行cat /etc/shadow命令查看shadow文件，操作系统中adm、lp、sync、shutdown、halt、mail、uucp、operator、games、gopher等账户均为nologin状态，存在默认账户root；2）执行more /etc/ssh/sshd\_config命令，查看“PermitRootLogin”参数设置为“yes”，即允许root远程登录；3）经访谈，root用户需通过公私钥方式进行身份鉴别。 |
| 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； | 1）执行cat /etc/shadow命令查看shadow文件，发现操作系统存在root、ysup、yops、yluser等在用账户，不存在多余的、过期账户；2）存在多个堡垒机账户登录操作系统时共用一个账户的情况。 |
| 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； | root账户具有系统所有权限，未实现管理用户的权限分离。 |
| e）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； | 经访谈，由系统管理员root配置访问控制策略，如：/etc/passwd，/etc/profile宿主为root、权限设置为644，audit文件为700、message文件为600，其他文件权限为750，实现用户对文件的权限控制。 |
| f）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； | 由管理用户进行用户访问权限分配进行设置，依据访问控制策略,对各类文件进行访问，重要文件和目录权限均在合理范围内，用户可根据文件不同的权限进行操作。 |
| g）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。 | 执 行more /etc/selinux/config 命令，查看config文件显示 SELINUX参数为 DISABLED，即未开启强制访问控制模式。 |
| 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）执行ps -ef|grep rsyslog和ps -ef|grep auditd命令，显示rsyslog和auditd进程正在运行；2）more /etc/audit/audit.rules，显示审计内容包括：\*.info、authriv.\*、mail.\*、cron.\*、\*.emerg、uucp、news.crit、local7.\*等事件。 |
| 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； | 执行tail -20 /var/log/audit/audit.log命令，查看近20条审计日志，内容包括：时间、对象、路径、用户ID、相关的系统调用、用户执行命令等。 |
| 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）通过访问权限对审计记录进行保护，日志文件/var/log/messages、/var/log/secure、/var/log/audit/audit.log访问 权限均为600；2）审计记录本地保存，且实时备份至360本地安全大脑，保存时间满足180天以上。 |
| d）应对审计进程进行保护，防止未经授权的中断。 | 执行service auditd status命令，系统开启auditd审计保护进程，审计进程由root用户维护，经现场使用yluser用户通过service auditd stop命令尝试中断审计进程，无法将审计进程单独中断。 |
| 入侵防范 | a）应遵循最小安装的原则，仅安装需要的组件和应用程序； | 1）系统安装遵循最小化安装原则；2）执行yum list installed命令查看操作系统已安装的程序包，存在Java、elasticsearch、SSH、天眼云镜agent等应用程序或组件，不存在与业务系统无关的组件和应用程序。 |
| b）应关闭不需要的系统服务、默认共享和高危端口； | 1）执行systemctl list-unit-files 命令，系统已关闭FTP、Telnet 等高危网络服务；2）执行netstat -pantu命令，系统关闭了135、445等高危端口，仅开启了22、8080等端口。 |
| c）应通过设定终端接入方式或网络地址范围对通过网络进行管理的管理终端进行限制； | 经核查，1）通过配置安全组策略限制仅允许通过堡垒机管理服务器；2）经核查防火墙中访问控制策略，具备堡垒机地址-服务器管理网段（10.33.0.0）的访问控制策略。 |
| d）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； | 根据GB∕T 28448-2019 《信息安全技术 网络安全等级保护测评要求》测评对象范围描述，服务器无该项要求，故判为“不适用”。 |
| e）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； | 1）经过漏洞扫描，服务器不存在高危安全漏洞；2）执行rpm -qa grep patch命令，查看系统补丁已更新至最新。 |
| f）应能够检测到对重要节点进行入侵的行为，并在发生严重入侵事件时提供报警。 | 经核查，服务器上安装有青藤云天眼云镜，对主机入侵行为进行检测，发现严重安全事件时通过钉钉告警。 |
| 恶意代码防范 | a）应采用免受恶意代码攻击的技术措施或主动免疫可信验证机制及时识别入侵和病毒行为，并将其有效阻断。 | 经核查，服务器上安装有青藤云天眼云镜，对主机恶意代码进行检测、清除，每天凌晨自动更新恶意代码特征库，经核查，具备恶意代码特征库更新记录。 |
| 可信验证 | a）可基于可信根对计算设备的系统引导程序、系统程序、重要配置参数和应用程序等进行可信验证，并在应用程序的关键执行环节进行动态可信验证，在检测到其可信性受到破坏后进行报警，并将验证结果形成审计记录送至安全管理中心。 | 未采用技术措施对计算设备的系统引导程序、系统程序、重要配置参数和通信应用程序等进行可信验证。 |
| 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； | 采用SSH协议连接操作系统，保证了鉴别信息以及管理数据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。 | 操作系统中对重要鉴别信息通过自身的加密及校验（SHA256），保证数据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； | 采用SSH协议连接操作系统，保证了鉴别信息以及管理数据在传输过程中的保密性。 |
| b）应采用密码技术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个人信息等。 | 通过系统自带的加密模块保证鉴别数据在存储过程中的保密性。 |
| 数据备份恢复 | a）应提供重要数据的本地数据备份与恢复功能； | 经核查，通过脚本每周将配置文件、代码仓库等数据备份至备份服务器中，依据需要验证备份数据的有效性。 |
| b）应提供异地实时备份功能，利用通信网络将重要数据实时备份至备份场地； | 系统无异地备份机制。 |
| c）应提供重要数据处理系统的热冗余，保证系统的高可用性。 | 服务器采用K8S容器部署，保证系统的高可用性。 |
| 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； | 操作系统提供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功能。 |
| 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。 | 操作系统提供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的功能。 |

4.1.3.63. 数据索引服务器2

|  |  |  |
| --- | --- | --- |
| **安全控制点** | **测评指标** | **结果记录** |
| 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）操作系统时采用用户名+SSHKey公私钥进行身份鉴别鉴别信息具有复杂度要求；2）执行cat /etc/shadow命令，查看shadow文件系统内用户身份标识唯一，不存在同名用户，且不存在空口令账号；3）经访谈，SSHKey公私钥每半年进行更换；4）查看sshd\_config配置文件中配置PasswordAuthentication no，拒绝使用密码方式进行身份鉴别。 |
| 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； | 操作系统采用用户名+SSHKey公私钥进行身份鉴别，可以防止鉴别信息被暴力破解；但未配置用户连接超时退出策略。 |
| 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； | 1）经核查，管理人员采用SSH协议连接操作系统；2）执行netatat –tpln| grep 23命令查看操作系统远程管理端口，不存在Telnet端口，防止鉴别信息在网络传输过程中的被窃听。 |
| 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。 | 未采用两种或两种以上组合的鉴别技术对用户进行身份鉴别。 |
| 访问控制 | a）应对登录的用户分配账户和权限； | 1）经访谈，通过root账户为登录的用户创建账户、分配权限；2）执行ls -l命令查看关键文件权限，均已为账户分配了相应权限，相关文件权限设置为/etc/shadow：000、/etc/passwd：644、/etc/group：644、/etc/profile：644、/etc/crontab：644、/ etc/securetty：600、/etc/ssh/sshd\_config：600。 |
| b）应重命名或删除默认账户，修改默认账户的默认口令； | 1）执行cat /etc/shadow命令查看shadow文件，操作系统中adm、lp、sync、shutdown、halt、mail、uucp、operator、games、gopher等账户均为nologin状态，存在默认账户root；2）执行more /etc/ssh/sshd\_config命令，查看“PermitRootLogin”参数设置为“yes”，即允许root远程登录；3）经访谈，root用户需通过公私钥方式进行身份鉴别。 |
| 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； | 1）执行cat /etc/shadow命令查看shadow文件，发现操作系统存在root、ysup、yops、yluser等在用账户，不存在多余的、过期账户；2）存在多个堡垒机账户登录操作系统时共用一个账户的情况。 |
| 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； | root账户具有系统所有权限，未实现管理用户的权限分离。 |
| e）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； | 经访谈，由系统管理员root配置访问控制策略，如：/etc/passwd，/etc/profile宿主为root、权限设置为644，audit文件为700、message文件为600，其他文件权限为750，实现用户对文件的权限控制。 |
| f）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； | 由管理用户进行用户访问权限分配进行设置，依据访问控制策略,对各类文件进行访问，重要文件和目录权限均在合理范围内，用户可根据文件不同的权限进行操作。 |
| g）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。 | 执 行more /etc/selinux/config 命令，查看config文件显示 SELINUX参数为 DISABLED，即未开启强制访问控制模式。 |
| 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）执行ps -ef|grep rsyslog和ps -ef|grep auditd命令，显示rsyslog和auditd进程正在运行；2）more /etc/audit/audit.rules，显示审计内容包括：\*.info、authriv.\*、mail.\*、cron.\*、\*.emerg、uucp、news.crit、local7.\*等事件。 |
| 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； | 执行tail -20 /var/log/audit/audit.log命令，查看近20条审计日志，内容包括：时间、对象、路径、用户ID、相关的系统调用、用户执行命令等。 |
| 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）通过访问权限对审计记录进行保护，日志文件/var/log/messages、/var/log/secure、/var/log/audit/audit.log访问 权限均为600；2）审计记录本地保存，且实时备份至360本地安全大脑，保存时间满足180天以上。 |
| d）应对审计进程进行保护，防止未经授权的中断。 | 执行service auditd status命令，系统开启auditd审计保护进程，审计进程由root用户维护，经现场使用yluser用户通过service auditd stop命令尝试中断审计进程，无法将审计进程单独中断。 |
| 入侵防范 | a）应遵循最小安装的原则，仅安装需要的组件和应用程序； | 1）系统安装遵循最小化安装原则；2）执行yum list installed命令查看操作系统已安装的程序包，存在Java、elasticsearch、SSH、天眼云镜agent等应用程序或组件，不存在与业务系统无关的组件和应用程序。 |
| b）应关闭不需要的系统服务、默认共享和高危端口； | 1）执行systemctl list-unit-files 命令，系统已关闭FTP、Telnet 等高危网络服务；2）执行netstat -pantu命令，系统关闭了135、445等高危端口，仅开启了22、8080等端口。 |
| c）应通过设定终端接入方式或网络地址范围对通过网络进行管理的管理终端进行限制； | 经核查，1）通过配置安全组策略限制仅允许通过堡垒机管理服务器；2）经核查防火墙中访问控制策略，具备堡垒机地址-服务器管理网段（10.33.0.0）的访问控制策略。 |
| d）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； | 根据GB∕T 28448-2019 《信息安全技术 网络安全等级保护测评要求》测评对象范围描述，服务器无该项要求，故判为“不适用”。 |
| e）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； | 1）经过漏洞扫描，服务器不存在高危安全漏洞；2）执行rpm -qa grep patch命令，查看系统补丁已更新至最新。 |
| f）应能够检测到对重要节点进行入侵的行为，并在发生严重入侵事件时提供报警。 | 经核查，服务器上安装有青藤云天眼云镜，对主机入侵行为进行检测，发现严重安全事件时通过钉钉告警。 |
| 恶意代码防范 | a）应采用免受恶意代码攻击的技术措施或主动免疫可信验证机制及时识别入侵和病毒行为，并将其有效阻断。 | 经核查，服务器上安装有青藤云天眼云镜，对主机恶意代码进行检测、清除，每天凌晨自动更新恶意代码特征库，经核查，具备恶意代码特征库更新记录。 |
| 可信验证 | a）可基于可信根对计算设备的系统引导程序、系统程序、重要配置参数和应用程序等进行可信验证，并在应用程序的关键执行环节进行动态可信验证，在检测到其可信性受到破坏后进行报警，并将验证结果形成审计记录送至安全管理中心。 | 未采用技术措施对计算设备的系统引导程序、系统程序、重要配置参数和通信应用程序等进行可信验证。 |
| 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； | 采用SSH协议连接操作系统，保证了鉴别信息以及管理数据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。 | 操作系统中对重要鉴别信息通过自身的加密及校验（SHA256），保证数据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； | 采用SSH协议连接操作系统，保证了鉴别信息以及管理数据在传输过程中的保密性。 |
| b）应采用密码技术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个人信息等。 | 通过系统自带的加密模块保证鉴别数据在存储过程中的保密性。 |
| 数据备份恢复 | a）应提供重要数据的本地数据备份与恢复功能； | 经核查，通过脚本每周将配置文件、代码仓库等数据备份至备份服务器中，依据需要验证备份数据的有效性。 |
| b）应提供异地实时备份功能，利用通信网络将重要数据实时备份至备份场地； | 系统无异地备份机制。 |
| c）应提供重要数据处理系统的热冗余，保证系统的高可用性。 | 服务器采用K8S容器部署，保证系统的高可用性。 |
| 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； | 操作系统提供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功能。 |
| 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。 | 操作系统提供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的功能。 |

4.1.3.64. 数据索引服务器3

|  |  |  |
| --- | --- | --- |
| **安全控制点** | **测评指标** | **结果记录** |
| 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）操作系统时采用用户名+SSHKey公私钥进行身份鉴别鉴别信息具有复杂度要求；2）执行cat /etc/shadow命令，查看shadow文件系统内用户身份标识唯一，不存在同名用户，且不存在空口令账号；3）经访谈，SSHKey公私钥每半年进行更换；4）查看sshd\_config配置文件中配置PasswordAuthentication no，拒绝使用密码方式进行身份鉴别。 |
| 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； | 操作系统采用用户名+SSHKey公私钥进行身份鉴别，可以防止鉴别信息被暴力破解；但未配置用户连接超时退出策略。 |
| 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； | 1）经核查，管理人员采用SSH协议连接操作系统；2）执行netatat –tpln| grep 23命令查看操作系统远程管理端口，不存在Telnet端口，防止鉴别信息在网络传输过程中的被窃听。 |
| 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。 | 未采用两种或两种以上组合的鉴别技术对用户进行身份鉴别。 |
| 访问控制 | a）应对登录的用户分配账户和权限； | 1）经访谈，通过root账户为登录的用户创建账户、分配权限；2）执行ls -l命令查看关键文件权限，均已为账户分配了相应权限，相关文件权限设置为/etc/shadow：000、/etc/passwd：644、/etc/group：644、/etc/profile：644、/etc/crontab：644、/ etc/securetty：600、/etc/ssh/sshd\_config：600。 |
| b）应重命名或删除默认账户，修改默认账户的默认口令； | 1）执行cat /etc/shadow命令查看shadow文件，操作系统中adm、lp、sync、shutdown、halt、mail、uucp、operator、games、gopher等账户均为nologin状态，存在默认账户root；2）执行more /etc/ssh/sshd\_config命令，查看“PermitRootLogin”参数设置为“yes”，即允许root远程登录；3）经访谈，root用户需通过公私钥方式进行身份鉴别。 |
| 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； | 1）执行cat /etc/shadow命令查看shadow文件，发现操作系统存在root、ysup、yops、yluser等在用账户，不存在多余的、过期账户；2）存在多个堡垒机账户登录操作系统时共用一个账户的情况。 |
| 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； | root账户具有系统所有权限，未实现管理用户的权限分离。 |
| e）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； | 经访谈，由系统管理员root配置访问控制策略，如：/etc/passwd，/etc/profile宿主为root、权限设置为644，audit文件为700、message文件为600，其他文件权限为750，实现用户对文件的权限控制。 |
| f）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； | 由管理用户进行用户访问权限分配进行设置，依据访问控制策略,对各类文件进行访问，重要文件和目录权限均在合理范围内，用户可根据文件不同的权限进行操作。 |
| g）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。 | 执 行more /etc/selinux/config 命令，查看config文件显示 SELINUX参数为 DISABLED，即未开启强制访问控制模式。 |
| 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）执行ps -ef|grep rsyslog和ps -ef|grep auditd命令，显示rsyslog和auditd进程正在运行；2）more /etc/audit/audit.rules，显示审计内容包括：\*.info、authriv.\*、mail.\*、cron.\*、\*.emerg、uucp、news.crit、local7.\*等事件。 |
| 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； | 执行tail -20 /var/log/audit/audit.log命令，查看近20条审计日志，内容包括：时间、对象、路径、用户ID、相关的系统调用、用户执行命令等。 |
| 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）通过访问权限对审计记录进行保护，日志文件/var/log/messages、/var/log/secure、/var/log/audit/audit.log访问 权限均为600；2）审计记录本地保存，且实时备份至360本地安全大脑，保存时间满足180天以上。 |
| d）应对审计进程进行保护，防止未经授权的中断。 | 执行service auditd status命令，系统开启auditd审计保护进程，审计进程由root用户维护，经现场使用yluser用户通过service auditd stop命令尝试中断审计进程，无法将审计进程单独中断。 |
| 入侵防范 | a）应遵循最小安装的原则，仅安装需要的组件和应用程序； | 1）系统安装遵循最小化安装原则；2）执行yum list installed命令查看操作系统已安装的程序包，存在Java、elasticsearch、SSH、天眼云镜agent等应用程序或组件，不存在与业务系统无关的组件和应用程序。 |
| b）应关闭不需要的系统服务、默认共享和高危端口； | 1）执行systemctl list-unit-files 命令，系统已关闭FTP、Telnet 等高危网络服务；2）执行netstat -pantu命令，系统关闭了135、445等高危端口，仅开启了22、8080等端口。 |
| c）应通过设定终端接入方式或网络地址范围对通过网络进行管理的管理终端进行限制； | 经核查，1）通过配置安全组策略限制仅允许通过堡垒机管理服务器；2）经核查防火墙中访问控制策略，具备堡垒机地址-服务器管理网段（10.33.0.0）的访问控制策略。 |
| d）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； | 根据GB∕T 28448-2019 《信息安全技术 网络安全等级保护测评要求》测评对象范围描述，服务器无该项要求，故判为“不适用”。 |
| e）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； | 1）经过漏洞扫描，服务器不存在高危安全漏洞；2）执行rpm -qa grep patch命令，查看系统补丁已更新至最新。 |
| f）应能够检测到对重要节点进行入侵的行为，并在发生严重入侵事件时提供报警。 | 经核查，服务器上安装有青藤云天眼云镜，对主机入侵行为进行检测，发现严重安全事件时通过钉钉告警。 |
| 恶意代码防范 | a）应采用免受恶意代码攻击的技术措施或主动免疫可信验证机制及时识别入侵和病毒行为，并将其有效阻断。 | 经核查，服务器上安装有青藤云天眼云镜，对主机恶意代码进行检测、清除，每天凌晨自动更新恶意代码特征库，经核查，具备恶意代码特征库更新记录。 |
| 可信验证 | a）可基于可信根对计算设备的系统引导程序、系统程序、重要配置参数和应用程序等进行可信验证，并在应用程序的关键执行环节进行动态可信验证，在检测到其可信性受到破坏后进行报警，并将验证结果形成审计记录送至安全管理中心。 | 未采用技术措施对计算设备的系统引导程序、系统程序、重要配置参数和通信应用程序等进行可信验证。 |
| 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； | 采用SSH协议连接操作系统，保证了鉴别信息以及管理数据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。 | 操作系统中对重要鉴别信息通过自身的加密及校验（SHA256），保证数据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； | 采用SSH协议连接操作系统，保证了鉴别信息以及管理数据在传输过程中的保密性。 |
| b）应采用密码技术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个人信息等。 | 通过系统自带的加密模块保证鉴别数据在存储过程中的保密性。 |
| 数据备份恢复 | a）应提供重要数据的本地数据备份与恢复功能； | 经核查，通过脚本每周将配置文件、代码仓库等数据备份至备份服务器中，依据需要验证备份数据的有效性。 |
| b）应提供异地实时备份功能，利用通信网络将重要数据实时备份至备份场地； | 系统无异地备份机制。 |
| c）应提供重要数据处理系统的热冗余，保证系统的高可用性。 | 服务器采用K8S容器部署，保证系统的高可用性。 |
| 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； | 操作系统提供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功能。 |
| 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。 | 操作系统提供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的功能。 |

4.1.3.65. 数据索引服务器4

|  |  |  |
| --- | --- | --- |
| **安全控制点** | **测评指标** | **结果记录** |
| 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）操作系统时采用用户名+SSHKey公私钥进行身份鉴别鉴别信息具有复杂度要求；2）执行cat /etc/shadow命令，查看shadow文件系统内用户身份标识唯一，不存在同名用户，且不存在空口令账号；3）经访谈，SSHKey公私钥每半年进行更换；4）查看sshd\_config配置文件中配置PasswordAuthentication no，拒绝使用密码方式进行身份鉴别。 |
| 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； | 操作系统采用用户名+SSHKey公私钥进行身份鉴别，可以防止鉴别信息被暴力破解；但未配置用户连接超时退出策略。 |
| 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； | 1）经核查，管理人员采用SSH协议连接操作系统；2）执行netatat –tpln| grep 23命令查看操作系统远程管理端口，不存在Telnet端口，防止鉴别信息在网络传输过程中的被窃听。 |
| 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。 | 未采用两种或两种以上组合的鉴别技术对用户进行身份鉴别。 |
| 访问控制 | a）应对登录的用户分配账户和权限； | 1）经访谈，通过root账户为登录的用户创建账户、分配权限；2）执行ls -l命令查看关键文件权限，均已为账户分配了相应权限，相关文件权限设置为/etc/shadow：000、/etc/passwd：644、/etc/group：644、/etc/profile：644、/etc/crontab：644、/ etc/securetty：600、/etc/ssh/sshd\_config：600。 |
| b）应重命名或删除默认账户，修改默认账户的默认口令； | 1）执行cat /etc/shadow命令查看shadow文件，操作系统中adm、lp、sync、shutdown、halt、mail、uucp、operator、games、gopher等账户均为nologin状态，存在默认账户root；2）执行more /etc/ssh/sshd\_config命令，查看“PermitRootLogin”参数设置为“yes”，即允许root远程登录；3）经访谈，root用户需通过公私钥方式进行身份鉴别。 |
| 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； | 1）执行cat /etc/shadow命令查看shadow文件，发现操作系统存在root、ysup、yops、yluser等在用账户，不存在多余的、过期账户；2）存在多个堡垒机账户登录操作系统时共用一个账户的情况。 |
| 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； | root账户具有系统所有权限，未实现管理用户的权限分离。 |
| e）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； | 经访谈，由系统管理员root配置访问控制策略，如：/etc/passwd，/etc/profile宿主为root、权限设置为644，audit文件为700、message文件为600，其他文件权限为750，实现用户对文件的权限控制。 |
| f）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； | 由管理用户进行用户访问权限分配进行设置，依据访问控制策略,对各类文件进行访问，重要文件和目录权限均在合理范围内，用户可根据文件不同的权限进行操作。 |
| g）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。 | 执 行more /etc/selinux/config 命令，查看config文件显示 SELINUX参数为 DISABLED，即未开启强制访问控制模式。 |
| 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）执行ps -ef|grep rsyslog和ps -ef|grep auditd命令，显示rsyslog和auditd进程正在运行；2）more /etc/audit/audit.rules，显示审计内容包括：\*.info、authriv.\*、mail.\*、cron.\*、\*.emerg、uucp、news.crit、local7.\*等事件。 |
| 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； | 执行tail -20 /var/log/audit/audit.log命令，查看近20条审计日志，内容包括：时间、对象、路径、用户ID、相关的系统调用、用户执行命令等。 |
| 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）通过访问权限对审计记录进行保护，日志文件/var/log/messages、/var/log/secure、/var/log/audit/audit.log访问 权限均为600；2）审计记录本地保存，且实时备份至360本地安全大脑，保存时间满足180天以上。 |
| d）应对审计进程进行保护，防止未经授权的中断。 | 执行service auditd status命令，系统开启auditd审计保护进程，审计进程由root用户维护，经现场使用yluser用户通过service auditd stop命令尝试中断审计进程，无法将审计进程单独中断。 |
| 入侵防范 | a）应遵循最小安装的原则，仅安装需要的组件和应用程序； | 1）系统安装遵循最小化安装原则；2）执行yum list installed命令查看操作系统已安装的程序包，存在Java、elasticsearch、SSH、天眼云镜agent等应用程序或组件，不存在与业务系统无关的组件和应用程序。 |
| b）应关闭不需要的系统服务、默认共享和高危端口； | 1）执行systemctl list-unit-files 命令，系统已关闭FTP、Telnet 等高危网络服务；2）执行netstat -pantu命令，系统关闭了135、445等高危端口，仅开启了22、8080等端口。 |
| c）应通过设定终端接入方式或网络地址范围对通过网络进行管理的管理终端进行限制； | 经核查，1）通过配置安全组策略限制仅允许通过堡垒机管理服务器；2）经核查防火墙中访问控制策略，具备堡垒机地址-服务器管理网段（10.33.0.0）的访问控制策略。 |
| d）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； | 根据GB∕T 28448-2019 《信息安全技术 网络安全等级保护测评要求》测评对象范围描述，服务器无该项要求，故判为“不适用”。 |
| e）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； | 1）经过漏洞扫描，服务器不存在高危安全漏洞；2）执行rpm -qa grep patch命令，查看系统补丁已更新至最新。 |
| f）应能够检测到对重要节点进行入侵的行为，并在发生严重入侵事件时提供报警。 | 经核查，服务器上安装有青藤云天眼云镜，对主机入侵行为进行检测，发现严重安全事件时通过钉钉告警。 |
| 恶意代码防范 | a）应采用免受恶意代码攻击的技术措施或主动免疫可信验证机制及时识别入侵和病毒行为，并将其有效阻断。 | 经核查，服务器上安装有青藤云天眼云镜，对主机恶意代码进行检测、清除，每天凌晨自动更新恶意代码特征库，经核查，具备恶意代码特征库更新记录。 |
| 可信验证 | a）可基于可信根对计算设备的系统引导程序、系统程序、重要配置参数和应用程序等进行可信验证，并在应用程序的关键执行环节进行动态可信验证，在检测到其可信性受到破坏后进行报警，并将验证结果形成审计记录送至安全管理中心。 | 未采用技术措施对计算设备的系统引导程序、系统程序、重要配置参数和通信应用程序等进行可信验证。 |
| 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； | 采用SSH协议连接操作系统，保证了鉴别信息以及管理数据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。 | 操作系统中对重要鉴别信息通过自身的加密及校验（SHA256），保证数据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； | 采用SSH协议连接操作系统，保证了鉴别信息以及管理数据在传输过程中的保密性。 |
| b）应采用密码技术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个人信息等。 | 通过系统自带的加密模块保证鉴别数据在存储过程中的保密性。 |
| 数据备份恢复 | a）应提供重要数据的本地数据备份与恢复功能； | 经核查，通过脚本每周将配置文件、代码仓库等数据备份至备份服务器中，依据需要验证备份数据的有效性。 |
| b）应提供异地实时备份功能，利用通信网络将重要数据实时备份至备份场地； | 系统无异地备份机制。 |
| c）应提供重要数据处理系统的热冗余，保证系统的高可用性。 | 服务器采用K8S容器部署，保证系统的高可用性。 |
| 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； | 操作系统提供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功能。 |
| 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。 | 操作系统提供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的功能。 |

4.1.3.66. 数据索引服务器8

|  |  |  |
| --- | --- | --- |
| **安全控制点** | **测评指标** | **结果记录** |
| 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）操作系统时采用用户名+SSHKey公私钥进行身份鉴别鉴别信息具有复杂度要求；2）执行cat /etc/shadow命令，查看shadow文件系统内用户身份标识唯一，不存在同名用户，且不存在空口令账号；3）经访谈，SSHKey公私钥每半年进行更换；4）查看sshd\_config配置文件中配置PasswordAuthentication no，拒绝使用密码方式进行身份鉴别。 |
| 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； | 操作系统采用用户名+SSHKey公私钥进行身份鉴别，可以防止鉴别信息被暴力破解；但未配置用户连接超时退出策略。 |
| 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； | 1）经核查，管理人员采用SSH协议连接操作系统；2）执行netatat –tpln| grep 23命令查看操作系统远程管理端口，不存在Telnet端口，防止鉴别信息在网络传输过程中的被窃听。 |
| 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。 | 未采用两种或两种以上组合的鉴别技术对用户进行身份鉴别。 |
| 访问控制 | a）应对登录的用户分配账户和权限； | 1）经访谈，通过root账户为登录的用户创建账户、分配权限；2）执行ls -l命令查看关键文件权限，均已为账户分配了相应权限，相关文件权限设置为/etc/shadow：000、/etc/passwd：644、/etc/group：644、/etc/profile：644、/etc/crontab：644、/ etc/securetty：600、/etc/ssh/sshd\_config：600。 |
| b）应重命名或删除默认账户，修改默认账户的默认口令； | 1）执行cat /etc/shadow命令查看shadow文件，操作系统中adm、lp、sync、shutdown、halt、mail、uucp、operator、games、gopher等账户均为nologin状态，存在默认账户root；2）执行more /etc/ssh/sshd\_config命令，查看“PermitRootLogin”参数设置为“yes”，即允许root远程登录；3）经访谈，root用户需通过公私钥方式进行身份鉴别。 |
| 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； | 1）执行cat /etc/shadow命令查看shadow文件，发现操作系统存在root、ysup、yops、yluser等在用账户，不存在多余的、过期账户；2）存在多个堡垒机账户登录操作系统时共用一个账户的情况。 |
| 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； | root账户具有系统所有权限，未实现管理用户的权限分离。 |
| e）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； | 经访谈，由系统管理员root配置访问控制策略，如：/etc/passwd，/etc/profile宿主为root、权限设置为644，audit文件为700、message文件为600，其他文件权限为750，实现用户对文件的权限控制。 |
| f）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； | 由管理用户进行用户访问权限分配进行设置，依据访问控制策略,对各类文件进行访问，重要文件和目录权限均在合理范围内，用户可根据文件不同的权限进行操作。 |
| g）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。 | 执 行more /etc/selinux/config 命令，查看config文件显示 SELINUX参数为 DISABLED，即未开启强制访问控制模式。 |
| 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）执行ps -ef|grep rsyslog和ps -ef|grep auditd命令，显示rsyslog和auditd进程正在运行；2）more /etc/audit/audit.rules，显示审计内容包括：\*.info、authriv.\*、mail.\*、cron.\*、\*.emerg、uucp、news.crit、local7.\*等事件。 |
| 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； | 执行tail -20 /var/log/audit/audit.log命令，查看近20条审计日志，内容包括：时间、对象、路径、用户ID、相关的系统调用、用户执行命令等。 |
| 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）通过访问权限对审计记录进行保护，日志文件/var/log/messages、/var/log/secure、/var/log/audit/audit.log访问 权限均为600；2）审计记录本地保存，且实时备份至360本地安全大脑，保存时间满足180天以上。 |
| d）应对审计进程进行保护，防止未经授权的中断。 | 执行service auditd status命令，系统开启auditd审计保护进程，审计进程由root用户维护，经现场使用yluser用户通过service auditd stop命令尝试中断审计进程，无法将审计进程单独中断。 |
| 入侵防范 | a）应遵循最小安装的原则，仅安装需要的组件和应用程序； | 1）系统安装遵循最小化安装原则；2）执行yum list installed命令查看操作系统已安装的程序包，存在Java、elasticsearch、SSH、天眼云镜agent等应用程序或组件，不存在与业务系统无关的组件和应用程序。 |
| b）应关闭不需要的系统服务、默认共享和高危端口； | 1）执行systemctl list-unit-files 命令，系统已关闭FTP、Telnet 等高危网络服务；2）执行netstat -pantu命令，系统关闭了135、445等高危端口，仅开启了22、8080等端口。 |
| c）应通过设定终端接入方式或网络地址范围对通过网络进行管理的管理终端进行限制； | 经核查，1）通过配置安全组策略限制仅允许通过堡垒机管理服务器；2）经核查防火墙中访问控制策略，具备堡垒机地址-服务器管理网段（10.33.0.0）的访问控制策略。 |
| d）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； | 根据GB∕T 28448-2019 《信息安全技术 网络安全等级保护测评要求》测评对象范围描述，服务器无该项要求，故判为“不适用”。 |
| e）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； | 1）经过漏洞扫描，服务器不存在高危安全漏洞；2）执行rpm -qa grep patch命令，查看系统补丁已更新至最新。 |
| f）应能够检测到对重要节点进行入侵的行为，并在发生严重入侵事件时提供报警。 | 经核查，服务器上安装有青藤云天眼云镜，对主机入侵行为进行检测，发现严重安全事件时通过钉钉告警。 |
| 恶意代码防范 | a）应采用免受恶意代码攻击的技术措施或主动免疫可信验证机制及时识别入侵和病毒行为，并将其有效阻断。 | 经核查，服务器上安装有青藤云天眼云镜，对主机恶意代码进行检测、清除，每天凌晨自动更新恶意代码特征库，经核查，具备恶意代码特征库更新记录。 |
| 可信验证 | a）可基于可信根对计算设备的系统引导程序、系统程序、重要配置参数和应用程序等进行可信验证，并在应用程序的关键执行环节进行动态可信验证，在检测到其可信性受到破坏后进行报警，并将验证结果形成审计记录送至安全管理中心。 | 未采用技术措施对计算设备的系统引导程序、系统程序、重要配置参数和通信应用程序等进行可信验证。 |
| 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； | 采用SSH协议连接操作系统，保证了鉴别信息以及管理数据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。 | 操作系统中对重要鉴别信息通过自身的加密及校验（SHA256），保证数据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； | 采用SSH协议连接操作系统，保证了鉴别信息以及管理数据在传输过程中的保密性。 |
| b）应采用密码技术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个人信息等。 | 通过系统自带的加密模块保证鉴别数据在存储过程中的保密性。 |
| 数据备份恢复 | a）应提供重要数据的本地数据备份与恢复功能； | 经核查，通过脚本每周将配置文件、代码仓库等数据备份至备份服务器中，依据需要验证备份数据的有效性。 |
| b）应提供异地实时备份功能，利用通信网络将重要数据实时备份至备份场地； | 系统无异地备份机制。 |
| c）应提供重要数据处理系统的热冗余，保证系统的高可用性。 | 服务器采用K8S容器部署，保证系统的高可用性。 |
| 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； | 操作系统提供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功能。 |
| 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。 | 操作系统提供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的功能。 |

4.1.3.67. 数据索引服务器12

|  |  |  |
| --- | --- | --- |
| **安全控制点** | **测评指标** | **结果记录** |
| 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）操作系统时采用用户名+SSHKey公私钥进行身份鉴别鉴别信息具有复杂度要求；2）执行cat /etc/shadow命令，查看shadow文件系统内用户身份标识唯一，不存在同名用户，且不存在空口令账号；3）经访谈，SSHKey公私钥每半年进行更换；4）查看sshd\_config配置文件中配置PasswordAuthentication no，拒绝使用密码方式进行身份鉴别。 |
| 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； | 操作系统采用用户名+SSHKey公私钥进行身份鉴别，可以防止鉴别信息被暴力破解；但未配置用户连接超时退出策略。 |
| 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； | 1）经核查，管理人员采用SSH协议连接操作系统；2）执行netatat –tpln| grep 23命令查看操作系统远程管理端口，不存在Telnet端口，防止鉴别信息在网络传输过程中的被窃听。 |
| 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。 | 未采用两种或两种以上组合的鉴别技术对用户进行身份鉴别。 |
| 访问控制 | a）应对登录的用户分配账户和权限； | 1）经访谈，通过root账户为登录的用户创建账户、分配权限；2）执行ls -l命令查看关键文件权限，均已为账户分配了相应权限，相关文件权限设置为/etc/shadow：000、/etc/passwd：644、/etc/group：644、/etc/profile：644、/etc/crontab：644、/ etc/securetty：600、/etc/ssh/sshd\_config：600。 |
| b）应重命名或删除默认账户，修改默认账户的默认口令； | 1）执行cat /etc/shadow命令查看shadow文件，操作系统中adm、lp、sync、shutdown、halt、mail、uucp、operator、games、gopher等账户均为nologin状态，存在默认账户root；2）执行more /etc/ssh/sshd\_config命令，查看“PermitRootLogin”参数设置为“yes”，即允许root远程登录；3）经访谈，root用户需通过公私钥方式进行身份鉴别。 |
| 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； | 1）执行cat /etc/shadow命令查看shadow文件，发现操作系统存在root、ysup、yops、yluser等在用账户，不存在多余的、过期账户；2）存在多个堡垒机账户登录操作系统时共用一个账户的情况。 |
| 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； | root账户具有系统所有权限，未实现管理用户的权限分离。 |
| e）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； | 经访谈，由系统管理员root配置访问控制策略，如：/etc/passwd，/etc/profile宿主为root、权限设置为644，audit文件为700、message文件为600，其他文件权限为750，实现用户对文件的权限控制。 |
| f）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； | 由管理用户进行用户访问权限分配进行设置，依据访问控制策略,对各类文件进行访问，重要文件和目录权限均在合理范围内，用户可根据文件不同的权限进行操作。 |
| g）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。 | 执 行more /etc/selinux/config 命令，查看config文件显示 SELINUX参数为 DISABLED，即未开启强制访问控制模式。 |
| 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）执行ps -ef|grep rsyslog和ps -ef|grep auditd命令，显示rsyslog和auditd进程正在运行；2）more /etc/audit/audit.rules，显示审计内容包括：\*.info、authriv.\*、mail.\*、cron.\*、\*.emerg、uucp、news.crit、local7.\*等事件。 |
| 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； | 执行tail -20 /var/log/audit/audit.log命令，查看近20条审计日志，内容包括：时间、对象、路径、用户ID、相关的系统调用、用户执行命令等。 |
| 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）通过访问权限对审计记录进行保护，日志文件/var/log/messages、/var/log/secure、/var/log/audit/audit.log访问 权限均为600；2）审计记录本地保存，且实时备份至360本地安全大脑，保存时间满足180天以上。 |
| d）应对审计进程进行保护，防止未经授权的中断。 | 执行service auditd status命令，系统开启auditd审计保护进程，审计进程由root用户维护，经现场使用yluser用户通过service auditd stop命令尝试中断审计进程，无法将审计进程单独中断。 |
| 入侵防范 | a）应遵循最小安装的原则，仅安装需要的组件和应用程序； | 1）系统安装遵循最小化安装原则；2）执行yum list installed命令查看操作系统已安装的程序包，存在Java、elasticsearch、SSH、天眼云镜agent等应用程序或组件，不存在与业务系统无关的组件和应用程序。 |
| b）应关闭不需要的系统服务、默认共享和高危端口； | 1）执行systemctl list-unit-files 命令，系统已关闭FTP、Telnet 等高危网络服务；2）执行netstat -pantu命令，系统关闭了135、445等高危端口，仅开启了22、8080等端口。 |
| c）应通过设定终端接入方式或网络地址范围对通过网络进行管理的管理终端进行限制； | 经核查，1）通过配置安全组策略限制仅允许通过堡垒机管理服务器；2）经核查防火墙中访问控制策略，具备堡垒机地址-服务器管理网段（10.33.0.0）的访问控制策略。 |
| d）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； | 根据GB∕T 28448-2019 《信息安全技术 网络安全等级保护测评要求》测评对象范围描述，服务器无该项要求，故判为“不适用”。 |
| e）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； | 1）经过漏洞扫描，服务器不存在高危安全漏洞；2）执行rpm -qa grep patch命令，查看系统补丁已更新至最新。 |
| f）应能够检测到对重要节点进行入侵的行为，并在发生严重入侵事件时提供报警。 | 经核查，服务器上安装有青藤云天眼云镜，对主机入侵行为进行检测，发现严重安全事件时通过钉钉告警。 |
| 恶意代码防范 | a）应采用免受恶意代码攻击的技术措施或主动免疫可信验证机制及时识别入侵和病毒行为，并将其有效阻断。 | 经核查，服务器上安装有青藤云天眼云镜，对主机恶意代码进行检测、清除，每天凌晨自动更新恶意代码特征库，经核查，具备恶意代码特征库更新记录。 |
| 可信验证 | a）可基于可信根对计算设备的系统引导程序、系统程序、重要配置参数和应用程序等进行可信验证，并在应用程序的关键执行环节进行动态可信验证，在检测到其可信性受到破坏后进行报警，并将验证结果形成审计记录送至安全管理中心。 | 未采用技术措施对计算设备的系统引导程序、系统程序、重要配置参数和通信应用程序等进行可信验证。 |
| 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； | 采用SSH协议连接操作系统，保证了鉴别信息以及管理数据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。 | 操作系统中对重要鉴别信息通过自身的加密及校验（SHA256），保证数据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； | 采用SSH协议连接操作系统，保证了鉴别信息以及管理数据在传输过程中的保密性。 |
| b）应采用密码技术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个人信息等。 | 通过系统自带的加密模块保证鉴别数据在存储过程中的保密性。 |
| 数据备份恢复 | a）应提供重要数据的本地数据备份与恢复功能； | 经核查，通过脚本每周将配置文件、代码仓库等数据备份至备份服务器中，依据需要验证备份数据的有效性。 |
| b）应提供异地实时备份功能，利用通信网络将重要数据实时备份至备份场地； | 系统无异地备份机制。 |
| c）应提供重要数据处理系统的热冗余，保证系统的高可用性。 | 服务器采用K8S容器部署，保证系统的高可用性。 |
| 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； | 操作系统提供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功能。 |
| 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。 | 操作系统提供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的功能。 |

4.1.3.68. 数据索引服务器17

|  |  |  |
| --- | --- | --- |
| **安全控制点** | **测评指标** | **结果记录** |
| 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）操作系统时采用用户名+SSHKey公私钥进行身份鉴别鉴别信息具有复杂度要求；2）执行cat /etc/shadow命令，查看shadow文件系统内用户身份标识唯一，不存在同名用户，且不存在空口令账号；3）经访谈，SSHKey公私钥每半年进行更换；4）查看sshd\_config配置文件中配置PasswordAuthentication no，拒绝使用密码方式进行身份鉴别。 |
| 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； | 操作系统采用用户名+SSHKey公私钥进行身份鉴别，可以防止鉴别信息被暴力破解；但未配置用户连接超时退出策略。 |
| 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； | 1）经核查，管理人员采用SSH协议连接操作系统；2）执行netatat –tpln| grep 23命令查看操作系统远程管理端口，不存在Telnet端口，防止鉴别信息在网络传输过程中的被窃听。 |
| 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。 | 未采用两种或两种以上组合的鉴别技术对用户进行身份鉴别。 |
| 访问控制 | a）应对登录的用户分配账户和权限； | 1）经访谈，通过root账户为登录的用户创建账户、分配权限；2）执行ls -l命令查看关键文件权限，均已为账户分配了相应权限，相关文件权限设置为/etc/shadow：000、/etc/passwd：644、/etc/group：644、/etc/profile：644、/etc/crontab：644、/ etc/securetty：600、/etc/ssh/sshd\_config：600。 |
| b）应重命名或删除默认账户，修改默认账户的默认口令； | 1）执行cat /etc/shadow命令查看shadow文件，操作系统中adm、lp、sync、shutdown、halt、mail、uucp、operator、games、gopher等账户均为nologin状态，存在默认账户root；2）执行more /etc/ssh/sshd\_config命令，查看“PermitRootLogin”参数设置为“yes”，即允许root远程登录；3）经访谈，root用户需通过公私钥方式进行身份鉴别。 |
| 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； | 1）执行cat /etc/shadow命令查看shadow文件，发现操作系统存在root、ysup、yops、yluser等在用账户，不存在多余的、过期账户；2）存在多个堡垒机账户登录操作系统时共用一个账户的情况。 |
| 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； | root账户具有系统所有权限，未实现管理用户的权限分离。 |
| e）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； | 经访谈，由系统管理员root配置访问控制策略，如：/etc/passwd，/etc/profile宿主为root、权限设置为644，audit文件为700、message文件为600，其他文件权限为750，实现用户对文件的权限控制。 |
| f）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； | 由管理用户进行用户访问权限分配进行设置，依据访问控制策略,对各类文件进行访问，重要文件和目录权限均在合理范围内，用户可根据文件不同的权限进行操作。 |
| g）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。 | 执 行more /etc/selinux/config 命令，查看config文件显示 SELINUX参数为 DISABLED，即未开启强制访问控制模式。 |
| 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）执行ps -ef|grep rsyslog和ps -ef|grep auditd命令，显示rsyslog和auditd进程正在运行；2）more /etc/audit/audit.rules，显示审计内容包括：\*.info、authriv.\*、mail.\*、cron.\*、\*.emerg、uucp、news.crit、local7.\*等事件。 |
| 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； | 执行tail -20 /var/log/audit/audit.log命令，查看近20条审计日志，内容包括：时间、对象、路径、用户ID、相关的系统调用、用户执行命令等。 |
| 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）通过访问权限对审计记录进行保护，日志文件/var/log/messages、/var/log/secure、/var/log/audit/audit.log访问 权限均为600；2）审计记录本地保存，且实时备份至360本地安全大脑，保存时间满足180天以上。 |
| d）应对审计进程进行保护，防止未经授权的中断。 | 执行service auditd status命令，系统开启auditd审计保护进程，审计进程由root用户维护，经现场使用yluser用户通过service auditd stop命令尝试中断审计进程，无法将审计进程单独中断。 |
| 入侵防范 | a）应遵循最小安装的原则，仅安装需要的组件和应用程序； | 1）系统安装遵循最小化安装原则；2）执行yum list installed命令查看操作系统已安装的程序包，存在Java、elasticsearch、SSH、天眼云镜agent等应用程序或组件，不存在与业务系统无关的组件和应用程序。 |
| b）应关闭不需要的系统服务、默认共享和高危端口； | 1）执行systemctl list-unit-files 命令，系统已关闭FTP、Telnet 等高危网络服务；2）执行netstat -pantu命令，系统关闭了135、445等高危端口，仅开启了22、8080等端口。 |
| c）应通过设定终端接入方式或网络地址范围对通过网络进行管理的管理终端进行限制； | 经核查，1）通过配置安全组策略限制仅允许通过堡垒机管理服务器；2）经核查防火墙中访问控制策略，具备堡垒机地址-服务器管理网段（10.33.0.0）的访问控制策略。 |
| d）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； | 根据GB∕T 28448-2019 《信息安全技术 网络安全等级保护测评要求》测评对象范围描述，服务器无该项要求，故判为“不适用”。 |
| e）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； | 1）经过漏洞扫描，服务器不存在高危安全漏洞；2）执行rpm -qa grep patch命令，查看系统补丁已更新至最新。 |
| f）应能够检测到对重要节点进行入侵的行为，并在发生严重入侵事件时提供报警。 | 经核查，服务器上安装有青藤云天眼云镜，对主机入侵行为进行检测，发现严重安全事件时通过钉钉告警。 |
| 恶意代码防范 | a）应采用免受恶意代码攻击的技术措施或主动免疫可信验证机制及时识别入侵和病毒行为，并将其有效阻断。 | 经核查，服务器上安装有青藤云天眼云镜，对主机恶意代码进行检测、清除，每天凌晨自动更新恶意代码特征库，经核查，具备恶意代码特征库更新记录。 |
| 可信验证 | a）可基于可信根对计算设备的系统引导程序、系统程序、重要配置参数和应用程序等进行可信验证，并在应用程序的关键执行环节进行动态可信验证，在检测到其可信性受到破坏后进行报警，并将验证结果形成审计记录送至安全管理中心。 | 未采用技术措施对计算设备的系统引导程序、系统程序、重要配置参数和通信应用程序等进行可信验证。 |
| 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； | 采用SSH协议连接操作系统，保证了鉴别信息以及管理数据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。 | 操作系统中对重要鉴别信息通过自身的加密及校验（SHA256），保证数据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； | 采用SSH协议连接操作系统，保证了鉴别信息以及管理数据在传输过程中的保密性。 |
| b）应采用密码技术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个人信息等。 | 通过系统自带的加密模块保证鉴别数据在存储过程中的保密性。 |
| 数据备份恢复 | a）应提供重要数据的本地数据备份与恢复功能； | 经核查，通过脚本每周将配置文件、代码仓库等数据备份至备份服务器中，依据需要验证备份数据的有效性。 |
| b）应提供异地实时备份功能，利用通信网络将重要数据实时备份至备份场地； | 系统无异地备份机制。 |
| c）应提供重要数据处理系统的热冗余，保证系统的高可用性。 | 服务器采用K8S容器部署，保证系统的高可用性。 |
| 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； | 操作系统提供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功能。 |
| 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。 | 操作系统提供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的功能。 |

4.1.3.69. 数据索引服务器18

|  |  |  |
| --- | --- | --- |
| **安全控制点** | **测评指标** | **结果记录** |
| 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）操作系统时采用用户名+SSHKey公私钥进行身份鉴别鉴别信息具有复杂度要求；2）执行cat /etc/shadow命令，查看shadow文件系统内用户身份标识唯一，不存在同名用户，且不存在空口令账号；3）经访谈，SSHKey公私钥每半年进行更换；4）查看sshd\_config配置文件中配置PasswordAuthentication no，拒绝使用密码方式进行身份鉴别。 |
| 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； | 操作系统采用用户名+SSHKey公私钥进行身份鉴别，可以防止鉴别信息被暴力破解；但未配置用户连接超时退出策略。 |
| 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； | 1）经核查，管理人员采用SSH协议连接操作系统；2）执行netatat –tpln| grep 23命令查看操作系统远程管理端口，不存在Telnet端口，防止鉴别信息在网络传输过程中的被窃听。 |
| 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。 | 未采用两种或两种以上组合的鉴别技术对用户进行身份鉴别。 |
| 访问控制 | a）应对登录的用户分配账户和权限； | 1）经访谈，通过root账户为登录的用户创建账户、分配权限；2）执行ls -l命令查看关键文件权限，均已为账户分配了相应权限，相关文件权限设置为/etc/shadow：000、/etc/passwd：644、/etc/group：644、/etc/profile：644、/etc/crontab：644、/ etc/securetty：600、/etc/ssh/sshd\_config：600。 |
| b）应重命名或删除默认账户，修改默认账户的默认口令； | 1）执行cat /etc/shadow命令查看shadow文件，操作系统中adm、lp、sync、shutdown、halt、mail、uucp、operator、games、gopher等账户均为nologin状态，存在默认账户root；2）执行more /etc/ssh/sshd\_config命令，查看“PermitRootLogin”参数设置为“yes”，即允许root远程登录；3）经访谈，root用户需通过公私钥方式进行身份鉴别。 |
| 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； | 1）执行cat /etc/shadow命令查看shadow文件，发现操作系统存在root、ysup、yops、yluser等在用账户，不存在多余的、过期账户；2）存在多个堡垒机账户登录操作系统时共用一个账户的情况。 |
| 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； | root账户具有系统所有权限，未实现管理用户的权限分离。 |
| e）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； | 经访谈，由系统管理员root配置访问控制策略，如：/etc/passwd，/etc/profile宿主为root、权限设置为644，audit文件为700、message文件为600，其他文件权限为750，实现用户对文件的权限控制。 |
| f）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； | 由管理用户进行用户访问权限分配进行设置，依据访问控制策略,对各类文件进行访问，重要文件和目录权限均在合理范围内，用户可根据文件不同的权限进行操作。 |
| g）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。 | 执 行more /etc/selinux/config 命令，查看config文件显示 SELINUX参数为 DISABLED，即未开启强制访问控制模式。 |
| 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）执行ps -ef|grep rsyslog和ps -ef|grep auditd命令，显示rsyslog和auditd进程正在运行；2）more /etc/audit/audit.rules，显示审计内容包括：\*.info、authriv.\*、mail.\*、cron.\*、\*.emerg、uucp、news.crit、local7.\*等事件。 |
| 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； | 执行tail -20 /var/log/audit/audit.log命令，查看近20条审计日志，内容包括：时间、对象、路径、用户ID、相关的系统调用、用户执行命令等。 |
| 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）通过访问权限对审计记录进行保护，日志文件/var/log/messages、/var/log/secure、/var/log/audit/audit.log访问 权限均为600；2）审计记录本地保存，且实时备份至360本地安全大脑，保存时间满足180天以上。 |
| d）应对审计进程进行保护，防止未经授权的中断。 | 执行service auditd status命令，系统开启auditd审计保护进程，审计进程由root用户维护，经现场使用yluser用户通过service auditd stop命令尝试中断审计进程，无法将审计进程单独中断。 |
| 入侵防范 | a）应遵循最小安装的原则，仅安装需要的组件和应用程序； | 1）系统安装遵循最小化安装原则；2）执行yum list installed命令查看操作系统已安装的程序包，存在Java、elasticsearch、SSH、天眼云镜agent等应用程序或组件，不存在与业务系统无关的组件和应用程序。 |
| b）应关闭不需要的系统服务、默认共享和高危端口； | 1）执行systemctl list-unit-files 命令，系统已关闭FTP、Telnet 等高危网络服务；2）执行netstat -pantu命令，系统关闭了135、445等高危端口，仅开启了22、8080等端口。 |
| c）应通过设定终端接入方式或网络地址范围对通过网络进行管理的管理终端进行限制； | 经核查，1）通过配置安全组策略限制仅允许通过堡垒机管理服务器；2）经核查防火墙中访问控制策略，具备堡垒机地址-服务器管理网段（10.33.0.0）的访问控制策略。 |
| d）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； | 根据GB∕T 28448-2019 《信息安全技术 网络安全等级保护测评要求》测评对象范围描述，服务器无该项要求，故判为“不适用”。 |
| e）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； | 1）经过漏洞扫描，服务器不存在高危安全漏洞；2）执行rpm -qa grep patch命令，查看系统补丁已更新至最新。 |
| f）应能够检测到对重要节点进行入侵的行为，并在发生严重入侵事件时提供报警。 | 经核查，服务器上安装有青藤云天眼云镜，对主机入侵行为进行检测，发现严重安全事件时通过钉钉告警。 |
| 恶意代码防范 | a）应采用免受恶意代码攻击的技术措施或主动免疫可信验证机制及时识别入侵和病毒行为，并将其有效阻断。 | 经核查，服务器上安装有青藤云天眼云镜，对主机恶意代码进行检测、清除，每天凌晨自动更新恶意代码特征库，经核查，具备恶意代码特征库更新记录。 |
| 可信验证 | a）可基于可信根对计算设备的系统引导程序、系统程序、重要配置参数和应用程序等进行可信验证，并在应用程序的关键执行环节进行动态可信验证，在检测到其可信性受到破坏后进行报警，并将验证结果形成审计记录送至安全管理中心。 | 未采用技术措施对计算设备的系统引导程序、系统程序、重要配置参数和通信应用程序等进行可信验证。 |
| 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； | 采用SSH协议连接操作系统，保证了鉴别信息以及管理数据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。 | 操作系统中对重要鉴别信息通过自身的加密及校验（SHA256），保证数据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； | 采用SSH协议连接操作系统，保证了鉴别信息以及管理数据在传输过程中的保密性。 |
| b）应采用密码技术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个人信息等。 | 通过系统自带的加密模块保证鉴别数据在存储过程中的保密性。 |
| 数据备份恢复 | a）应提供重要数据的本地数据备份与恢复功能； | 经核查，通过脚本每周将配置文件、代码仓库等数据备份至备份服务器中，依据需要验证备份数据的有效性。 |
| b）应提供异地实时备份功能，利用通信网络将重要数据实时备份至备份场地； | 系统无异地备份机制。 |
| c）应提供重要数据处理系统的热冗余，保证系统的高可用性。 | 服务器采用K8S容器部署，保证系统的高可用性。 |
| 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； | 操作系统提供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功能。 |
| 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。 | 操作系统提供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的功能。 |

4.1.3.70. 数据索引服务器21

|  |  |  |
| --- | --- | --- |
| **安全控制点** | **测评指标** | **结果记录** |
| 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）操作系统时采用用户名+SSHKey公私钥进行身份鉴别鉴别信息具有复杂度要求；2）执行cat /etc/shadow命令，查看shadow文件系统内用户身份标识唯一，不存在同名用户，且不存在空口令账号；3）经访谈，SSHKey公私钥每半年进行更换；4）查看sshd\_config配置文件中配置PasswordAuthentication no，拒绝使用密码方式进行身份鉴别。 |
| 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； | 操作系统采用用户名+SSHKey公私钥进行身份鉴别，可以防止鉴别信息被暴力破解；但未配置用户连接超时退出策略。 |
| 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； | 1）经核查，管理人员采用SSH协议连接操作系统；2）执行netatat –tpln| grep 23命令查看操作系统远程管理端口，不存在Telnet端口，防止鉴别信息在网络传输过程中的被窃听。 |
| 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。 | 未采用两种或两种以上组合的鉴别技术对用户进行身份鉴别。 |
| 访问控制 | a）应对登录的用户分配账户和权限； | 1）经访谈，通过root账户为登录的用户创建账户、分配权限；2）执行ls -l命令查看关键文件权限，均已为账户分配了相应权限，相关文件权限设置为/etc/shadow：000、/etc/passwd：644、/etc/group：644、/etc/profile：644、/etc/crontab：644、/ etc/securetty：600、/etc/ssh/sshd\_config：600。 |
| b）应重命名或删除默认账户，修改默认账户的默认口令； | 1）执行cat /etc/shadow命令查看shadow文件，操作系统中adm、lp、sync、shutdown、halt、mail、uucp、operator、games、gopher等账户均为nologin状态，存在默认账户root；2）执行more /etc/ssh/sshd\_config命令，查看“PermitRootLogin”参数设置为“yes”，即允许root远程登录；3）经访谈，root用户需通过公私钥方式进行身份鉴别。 |
| 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； | 1）执行cat /etc/shadow命令查看shadow文件，发现操作系统存在root、ysup、yops、yluser等在用账户，不存在多余的、过期账户；2）存在多个堡垒机账户登录操作系统时共用一个账户的情况。 |
| 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； | root账户具有系统所有权限，未实现管理用户的权限分离。 |
| e）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； | 经访谈，由系统管理员root配置访问控制策略，如：/etc/passwd，/etc/profile宿主为root、权限设置为644，audit文件为700、message文件为600，其他文件权限为750，实现用户对文件的权限控制。 |
| f）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； | 由管理用户进行用户访问权限分配进行设置，依据访问控制策略,对各类文件进行访问，重要文件和目录权限均在合理范围内，用户可根据文件不同的权限进行操作。 |
| g）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。 | 执 行more /etc/selinux/config 命令，查看config文件显示 SELINUX参数为 DISABLED，即未开启强制访问控制模式。 |
| 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）执行ps -ef|grep rsyslog和ps -ef|grep auditd命令，显示rsyslog和auditd进程正在运行；2）more /etc/audit/audit.rules，显示审计内容包括：\*.info、authriv.\*、mail.\*、cron.\*、\*.emerg、uucp、news.crit、local7.\*等事件。 |
| 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； | 执行tail -20 /var/log/audit/audit.log命令，查看近20条审计日志，内容包括：时间、对象、路径、用户ID、相关的系统调用、用户执行命令等。 |
| 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）通过访问权限对审计记录进行保护，日志文件/var/log/messages、/var/log/secure、/var/log/audit/audit.log访问 权限均为600；2）审计记录本地保存，且实时备份至360本地安全大脑，保存时间满足180天以上。 |
| d）应对审计进程进行保护，防止未经授权的中断。 | 执行service auditd status命令，系统开启auditd审计保护进程，审计进程由root用户维护，经现场使用yluser用户通过service auditd stop命令尝试中断审计进程，无法将审计进程单独中断。 |
| 入侵防范 | a）应遵循最小安装的原则，仅安装需要的组件和应用程序； | 1）系统安装遵循最小化安装原则；2）执行yum list installed命令查看操作系统已安装的程序包，存在Java、elasticsearch、SSH、天眼云镜agent等应用程序或组件，不存在与业务系统无关的组件和应用程序。 |
| b）应关闭不需要的系统服务、默认共享和高危端口； | 1）执行systemctl list-unit-files 命令，系统已关闭FTP、Telnet 等高危网络服务；2）执行netstat -pantu命令，系统关闭了135、445等高危端口，仅开启了22、8080等端口。 |
| c）应通过设定终端接入方式或网络地址范围对通过网络进行管理的管理终端进行限制； | 经核查，1）通过配置安全组策略限制仅允许通过堡垒机管理服务器；2）经核查防火墙中访问控制策略，具备堡垒机地址-服务器管理网段（10.33.0.0）的访问控制策略。 |
| d）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； | 根据GB∕T 28448-2019 《信息安全技术 网络安全等级保护测评要求》测评对象范围描述，服务器无该项要求，故判为“不适用”。 |
| e）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； | 1）经过漏洞扫描，服务器不存在高危安全漏洞；2）执行rpm -qa grep patch命令，查看系统补丁已更新至最新。 |
| f）应能够检测到对重要节点进行入侵的行为，并在发生严重入侵事件时提供报警。 | 经核查，服务器上安装有青藤云天眼云镜，对主机入侵行为进行检测，发现严重安全事件时通过钉钉告警。 |
| 恶意代码防范 | a）应采用免受恶意代码攻击的技术措施或主动免疫可信验证机制及时识别入侵和病毒行为，并将其有效阻断。 | 经核查，服务器上安装有青藤云天眼云镜，对主机恶意代码进行检测、清除，每天凌晨自动更新恶意代码特征库，经核查，具备恶意代码特征库更新记录。 |
| 可信验证 | a）可基于可信根对计算设备的系统引导程序、系统程序、重要配置参数和应用程序等进行可信验证，并在应用程序的关键执行环节进行动态可信验证，在检测到其可信性受到破坏后进行报警，并将验证结果形成审计记录送至安全管理中心。 | 未采用技术措施对计算设备的系统引导程序、系统程序、重要配置参数和通信应用程序等进行可信验证。 |
| 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； | 采用SSH协议连接操作系统，保证了鉴别信息以及管理数据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。 | 操作系统中对重要鉴别信息通过自身的加密及校验（SHA256），保证数据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； | 采用SSH协议连接操作系统，保证了鉴别信息以及管理数据在传输过程中的保密性。 |
| b）应采用密码技术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个人信息等。 | 通过系统自带的加密模块保证鉴别数据在存储过程中的保密性。 |
| 数据备份恢复 | a）应提供重要数据的本地数据备份与恢复功能； | 经核查，通过脚本每周将配置文件、代码仓库等数据备份至备份服务器中，依据需要验证备份数据的有效性。 |
| b）应提供异地实时备份功能，利用通信网络将重要数据实时备份至备份场地； | 系统无异地备份机制。 |
| c）应提供重要数据处理系统的热冗余，保证系统的高可用性。 | 服务器采用K8S容器部署，保证系统的高可用性。 |
| 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； | 操作系统提供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功能。 |
| 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。 | 操作系统提供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的功能。 |

4.1.3.71. 数据索引服务器22

|  |  |  |
| --- | --- | --- |
| **安全控制点** | **测评指标** | **结果记录** |
| 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）操作系统时采用用户名+SSHKey公私钥进行身份鉴别鉴别信息具有复杂度要求；2）执行cat /etc/shadow命令，查看shadow文件系统内用户身份标识唯一，不存在同名用户，且不存在空口令账号；3）经访谈，SSHKey公私钥每半年进行更换；4）查看sshd\_config配置文件中配置PasswordAuthentication no，拒绝使用密码方式进行身份鉴别。 |
| 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； | 操作系统采用用户名+SSHKey公私钥进行身份鉴别，可以防止鉴别信息被暴力破解；但未配置用户连接超时退出策略。 |
| 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； | 1）经核查，管理人员采用SSH协议连接操作系统；2）执行netatat –tpln| grep 23命令查看操作系统远程管理端口，不存在Telnet端口，防止鉴别信息在网络传输过程中的被窃听。 |
| 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。 | 未采用两种或两种以上组合的鉴别技术对用户进行身份鉴别。 |
| 访问控制 | a）应对登录的用户分配账户和权限； | 1）经访谈，通过root账户为登录的用户创建账户、分配权限；2）执行ls -l命令查看关键文件权限，均已为账户分配了相应权限，相关文件权限设置为/etc/shadow：000、/etc/passwd：644、/etc/group：644、/etc/profile：644、/etc/crontab：644、/ etc/securetty：600、/etc/ssh/sshd\_config：600。 |
| b）应重命名或删除默认账户，修改默认账户的默认口令； | 1）执行cat /etc/shadow命令查看shadow文件，操作系统中adm、lp、sync、shutdown、halt、mail、uucp、operator、games、gopher等账户均为nologin状态，存在默认账户root；2）执行more /etc/ssh/sshd\_config命令，查看“PermitRootLogin”参数设置为“yes”，即允许root远程登录；3）经访谈，root用户需通过公私钥方式进行身份鉴别。 |
| 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； | 1）执行cat /etc/shadow命令查看shadow文件，发现操作系统存在root、ysup、yops、yluser等在用账户，不存在多余的、过期账户；2）存在多个堡垒机账户登录操作系统时共用一个账户的情况。 |
| 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； | root账户具有系统所有权限，未实现管理用户的权限分离。 |
| e）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； | 经访谈，由系统管理员root配置访问控制策略，如：/etc/passwd，/etc/profile宿主为root、权限设置为644，audit文件为700、message文件为600，其他文件权限为750，实现用户对文件的权限控制。 |
| f）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； | 由管理用户进行用户访问权限分配进行设置，依据访问控制策略,对各类文件进行访问，重要文件和目录权限均在合理范围内，用户可根据文件不同的权限进行操作。 |
| g）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。 | 执 行more /etc/selinux/config 命令，查看config文件显示 SELINUX参数为 DISABLED，即未开启强制访问控制模式。 |
| 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）执行ps -ef|grep rsyslog和ps -ef|grep auditd命令，显示rsyslog和auditd进程正在运行；2）more /etc/audit/audit.rules，显示审计内容包括：\*.info、authriv.\*、mail.\*、cron.\*、\*.emerg、uucp、news.crit、local7.\*等事件。 |
| 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； | 执行tail -20 /var/log/audit/audit.log命令，查看近20条审计日志，内容包括：时间、对象、路径、用户ID、相关的系统调用、用户执行命令等。 |
| 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）通过访问权限对审计记录进行保护，日志文件/var/log/messages、/var/log/secure、/var/log/audit/audit.log访问 权限均为600；2）审计记录本地保存，且实时备份至360本地安全大脑，保存时间满足180天以上。 |
| d）应对审计进程进行保护，防止未经授权的中断。 | 执行service auditd status命令，系统开启auditd审计保护进程，审计进程由root用户维护，经现场使用yluser用户通过service auditd stop命令尝试中断审计进程，无法将审计进程单独中断。 |
| 入侵防范 | a）应遵循最小安装的原则，仅安装需要的组件和应用程序； | 1）系统安装遵循最小化安装原则；2）执行yum list installed命令查看操作系统已安装的程序包，存在Java、elasticsearch、SSH、天眼云镜agent等应用程序或组件，不存在与业务系统无关的组件和应用程序。 |
| b）应关闭不需要的系统服务、默认共享和高危端口； | 1）执行systemctl list-unit-files 命令，系统已关闭FTP、Telnet 等高危网络服务；2）执行netstat -pantu命令，系统关闭了135、445等高危端口，仅开启了22、8080等端口。 |
| c）应通过设定终端接入方式或网络地址范围对通过网络进行管理的管理终端进行限制； | 经核查，1）通过配置安全组策略限制仅允许通过堡垒机管理服务器；2）经核查防火墙中访问控制策略，具备堡垒机地址-服务器管理网段（10.33.0.0）的访问控制策略。 |
| d）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； | 根据GB∕T 28448-2019 《信息安全技术 网络安全等级保护测评要求》测评对象范围描述，服务器无该项要求，故判为“不适用”。 |
| e）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； | 1）经过漏洞扫描，服务器不存在高危安全漏洞；2）执行rpm -qa grep patch命令，查看系统补丁已更新至最新。 |
| f）应能够检测到对重要节点进行入侵的行为，并在发生严重入侵事件时提供报警。 | 经核查，服务器上安装有青藤云天眼云镜，对主机入侵行为进行检测，发现严重安全事件时通过钉钉告警。 |
| 恶意代码防范 | a）应采用免受恶意代码攻击的技术措施或主动免疫可信验证机制及时识别入侵和病毒行为，并将其有效阻断。 | 经核查，服务器上安装有青藤云天眼云镜，对主机恶意代码进行检测、清除，每天凌晨自动更新恶意代码特征库，经核查，具备恶意代码特征库更新记录。 |
| 可信验证 | a）可基于可信根对计算设备的系统引导程序、系统程序、重要配置参数和应用程序等进行可信验证，并在应用程序的关键执行环节进行动态可信验证，在检测到其可信性受到破坏后进行报警，并将验证结果形成审计记录送至安全管理中心。 | 未采用技术措施对计算设备的系统引导程序、系统程序、重要配置参数和通信应用程序等进行可信验证。 |
| 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； | 采用SSH协议连接操作系统，保证了鉴别信息以及管理数据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。 | 操作系统中对重要鉴别信息通过自身的加密及校验（SHA256），保证数据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； | 采用SSH协议连接操作系统，保证了鉴别信息以及管理数据在传输过程中的保密性。 |
| b）应采用密码技术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个人信息等。 | 通过系统自带的加密模块保证鉴别数据在存储过程中的保密性。 |
| 数据备份恢复 | a）应提供重要数据的本地数据备份与恢复功能； | 经核查，通过脚本每周将配置文件、代码仓库等数据备份至备份服务器中，依据需要验证备份数据的有效性。 |
| b）应提供异地实时备份功能，利用通信网络将重要数据实时备份至备份场地； | 系统无异地备份机制。 |
| c）应提供重要数据处理系统的热冗余，保证系统的高可用性。 | 服务器采用K8S容器部署，保证系统的高可用性。 |
| 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； | 操作系统提供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功能。 |
| 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。 | 操作系统提供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的功能。 |

4.1.3.72. 中间件服务器1

|  |  |  |
| --- | --- | --- |
| **安全控制点** | **测评指标** | **结果记录** |
| 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）操作系统时采用用户名+SSHKey公私钥进行身份鉴别鉴别信息具有复杂度要求；2）执行cat /etc/shadow命令，查看shadow文件系统内用户身份标识唯一，不存在同名用户，且不存在空口令账号；3）经访谈，SSHKey公私钥每半年进行更换；4）查看sshd\_config配置文件中配置PasswordAuthentication no，拒绝使用密码方式进行身份鉴别。 |
| 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； | 操作系统采用用户名+SSHKey公私钥进行身份鉴别，可以防止鉴别信息被暴力破解；但未配置用户连接超时退出策略。 |
| 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； | 1）经核查，管理人员采用SSH协议连接操作系统；2）执行netatat –tpln| grep 23命令查看操作系统远程管理端口，不存在Telnet端口，防止鉴别信息在网络传输过程中的被窃听。 |
| 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。 | 未采用两种或两种以上组合的鉴别技术对用户进行身份鉴别。 |
| 访问控制 | a）应对登录的用户分配账户和权限； | 1）经访谈，通过root账户为登录的用户创建账户、分配权限；2）执行ls -l命令查看关键文件权限，均已为账户分配了相应权限，相关文件权限设置为/etc/shadow：000、/etc/passwd：644、/etc/group：644、/etc/profile：644、/etc/crontab：644、/ etc/securetty：600、/etc/ssh/sshd\_config：600。 |
| b）应重命名或删除默认账户，修改默认账户的默认口令； | 1）执行cat /etc/shadow命令查看shadow文件，操作系统中adm、lp、sync、shutdown、halt、mail、uucp、operator、games、gopher等账户均为nologin状态，存在默认账户root；2）执行more /etc/ssh/sshd\_config命令，查看“PermitRootLogin”参数设置为“yes”，即允许root远程登录；3）经访谈，root用户需通过公私钥方式进行身份鉴别。 |
| 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； | 1）执行cat /etc/shadow命令查看shadow文件，发现操作系统存在root、ysup、yops、yluser等在用账户，不存在多余的、过期账户；2）存在多个堡垒机账户登录操作系统时共用一个账户的情况。 |
| 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； | root账户具有系统所有权限，未实现管理用户的权限分离。 |
| e）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； | 经访谈，由系统管理员root配置访问控制策略，如：/etc/passwd，/etc/profile宿主为root、权限设置为644，audit文件为700、message文件为600，其他文件权限为750，实现用户对文件的权限控制。 |
| f）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； | 由管理用户进行用户访问权限分配进行设置，依据访问控制策略,对各类文件进行访问，重要文件和目录权限均在合理范围内，用户可根据文件不同的权限进行操作。 |
| g）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。 | 执 行more /etc/selinux/config 命令，查看config文件显示 SELINUX参数为 DISABLED，即未开启强制访问控制模式。 |
| 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）执行ps -ef|grep rsyslog和ps -ef|grep auditd命令，显示rsyslog和auditd进程正在运行；2）more /etc/audit/audit.rules，显示审计内容包括：\*.info、authriv.\*、mail.\*、cron.\*、\*.emerg、uucp、news.crit、local7.\*等事件。 |
| 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； | 执行tail -20 /var/log/audit/audit.log命令，查看近20条审计日志，内容包括：时间、对象、路径、用户ID、相关的系统调用、用户执行命令等。 |
| 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）通过访问权限对审计记录进行保护，日志文件/var/log/messages、/var/log/secure、/var/log/audit/audit.log访问 权限均为600；2）审计记录本地保存，且实时备份至360本地安全大脑，保存时间满足180天以上。 |
| d）应对审计进程进行保护，防止未经授权的中断。 | 执行service auditd status命令，系统开启auditd审计保护进程，审计进程由root用户维护，经现场使用yluser用户通过service auditd stop命令尝试中断审计进程，无法将审计进程单独中断。 |
| 入侵防范 | a）应遵循最小安装的原则，仅安装需要的组件和应用程序； | 1）系统安装遵循最小化安装原则；2）执行yum list installed命令查看操作系统已安装的程序包，存在Java、Rabbit MQ、SSH、天眼云镜agent等应用程序或组件，不存在与业务系统无关的组件和应用程序。 |
| b）应关闭不需要的系统服务、默认共享和高危端口； | 1）执行systemctl list-unit-files 命令，系统已关闭FTP、Telnet 等高危网络服务；2）执行netstat -pantu命令，系统关闭了135、445等高危端口，仅开启了22、8080等端口。 |
| c）应通过设定终端接入方式或网络地址范围对通过网络进行管理的管理终端进行限制； | 经核查，1）通过配置安全组策略限制仅允许通过堡垒机管理服务器；2）经核查防火墙中访问控制策略，具备堡垒机地址-服务器管理网段（10.33.0.0）的访问控制策略。 |
| d）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； | 根据GB∕T 28448-2019 《信息安全技术 网络安全等级保护测评要求》测评对象范围描述，服务器无该项要求，故判为“不适用”。 |
| e）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； | 1）经过漏洞扫描，服务器不存在高危安全漏洞；2）执行rpm -qa grep patch命令，查看系统补丁已更新至最新。 |
| f）应能够检测到对重要节点进行入侵的行为，并在发生严重入侵事件时提供报警。 | 经核查，服务器上安装有青藤云天眼云镜，对主机入侵行为进行检测，发现严重安全事件时通过钉钉告警。 |
| 恶意代码防范 | a）应采用免受恶意代码攻击的技术措施或主动免疫可信验证机制及时识别入侵和病毒行为，并将其有效阻断。 | 经核查，服务器上安装有青藤云天眼云镜，对主机恶意代码进行检测、清除，每天凌晨自动更新恶意代码特征库，经核查，具备恶意代码特征库更新记录。 |
| 可信验证 | a）可基于可信根对计算设备的系统引导程序、系统程序、重要配置参数和应用程序等进行可信验证，并在应用程序的关键执行环节进行动态可信验证，在检测到其可信性受到破坏后进行报警，并将验证结果形成审计记录送至安全管理中心。 | 未采用技术措施对计算设备的系统引导程序、系统程序、重要配置参数和通信应用程序等进行可信验证。 |
| 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； | 采用SSH协议连接操作系统，保证了鉴别信息以及管理数据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。 | 操作系统中对重要鉴别信息通过自身的加密及校验（SHA256），保证数据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； | 采用SSH协议连接操作系统，保证了鉴别信息以及管理数据在传输过程中的保密性。 |
| b）应采用密码技术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个人信息等。 | 通过系统自带的加密模块保证鉴别数据在存储过程中的保密性。 |
| 数据备份恢复 | a）应提供重要数据的本地数据备份与恢复功能； | 经核查，通过脚本每周将配置文件、代码仓库等数据备份至备份服务器中，依据需要验证备份数据的有效性。 |
| b）应提供异地实时备份功能，利用通信网络将重要数据实时备份至备份场地； | 系统无异地备份机制。 |
| c）应提供重要数据处理系统的热冗余，保证系统的高可用性。 | 服务器采用K8S容器部署，保证系统的高可用性。 |
| 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； | 操作系统提供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功能。 |
| 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。 | 操作系统提供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的功能。 |

4.1.3.73. 中间件服务器2

|  |  |  |
| --- | --- | --- |
| **安全控制点** | **测评指标** | **结果记录** |
| 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）操作系统时采用用户名+SSHKey公私钥进行身份鉴别鉴别信息具有复杂度要求；2）执行cat /etc/shadow命令，查看shadow文件系统内用户身份标识唯一，不存在同名用户，且不存在空口令账号；3）经访谈，SSHKey公私钥每半年进行更换；4）查看sshd\_config配置文件中配置PasswordAuthentication no，拒绝使用密码方式进行身份鉴别。 |
| 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； | 操作系统采用用户名+SSHKey公私钥进行身份鉴别，可以防止鉴别信息被暴力破解；但未配置用户连接超时退出策略。 |
| 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； | 1）经核查，管理人员采用SSH协议连接操作系统；2）执行netatat –tpln| grep 23命令查看操作系统远程管理端口，不存在Telnet端口，防止鉴别信息在网络传输过程中的被窃听。 |
| 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。 | 未采用两种或两种以上组合的鉴别技术对用户进行身份鉴别。 |
| 访问控制 | a）应对登录的用户分配账户和权限； | 1）经访谈，通过root账户为登录的用户创建账户、分配权限；2）执行ls -l命令查看关键文件权限，均已为账户分配了相应权限，相关文件权限设置为/etc/shadow：000、/etc/passwd：644、/etc/group：644、/etc/profile：644、/etc/crontab：644、/ etc/securetty：600、/etc/ssh/sshd\_config：600。 |
| b）应重命名或删除默认账户，修改默认账户的默认口令； | 1）执行cat /etc/shadow命令查看shadow文件，操作系统中adm、lp、sync、shutdown、halt、mail、uucp、operator、games、gopher等账户均为nologin状态，存在默认账户root；2）执行more /etc/ssh/sshd\_config命令，查看“PermitRootLogin”参数设置为“yes”，即允许root远程登录；3）经访谈，root用户需通过公私钥方式进行身份鉴别。 |
| 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； | 1）执行cat /etc/shadow命令查看shadow文件，发现操作系统存在root、ysup、yops、yluser等在用账户，不存在多余的、过期账户；2）存在多个堡垒机账户登录操作系统时共用一个账户的情况。 |
| 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； | root账户具有系统所有权限，未实现管理用户的权限分离。 |
| e）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； | 经访谈，由系统管理员root配置访问控制策略，如：/etc/passwd，/etc/profile宿主为root、权限设置为644，audit文件为700、message文件为600，其他文件权限为750，实现用户对文件的权限控制。 |
| f）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； | 由管理用户进行用户访问权限分配进行设置，依据访问控制策略,对各类文件进行访问，重要文件和目录权限均在合理范围内，用户可根据文件不同的权限进行操作。 |
| g）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。 | 执 行more /etc/selinux/config 命令，查看config文件显示 SELINUX参数为 DISABLED，即未开启强制访问控制模式。 |
| 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）执行ps -ef|grep rsyslog和ps -ef|grep auditd命令，显示rsyslog和auditd进程正在运行；2）more /etc/audit/audit.rules，显示审计内容包括：\*.info、authriv.\*、mail.\*、cron.\*、\*.emerg、uucp、news.crit、local7.\*等事件。 |
| 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； | 执行tail -20 /var/log/audit/audit.log命令，查看近20条审计日志，内容包括：时间、对象、路径、用户ID、相关的系统调用、用户执行命令等。 |
| 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）通过访问权限对审计记录进行保护，日志文件/var/log/messages、/var/log/secure、/var/log/audit/audit.log访问 权限均为600；2）审计记录本地保存，且实时备份至360本地安全大脑，保存时间满足180天以上。 |
| d）应对审计进程进行保护，防止未经授权的中断。 | 执行service auditd status命令，系统开启auditd审计保护进程，审计进程由root用户维护，经现场使用yluser用户通过service auditd stop命令尝试中断审计进程，无法将审计进程单独中断。 |
| 入侵防范 | a）应遵循最小安装的原则，仅安装需要的组件和应用程序； | 1）系统安装遵循最小化安装原则；2）执行yum list installed命令查看操作系统已安装的程序包，存在Java、Rabbit MQ、SSH、天眼云镜agent等应用程序或组件，不存在与业务系统无关的组件和应用程序。 |
| b）应关闭不需要的系统服务、默认共享和高危端口； | 1）执行systemctl list-unit-files 命令，系统已关闭FTP、Telnet 等高危网络服务；2）执行netstat -pantu命令，系统关闭了135、445等高危端口，仅开启了22、8080等端口。 |
| c）应通过设定终端接入方式或网络地址范围对通过网络进行管理的管理终端进行限制； | 经核查，1）通过配置安全组策略限制仅允许通过堡垒机管理服务器；2）经核查防火墙中访问控制策略，具备堡垒机地址-服务器管理网段（10.33.0.0）的访问控制策略。 |
| d）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； | 根据GB∕T 28448-2019 《信息安全技术 网络安全等级保护测评要求》测评对象范围描述，服务器无该项要求，故判为“不适用”。 |
| e）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； | 1）经过漏洞扫描，服务器不存在高危安全漏洞；2）执行rpm -qa grep patch命令，查看系统补丁已更新至最新。 |
| f）应能够检测到对重要节点进行入侵的行为，并在发生严重入侵事件时提供报警。 | 经核查，服务器上安装有青藤云天眼云镜，对主机入侵行为进行检测，发现严重安全事件时通过钉钉告警。 |
| 恶意代码防范 | a）应采用免受恶意代码攻击的技术措施或主动免疫可信验证机制及时识别入侵和病毒行为，并将其有效阻断。 | 经核查，服务器上安装有青藤云天眼云镜，对主机恶意代码进行检测、清除，每天凌晨自动更新恶意代码特征库，经核查，具备恶意代码特征库更新记录。 |
| 可信验证 | a）可基于可信根对计算设备的系统引导程序、系统程序、重要配置参数和应用程序等进行可信验证，并在应用程序的关键执行环节进行动态可信验证，在检测到其可信性受到破坏后进行报警，并将验证结果形成审计记录送至安全管理中心。 | 未采用技术措施对计算设备的系统引导程序、系统程序、重要配置参数和通信应用程序等进行可信验证。 |
| 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； | 采用SSH协议连接操作系统，保证了鉴别信息以及管理数据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。 | 操作系统中对重要鉴别信息通过自身的加密及校验（SHA256），保证数据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； | 采用SSH协议连接操作系统，保证了鉴别信息以及管理数据在传输过程中的保密性。 |
| b）应采用密码技术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个人信息等。 | 通过系统自带的加密模块保证鉴别数据在存储过程中的保密性。 |
| 数据备份恢复 | a）应提供重要数据的本地数据备份与恢复功能； | 经核查，通过脚本每周将配置文件、代码仓库等数据备份至备份服务器中，依据需要验证备份数据的有效性。 |
| b）应提供异地实时备份功能，利用通信网络将重要数据实时备份至备份场地； | 系统无异地备份机制。 |
| c）应提供重要数据处理系统的热冗余，保证系统的高可用性。 | 服务器采用K8S容器部署，保证系统的高可用性。 |
| 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； | 操作系统提供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功能。 |
| 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。 | 操作系统提供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的功能。 |

4.1.3.74. 中间件服务器3

|  |  |  |
| --- | --- | --- |
| **安全控制点** | **测评指标** | **结果记录** |
| 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）操作系统时采用用户名+SSHKey公私钥进行身份鉴别鉴别信息具有复杂度要求；2）执行cat /etc/shadow命令，查看shadow文件系统内用户身份标识唯一，不存在同名用户，且不存在空口令账号；3）经访谈，SSHKey公私钥每半年进行更换；4）查看sshd\_config配置文件中配置PasswordAuthentication no，拒绝使用密码方式进行身份鉴别。 |
| 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； | 操作系统采用用户名+SSHKey公私钥进行身份鉴别，可以防止鉴别信息被暴力破解；但未配置用户连接超时退出策略。 |
| 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； | 1）经核查，管理人员采用SSH协议连接操作系统；2）执行netatat –tpln| grep 23命令查看操作系统远程管理端口，不存在Telnet端口，防止鉴别信息在网络传输过程中的被窃听。 |
| 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。 | 未采用两种或两种以上组合的鉴别技术对用户进行身份鉴别。 |
| 访问控制 | a）应对登录的用户分配账户和权限； | 1）经访谈，通过root账户为登录的用户创建账户、分配权限；2）执行ls -l命令查看关键文件权限，均已为账户分配了相应权限，相关文件权限设置为/etc/shadow：000、/etc/passwd：644、/etc/group：644、/etc/profile：644、/etc/crontab：644、/ etc/securetty：600、/etc/ssh/sshd\_config：600。 |
| b）应重命名或删除默认账户，修改默认账户的默认口令； | 1）执行cat /etc/shadow命令查看shadow文件，操作系统中adm、lp、sync、shutdown、halt、mail、uucp、operator、games、gopher等账户均为nologin状态，存在默认账户root；2）执行more /etc/ssh/sshd\_config命令，查看“PermitRootLogin”参数设置为“yes”，即允许root远程登录；3）经访谈，root用户需通过公私钥方式进行身份鉴别。 |
| 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； | 1）执行cat /etc/shadow命令查看shadow文件，发现操作系统存在root、ysup、yops、yluser等在用账户，不存在多余的、过期账户；2）存在多个堡垒机账户登录操作系统时共用一个账户的情况。 |
| 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； | root账户具有系统所有权限，未实现管理用户的权限分离。 |
| e）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； | 经访谈，由系统管理员root配置访问控制策略，如：/etc/passwd，/etc/profile宿主为root、权限设置为644，audit文件为700、message文件为600，其他文件权限为750，实现用户对文件的权限控制。 |
| f）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； | 由管理用户进行用户访问权限分配进行设置，依据访问控制策略,对各类文件进行访问，重要文件和目录权限均在合理范围内，用户可根据文件不同的权限进行操作。 |
| g）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。 | 执 行more /etc/selinux/config 命令，查看config文件显示 SELINUX参数为 DISABLED，即未开启强制访问控制模式。 |
| 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）执行ps -ef|grep rsyslog和ps -ef|grep auditd命令，显示rsyslog和auditd进程正在运行；2）more /etc/audit/audit.rules，显示审计内容包括：\*.info、authriv.\*、mail.\*、cron.\*、\*.emerg、uucp、news.crit、local7.\*等事件。 |
| 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； | 执行tail -20 /var/log/audit/audit.log命令，查看近20条审计日志，内容包括：时间、对象、路径、用户ID、相关的系统调用、用户执行命令等。 |
| 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）通过访问权限对审计记录进行保护，日志文件/var/log/messages、/var/log/secure、/var/log/audit/audit.log访问 权限均为600；2）审计记录本地保存，且实时备份至360本地安全大脑，保存时间满足180天以上。 |
| d）应对审计进程进行保护，防止未经授权的中断。 | 执行service auditd status命令，系统开启auditd审计保护进程，审计进程由root用户维护，经现场使用yluser用户通过service auditd stop命令尝试中断审计进程，无法将审计进程单独中断。 |
| 入侵防范 | a）应遵循最小安装的原则，仅安装需要的组件和应用程序； | 1）系统安装遵循最小化安装原则；2）执行yum list installed命令查看操作系统已安装的程序包，存在Java、Rabbit MQ、SSH、天眼云镜agent等应用程序或组件，不存在与业务系统无关的组件和应用程序。 |
| b）应关闭不需要的系统服务、默认共享和高危端口； | 1）执行systemctl list-unit-files 命令，系统已关闭FTP、Telnet 等高危网络服务；2）执行netstat -pantu命令，系统关闭了135、445等高危端口，仅开启了22、8080等端口。 |
| c）应通过设定终端接入方式或网络地址范围对通过网络进行管理的管理终端进行限制； | 经核查，1）通过配置安全组策略限制仅允许通过堡垒机管理服务器；2）经核查防火墙中访问控制策略，具备堡垒机地址-服务器管理网段（10.33.0.0）的访问控制策略。 |
| d）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； | 根据GB∕T 28448-2019 《信息安全技术 网络安全等级保护测评要求》测评对象范围描述，服务器无该项要求，故判为“不适用”。 |
| e）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； | 1）经过漏洞扫描，服务器不存在高危安全漏洞；2）执行rpm -qa grep patch命令，查看系统补丁已更新至最新。 |
| f）应能够检测到对重要节点进行入侵的行为，并在发生严重入侵事件时提供报警。 | 经核查，服务器上安装有青藤云天眼云镜，对主机入侵行为进行检测，发现严重安全事件时通过钉钉告警。 |
| 恶意代码防范 | a）应采用免受恶意代码攻击的技术措施或主动免疫可信验证机制及时识别入侵和病毒行为，并将其有效阻断。 | 经核查，服务器上安装有青藤云天眼云镜，对主机恶意代码进行检测、清除，每天凌晨自动更新恶意代码特征库，经核查，具备恶意代码特征库更新记录。 |
| 可信验证 | a）可基于可信根对计算设备的系统引导程序、系统程序、重要配置参数和应用程序等进行可信验证，并在应用程序的关键执行环节进行动态可信验证，在检测到其可信性受到破坏后进行报警，并将验证结果形成审计记录送至安全管理中心。 | 未采用技术措施对计算设备的系统引导程序、系统程序、重要配置参数和通信应用程序等进行可信验证。 |
| 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； | 采用SSH协议连接操作系统，保证了鉴别信息以及管理数据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。 | 操作系统中对重要鉴别信息通过自身的加密及校验（SHA256），保证数据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； | 采用SSH协议连接操作系统，保证了鉴别信息以及管理数据在传输过程中的保密性。 |
| b）应采用密码技术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个人信息等。 | 通过系统自带的加密模块保证鉴别数据在存储过程中的保密性。 |
| 数据备份恢复 | a）应提供重要数据的本地数据备份与恢复功能； | 经核查，通过脚本每周将配置文件、代码仓库等数据备份至备份服务器中，依据需要验证备份数据的有效性。 |
| b）应提供异地实时备份功能，利用通信网络将重要数据实时备份至备份场地； | 系统无异地备份机制。 |
| c）应提供重要数据处理系统的热冗余，保证系统的高可用性。 | 服务器采用K8S容器部署，保证系统的高可用性。 |
| 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； | 操作系统提供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功能。 |
| 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。 | 操作系统提供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的功能。 |

4.1.3.75. 中间件服务器4

|  |  |  |
| --- | --- | --- |
| **安全控制点** | **测评指标** | **结果记录** |
| 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）操作系统时采用用户名+SSHKey公私钥进行身份鉴别鉴别信息具有复杂度要求；2）执行cat /etc/shadow命令，查看shadow文件系统内用户身份标识唯一，不存在同名用户，且不存在空口令账号；3）经访谈，SSHKey公私钥每半年进行更换；4）查看sshd\_config配置文件中配置PasswordAuthentication no，拒绝使用密码方式进行身份鉴别。 |
| 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； | 操作系统采用用户名+SSHKey公私钥进行身份鉴别，可以防止鉴别信息被暴力破解；但未配置用户连接超时退出策略。 |
| 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； | 1）经核查，管理人员采用SSH协议连接操作系统；2）执行netatat –tpln| grep 23命令查看操作系统远程管理端口，不存在Telnet端口，防止鉴别信息在网络传输过程中的被窃听。 |
| 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。 | 未采用两种或两种以上组合的鉴别技术对用户进行身份鉴别。 |
| 访问控制 | a）应对登录的用户分配账户和权限； | 1）经访谈，通过root账户为登录的用户创建账户、分配权限；2）执行ls -l命令查看关键文件权限，均已为账户分配了相应权限，相关文件权限设置为/etc/shadow：000、/etc/passwd：644、/etc/group：644、/etc/profile：644、/etc/crontab：644、/ etc/securetty：600、/etc/ssh/sshd\_config：600。 |
| b）应重命名或删除默认账户，修改默认账户的默认口令； | 1）执行cat /etc/shadow命令查看shadow文件，操作系统中adm、lp、sync、shutdown、halt、mail、uucp、operator、games、gopher等账户均为nologin状态，存在默认账户root；2）执行more /etc/ssh/sshd\_config命令，查看“PermitRootLogin”参数设置为“yes”，即允许root远程登录；3）经访谈，root用户需通过公私钥方式进行身份鉴别。 |
| 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； | 1）执行cat /etc/shadow命令查看shadow文件，发现操作系统存在root、ysup、yops、yluser等在用账户，不存在多余的、过期账户；2）存在多个堡垒机账户登录操作系统时共用一个账户的情况。 |
| 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； | root账户具有系统所有权限，未实现管理用户的权限分离。 |
| e）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； | 经访谈，由系统管理员root配置访问控制策略，如：/etc/passwd，/etc/profile宿主为root、权限设置为644，audit文件为700、message文件为600，其他文件权限为750，实现用户对文件的权限控制。 |
| f）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； | 由管理用户进行用户访问权限分配进行设置，依据访问控制策略,对各类文件进行访问，重要文件和目录权限均在合理范围内，用户可根据文件不同的权限进行操作。 |
| g）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。 | 执 行more /etc/selinux/config 命令，查看config文件显示 SELINUX参数为 DISABLED，即未开启强制访问控制模式。 |
| 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）执行ps -ef|grep rsyslog和ps -ef|grep auditd命令，显示rsyslog和auditd进程正在运行；2）more /etc/audit/audit.rules，显示审计内容包括：\*.info、authriv.\*、mail.\*、cron.\*、\*.emerg、uucp、news.crit、local7.\*等事件。 |
| 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； | 执行tail -20 /var/log/audit/audit.log命令，查看近20条审计日志，内容包括：时间、对象、路径、用户ID、相关的系统调用、用户执行命令等。 |
| 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）通过访问权限对审计记录进行保护，日志文件/var/log/messages、/var/log/secure、/var/log/audit/audit.log访问 权限均为600；2）审计记录本地保存，且实时备份至360本地安全大脑，保存时间满足180天以上。 |
| d）应对审计进程进行保护，防止未经授权的中断。 | 执行service auditd status命令，系统开启auditd审计保护进程，审计进程由root用户维护，经现场使用yluser用户通过service auditd stop命令尝试中断审计进程，无法将审计进程单独中断。 |
| 入侵防范 | a）应遵循最小安装的原则，仅安装需要的组件和应用程序； | 1）系统安装遵循最小化安装原则；2）执行yum list installed命令查看操作系统已安装的程序包，存在Java、Rabbit MQ、SSH、天眼云镜agent等应用程序或组件，不存在与业务系统无关的组件和应用程序。 |
| b）应关闭不需要的系统服务、默认共享和高危端口； | 1）执行systemctl list-unit-files 命令，系统已关闭FTP、Telnet 等高危网络服务；2）执行netstat -pantu命令，系统关闭了135、445等高危端口，仅开启了22、8080等端口。 |
| c）应通过设定终端接入方式或网络地址范围对通过网络进行管理的管理终端进行限制； | 经核查，1）通过配置安全组策略限制仅允许通过堡垒机管理服务器；2）经核查防火墙中访问控制策略，具备堡垒机地址-服务器管理网段（10.33.0.0）的访问控制策略。 |
| d）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； | 根据GB∕T 28448-2019 《信息安全技术 网络安全等级保护测评要求》测评对象范围描述，服务器无该项要求，故判为“不适用”。 |
| e）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； | 1）经过漏洞扫描，服务器不存在高危安全漏洞；2）执行rpm -qa grep patch命令，查看系统补丁已更新至最新。 |
| f）应能够检测到对重要节点进行入侵的行为，并在发生严重入侵事件时提供报警。 | 经核查，服务器上安装有青藤云天眼云镜，对主机入侵行为进行检测，发现严重安全事件时通过钉钉告警。 |
| 恶意代码防范 | a）应采用免受恶意代码攻击的技术措施或主动免疫可信验证机制及时识别入侵和病毒行为，并将其有效阻断。 | 经核查，服务器上安装有青藤云天眼云镜，对主机恶意代码进行检测、清除，每天凌晨自动更新恶意代码特征库，经核查，具备恶意代码特征库更新记录。 |
| 可信验证 | a）可基于可信根对计算设备的系统引导程序、系统程序、重要配置参数和应用程序等进行可信验证，并在应用程序的关键执行环节进行动态可信验证，在检测到其可信性受到破坏后进行报警，并将验证结果形成审计记录送至安全管理中心。 | 未采用技术措施对计算设备的系统引导程序、系统程序、重要配置参数和通信应用程序等进行可信验证。 |
| 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； | 采用SSH协议连接操作系统，保证了鉴别信息以及管理数据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。 | 操作系统中对重要鉴别信息通过自身的加密及校验（SHA256），保证数据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； | 采用SSH协议连接操作系统，保证了鉴别信息以及管理数据在传输过程中的保密性。 |
| b）应采用密码技术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个人信息等。 | 通过系统自带的加密模块保证鉴别数据在存储过程中的保密性。 |
| 数据备份恢复 | a）应提供重要数据的本地数据备份与恢复功能； | 经核查，通过脚本每周将配置文件、代码仓库等数据备份至备份服务器中，依据需要验证备份数据的有效性。 |
| b）应提供异地实时备份功能，利用通信网络将重要数据实时备份至备份场地； | 系统无异地备份机制。 |
| c）应提供重要数据处理系统的热冗余，保证系统的高可用性。 | 服务器采用K8S容器部署，保证系统的高可用性。 |
| 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； | 操作系统提供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功能。 |
| 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。 | 操作系统提供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的功能。 |

4.1.3.76. 中间件服务器5

|  |  |  |
| --- | --- | --- |
| **安全控制点** | **测评指标** | **结果记录** |
| 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）操作系统时采用用户名+SSHKey公私钥进行身份鉴别鉴别信息具有复杂度要求；2）执行cat /etc/shadow命令，查看shadow文件系统内用户身份标识唯一，不存在同名用户，且不存在空口令账号；3）经访谈，SSHKey公私钥每半年进行更换；4）查看sshd\_config配置文件中配置PasswordAuthentication no，拒绝使用密码方式进行身份鉴别。 |
| 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； | 操作系统采用用户名+SSHKey公私钥进行身份鉴别，可以防止鉴别信息被暴力破解；但未配置用户连接超时退出策略。 |
| 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； | 1）经核查，管理人员采用SSH协议连接操作系统；2）执行netatat –tpln| grep 23命令查看操作系统远程管理端口，不存在Telnet端口，防止鉴别信息在网络传输过程中的被窃听。 |
| 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。 | 未采用两种或两种以上组合的鉴别技术对用户进行身份鉴别。 |
| 访问控制 | a）应对登录的用户分配账户和权限； | 1）经访谈，通过root账户为登录的用户创建账户、分配权限；2）执行ls -l命令查看关键文件权限，均已为账户分配了相应权限，相关文件权限设置为/etc/shadow：000、/etc/passwd：644、/etc/group：644、/etc/profile：644、/etc/crontab：644、/ etc/securetty：600、/etc/ssh/sshd\_config：600。 |
| b）应重命名或删除默认账户，修改默认账户的默认口令； | 1）执行cat /etc/shadow命令查看shadow文件，操作系统中adm、lp、sync、shutdown、halt、mail、uucp、operator、games、gopher等账户均为nologin状态，存在默认账户root；2）执行more /etc/ssh/sshd\_config命令，查看“PermitRootLogin”参数设置为“yes”，即允许root远程登录；3）经访谈，root用户需通过公私钥方式进行身份鉴别。 |
| 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； | 1）执行cat /etc/shadow命令查看shadow文件，发现操作系统存在root、ysup、yops、yluser等在用账户，不存在多余的、过期账户；2）存在多个堡垒机账户登录操作系统时共用一个账户的情况。 |
| 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； | root账户具有系统所有权限，未实现管理用户的权限分离。 |
| e）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； | 经访谈，由系统管理员root配置访问控制策略，如：/etc/passwd，/etc/profile宿主为root、权限设置为644，audit文件为700、message文件为600，其他文件权限为750，实现用户对文件的权限控制。 |
| f）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； | 由管理用户进行用户访问权限分配进行设置，依据访问控制策略,对各类文件进行访问，重要文件和目录权限均在合理范围内，用户可根据文件不同的权限进行操作。 |
| g）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。 | 执 行more /etc/selinux/config 命令，查看config文件显示 SELINUX参数为 DISABLED，即未开启强制访问控制模式。 |
| 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）执行ps -ef|grep rsyslog和ps -ef|grep auditd命令，显示rsyslog和auditd进程正在运行；2）more /etc/audit/audit.rules，显示审计内容包括：\*.info、authriv.\*、mail.\*、cron.\*、\*.emerg、uucp、news.crit、local7.\*等事件。 |
| 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； | 执行tail -20 /var/log/audit/audit.log命令，查看近20条审计日志，内容包括：时间、对象、路径、用户ID、相关的系统调用、用户执行命令等。 |
| 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）通过访问权限对审计记录进行保护，日志文件/var/log/messages、/var/log/secure、/var/log/audit/audit.log访问 权限均为600；2）审计记录本地保存，且实时备份至360本地安全大脑，保存时间满足180天以上。 |
| d）应对审计进程进行保护，防止未经授权的中断。 | 执行service auditd status命令，系统开启auditd审计保护进程，审计进程由root用户维护，经现场使用yluser用户通过service auditd stop命令尝试中断审计进程，无法将审计进程单独中断。 |
| 入侵防范 | a）应遵循最小安装的原则，仅安装需要的组件和应用程序； | 1）系统安装遵循最小化安装原则；2）执行yum list installed命令查看操作系统已安装的程序包，存在Java、Rabbit MQ、SSH、天眼云镜agent等应用程序或组件，不存在与业务系统无关的组件和应用程序。 |
| b）应关闭不需要的系统服务、默认共享和高危端口； | 1）执行systemctl list-unit-files 命令，系统已关闭FTP、Telnet 等高危网络服务；2）执行netstat -pantu命令，系统关闭了135、445等高危端口，仅开启了22、8080等端口。 |
| c）应通过设定终端接入方式或网络地址范围对通过网络进行管理的管理终端进行限制； | 经核查，1）通过配置安全组策略限制仅允许通过堡垒机管理服务器；2）经核查防火墙中访问控制策略，具备堡垒机地址-服务器管理网段（10.33.0.0）的访问控制策略。 |
| d）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； | 根据GB∕T 28448-2019 《信息安全技术 网络安全等级保护测评要求》测评对象范围描述，服务器无该项要求，故判为“不适用”。 |
| e）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； | 1）经过漏洞扫描，服务器不存在高危安全漏洞；2）执行rpm -qa grep patch命令，查看系统补丁已更新至最新。 |
| f）应能够检测到对重要节点进行入侵的行为，并在发生严重入侵事件时提供报警。 | 经核查，服务器上安装有青藤云天眼云镜，对主机入侵行为进行检测，发现严重安全事件时通过钉钉告警。 |
| 恶意代码防范 | a）应采用免受恶意代码攻击的技术措施或主动免疫可信验证机制及时识别入侵和病毒行为，并将其有效阻断。 | 经核查，服务器上安装有青藤云天眼云镜，对主机恶意代码进行检测、清除，每天凌晨自动更新恶意代码特征库，经核查，具备恶意代码特征库更新记录。 |
| 可信验证 | a）可基于可信根对计算设备的系统引导程序、系统程序、重要配置参数和应用程序等进行可信验证，并在应用程序的关键执行环节进行动态可信验证，在检测到其可信性受到破坏后进行报警，并将验证结果形成审计记录送至安全管理中心。 | 未采用技术措施对计算设备的系统引导程序、系统程序、重要配置参数和通信应用程序等进行可信验证。 |
| 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； | 采用SSH协议连接操作系统，保证了鉴别信息以及管理数据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。 | 操作系统中对重要鉴别信息通过自身的加密及校验（SHA256），保证数据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； | 采用SSH协议连接操作系统，保证了鉴别信息以及管理数据在传输过程中的保密性。 |
| b）应采用密码技术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个人信息等。 | 通过系统自带的加密模块保证鉴别数据在存储过程中的保密性。 |
| 数据备份恢复 | a）应提供重要数据的本地数据备份与恢复功能； | 经核查，通过脚本每周将配置文件、代码仓库等数据备份至备份服务器中，依据需要验证备份数据的有效性。 |
| b）应提供异地实时备份功能，利用通信网络将重要数据实时备份至备份场地； | 系统无异地备份机制。 |
| c）应提供重要数据处理系统的热冗余，保证系统的高可用性。 | 服务器采用K8S容器部署，保证系统的高可用性。 |
| 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； | 操作系统提供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功能。 |
| 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。 | 操作系统提供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的功能。 |

4.1.3.77. 中间件服务器6

|  |  |  |
| --- | --- | --- |
| **安全控制点** | **测评指标** | **结果记录** |
| 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）操作系统时采用用户名+SSHKey公私钥进行身份鉴别鉴别信息具有复杂度要求；2）执行cat /etc/shadow命令，查看shadow文件系统内用户身份标识唯一，不存在同名用户，且不存在空口令账号；3）经访谈，SSHKey公私钥每半年进行更换；4）查看sshd\_config配置文件中配置PasswordAuthentication no，拒绝使用密码方式进行身份鉴别。 |
| 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； | 操作系统采用用户名+SSHKey公私钥进行身份鉴别，可以防止鉴别信息被暴力破解；但未配置用户连接超时退出策略。 |
| 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； | 1）经核查，管理人员采用SSH协议连接操作系统；2）执行netatat –tpln| grep 23命令查看操作系统远程管理端口，不存在Telnet端口，防止鉴别信息在网络传输过程中的被窃听。 |
| 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。 | 未采用两种或两种以上组合的鉴别技术对用户进行身份鉴别。 |
| 访问控制 | a）应对登录的用户分配账户和权限； | 1）经访谈，通过root账户为登录的用户创建账户、分配权限；2）执行ls -l命令查看关键文件权限，均已为账户分配了相应权限，相关文件权限设置为/etc/shadow：000、/etc/passwd：644、/etc/group：644、/etc/profile：644、/etc/crontab：644、/ etc/securetty：600、/etc/ssh/sshd\_config：600。 |
| b）应重命名或删除默认账户，修改默认账户的默认口令； | 1）执行cat /etc/shadow命令查看shadow文件，操作系统中adm、lp、sync、shutdown、halt、mail、uucp、operator、games、gopher等账户均为nologin状态，存在默认账户root；2）执行more /etc/ssh/sshd\_config命令，查看“PermitRootLogin”参数设置为“yes”，即允许root远程登录；3）经访谈，root用户需通过公私钥方式进行身份鉴别。 |
| 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； | 1）执行cat /etc/shadow命令查看shadow文件，发现操作系统存在root、ysup、yops、yluser等在用账户，不存在多余的、过期账户；2）存在多个堡垒机账户登录操作系统时共用一个账户的情况。 |
| 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； | root账户具有系统所有权限，未实现管理用户的权限分离。 |
| e）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； | 经访谈，由系统管理员root配置访问控制策略，如：/etc/passwd，/etc/profile宿主为root、权限设置为644，audit文件为700、message文件为600，其他文件权限为750，实现用户对文件的权限控制。 |
| f）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； | 由管理用户进行用户访问权限分配进行设置，依据访问控制策略,对各类文件进行访问，重要文件和目录权限均在合理范围内，用户可根据文件不同的权限进行操作。 |
| g）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。 | 执 行more /etc/selinux/config 命令，查看config文件显示 SELINUX参数为 DISABLED，即未开启强制访问控制模式。 |
| 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）执行ps -ef|grep rsyslog和ps -ef|grep auditd命令，显示rsyslog和auditd进程正在运行；2）more /etc/audit/audit.rules，显示审计内容包括：\*.info、authriv.\*、mail.\*、cron.\*、\*.emerg、uucp、news.crit、local7.\*等事件。 |
| 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； | 执行tail -20 /var/log/audit/audit.log命令，查看近20条审计日志，内容包括：时间、对象、路径、用户ID、相关的系统调用、用户执行命令等。 |
| 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）通过访问权限对审计记录进行保护，日志文件/var/log/messages、/var/log/secure、/var/log/audit/audit.log访问 权限均为600；2）审计记录本地保存，且实时备份至360本地安全大脑，保存时间满足180天以上。 |
| d）应对审计进程进行保护，防止未经授权的中断。 | 执行service auditd status命令，系统开启auditd审计保护进程，审计进程由root用户维护，经现场使用yluser用户通过service auditd stop命令尝试中断审计进程，无法将审计进程单独中断。 |
| 入侵防范 | a）应遵循最小安装的原则，仅安装需要的组件和应用程序； | 1）系统安装遵循最小化安装原则；2）执行yum list installed命令查看操作系统已安装的程序包，存在Java、Rabbit MQ、SSH、天眼云镜agent等应用程序或组件，不存在与业务系统无关的组件和应用程序。 |
| b）应关闭不需要的系统服务、默认共享和高危端口； | 1）执行systemctl list-unit-files 命令，系统已关闭FTP、Telnet 等高危网络服务；2）执行netstat -pantu命令，系统关闭了135、445等高危端口，仅开启了22、8080等端口。 |
| c）应通过设定终端接入方式或网络地址范围对通过网络进行管理的管理终端进行限制； | 经核查，1）通过配置安全组策略限制仅允许通过堡垒机管理服务器；2）经核查防火墙中访问控制策略，具备堡垒机地址-服务器管理网段（10.33.0.0）的访问控制策略。 |
| d）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； | 根据GB∕T 28448-2019 《信息安全技术 网络安全等级保护测评要求》测评对象范围描述，服务器无该项要求，故判为“不适用”。 |
| e）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； | 1）经过漏洞扫描，服务器不存在高危安全漏洞；2）执行rpm -qa grep patch命令，查看系统补丁已更新至最新。 |
| f）应能够检测到对重要节点进行入侵的行为，并在发生严重入侵事件时提供报警。 | 经核查，服务器上安装有青藤云天眼云镜，对主机入侵行为进行检测，发现严重安全事件时通过钉钉告警。 |
| 恶意代码防范 | a）应采用免受恶意代码攻击的技术措施或主动免疫可信验证机制及时识别入侵和病毒行为，并将其有效阻断。 | 经核查，服务器上安装有青藤云天眼云镜，对主机恶意代码进行检测、清除，每天凌晨自动更新恶意代码特征库，经核查，具备恶意代码特征库更新记录。 |
| 可信验证 | a）可基于可信根对计算设备的系统引导程序、系统程序、重要配置参数和应用程序等进行可信验证，并在应用程序的关键执行环节进行动态可信验证，在检测到其可信性受到破坏后进行报警，并将验证结果形成审计记录送至安全管理中心。 | 未采用技术措施对计算设备的系统引导程序、系统程序、重要配置参数和通信应用程序等进行可信验证。 |
| 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； | 采用SSH协议连接操作系统，保证了鉴别信息以及管理数据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。 | 操作系统中对重要鉴别信息通过自身的加密及校验（SHA256），保证数据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； | 采用SSH协议连接操作系统，保证了鉴别信息以及管理数据在传输过程中的保密性。 |
| b）应采用密码技术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个人信息等。 | 通过系统自带的加密模块保证鉴别数据在存储过程中的保密性。 |
| 数据备份恢复 | a）应提供重要数据的本地数据备份与恢复功能； | 经核查，通过脚本每周将配置文件、代码仓库等数据备份至备份服务器中，依据需要验证备份数据的有效性。 |
| b）应提供异地实时备份功能，利用通信网络将重要数据实时备份至备份场地； | 系统无异地备份机制。 |
| c）应提供重要数据处理系统的热冗余，保证系统的高可用性。 | 服务器采用K8S容器部署，保证系统的高可用性。 |
| 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； | 操作系统提供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功能。 |
| 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。 | 操作系统提供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的功能。 |

4.1.3.78. 枢纽库集群节点1

|  |  |  |
| --- | --- | --- |
| **安全控制点** | **测评指标** | **结果记录** |
| 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）操作系统时采用用户名+SSHKey公私钥进行身份鉴别鉴别信息具有复杂度要求；2）执行cat /etc/shadow命令，查看shadow文件系统内用户身份标识唯一，不存在同名用户，且不存在空口令账号；3）经访谈，SSHKey公私钥每半年进行更换；4）查看sshd\_config配置文件中配置PasswordAuthentication no，拒绝使用密码方式进行身份鉴别。 |
| 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； | 操作系统采用用户名+SSHKey公私钥进行身份鉴别，可以防止鉴别信息被暴力破解；但未配置用户连接超时退出策略。 |
| 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； | 1）经核查，管理人员采用SSH协议连接操作系统；2）执行netatat –tpln| grep 23命令查看操作系统远程管理端口，不存在Telnet端口，防止鉴别信息在网络传输过程中的被窃听。 |
| 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。 | 未采用两种或两种以上组合的鉴别技术对用户进行身份鉴别。 |
| 访问控制 | a）应对登录的用户分配账户和权限； | 1）经访谈，通过root账户为登录的用户创建账户、分配权限；2）执行ls -l命令查看关键文件权限，均已为账户分配了相应权限，相关文件权限设置为/etc/shadow：000、/etc/passwd：644、/etc/group：644、/etc/profile：644、/etc/crontab：644、/ etc/securetty：600、/etc/ssh/sshd\_config：600。 |
| b）应重命名或删除默认账户，修改默认账户的默认口令； | 1）执行cat /etc/shadow命令查看shadow文件，操作系统中adm、lp、sync、shutdown、halt、mail、uucp、operator、games、gopher等账户均为nologin状态，存在默认账户root；2）执行more /etc/ssh/sshd\_config命令，查看“PermitRootLogin”参数设置为“yes”，即允许root远程登录；3）经访谈，root用户需通过公私钥方式进行身份鉴别。 |
| 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； | 1）执行cat /etc/shadow命令查看shadow文件，发现操作系统存在root、ysup、yops、yluser等在用账户，不存在多余的、过期账户；2）存在多个堡垒机账户登录操作系统时共用一个账户的情况。 |
| 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； | root账户具有系统所有权限，未实现管理用户的权限分离。 |
| e）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； | 经访谈，由系统管理员root配置访问控制策略，如：/etc/passwd，/etc/profile宿主为root、权限设置为644，audit文件为700、message文件为600，其他文件权限为750，实现用户对文件的权限控制。 |
| f）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； | 由管理用户进行用户访问权限分配进行设置，依据访问控制策略,对各类文件进行访问，重要文件和目录权限均在合理范围内，用户可根据文件不同的权限进行操作。 |
| g）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。 | 执 行more /etc/selinux/config 命令，查看config文件显示 SELINUX参数为 DISABLED，即未开启强制访问控制模式。 |
| 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）执行ps -ef|grep rsyslog和ps -ef|grep auditd命令，显示rsyslog和auditd进程正在运行；2）more /etc/audit/audit.rules，显示审计内容包括：\*.info、authriv.\*、mail.\*、cron.\*、\*.emerg、uucp、news.crit、local7.\*等事件。 |
| 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； | 执行tail -20 /var/log/audit/audit.log命令，查看近20条审计日志，内容包括：时间、对象、路径、用户ID、相关的系统调用、用户执行命令等。 |
| 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）通过访问权限对审计记录进行保护，日志文件/var/log/messages、/var/log/secure、/var/log/audit/audit.log访问 权限均为600；2）审计记录本地保存，且实时备份至360本地安全大脑，保存时间满足180天以上。 |
| d）应对审计进程进行保护，防止未经授权的中断。 | 执行service auditd status命令，系统开启auditd审计保护进程，审计进程由root用户维护，经现场使用yluser用户通过service auditd stop命令尝试中断审计进程，无法将审计进程单独中断。 |
| 入侵防范 | a）应遵循最小安装的原则，仅安装需要的组件和应用程序； | 1）系统安装遵循最小化安装原则；2）执行yum list installed命令查看操作系统已安装的程序包，存在Java、oracle、SSH、天眼云镜agent等应用程序或组件，不存在与业务系统无关的组件和应用程序。 |
| b）应关闭不需要的系统服务、默认共享和高危端口； | 1）执行systemctl list-unit-files 命令，系统已关闭FTP、Telnet 等高危网络服务；2）执行netstat -pantu命令，系统关闭了135、445等高危端口，仅开启了22、1521等端口。 |
| c）应通过设定终端接入方式或网络地址范围对通过网络进行管理的管理终端进行限制； | 经核查，1）通过配置安全组策略限制仅允许通过堡垒机管理服务器；2）经核查防火墙中访问控制策略，具备堡垒机地址-服务器管理网段（10.33.0.0）的访问控制策略。 |
| d）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； | 根据GB∕T 28448-2019 《信息安全技术 网络安全等级保护测评要求》测评对象范围描述，服务器无该项要求，故判为“不适用”。 |
| e）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； | 1）经过漏洞扫描，服务器不存在高危安全漏洞；2）执行rpm -qa grep patch命令，查看系统补丁已更新至最新。 |
| f）应能够检测到对重要节点进行入侵的行为，并在发生严重入侵事件时提供报警。 | 经核查，服务器上安装有青藤云天眼云镜，对主机入侵行为进行检测，发现严重安全事件时通过钉钉告警。 |
| 恶意代码防范 | a）应采用免受恶意代码攻击的技术措施或主动免疫可信验证机制及时识别入侵和病毒行为，并将其有效阻断。 | 经核查，服务器上安装有青藤云天眼云镜，对主机恶意代码进行检测、清除，每天凌晨自动更新恶意代码特征库，经核查，具备恶意代码特征库更新记录。 |
| 可信验证 | a）可基于可信根对计算设备的系统引导程序、系统程序、重要配置参数和应用程序等进行可信验证，并在应用程序的关键执行环节进行动态可信验证，在检测到其可信性受到破坏后进行报警，并将验证结果形成审计记录送至安全管理中心。 | 未采用技术措施对计算设备的系统引导程序、系统程序、重要配置参数和通信应用程序等进行可信验证。 |
| 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； | 采用SSH协议连接操作系统，保证了鉴别信息以及管理数据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。 | 操作系统中对重要鉴别信息通过自身的加密及校验（SHA256），保证数据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； | 采用SSH协议连接操作系统，保证了鉴别信息以及管理数据在传输过程中的保密性。 |
| b）应采用密码技术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个人信息等。 | 通过系统自带的加密模块保证鉴别数据在存储过程中的保密性。 |
| 数据备份恢复 | a）应提供重要数据的本地数据备份与恢复功能； | 经核查，通过脚本每周将配置文件、代码仓库等数据备份至备份服务器中，依据需要验证备份数据的有效性。 |
| b）应提供异地实时备份功能，利用通信网络将重要数据实时备份至备份场地； | 系统无异地备份机制。 |
| c）应提供重要数据处理系统的热冗余，保证系统的高可用性。 | 服务器采用集群方式部署，保证系统的高可用性。 |
| 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； | 操作系统提供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功能。 |
| 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。 | 操作系统提供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的功能。 |

4.1.3.79. 枢纽库集群节点2

|  |  |  |
| --- | --- | --- |
| **安全控制点** | **测评指标** | **结果记录** |
| 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）操作系统时采用用户名+SSHKey公私钥进行身份鉴别鉴别信息具有复杂度要求；2）执行cat /etc/shadow命令，查看shadow文件系统内用户身份标识唯一，不存在同名用户，且不存在空口令账号；3）经访谈，SSHKey公私钥每半年进行更换；4）查看sshd\_config配置文件中配置PasswordAuthentication no，拒绝使用密码方式进行身份鉴别。 |
| 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； | 操作系统采用用户名+SSHKey公私钥进行身份鉴别，可以防止鉴别信息被暴力破解；但未配置用户连接超时退出策略。 |
| 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； | 1）经核查，管理人员采用SSH协议连接操作系统；2）执行netatat –tpln| grep 23命令查看操作系统远程管理端口，不存在Telnet端口，防止鉴别信息在网络传输过程中的被窃听。 |
| 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。 | 未采用两种或两种以上组合的鉴别技术对用户进行身份鉴别。 |
| 访问控制 | a）应对登录的用户分配账户和权限； | 1）经访谈，通过root账户为登录的用户创建账户、分配权限；2）执行ls -l命令查看关键文件权限，均已为账户分配了相应权限，相关文件权限设置为/etc/shadow：000、/etc/passwd：644、/etc/group：644、/etc/profile：644、/etc/crontab：644、/ etc/securetty：600、/etc/ssh/sshd\_config：600。 |
| b）应重命名或删除默认账户，修改默认账户的默认口令； | 1）执行cat /etc/shadow命令查看shadow文件，操作系统中adm、lp、sync、shutdown、halt、mail、uucp、operator、games、gopher等账户均为nologin状态，存在默认账户root；2）执行more /etc/ssh/sshd\_config命令，查看“PermitRootLogin”参数设置为“yes”，即允许root远程登录；3）经访谈，root用户需通过公私钥方式进行身份鉴别。 |
| 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； | 1）执行cat /etc/shadow命令查看shadow文件，发现操作系统存在root、ysup、yops、yluser等在用账户，不存在多余的、过期账户；2）存在多个堡垒机账户登录操作系统时共用一个账户的情况。 |
| 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； | root账户具有系统所有权限，未实现管理用户的权限分离。 |
| e）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； | 经访谈，由系统管理员root配置访问控制策略，如：/etc/passwd，/etc/profile宿主为root、权限设置为644，audit文件为700、message文件为600，其他文件权限为750，实现用户对文件的权限控制。 |
| f）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； | 由管理用户进行用户访问权限分配进行设置，依据访问控制策略,对各类文件进行访问，重要文件和目录权限均在合理范围内，用户可根据文件不同的权限进行操作。 |
| g）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。 | 执 行more /etc/selinux/config 命令，查看config文件显示 SELINUX参数为 DISABLED，即未开启强制访问控制模式。 |
| 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）执行ps -ef|grep rsyslog和ps -ef|grep auditd命令，显示rsyslog和auditd进程正在运行；2）more /etc/audit/audit.rules，显示审计内容包括：\*.info、authriv.\*、mail.\*、cron.\*、\*.emerg、uucp、news.crit、local7.\*等事件。 |
| 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； | 执行tail -20 /var/log/audit/audit.log命令，查看近20条审计日志，内容包括：时间、对象、路径、用户ID、相关的系统调用、用户执行命令等。 |
| 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）通过访问权限对审计记录进行保护，日志文件/var/log/messages、/var/log/secure、/var/log/audit/audit.log访问 权限均为600；2）审计记录本地保存，且实时备份至360本地安全大脑，保存时间满足180天以上。 |
| d）应对审计进程进行保护，防止未经授权的中断。 | 执行service auditd status命令，系统开启auditd审计保护进程，审计进程由root用户维护，经现场使用yluser用户通过service auditd stop命令尝试中断审计进程，无法将审计进程单独中断。 |
| 入侵防范 | a）应遵循最小安装的原则，仅安装需要的组件和应用程序； | 1）系统安装遵循最小化安装原则；2）执行yum list installed命令查看操作系统已安装的程序包，存在Java、oracle、SSH、天眼云镜agent等应用程序或组件，不存在与业务系统无关的组件和应用程序。 |
| b）应关闭不需要的系统服务、默认共享和高危端口； | 1）执行systemctl list-unit-files 命令，系统已关闭FTP、Telnet 等高危网络服务；2）执行netstat -pantu命令，系统关闭了135、445等高危端口，仅开启了22、1521等端口。 |
| c）应通过设定终端接入方式或网络地址范围对通过网络进行管理的管理终端进行限制； | 经核查，1）通过配置安全组策略限制仅允许通过堡垒机管理服务器；2）经核查防火墙中访问控制策略，具备堡垒机地址-服务器管理网段（10.33.0.0）的访问控制策略。 |
| d）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； | 根据GB∕T 28448-2019 《信息安全技术 网络安全等级保护测评要求》测评对象范围描述，服务器无该项要求，故判为“不适用”。 |
| e）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； | 1）经过漏洞扫描，服务器不存在高危安全漏洞；2）执行rpm -qa grep patch命令，查看系统补丁已更新至最新。 |
| f）应能够检测到对重要节点进行入侵的行为，并在发生严重入侵事件时提供报警。 | 经核查，服务器上安装有青藤云天眼云镜，对主机入侵行为进行检测，发现严重安全事件时通过钉钉告警。 |
| 恶意代码防范 | a）应采用免受恶意代码攻击的技术措施或主动免疫可信验证机制及时识别入侵和病毒行为，并将其有效阻断。 | 经核查，服务器上安装有青藤云天眼云镜，对主机恶意代码进行检测、清除，每天凌晨自动更新恶意代码特征库，经核查，具备恶意代码特征库更新记录。 |
| 可信验证 | a）可基于可信根对计算设备的系统引导程序、系统程序、重要配置参数和应用程序等进行可信验证，并在应用程序的关键执行环节进行动态可信验证，在检测到其可信性受到破坏后进行报警，并将验证结果形成审计记录送至安全管理中心。 | 未采用技术措施对计算设备的系统引导程序、系统程序、重要配置参数和通信应用程序等进行可信验证。 |
| 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； | 采用SSH协议连接操作系统，保证了鉴别信息以及管理数据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。 | 操作系统中对重要鉴别信息通过自身的加密及校验（SHA256），保证数据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； | 采用SSH协议连接操作系统，保证了鉴别信息以及管理数据在传输过程中的保密性。 |
| b）应采用密码技术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个人信息等。 | 通过系统自带的加密模块保证鉴别数据在存储过程中的保密性。 |
| 数据备份恢复 | a）应提供重要数据的本地数据备份与恢复功能； | 经核查，通过脚本每周将配置文件、代码仓库等数据备份至备份服务器中，依据需要验证备份数据的有效性。 |
| b）应提供异地实时备份功能，利用通信网络将重要数据实时备份至备份场地； | 系统无异地备份机制。 |
| c）应提供重要数据处理系统的热冗余，保证系统的高可用性。 | 服务器采用集群方式部署，保证系统的高可用性。 |
| 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； | 操作系统提供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功能。 |
| 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。 | 操作系统提供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的功能。 |

4.1.3.80. 枢纽库集群备库

|  |  |  |
| --- | --- | --- |
| **安全控制点** | **测评指标** | **结果记录** |
| 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）操作系统时采用用户名+SSHKey公私钥进行身份鉴别鉴别信息具有复杂度要求；2）执行cat /etc/shadow命令，查看shadow文件系统内用户身份标识唯一，不存在同名用户，且不存在空口令账号；3）经访谈，SSHKey公私钥每半年进行更换；4）查看sshd\_config配置文件中配置PasswordAuthentication no，拒绝使用密码方式进行身份鉴别。 |
| 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； | 操作系统采用用户名+SSHKey公私钥进行身份鉴别，可以防止鉴别信息被暴力破解；但未配置用户连接超时退出策略。 |
| 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； | 1）经核查，管理人员采用SSH协议连接操作系统；2）执行netatat –tpln| grep 23命令查看操作系统远程管理端口，不存在Telnet端口，防止鉴别信息在网络传输过程中的被窃听。 |
| 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。 | 未采用两种或两种以上组合的鉴别技术对用户进行身份鉴别。 |
| 访问控制 | a）应对登录的用户分配账户和权限； | 1）经访谈，通过root账户为登录的用户创建账户、分配权限；2）执行ls -l命令查看关键文件权限，均已为账户分配了相应权限，相关文件权限设置为/etc/shadow：000、/etc/passwd：644、/etc/group：644、/etc/profile：644、/etc/crontab：644、/ etc/securetty：600、/etc/ssh/sshd\_config：600。 |
| b）应重命名或删除默认账户，修改默认账户的默认口令； | 1）执行cat /etc/shadow命令查看shadow文件，操作系统中adm、lp、sync、shutdown、halt、mail、uucp、operator、games、gopher等账户均为nologin状态，存在默认账户root；2）执行more /etc/ssh/sshd\_config命令，查看“PermitRootLogin”参数设置为“yes”，即允许root远程登录；3）经访谈，root用户需通过公私钥方式进行身份鉴别。 |
| 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； | 1）执行cat /etc/shadow命令查看shadow文件，发现操作系统存在root、ysup、yops、yluser等在用账户，不存在多余的、过期账户；2）存在多个堡垒机账户登录操作系统时共用一个账户的情况。 |
| 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； | root账户具有系统所有权限，未实现管理用户的权限分离。 |
| e）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； | 经访谈，由系统管理员root配置访问控制策略，如：/etc/passwd，/etc/profile宿主为root、权限设置为644，audit文件为700、message文件为600，其他文件权限为750，实现用户对文件的权限控制。 |
| f）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； | 由管理用户进行用户访问权限分配进行设置，依据访问控制策略,对各类文件进行访问，重要文件和目录权限均在合理范围内，用户可根据文件不同的权限进行操作。 |
| g）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。 | 执 行more /etc/selinux/config 命令，查看config文件显示 SELINUX参数为 DISABLED，即未开启强制访问控制模式。 |
| 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）执行ps -ef|grep rsyslog和ps -ef|grep auditd命令，显示rsyslog和auditd进程正在运行；2）more /etc/audit/audit.rules，显示审计内容包括：\*.info、authriv.\*、mail.\*、cron.\*、\*.emerg、uucp、news.crit、local7.\*等事件。 |
| 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； | 执行tail -20 /var/log/audit/audit.log命令，查看近20条审计日志，内容包括：时间、对象、路径、用户ID、相关的系统调用、用户执行命令等。 |
| 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）通过访问权限对审计记录进行保护，日志文件/var/log/messages、/var/log/secure、/var/log/audit/audit.log访问 权限均为600；2）审计记录本地保存，且实时备份至360本地安全大脑，保存时间满足180天以上。 |
| d）应对审计进程进行保护，防止未经授权的中断。 | 执行service auditd status命令，系统开启auditd审计保护进程，审计进程由root用户维护，经现场使用yluser用户通过service auditd stop命令尝试中断审计进程，无法将审计进程单独中断。 |
| 入侵防范 | a）应遵循最小安装的原则，仅安装需要的组件和应用程序； | 1）系统安装遵循最小化安装原则；2）执行yum list installed命令查看操作系统已安装的程序包，存在Java、oracle、SSH、天眼云镜agent等应用程序或组件，不存在与业务系统无关的组件和应用程序。 |
| b）应关闭不需要的系统服务、默认共享和高危端口； | 1）执行systemctl list-unit-files 命令，系统已关闭FTP、Telnet 等高危网络服务；2）执行netstat -pantu命令，系统关闭了135、445等高危端口，仅开启了22、1521等端口。 |
| c）应通过设定终端接入方式或网络地址范围对通过网络进行管理的管理终端进行限制； | 经核查，1）通过配置安全组策略限制仅允许通过堡垒机管理服务器；2）经核查防火墙中访问控制策略，具备堡垒机地址-服务器管理网段（10.33.0.0）的访问控制策略。 |
| d）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； | 根据GB∕T 28448-2019 《信息安全技术 网络安全等级保护测评要求》测评对象范围描述，服务器无该项要求，故判为“不适用”。 |
| e）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； | 1）经过漏洞扫描，服务器不存在高危安全漏洞；2）执行rpm -qa grep patch命令，查看系统补丁已更新至最新。 |
| f）应能够检测到对重要节点进行入侵的行为，并在发生严重入侵事件时提供报警。 | 经核查，服务器上安装有青藤云天眼云镜，对主机入侵行为进行检测，发现严重安全事件时通过钉钉告警。 |
| 恶意代码防范 | a）应采用免受恶意代码攻击的技术措施或主动免疫可信验证机制及时识别入侵和病毒行为，并将其有效阻断。 | 经核查，服务器上安装有青藤云天眼云镜，对主机恶意代码进行检测、清除，每天凌晨自动更新恶意代码特征库，经核查，具备恶意代码特征库更新记录。 |
| 可信验证 | a）可基于可信根对计算设备的系统引导程序、系统程序、重要配置参数和应用程序等进行可信验证，并在应用程序的关键执行环节进行动态可信验证，在检测到其可信性受到破坏后进行报警，并将验证结果形成审计记录送至安全管理中心。 | 未采用技术措施对计算设备的系统引导程序、系统程序、重要配置参数和通信应用程序等进行可信验证。 |
| 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； | 采用SSH协议连接操作系统，保证了鉴别信息以及管理数据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。 | 操作系统中对重要鉴别信息通过自身的加密及校验（SHA256），保证数据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； | 采用SSH协议连接操作系统，保证了鉴别信息以及管理数据在传输过程中的保密性。 |
| b）应采用密码技术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个人信息等。 | 通过系统自带的加密模块保证鉴别数据在存储过程中的保密性。 |
| 数据备份恢复 | a）应提供重要数据的本地数据备份与恢复功能； | 经核查，通过脚本每周将配置文件、代码仓库等数据备份至备份服务器中，依据需要验证备份数据的有效性。 |
| b）应提供异地实时备份功能，利用通信网络将重要数据实时备份至备份场地； | 系统无异地备份机制。 |
| c）应提供重要数据处理系统的热冗余，保证系统的高可用性。 | 服务器采用集群方式部署，保证系统的高可用性。 |
| 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； | 操作系统提供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功能。 |
| 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。 | 操作系统提供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的功能。 |

4.1.3.81. 计算库1库

|  |  |  |
| --- | --- | --- |
| **安全控制点** | **测评指标** | **结果记录** |
| 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）操作系统时采用用户名+SSHKey公私钥进行身份鉴别鉴别信息具有复杂度要求；2）执行cat /etc/shadow命令，查看shadow文件系统内用户身份标识唯一，不存在同名用户，且不存在空口令账号；3）经访谈，SSHKey公私钥每半年进行更换；4）查看sshd\_config配置文件中配置PasswordAuthentication no，拒绝使用密码方式进行身份鉴别。 |
| 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； | 操作系统采用用户名+SSHKey公私钥进行身份鉴别，可以防止鉴别信息被暴力破解；但未配置用户连接超时退出策略。 |
| 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； | 1）经核查，管理人员采用SSH协议连接操作系统；2）执行netatat –tpln| grep 23命令查看操作系统远程管理端口，不存在Telnet端口，防止鉴别信息在网络传输过程中的被窃听。 |
| 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。 | 未采用两种或两种以上组合的鉴别技术对用户进行身份鉴别。 |
| 访问控制 | a）应对登录的用户分配账户和权限； | 1）经访谈，通过root账户为登录的用户创建账户、分配权限；2）执行ls -l命令查看关键文件权限，均已为账户分配了相应权限，相关文件权限设置为/etc/shadow：000、/etc/passwd：644、/etc/group：644、/etc/profile：644、/etc/crontab：644、/ etc/securetty：600、/etc/ssh/sshd\_config：600。 |
| b）应重命名或删除默认账户，修改默认账户的默认口令； | 1）执行cat /etc/shadow命令查看shadow文件，操作系统中adm、lp、sync、shutdown、halt、mail、uucp、operator、games、gopher等账户均为nologin状态，存在默认账户root；2）执行more /etc/ssh/sshd\_config命令，查看“PermitRootLogin”参数设置为“yes”，即允许root远程登录；3）经访谈，root用户需通过公私钥方式进行身份鉴别。 |
| 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； | 1）执行cat /etc/shadow命令查看shadow文件，发现操作系统存在root、ysup、yops、yluser等在用账户，不存在多余的、过期账户；2）存在多个堡垒机账户登录操作系统时共用一个账户的情况。 |
| 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； | root账户具有系统所有权限，未实现管理用户的权限分离。 |
| e）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； | 经访谈，由系统管理员root配置访问控制策略，如：/etc/passwd，/etc/profile宿主为root、权限设置为644，audit文件为700、message文件为600，其他文件权限为750，实现用户对文件的权限控制。 |
| f）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； | 由管理用户进行用户访问权限分配进行设置，依据访问控制策略,对各类文件进行访问，重要文件和目录权限均在合理范围内，用户可根据文件不同的权限进行操作。 |
| g）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。 | 执 行more /etc/selinux/config 命令，查看config文件显示 SELINUX参数为 DISABLED，即未开启强制访问控制模式。 |
| 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）执行ps -ef|grep rsyslog和ps -ef|grep auditd命令，显示rsyslog和auditd进程正在运行；2）more /etc/audit/audit.rules，显示审计内容包括：\*.info、authriv.\*、mail.\*、cron.\*、\*.emerg、uucp、news.crit、local7.\*等事件。 |
| 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； | 执行tail -20 /var/log/audit/audit.log命令，查看近20条审计日志，内容包括：时间、对象、路径、用户ID、相关的系统调用、用户执行命令等。 |
| 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）通过访问权限对审计记录进行保护，日志文件/var/log/messages、/var/log/secure、/var/log/audit/audit.log访问 权限均为600；2）审计记录本地保存，且实时备份至360本地安全大脑，保存时间满足180天以上。 |
| d）应对审计进程进行保护，防止未经授权的中断。 | 执行service auditd status命令，系统开启auditd审计保护进程，审计进程由root用户维护，经现场使用yluser用户通过service auditd stop命令尝试中断审计进程，无法将审计进程单独中断。 |
| 入侵防范 | a）应遵循最小安装的原则，仅安装需要的组件和应用程序； | 1）系统安装遵循最小化安装原则；2）执行yum list installed命令查看操作系统已安装的程序包，存在Java、oracle、SSH、天眼云镜agent等应用程序或组件，不存在与业务系统无关的组件和应用程序。 |
| b）应关闭不需要的系统服务、默认共享和高危端口； | 1）执行systemctl list-unit-files 命令，系统已关闭FTP、Telnet 等高危网络服务；2）执行netstat -pantu命令，系统关闭了135、445等高危端口，仅开启了22、1521等端口。 |
| c）应通过设定终端接入方式或网络地址范围对通过网络进行管理的管理终端进行限制； | 经核查，1）通过配置安全组策略限制仅允许通过堡垒机管理服务器；2）经核查防火墙中访问控制策略，具备堡垒机地址-服务器管理网段（10.33.0.0）的访问控制策略。 |
| d）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； | 根据GB∕T 28448-2019 《信息安全技术 网络安全等级保护测评要求》测评对象范围描述，服务器无该项要求，故判为“不适用”。 |
| e）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； | 1）经过漏洞扫描，服务器不存在高危安全漏洞；2）执行rpm -qa grep patch命令，查看系统补丁已更新至最新。 |
| f）应能够检测到对重要节点进行入侵的行为，并在发生严重入侵事件时提供报警。 | 经核查，服务器上安装有青藤云天眼云镜，对主机入侵行为进行检测，发现严重安全事件时通过钉钉告警。 |
| 恶意代码防范 | a）应采用免受恶意代码攻击的技术措施或主动免疫可信验证机制及时识别入侵和病毒行为，并将其有效阻断。 | 经核查，服务器上安装有青藤云天眼云镜，对主机恶意代码进行检测、清除，每天凌晨自动更新恶意代码特征库，经核查，具备恶意代码特征库更新记录。 |
| 可信验证 | a）可基于可信根对计算设备的系统引导程序、系统程序、重要配置参数和应用程序等进行可信验证，并在应用程序的关键执行环节进行动态可信验证，在检测到其可信性受到破坏后进行报警，并将验证结果形成审计记录送至安全管理中心。 | 未采用技术措施对计算设备的系统引导程序、系统程序、重要配置参数和通信应用程序等进行可信验证。 |
| 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； | 采用SSH协议连接操作系统，保证了鉴别信息以及管理数据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。 | 操作系统中对重要鉴别信息通过自身的加密及校验（SHA256），保证数据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； | 采用SSH协议连接操作系统，保证了鉴别信息以及管理数据在传输过程中的保密性。 |
| b）应采用密码技术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个人信息等。 | 通过系统自带的加密模块保证鉴别数据在存储过程中的保密性。 |
| 数据备份恢复 | a）应提供重要数据的本地数据备份与恢复功能； | 经核查，通过脚本每周将配置文件、代码仓库等数据备份至备份服务器中，依据需要验证备份数据的有效性。 |
| b）应提供异地实时备份功能，利用通信网络将重要数据实时备份至备份场地； | 系统无异地备份机制。 |
| c）应提供重要数据处理系统的热冗余，保证系统的高可用性。 | 服务器采用集群方式部署，保证系统的高可用性。 |
| 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； | 操作系统提供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功能。 |
| 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。 | 操作系统提供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的功能。 |

4.1.3.82. 计算库2库

|  |  |  |
| --- | --- | --- |
| **安全控制点** | **测评指标** | **结果记录** |
| 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）操作系统时采用用户名+SSHKey公私钥进行身份鉴别鉴别信息具有复杂度要求；2）执行cat /etc/shadow命令，查看shadow文件系统内用户身份标识唯一，不存在同名用户，且不存在空口令账号；3）经访谈，SSHKey公私钥每半年进行更换；4）查看sshd\_config配置文件中配置PasswordAuthentication no，拒绝使用密码方式进行身份鉴别。 |
| 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； | 操作系统采用用户名+SSHKey公私钥进行身份鉴别，可以防止鉴别信息被暴力破解；但未配置用户连接超时退出策略。 |
| 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； | 1）经核查，管理人员采用SSH协议连接操作系统；2）执行netatat –tpln| grep 23命令查看操作系统远程管理端口，不存在Telnet端口，防止鉴别信息在网络传输过程中的被窃听。 |
| 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。 | 未采用两种或两种以上组合的鉴别技术对用户进行身份鉴别。 |
| 访问控制 | a）应对登录的用户分配账户和权限； | 1）经访谈，通过root账户为登录的用户创建账户、分配权限；2）执行ls -l命令查看关键文件权限，均已为账户分配了相应权限，相关文件权限设置为/etc/shadow：000、/etc/passwd：644、/etc/group：644、/etc/profile：644、/etc/crontab：644、/ etc/securetty：600、/etc/ssh/sshd\_config：600。 |
| b）应重命名或删除默认账户，修改默认账户的默认口令； | 1）执行cat /etc/shadow命令查看shadow文件，操作系统中adm、lp、sync、shutdown、halt、mail、uucp、operator、games、gopher等账户均为nologin状态，存在默认账户root；2）执行more /etc/ssh/sshd\_config命令，查看“PermitRootLogin”参数设置为“yes”，即允许root远程登录；3）经访谈，root用户需通过公私钥方式进行身份鉴别。 |
| 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； | 1）执行cat /etc/shadow命令查看shadow文件，发现操作系统存在root、ysup、yops、yluser等在用账户，不存在多余的、过期账户；2）存在多个堡垒机账户登录操作系统时共用一个账户的情况。 |
| 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； | root账户具有系统所有权限，未实现管理用户的权限分离。 |
| e）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； | 经访谈，由系统管理员root配置访问控制策略，如：/etc/passwd，/etc/profile宿主为root、权限设置为644，audit文件为700、message文件为600，其他文件权限为750，实现用户对文件的权限控制。 |
| f）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； | 由管理用户进行用户访问权限分配进行设置，依据访问控制策略,对各类文件进行访问，重要文件和目录权限均在合理范围内，用户可根据文件不同的权限进行操作。 |
| g）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。 | 执 行more /etc/selinux/config 命令，查看config文件显示 SELINUX参数为 DISABLED，即未开启强制访问控制模式。 |
| 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）执行ps -ef|grep rsyslog和ps -ef|grep auditd命令，显示rsyslog和auditd进程正在运行；2）more /etc/audit/audit.rules，显示审计内容包括：\*.info、authriv.\*、mail.\*、cron.\*、\*.emerg、uucp、news.crit、local7.\*等事件。 |
| 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； | 执行tail -20 /var/log/audit/audit.log命令，查看近20条审计日志，内容包括：时间、对象、路径、用户ID、相关的系统调用、用户执行命令等。 |
| 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）通过访问权限对审计记录进行保护，日志文件/var/log/messages、/var/log/secure、/var/log/audit/audit.log访问 权限均为600；2）审计记录本地保存，且实时备份至360本地安全大脑，保存时间满足180天以上。 |
| d）应对审计进程进行保护，防止未经授权的中断。 | 执行service auditd status命令，系统开启auditd审计保护进程，审计进程由root用户维护，经现场使用yluser用户通过service auditd stop命令尝试中断审计进程，无法将审计进程单独中断。 |
| 入侵防范 | a）应遵循最小安装的原则，仅安装需要的组件和应用程序； | 1）系统安装遵循最小化安装原则；2）执行yum list installed命令查看操作系统已安装的程序包，存在Java、oracle、SSH、天眼云镜agent等应用程序或组件，不存在与业务系统无关的组件和应用程序。 |
| b）应关闭不需要的系统服务、默认共享和高危端口； | 1）执行systemctl list-unit-files 命令，系统已关闭FTP、Telnet 等高危网络服务；2）执行netstat -pantu命令，系统关闭了135、445等高危端口，仅开启了22、1521等端口。 |
| c）应通过设定终端接入方式或网络地址范围对通过网络进行管理的管理终端进行限制； | 经核查，1）通过配置安全组策略限制仅允许通过堡垒机管理服务器；2）经核查防火墙中访问控制策略，具备堡垒机地址-服务器管理网段（10.33.0.0）的访问控制策略。 |
| d）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； | 根据GB∕T 28448-2019 《信息安全技术 网络安全等级保护测评要求》测评对象范围描述，服务器无该项要求，故判为“不适用”。 |
| e）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； | 1）经过漏洞扫描，服务器不存在高危安全漏洞；2）执行rpm -qa grep patch命令，查看系统补丁已更新至最新。 |
| f）应能够检测到对重要节点进行入侵的行为，并在发生严重入侵事件时提供报警。 | 经核查，服务器上安装有青藤云天眼云镜，对主机入侵行为进行检测，发现严重安全事件时通过钉钉告警。 |
| 恶意代码防范 | a）应采用免受恶意代码攻击的技术措施或主动免疫可信验证机制及时识别入侵和病毒行为，并将其有效阻断。 | 经核查，服务器上安装有青藤云天眼云镜，对主机恶意代码进行检测、清除，每天凌晨自动更新恶意代码特征库，经核查，具备恶意代码特征库更新记录。 |
| 可信验证 | a）可基于可信根对计算设备的系统引导程序、系统程序、重要配置参数和应用程序等进行可信验证，并在应用程序的关键执行环节进行动态可信验证，在检测到其可信性受到破坏后进行报警，并将验证结果形成审计记录送至安全管理中心。 | 未采用技术措施对计算设备的系统引导程序、系统程序、重要配置参数和通信应用程序等进行可信验证。 |
| 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； | 采用SSH协议连接操作系统，保证了鉴别信息以及管理数据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。 | 操作系统中对重要鉴别信息通过自身的加密及校验（SHA256），保证数据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； | 采用SSH协议连接操作系统，保证了鉴别信息以及管理数据在传输过程中的保密性。 |
| b）应采用密码技术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个人信息等。 | 通过系统自带的加密模块保证鉴别数据在存储过程中的保密性。 |
| 数据备份恢复 | a）应提供重要数据的本地数据备份与恢复功能； | 经核查，通过脚本每周将配置文件、代码仓库等数据备份至备份服务器中，依据需要验证备份数据的有效性。 |
| b）应提供异地实时备份功能，利用通信网络将重要数据实时备份至备份场地； | 系统无异地备份机制。 |
| c）应提供重要数据处理系统的热冗余，保证系统的高可用性。 | 服务器采用集群方式部署，保证系统的高可用性。 |
| 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； | 操作系统提供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功能。 |
| 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。 | 操作系统提供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的功能。 |

4.1.3.83. 对外轨迹查询备库2

|  |  |  |
| --- | --- | --- |
| **安全控制点** | **测评指标** | **结果记录** |
| 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）操作系统时采用用户名+SSHKey公私钥进行身份鉴别鉴别信息具有复杂度要求；2）执行cat /etc/shadow命令，查看shadow文件系统内用户身份标识唯一，不存在同名用户，且不存在空口令账号；3）经访谈，SSHKey公私钥每半年进行更换；4）查看sshd\_config配置文件中配置PasswordAuthentication no，拒绝使用密码方式进行身份鉴别。 |
| 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； | 操作系统采用用户名+SSHKey公私钥进行身份鉴别，可以防止鉴别信息被暴力破解；但未配置用户连接超时退出策略。 |
| 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； | 1）经核查，管理人员采用SSH协议连接操作系统；2）执行netatat –tpln| grep 23命令查看操作系统远程管理端口，不存在Telnet端口，防止鉴别信息在网络传输过程中的被窃听。 |
| 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。 | 未采用两种或两种以上组合的鉴别技术对用户进行身份鉴别。 |
| 访问控制 | a）应对登录的用户分配账户和权限； | 1）经访谈，通过root账户为登录的用户创建账户、分配权限；2）执行ls -l命令查看关键文件权限，均已为账户分配了相应权限，相关文件权限设置为/etc/shadow：000、/etc/passwd：644、/etc/group：644、/etc/profile：644、/etc/crontab：644、/ etc/securetty：600、/etc/ssh/sshd\_config：600。 |
| b）应重命名或删除默认账户，修改默认账户的默认口令； | 1）执行cat /etc/shadow命令查看shadow文件，操作系统中adm、lp、sync、shutdown、halt、mail、uucp、operator、games、gopher等账户均为nologin状态，存在默认账户root；2）执行more /etc/ssh/sshd\_config命令，查看“PermitRootLogin”参数设置为“yes”，即允许root远程登录；3）经访谈，root用户需通过公私钥方式进行身份鉴别。 |
| 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； | 1）执行cat /etc/shadow命令查看shadow文件，发现操作系统存在root、ysup、yops、yluser等在用账户，不存在多余的、过期账户；2）存在多个堡垒机账户登录操作系统时共用一个账户的情况。 |
| 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； | root账户具有系统所有权限，未实现管理用户的权限分离。 |
| e）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； | 经访谈，由系统管理员root配置访问控制策略，如：/etc/passwd，/etc/profile宿主为root、权限设置为644，audit文件为700、message文件为600，其他文件权限为750，实现用户对文件的权限控制。 |
| f）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； | 由管理用户进行用户访问权限分配进行设置，依据访问控制策略,对各类文件进行访问，重要文件和目录权限均在合理范围内，用户可根据文件不同的权限进行操作。 |
| g）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。 | 执 行more /etc/selinux/config 命令，查看config文件显示 SELINUX参数为 DISABLED，即未开启强制访问控制模式。 |
| 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）执行ps -ef|grep rsyslog和ps -ef|grep auditd命令，显示rsyslog和auditd进程正在运行；2）more /etc/audit/audit.rules，显示审计内容包括：\*.info、authriv.\*、mail.\*、cron.\*、\*.emerg、uucp、news.crit、local7.\*等事件。 |
| 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； | 执行tail -20 /var/log/audit/audit.log命令，查看近20条审计日志，内容包括：时间、对象、路径、用户ID、相关的系统调用、用户执行命令等。 |
| 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）通过访问权限对审计记录进行保护，日志文件/var/log/messages、/var/log/secure、/var/log/audit/audit.log访问 权限均为600；2）审计记录本地保存，且实时备份至360本地安全大脑，保存时间满足180天以上。 |
| d）应对审计进程进行保护，防止未经授权的中断。 | 执行service auditd status命令，系统开启auditd审计保护进程，审计进程由root用户维护，经现场使用yluser用户通过service auditd stop命令尝试中断审计进程，无法将审计进程单独中断。 |
| 入侵防范 | a）应遵循最小安装的原则，仅安装需要的组件和应用程序； | 1）系统安装遵循最小化安装原则；2）执行yum list installed命令查看操作系统已安装的程序包，存在Java、oracle、SSH、天眼云镜agent等应用程序或组件，不存在与业务系统无关的组件和应用程序。 |
| b）应关闭不需要的系统服务、默认共享和高危端口； | 1）执行systemctl list-unit-files 命令，系统已关闭FTP、Telnet 等高危网络服务；2）执行netstat -pantu命令，系统关闭了135、445等高危端口，仅开启了22、1521等端口。 |
| c）应通过设定终端接入方式或网络地址范围对通过网络进行管理的管理终端进行限制； | 经核查，1）通过配置安全组策略限制仅允许通过堡垒机管理服务器；2）经核查防火墙中访问控制策略，具备堡垒机地址-服务器管理网段（10.33.0.0）的访问控制策略。 |
| d）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； | 根据GB∕T 28448-2019 《信息安全技术 网络安全等级保护测评要求》测评对象范围描述，服务器无该项要求，故判为“不适用”。 |
| e）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； | 1）经过漏洞扫描，服务器不存在高危安全漏洞；2）执行rpm -qa grep patch命令，查看系统补丁已更新至最新。 |
| f）应能够检测到对重要节点进行入侵的行为，并在发生严重入侵事件时提供报警。 | 经核查，服务器上安装有青藤云天眼云镜，对主机入侵行为进行检测，发现严重安全事件时通过钉钉告警。 |
| 恶意代码防范 | a）应采用免受恶意代码攻击的技术措施或主动免疫可信验证机制及时识别入侵和病毒行为，并将其有效阻断。 | 经核查，服务器上安装有青藤云天眼云镜，对主机恶意代码进行检测、清除，每天凌晨自动更新恶意代码特征库，经核查，具备恶意代码特征库更新记录。 |
| 可信验证 | a）可基于可信根对计算设备的系统引导程序、系统程序、重要配置参数和应用程序等进行可信验证，并在应用程序的关键执行环节进行动态可信验证，在检测到其可信性受到破坏后进行报警，并将验证结果形成审计记录送至安全管理中心。 | 未采用技术措施对计算设备的系统引导程序、系统程序、重要配置参数和通信应用程序等进行可信验证。 |
| 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； | 采用SSH协议连接操作系统，保证了鉴别信息以及管理数据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。 | 操作系统中对重要鉴别信息通过自身的加密及校验（SHA256），保证数据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； | 采用SSH协议连接操作系统，保证了鉴别信息以及管理数据在传输过程中的保密性。 |
| b）应采用密码技术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个人信息等。 | 通过系统自带的加密模块保证鉴别数据在存储过程中的保密性。 |
| 数据备份恢复 | a）应提供重要数据的本地数据备份与恢复功能； | 经核查，通过脚本每周将配置文件、代码仓库等数据备份至备份服务器中，依据需要验证备份数据的有效性。 |
| b）应提供异地实时备份功能，利用通信网络将重要数据实时备份至备份场地； | 系统无异地备份机制。 |
| c）应提供重要数据处理系统的热冗余，保证系统的高可用性。 | 服务器采用集群方式部署，保证系统的高可用性。 |
| 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； | 操作系统提供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功能。 |
| 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。 | 操作系统提供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的功能。 |

4.1.3.84. 推送2库

|  |  |  |
| --- | --- | --- |
| **安全控制点** | **测评指标** | **结果记录** |
| 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）操作系统时采用用户名+SSHKey公私钥进行身份鉴别鉴别信息具有复杂度要求；2）执行cat /etc/shadow命令，查看shadow文件系统内用户身份标识唯一，不存在同名用户，且不存在空口令账号；3）经访谈，SSHKey公私钥每半年进行更换；4）查看sshd\_config配置文件中配置PasswordAuthentication no，拒绝使用密码方式进行身份鉴别。 |
| 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； | 操作系统采用用户名+SSHKey公私钥进行身份鉴别，可以防止鉴别信息被暴力破解；但未配置用户连接超时退出策略。 |
| 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； | 1）经核查，管理人员采用SSH协议连接操作系统；2）执行netatat –tpln| grep 23命令查看操作系统远程管理端口，不存在Telnet端口，防止鉴别信息在网络传输过程中的被窃听。 |
| 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。 | 未采用两种或两种以上组合的鉴别技术对用户进行身份鉴别。 |
| 访问控制 | a）应对登录的用户分配账户和权限； | 1）经访谈，通过root账户为登录的用户创建账户、分配权限；2）执行ls -l命令查看关键文件权限，均已为账户分配了相应权限，相关文件权限设置为/etc/shadow：000、/etc/passwd：644、/etc/group：644、/etc/profile：644、/etc/crontab：644、/ etc/securetty：600、/etc/ssh/sshd\_config：600。 |
| b）应重命名或删除默认账户，修改默认账户的默认口令； | 1）执行cat /etc/shadow命令查看shadow文件，操作系统中adm、lp、sync、shutdown、halt、mail、uucp、operator、games、gopher等账户均为nologin状态，存在默认账户root；2）执行more /etc/ssh/sshd\_config命令，查看“PermitRootLogin”参数设置为“yes”，即允许root远程登录；3）经访谈，root用户需通过公私钥方式进行身份鉴别。 |
| 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； | 1）执行cat /etc/shadow命令查看shadow文件，发现操作系统存在root、ysup、yops、yluser等在用账户，不存在多余的、过期账户；2）存在多个堡垒机账户登录操作系统时共用一个账户的情况。 |
| 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； | root账户具有系统所有权限，未实现管理用户的权限分离。 |
| e）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； | 经访谈，由系统管理员root配置访问控制策略，如：/etc/passwd，/etc/profile宿主为root、权限设置为644，audit文件为700、message文件为600，其他文件权限为750，实现用户对文件的权限控制。 |
| f）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； | 由管理用户进行用户访问权限分配进行设置，依据访问控制策略,对各类文件进行访问，重要文件和目录权限均在合理范围内，用户可根据文件不同的权限进行操作。 |
| g）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。 | 执 行more /etc/selinux/config 命令，查看config文件显示 SELINUX参数为 DISABLED，即未开启强制访问控制模式。 |
| 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）执行ps -ef|grep rsyslog和ps -ef|grep auditd命令，显示rsyslog和auditd进程正在运行；2）more /etc/audit/audit.rules，显示审计内容包括：\*.info、authriv.\*、mail.\*、cron.\*、\*.emerg、uucp、news.crit、local7.\*等事件。 |
| 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； | 执行tail -20 /var/log/audit/audit.log命令，查看近20条审计日志，内容包括：时间、对象、路径、用户ID、相关的系统调用、用户执行命令等。 |
| 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）通过访问权限对审计记录进行保护，日志文件/var/log/messages、/var/log/secure、/var/log/audit/audit.log访问 权限均为600；2）审计记录本地保存，且实时备份至360本地安全大脑，保存时间满足180天以上。 |
| d）应对审计进程进行保护，防止未经授权的中断。 | 执行service auditd status命令，系统开启auditd审计保护进程，审计进程由root用户维护，经现场使用yluser用户通过service auditd stop命令尝试中断审计进程，无法将审计进程单独中断。 |
| 入侵防范 | a）应遵循最小安装的原则，仅安装需要的组件和应用程序； | 1）系统安装遵循最小化安装原则；2）执行yum list installed命令查看操作系统已安装的程序包，存在Java、oracle、SSH、天眼云镜agent等应用程序或组件，不存在与业务系统无关的组件和应用程序。 |
| b）应关闭不需要的系统服务、默认共享和高危端口； | 1）执行systemctl list-unit-files 命令，系统已关闭FTP、Telnet 等高危网络服务；2）执行netstat -pantu命令，系统关闭了135、445等高危端口，仅开启了22、1521等端口。 |
| c）应通过设定终端接入方式或网络地址范围对通过网络进行管理的管理终端进行限制； | 经核查，1）通过配置安全组策略限制仅允许通过堡垒机管理服务器；2）经核查防火墙中访问控制策略，具备堡垒机地址-服务器管理网段（10.33.0.0）的访问控制策略。 |
| d）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； | 根据GB∕T 28448-2019 《信息安全技术 网络安全等级保护测评要求》测评对象范围描述，服务器无该项要求，故判为“不适用”。 |
| e）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； | 1）经过漏洞扫描，服务器不存在高危安全漏洞；2）执行rpm -qa grep patch命令，查看系统补丁已更新至最新。 |
| f）应能够检测到对重要节点进行入侵的行为，并在发生严重入侵事件时提供报警。 | 经核查，服务器上安装有青藤云天眼云镜，对主机入侵行为进行检测，发现严重安全事件时通过钉钉告警。 |
| 恶意代码防范 | a）应采用免受恶意代码攻击的技术措施或主动免疫可信验证机制及时识别入侵和病毒行为，并将其有效阻断。 | 经核查，服务器上安装有青藤云天眼云镜，对主机恶意代码进行检测、清除，每天凌晨自动更新恶意代码特征库，经核查，具备恶意代码特征库更新记录。 |
| 可信验证 | a）可基于可信根对计算设备的系统引导程序、系统程序、重要配置参数和应用程序等进行可信验证，并在应用程序的关键执行环节进行动态可信验证，在检测到其可信性受到破坏后进行报警，并将验证结果形成审计记录送至安全管理中心。 | 未采用技术措施对计算设备的系统引导程序、系统程序、重要配置参数和通信应用程序等进行可信验证。 |
| 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； | 采用SSH协议连接操作系统，保证了鉴别信息以及管理数据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。 | 操作系统中对重要鉴别信息通过自身的加密及校验（SHA256），保证数据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； | 采用SSH协议连接操作系统，保证了鉴别信息以及管理数据在传输过程中的保密性。 |
| b）应采用密码技术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个人信息等。 | 通过系统自带的加密模块保证鉴别数据在存储过程中的保密性。 |
| 数据备份恢复 | a）应提供重要数据的本地数据备份与恢复功能； | 经核查，通过脚本每周将配置文件、代码仓库等数据备份至备份服务器中，依据需要验证备份数据的有效性。 |
| b）应提供异地实时备份功能，利用通信网络将重要数据实时备份至备份场地； | 系统无异地备份机制。 |
| c）应提供重要数据处理系统的热冗余，保证系统的高可用性。 | 服务器采用集群方式部署，保证系统的高可用性。 |
| 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； | 操作系统提供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功能。 |
| 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。 | 操作系统提供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的功能。 |

4.1.3.85. bigdata01

|  |  |  |
| --- | --- | --- |
| **安全控制点** | **测评指标** | **结果记录** |
| 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）操作系统时采用用户名+SSHKey公私钥进行身份鉴别鉴别信息具有复杂度要求；2）执行cat /etc/shadow命令，查看shadow文件系统内用户身份标识唯一，不存在同名用户，且不存在空口令账号；3）经访谈，SSHKey公私钥每半年进行更换；4）查看sshd\_config配置文件中配置PasswordAuthentication no，拒绝使用密码方式进行身份鉴别。 |
| 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； | 操作系统采用用户名+SSHKey公私钥进行身份鉴别，可以防止鉴别信息被暴力破解；但未配置用户连接超时退出策略。 |
| 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； | 1）经核查，管理人员采用SSH协议连接操作系统；2）执行netatat –tpln| grep 23命令查看操作系统远程管理端口，不存在Telnet端口，防止鉴别信息在网络传输过程中的被窃听。 |
| 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。 | 未采用两种或两种以上组合的鉴别技术对用户进行身份鉴别。 |
| 访问控制 | a）应对登录的用户分配账户和权限； | 1）经访谈，通过root账户为登录的用户创建账户、分配权限；2）执行ls -l命令查看关键文件权限，均已为账户分配了相应权限，相关文件权限设置为/etc/shadow：000、/etc/passwd：644、/etc/group：644、/etc/profile：644、/etc/crontab：644、/ etc/securetty：600、/etc/ssh/sshd\_config：600。 |
| b）应重命名或删除默认账户，修改默认账户的默认口令； | 1）执行cat /etc/shadow命令查看shadow文件，操作系统中adm、lp、sync、shutdown、halt、mail、uucp、operator、games、gopher等账户均为nologin状态，存在默认账户root；2）执行more /etc/ssh/sshd\_config命令，查看“PermitRootLogin”参数设置为“yes”，即允许root远程登录；3）经访谈，root用户需通过公私钥方式进行身份鉴别。 |
| 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； | 1）执行cat /etc/shadow命令查看shadow文件，发现操作系统存在root、ysup、yops、yluser等在用账户，不存在多余的、过期账户；2）存在多个堡垒机账户登录操作系统时共用一个账户的情况。 |
| 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； | root账户具有系统所有权限，未实现管理用户的权限分离。 |
| e）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； | 经访谈，由系统管理员root配置访问控制策略，如：/etc/passwd，/etc/profile宿主为root、权限设置为644，audit文件为700、message文件为600，其他文件权限为750，实现用户对文件的权限控制。 |
| f）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； | 由管理用户进行用户访问权限分配进行设置，依据访问控制策略,对各类文件进行访问，重要文件和目录权限均在合理范围内，用户可根据文件不同的权限进行操作。 |
| g）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。 | 执 行more /etc/selinux/config 命令，查看config文件显示 SELINUX参数为 DISABLED，即未开启强制访问控制模式。 |
| 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）执行ps -ef|grep rsyslog和ps -ef|grep auditd命令，显示rsyslog和auditd进程正在运行；2）more /etc/audit/audit.rules，显示审计内容包括：\*.info、authriv.\*、mail.\*、cron.\*、\*.emerg、uucp、news.crit、local7.\*等事件。 |
| 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； | 执行tail -20 /var/log/audit/audit.log命令，查看近20条审计日志，内容包括：时间、对象、路径、用户ID、相关的系统调用、用户执行命令等。 |
| 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）通过访问权限对审计记录进行保护，日志文件/var/log/messages、/var/log/secure、/var/log/audit/audit.log访问 权限均为600；2）审计记录本地保存，且实时备份至360本地安全大脑，保存时间满足180天以上。 |
| d）应对审计进程进行保护，防止未经授权的中断。 | 执行service auditd status命令，系统开启auditd审计保护进程，审计进程由root用户维护，经现场使用yluser用户通过service auditd stop命令尝试中断审计进程，无法将审计进程单独中断。 |
| 入侵防范 | a）应遵循最小安装的原则，仅安装需要的组件和应用程序； | 1）系统安装遵循最小化安装原则；2）执行yum list installed命令查看操作系统已安装的程序包，存在Java、oracle、SSH、天眼云镜agent等应用程序或组件，不存在与业务系统无关的组件和应用程序。 |
| b）应关闭不需要的系统服务、默认共享和高危端口； | 1）执行systemctl list-unit-files 命令，系统已关闭FTP、Telnet 等高危网络服务；2）执行netstat -pantu命令，系统关闭了135、445等高危端口，仅开启了22、1521等端口。 |
| c）应通过设定终端接入方式或网络地址范围对通过网络进行管理的管理终端进行限制； | 经核查，1）通过配置安全组策略限制仅允许通过堡垒机管理服务器；2）经核查防火墙中访问控制策略，具备堡垒机地址-服务器管理网段（10.33.0.0）的访问控制策略。 |
| d）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； | 根据GB∕T 28448-2019 《信息安全技术 网络安全等级保护测评要求》测评对象范围描述，服务器无该项要求，故判为“不适用”。 |
| e）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； | 1）经过漏洞扫描，服务器不存在高危安全漏洞；2）执行rpm -qa grep patch命令，查看系统补丁已更新至最新。 |
| f）应能够检测到对重要节点进行入侵的行为，并在发生严重入侵事件时提供报警。 | 经核查，服务器上安装有青藤云天眼云镜，对主机入侵行为进行检测，发现严重安全事件时通过钉钉告警。 |
| 恶意代码防范 | a）应采用免受恶意代码攻击的技术措施或主动免疫可信验证机制及时识别入侵和病毒行为，并将其有效阻断。 | 经核查，服务器上安装有青藤云天眼云镜，对主机恶意代码进行检测、清除，每天凌晨自动更新恶意代码特征库，经核查，具备恶意代码特征库更新记录。 |
| 可信验证 | a）可基于可信根对计算设备的系统引导程序、系统程序、重要配置参数和应用程序等进行可信验证，并在应用程序的关键执行环节进行动态可信验证，在检测到其可信性受到破坏后进行报警，并将验证结果形成审计记录送至安全管理中心。 | 未采用技术措施对计算设备的系统引导程序、系统程序、重要配置参数和通信应用程序等进行可信验证。 |
| 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； | 采用SSH协议连接操作系统，保证了鉴别信息以及管理数据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。 | 操作系统中对重要鉴别信息通过自身的加密及校验（SHA256），保证数据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； | 采用SSH协议连接操作系统，保证了鉴别信息以及管理数据在传输过程中的保密性。 |
| b）应采用密码技术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个人信息等。 | 通过系统自带的加密模块保证鉴别数据在存储过程中的保密性。 |
| 数据备份恢复 | a）应提供重要数据的本地数据备份与恢复功能； | 经核查，通过脚本每周将配置文件、代码仓库等数据备份至备份服务器中，依据需要验证备份数据的有效性。 |
| b）应提供异地实时备份功能，利用通信网络将重要数据实时备份至备份场地； | 系统无异地备份机制。 |
| c）应提供重要数据处理系统的热冗余，保证系统的高可用性。 | 服务器采用集群方式部署，保证系统的高可用性。 |
| 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； | 操作系统提供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功能。 |
| 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。 | 操作系统提供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的功能。 |

4.1.3.86. 查询库23备库

|  |  |  |
| --- | --- | --- |
| **安全控制点** | **测评指标** | **结果记录** |
| 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）操作系统时采用用户名+SSHKey公私钥进行身份鉴别鉴别信息具有复杂度要求；2）执行cat /etc/shadow命令，查看shadow文件系统内用户身份标识唯一，不存在同名用户，且不存在空口令账号；3）经访谈，SSHKey公私钥每半年进行更换；4）查看sshd\_config配置文件中配置PasswordAuthentication no，拒绝使用密码方式进行身份鉴别。 |
| 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； | 操作系统采用用户名+SSHKey公私钥进行身份鉴别，可以防止鉴别信息被暴力破解；但未配置用户连接超时退出策略。 |
| 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； | 1）经核查，管理人员采用SSH协议连接操作系统；2）执行netatat –tpln| grep 23命令查看操作系统远程管理端口，不存在Telnet端口，防止鉴别信息在网络传输过程中的被窃听。 |
| 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。 | 未采用两种或两种以上组合的鉴别技术对用户进行身份鉴别。 |
| 访问控制 | a）应对登录的用户分配账户和权限； | 1）经访谈，通过root账户为登录的用户创建账户、分配权限；2）执行ls -l命令查看关键文件权限，均已为账户分配了相应权限，相关文件权限设置为/etc/shadow：000、/etc/passwd：644、/etc/group：644、/etc/profile：644、/etc/crontab：644、/ etc/securetty：600、/etc/ssh/sshd\_config：600。 |
| b）应重命名或删除默认账户，修改默认账户的默认口令； | 1）执行cat /etc/shadow命令查看shadow文件，操作系统中adm、lp、sync、shutdown、halt、mail、uucp、operator、games、gopher等账户均为nologin状态，存在默认账户root；2）执行more /etc/ssh/sshd\_config命令，查看“PermitRootLogin”参数设置为“yes”，即允许root远程登录；3）经访谈，root用户需通过公私钥方式进行身份鉴别。 |
| 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； | 1）执行cat /etc/shadow命令查看shadow文件，发现操作系统存在root、ysup、yops、yluser等在用账户，不存在多余的、过期账户；2）存在多个堡垒机账户登录操作系统时共用一个账户的情况。 |
| 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； | root账户具有系统所有权限，未实现管理用户的权限分离。 |
| e）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； | 经访谈，由系统管理员root配置访问控制策略，如：/etc/passwd，/etc/profile宿主为root、权限设置为644，audit文件为700、message文件为600，其他文件权限为750，实现用户对文件的权限控制。 |
| f）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； | 由管理用户进行用户访问权限分配进行设置，依据访问控制策略,对各类文件进行访问，重要文件和目录权限均在合理范围内，用户可根据文件不同的权限进行操作。 |
| g）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。 | 执 行more /etc/selinux/config 命令，查看config文件显示 SELINUX参数为 DISABLED，即未开启强制访问控制模式。 |
| 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）执行ps -ef|grep rsyslog和ps -ef|grep auditd命令，显示rsyslog和auditd进程正在运行；2）more /etc/audit/audit.rules，显示审计内容包括：\*.info、authriv.\*、mail.\*、cron.\*、\*.emerg、uucp、news.crit、local7.\*等事件。 |
| 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； | 执行tail -20 /var/log/audit/audit.log命令，查看近20条审计日志，内容包括：时间、对象、路径、用户ID、相关的系统调用、用户执行命令等。 |
| 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）通过访问权限对审计记录进行保护，日志文件/var/log/messages、/var/log/secure、/var/log/audit/audit.log访问 权限均为600；2）审计记录本地保存，且实时备份至360本地安全大脑，保存时间满足180天以上。 |
| d）应对审计进程进行保护，防止未经授权的中断。 | 执行service auditd status命令，系统开启auditd审计保护进程，审计进程由root用户维护，经现场使用yluser用户通过service auditd stop命令尝试中断审计进程，无法将审计进程单独中断。 |
| 入侵防范 | a）应遵循最小安装的原则，仅安装需要的组件和应用程序； | 1）系统安装遵循最小化安装原则；2）执行yum list installed命令查看操作系统已安装的程序包，存在Java、oracle、SSH、天眼云镜agent等应用程序或组件，不存在与业务系统无关的组件和应用程序。 |
| b）应关闭不需要的系统服务、默认共享和高危端口； | 1）执行systemctl list-unit-files 命令，系统已关闭FTP、Telnet 等高危网络服务；2）执行netstat -pantu命令，系统关闭了135、445等高危端口，仅开启了22、1521等端口。 |
| c）应通过设定终端接入方式或网络地址范围对通过网络进行管理的管理终端进行限制； | 经核查，1）通过配置安全组策略限制仅允许通过堡垒机管理服务器；2）经核查防火墙中访问控制策略，具备堡垒机地址-服务器管理网段（10.33.0.0）的访问控制策略。 |
| d）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； | 根据GB∕T 28448-2019 《信息安全技术 网络安全等级保护测评要求》测评对象范围描述，服务器无该项要求，故判为“不适用”。 |
| e）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； | 1）经过漏洞扫描，服务器不存在高危安全漏洞；2）执行rpm -qa grep patch命令，查看系统补丁已更新至最新。 |
| f）应能够检测到对重要节点进行入侵的行为，并在发生严重入侵事件时提供报警。 | 经核查，服务器上安装有青藤云天眼云镜，对主机入侵行为进行检测，发现严重安全事件时通过钉钉告警。 |
| 恶意代码防范 | a）应采用免受恶意代码攻击的技术措施或主动免疫可信验证机制及时识别入侵和病毒行为，并将其有效阻断。 | 经核查，服务器上安装有青藤云天眼云镜，对主机恶意代码进行检测、清除，每天凌晨自动更新恶意代码特征库，经核查，具备恶意代码特征库更新记录。 |
| 可信验证 | a）可基于可信根对计算设备的系统引导程序、系统程序、重要配置参数和应用程序等进行可信验证，并在应用程序的关键执行环节进行动态可信验证，在检测到其可信性受到破坏后进行报警，并将验证结果形成审计记录送至安全管理中心。 | 未采用技术措施对计算设备的系统引导程序、系统程序、重要配置参数和通信应用程序等进行可信验证。 |
| 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； | 采用SSH协议连接操作系统，保证了鉴别信息以及管理数据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。 | 操作系统中对重要鉴别信息通过自身的加密及校验（SHA256），保证数据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； | 采用SSH协议连接操作系统，保证了鉴别信息以及管理数据在传输过程中的保密性。 |
| b）应采用密码技术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个人信息等。 | 通过系统自带的加密模块保证鉴别数据在存储过程中的保密性。 |
| 数据备份恢复 | a）应提供重要数据的本地数据备份与恢复功能； | 经核查，通过脚本每周将配置文件、代码仓库等数据备份至备份服务器中，依据需要验证备份数据的有效性。 |
| b）应提供异地实时备份功能，利用通信网络将重要数据实时备份至备份场地； | 系统无异地备份机制。 |
| c）应提供重要数据处理系统的热冗余，保证系统的高可用性。 | 服务器采用集群方式部署，保证系统的高可用性。 |
| 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； | 操作系统提供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功能。 |
| 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。 | 操作系统提供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的功能。 |

4.1.3.87. 查询库24主库

|  |  |  |
| --- | --- | --- |
| **安全控制点** | **测评指标** | **结果记录** |
| 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）操作系统时采用用户名+SSHKey公私钥进行身份鉴别鉴别信息具有复杂度要求；2）执行cat /etc/shadow命令，查看shadow文件系统内用户身份标识唯一，不存在同名用户，且不存在空口令账号；3）经访谈，SSHKey公私钥每半年进行更换；4）查看sshd\_config配置文件中配置PasswordAuthentication no，拒绝使用密码方式进行身份鉴别。 |
| 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； | 操作系统采用用户名+SSHKey公私钥进行身份鉴别，可以防止鉴别信息被暴力破解；但未配置用户连接超时退出策略。 |
| 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； | 1）经核查，管理人员采用SSH协议连接操作系统；2）执行netatat –tpln| grep 23命令查看操作系统远程管理端口，不存在Telnet端口，防止鉴别信息在网络传输过程中的被窃听。 |
| 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。 | 未采用两种或两种以上组合的鉴别技术对用户进行身份鉴别。 |
| 访问控制 | a）应对登录的用户分配账户和权限； | 1）经访谈，通过root账户为登录的用户创建账户、分配权限；2）执行ls -l命令查看关键文件权限，均已为账户分配了相应权限，相关文件权限设置为/etc/shadow：000、/etc/passwd：644、/etc/group：644、/etc/profile：644、/etc/crontab：644、/ etc/securetty：600、/etc/ssh/sshd\_config：600。 |
| b）应重命名或删除默认账户，修改默认账户的默认口令； | 1）执行cat /etc/shadow命令查看shadow文件，操作系统中adm、lp、sync、shutdown、halt、mail、uucp、operator、games、gopher等账户均为nologin状态，存在默认账户root；2）执行more /etc/ssh/sshd\_config命令，查看“PermitRootLogin”参数设置为“yes”，即允许root远程登录；3）经访谈，root用户需通过公私钥方式进行身份鉴别。 |
| 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； | 1）执行cat /etc/shadow命令查看shadow文件，发现操作系统存在root、ysup、yops、yluser等在用账户，不存在多余的、过期账户；2）存在多个堡垒机账户登录操作系统时共用一个账户的情况。 |
| 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； | root账户具有系统所有权限，未实现管理用户的权限分离。 |
| e）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； | 经访谈，由系统管理员root配置访问控制策略，如：/etc/passwd，/etc/profile宿主为root、权限设置为644，audit文件为700、message文件为600，其他文件权限为750，实现用户对文件的权限控制。 |
| f）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； | 由管理用户进行用户访问权限分配进行设置，依据访问控制策略,对各类文件进行访问，重要文件和目录权限均在合理范围内，用户可根据文件不同的权限进行操作。 |
| g）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。 | 执 行more /etc/selinux/config 命令，查看config文件显示 SELINUX参数为 DISABLED，即未开启强制访问控制模式。 |
| 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）执行ps -ef|grep rsyslog和ps -ef|grep auditd命令，显示rsyslog和auditd进程正在运行；2）more /etc/audit/audit.rules，显示审计内容包括：\*.info、authriv.\*、mail.\*、cron.\*、\*.emerg、uucp、news.crit、local7.\*等事件。 |
| 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； | 执行tail -20 /var/log/audit/audit.log命令，查看近20条审计日志，内容包括：时间、对象、路径、用户ID、相关的系统调用、用户执行命令等。 |
| 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）通过访问权限对审计记录进行保护，日志文件/var/log/messages、/var/log/secure、/var/log/audit/audit.log访问 权限均为600；2）审计记录本地保存，且实时备份至360本地安全大脑，保存时间满足180天以上。 |
| d）应对审计进程进行保护，防止未经授权的中断。 | 执行service auditd status命令，系统开启auditd审计保护进程，审计进程由root用户维护，经现场使用yluser用户通过service auditd stop命令尝试中断审计进程，无法将审计进程单独中断。 |
| 入侵防范 | a）应遵循最小安装的原则，仅安装需要的组件和应用程序； | 1）系统安装遵循最小化安装原则；2）执行yum list installed命令查看操作系统已安装的程序包，存在Java、oracle、SSH、天眼云镜agent等应用程序或组件，不存在与业务系统无关的组件和应用程序。 |
| b）应关闭不需要的系统服务、默认共享和高危端口； | 1）执行systemctl list-unit-files 命令，系统已关闭FTP、Telnet 等高危网络服务；2）执行netstat -pantu命令，系统关闭了135、445等高危端口，仅开启了22、1521等端口。 |
| c）应通过设定终端接入方式或网络地址范围对通过网络进行管理的管理终端进行限制； | 经核查，1）通过配置安全组策略限制仅允许通过堡垒机管理服务器；2）经核查防火墙中访问控制策略，具备堡垒机地址-服务器管理网段（10.33.0.0）的访问控制策略。 |
| d）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； | 根据GB∕T 28448-2019 《信息安全技术 网络安全等级保护测评要求》测评对象范围描述，服务器无该项要求，故判为“不适用”。 |
| e）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； | 1）经过漏洞扫描，服务器不存在高危安全漏洞；2）执行rpm -qa grep patch命令，查看系统补丁已更新至最新。 |
| f）应能够检测到对重要节点进行入侵的行为，并在发生严重入侵事件时提供报警。 | 经核查，服务器上安装有青藤云天眼云镜，对主机入侵行为进行检测，发现严重安全事件时通过钉钉告警。 |
| 恶意代码防范 | a）应采用免受恶意代码攻击的技术措施或主动免疫可信验证机制及时识别入侵和病毒行为，并将其有效阻断。 | 经核查，服务器上安装有青藤云天眼云镜，对主机恶意代码进行检测、清除，每天凌晨自动更新恶意代码特征库，经核查，具备恶意代码特征库更新记录。 |
| 可信验证 | a）可基于可信根对计算设备的系统引导程序、系统程序、重要配置参数和应用程序等进行可信验证，并在应用程序的关键执行环节进行动态可信验证，在检测到其可信性受到破坏后进行报警，并将验证结果形成审计记录送至安全管理中心。 | 未采用技术措施对计算设备的系统引导程序、系统程序、重要配置参数和通信应用程序等进行可信验证。 |
| 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； | 采用SSH协议连接操作系统，保证了鉴别信息以及管理数据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。 | 操作系统中对重要鉴别信息通过自身的加密及校验（SHA256），保证数据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； | 采用SSH协议连接操作系统，保证了鉴别信息以及管理数据在传输过程中的保密性。 |
| b）应采用密码技术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个人信息等。 | 通过系统自带的加密模块保证鉴别数据在存储过程中的保密性。 |
| 数据备份恢复 | a）应提供重要数据的本地数据备份与恢复功能； | 经核查，通过脚本每周将配置文件、代码仓库等数据备份至备份服务器中，依据需要验证备份数据的有效性。 |
| b）应提供异地实时备份功能，利用通信网络将重要数据实时备份至备份场地； | 系统无异地备份机制。 |
| c）应提供重要数据处理系统的热冗余，保证系统的高可用性。 | 服务器采用集群方式部署，保证系统的高可用性。 |
| 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； | 操作系统提供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功能。 |
| 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。 | 操作系统提供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的功能。 |

4.1.3.88. 查询库26主库

|  |  |  |
| --- | --- | --- |
| **安全控制点** | **测评指标** | **结果记录** |
| 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）操作系统时采用用户名+SSHKey公私钥进行身份鉴别鉴别信息具有复杂度要求；2）执行cat /etc/shadow命令，查看shadow文件系统内用户身份标识唯一，不存在同名用户，且不存在空口令账号；3）经访谈，SSHKey公私钥每半年进行更换；4）查看sshd\_config配置文件中配置PasswordAuthentication no，拒绝使用密码方式进行身份鉴别。 |
| 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； | 操作系统采用用户名+SSHKey公私钥进行身份鉴别，可以防止鉴别信息被暴力破解；但未配置用户连接超时退出策略。 |
| 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； | 1）经核查，管理人员采用SSH协议连接操作系统；2）执行netatat –tpln| grep 23命令查看操作系统远程管理端口，不存在Telnet端口，防止鉴别信息在网络传输过程中的被窃听。 |
| 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。 | 未采用两种或两种以上组合的鉴别技术对用户进行身份鉴别。 |
| 访问控制 | a）应对登录的用户分配账户和权限； | 1）经访谈，通过root账户为登录的用户创建账户、分配权限；2）执行ls -l命令查看关键文件权限，均已为账户分配了相应权限，相关文件权限设置为/etc/shadow：000、/etc/passwd：644、/etc/group：644、/etc/profile：644、/etc/crontab：644、/ etc/securetty：600、/etc/ssh/sshd\_config：600。 |
| b）应重命名或删除默认账户，修改默认账户的默认口令； | 1）执行cat /etc/shadow命令查看shadow文件，操作系统中adm、lp、sync、shutdown、halt、mail、uucp、operator、games、gopher等账户均为nologin状态，存在默认账户root；2）执行more /etc/ssh/sshd\_config命令，查看“PermitRootLogin”参数设置为“yes”，即允许root远程登录；3）经访谈，root用户需通过公私钥方式进行身份鉴别。 |
| 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； | 1）执行cat /etc/shadow命令查看shadow文件，发现操作系统存在root、ysup、yops、yluser等在用账户，不存在多余的、过期账户；2）存在多个堡垒机账户登录操作系统时共用一个账户的情况。 |
| 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； | root账户具有系统所有权限，未实现管理用户的权限分离。 |
| e）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； | 经访谈，由系统管理员root配置访问控制策略，如：/etc/passwd，/etc/profile宿主为root、权限设置为644，audit文件为700、message文件为600，其他文件权限为750，实现用户对文件的权限控制。 |
| f）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； | 由管理用户进行用户访问权限分配进行设置，依据访问控制策略,对各类文件进行访问，重要文件和目录权限均在合理范围内，用户可根据文件不同的权限进行操作。 |
| g）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。 | 执 行more /etc/selinux/config 命令，查看config文件显示 SELINUX参数为 DISABLED，即未开启强制访问控制模式。 |
| 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）执行ps -ef|grep rsyslog和ps -ef|grep auditd命令，显示rsyslog和auditd进程正在运行；2）more /etc/audit/audit.rules，显示审计内容包括：\*.info、authriv.\*、mail.\*、cron.\*、\*.emerg、uucp、news.crit、local7.\*等事件。 |
| 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； | 执行tail -20 /var/log/audit/audit.log命令，查看近20条审计日志，内容包括：时间、对象、路径、用户ID、相关的系统调用、用户执行命令等。 |
| 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）通过访问权限对审计记录进行保护，日志文件/var/log/messages、/var/log/secure、/var/log/audit/audit.log访问 权限均为600；2）审计记录本地保存，且实时备份至360本地安全大脑，保存时间满足180天以上。 |
| d）应对审计进程进行保护，防止未经授权的中断。 | 执行service auditd status命令，系统开启auditd审计保护进程，审计进程由root用户维护，经现场使用yluser用户通过service auditd stop命令尝试中断审计进程，无法将审计进程单独中断。 |
| 入侵防范 | a）应遵循最小安装的原则，仅安装需要的组件和应用程序； | 1）系统安装遵循最小化安装原则；2）执行yum list installed命令查看操作系统已安装的程序包，存在Java、oracle、SSH、天眼云镜agent等应用程序或组件，不存在与业务系统无关的组件和应用程序。 |
| b）应关闭不需要的系统服务、默认共享和高危端口； | 1）执行systemctl list-unit-files 命令，系统已关闭FTP、Telnet 等高危网络服务；2）执行netstat -pantu命令，系统关闭了135、445等高危端口，仅开启了22、1521等端口。 |
| c）应通过设定终端接入方式或网络地址范围对通过网络进行管理的管理终端进行限制； | 经核查，1）通过配置安全组策略限制仅允许通过堡垒机管理服务器；2）经核查防火墙中访问控制策略，具备堡垒机地址-服务器管理网段（10.33.0.0）的访问控制策略。 |
| d）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； | 根据GB∕T 28448-2019 《信息安全技术 网络安全等级保护测评要求》测评对象范围描述，服务器无该项要求，故判为“不适用”。 |
| e）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； | 1）经过漏洞扫描，服务器不存在高危安全漏洞；2）执行rpm -qa grep patch命令，查看系统补丁已更新至最新。 |
| f）应能够检测到对重要节点进行入侵的行为，并在发生严重入侵事件时提供报警。 | 经核查，服务器上安装有青藤云天眼云镜，对主机入侵行为进行检测，发现严重安全事件时通过钉钉告警。 |
| 恶意代码防范 | a）应采用免受恶意代码攻击的技术措施或主动免疫可信验证机制及时识别入侵和病毒行为，并将其有效阻断。 | 经核查，服务器上安装有青藤云天眼云镜，对主机恶意代码进行检测、清除，每天凌晨自动更新恶意代码特征库，经核查，具备恶意代码特征库更新记录。 |
| 可信验证 | a）可基于可信根对计算设备的系统引导程序、系统程序、重要配置参数和应用程序等进行可信验证，并在应用程序的关键执行环节进行动态可信验证，在检测到其可信性受到破坏后进行报警，并将验证结果形成审计记录送至安全管理中心。 | 未采用技术措施对计算设备的系统引导程序、系统程序、重要配置参数和通信应用程序等进行可信验证。 |
| 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； | 采用SSH协议连接操作系统，保证了鉴别信息以及管理数据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。 | 操作系统中对重要鉴别信息通过自身的加密及校验（SHA256），保证数据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； | 采用SSH协议连接操作系统，保证了鉴别信息以及管理数据在传输过程中的保密性。 |
| b）应采用密码技术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个人信息等。 | 通过系统自带的加密模块保证鉴别数据在存储过程中的保密性。 |
| 数据备份恢复 | a）应提供重要数据的本地数据备份与恢复功能； | 经核查，通过脚本每周将配置文件、代码仓库等数据备份至备份服务器中，依据需要验证备份数据的有效性。 |
| b）应提供异地实时备份功能，利用通信网络将重要数据实时备份至备份场地； | 系统无异地备份机制。 |
| c）应提供重要数据处理系统的热冗余，保证系统的高可用性。 | 服务器采用集群方式部署，保证系统的高可用性。 |
| 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； | 操作系统提供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功能。 |
| 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。 | 操作系统提供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的功能。 |

4.1.3.89. BI1备库

|  |  |  |
| --- | --- | --- |
| **安全控制点** | **测评指标** | **结果记录** |
| 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）操作系统时采用用户名+SSHKey公私钥进行身份鉴别鉴别信息具有复杂度要求；2）执行cat /etc/shadow命令，查看shadow文件系统内用户身份标识唯一，不存在同名用户，且不存在空口令账号；3）经访谈，SSHKey公私钥每半年进行更换；4）查看sshd\_config配置文件中配置PasswordAuthentication no，拒绝使用密码方式进行身份鉴别。 |
| 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； | 操作系统采用用户名+SSHKey公私钥进行身份鉴别，可以防止鉴别信息被暴力破解；但未配置用户连接超时退出策略。 |
| 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； | 1）经核查，管理人员采用SSH协议连接操作系统；2）执行netatat –tpln| grep 23命令查看操作系统远程管理端口，不存在Telnet端口，防止鉴别信息在网络传输过程中的被窃听。 |
| 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。 | 未采用两种或两种以上组合的鉴别技术对用户进行身份鉴别。 |
| 访问控制 | a）应对登录的用户分配账户和权限； | 1）经访谈，通过root账户为登录的用户创建账户、分配权限；2）执行ls -l命令查看关键文件权限，均已为账户分配了相应权限，相关文件权限设置为/etc/shadow：000、/etc/passwd：644、/etc/group：644、/etc/profile：644、/etc/crontab：644、/ etc/securetty：600、/etc/ssh/sshd\_config：600。 |
| b）应重命名或删除默认账户，修改默认账户的默认口令； | 1）执行cat /etc/shadow命令查看shadow文件，操作系统中adm、lp、sync、shutdown、halt、mail、uucp、operator、games、gopher等账户均为nologin状态，存在默认账户root；2）执行more /etc/ssh/sshd\_config命令，查看“PermitRootLogin”参数设置为“yes”，即允许root远程登录；3）经访谈，root用户需通过公私钥方式进行身份鉴别。 |
| 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； | 1）执行cat /etc/shadow命令查看shadow文件，发现操作系统存在root、ysup、yops、yluser等在用账户，不存在多余的、过期账户；2）存在多个堡垒机账户登录操作系统时共用一个账户的情况。 |
| 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； | root账户具有系统所有权限，未实现管理用户的权限分离。 |
| e）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； | 经访谈，由系统管理员root配置访问控制策略，如：/etc/passwd，/etc/profile宿主为root、权限设置为644，audit文件为700、message文件为600，其他文件权限为750，实现用户对文件的权限控制。 |
| f）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； | 由管理用户进行用户访问权限分配进行设置，依据访问控制策略,对各类文件进行访问，重要文件和目录权限均在合理范围内，用户可根据文件不同的权限进行操作。 |
| g）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。 | 执 行more /etc/selinux/config 命令，查看config文件显示 SELINUX参数为 DISABLED，即未开启强制访问控制模式。 |
| 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）执行ps -ef|grep rsyslog和ps -ef|grep auditd命令，显示rsyslog和auditd进程正在运行；2）more /etc/audit/audit.rules，显示审计内容包括：\*.info、authriv.\*、mail.\*、cron.\*、\*.emerg、uucp、news.crit、local7.\*等事件。 |
| 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； | 执行tail -20 /var/log/audit/audit.log命令，查看近20条审计日志，内容包括：时间、对象、路径、用户ID、相关的系统调用、用户执行命令等。 |
| 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）通过访问权限对审计记录进行保护，日志文件/var/log/messages、/var/log/secure、/var/log/audit/audit.log访问 权限均为600；2）审计记录本地保存，且实时备份至360本地安全大脑，保存时间满足180天以上。 |
| d）应对审计进程进行保护，防止未经授权的中断。 | 执行service auditd status命令，系统开启auditd审计保护进程，审计进程由root用户维护，经现场使用yluser用户通过service auditd stop命令尝试中断审计进程，无法将审计进程单独中断。 |
| 入侵防范 | a）应遵循最小安装的原则，仅安装需要的组件和应用程序； | 1）系统安装遵循最小化安装原则；2）执行yum list installed命令查看操作系统已安装的程序包，存在Java、oracle、SSH、天眼云镜agent等应用程序或组件，不存在与业务系统无关的组件和应用程序。 |
| b）应关闭不需要的系统服务、默认共享和高危端口； | 1）执行systemctl list-unit-files 命令，系统已关闭FTP、Telnet 等高危网络服务；2）执行netstat -pantu命令，系统关闭了135、445等高危端口，仅开启了22、1521等端口。 |
| c）应通过设定终端接入方式或网络地址范围对通过网络进行管理的管理终端进行限制； | 经核查，1）通过配置安全组策略限制仅允许通过堡垒机管理服务器；2）经核查防火墙中访问控制策略，具备堡垒机地址-服务器管理网段（10.33.0.0）的访问控制策略。 |
| d）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； | 根据GB∕T 28448-2019 《信息安全技术 网络安全等级保护测评要求》测评对象范围描述，服务器无该项要求，故判为“不适用”。 |
| e）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； | 1）经过漏洞扫描，服务器不存在高危安全漏洞；2）执行rpm -qa grep patch命令，查看系统补丁已更新至最新。 |
| f）应能够检测到对重要节点进行入侵的行为，并在发生严重入侵事件时提供报警。 | 经核查，服务器上安装有青藤云天眼云镜，对主机入侵行为进行检测，发现严重安全事件时通过钉钉告警。 |
| 恶意代码防范 | a）应采用免受恶意代码攻击的技术措施或主动免疫可信验证机制及时识别入侵和病毒行为，并将其有效阻断。 | 经核查，服务器上安装有青藤云天眼云镜，对主机恶意代码进行检测、清除，每天凌晨自动更新恶意代码特征库，经核查，具备恶意代码特征库更新记录。 |
| 可信验证 | a）可基于可信根对计算设备的系统引导程序、系统程序、重要配置参数和应用程序等进行可信验证，并在应用程序的关键执行环节进行动态可信验证，在检测到其可信性受到破坏后进行报警，并将验证结果形成审计记录送至安全管理中心。 | 未采用技术措施对计算设备的系统引导程序、系统程序、重要配置参数和通信应用程序等进行可信验证。 |
| 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； | 采用SSH协议连接操作系统，保证了鉴别信息以及管理数据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。 | 操作系统中对重要鉴别信息通过自身的加密及校验（SHA256），保证数据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； | 采用SSH协议连接操作系统，保证了鉴别信息以及管理数据在传输过程中的保密性。 |
| b）应采用密码技术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个人信息等。 | 通过系统自带的加密模块保证鉴别数据在存储过程中的保密性。 |
| 数据备份恢复 | a）应提供重要数据的本地数据备份与恢复功能； | 经核查，通过脚本每周将配置文件、代码仓库等数据备份至备份服务器中，依据需要验证备份数据的有效性。 |
| b）应提供异地实时备份功能，利用通信网络将重要数据实时备份至备份场地； | 系统无异地备份机制。 |
| c）应提供重要数据处理系统的热冗余，保证系统的高可用性。 | 服务器采用集群方式部署，保证系统的高可用性。 |
| 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； | 操作系统提供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功能。 |
| 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。 | 操作系统提供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的功能。 |

4.1.3.90. BI集群1节点1

|  |  |  |
| --- | --- | --- |
| **安全控制点** | **测评指标** | **结果记录** |
| 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）操作系统时采用用户名+SSHKey公私钥进行身份鉴别鉴别信息具有复杂度要求；2）执行cat /etc/shadow命令，查看shadow文件系统内用户身份标识唯一，不存在同名用户，且不存在空口令账号；3）经访谈，SSHKey公私钥每半年进行更换；4）查看sshd\_config配置文件中配置PasswordAuthentication no，拒绝使用密码方式进行身份鉴别。 |
| 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； | 操作系统采用用户名+SSHKey公私钥进行身份鉴别，可以防止鉴别信息被暴力破解；但未配置用户连接超时退出策略。 |
| 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； | 1）经核查，管理人员采用SSH协议连接操作系统；2）执行netatat –tpln| grep 23命令查看操作系统远程管理端口，不存在Telnet端口，防止鉴别信息在网络传输过程中的被窃听。 |
| 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。 | 未采用两种或两种以上组合的鉴别技术对用户进行身份鉴别。 |
| 访问控制 | a）应对登录的用户分配账户和权限； | 1）经访谈，通过root账户为登录的用户创建账户、分配权限；2）执行ls -l命令查看关键文件权限，均已为账户分配了相应权限，相关文件权限设置为/etc/shadow：000、/etc/passwd：644、/etc/group：644、/etc/profile：644、/etc/crontab：644、/ etc/securetty：600、/etc/ssh/sshd\_config：600。 |
| b）应重命名或删除默认账户，修改默认账户的默认口令； | 1）执行cat /etc/shadow命令查看shadow文件，操作系统中adm、lp、sync、shutdown、halt、mail、uucp、operator、games、gopher等账户均为nologin状态，存在默认账户root；2）执行more /etc/ssh/sshd\_config命令，查看“PermitRootLogin”参数设置为“yes”，即允许root远程登录；3）经访谈，root用户需通过公私钥方式进行身份鉴别。 |
| 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； | 1）执行cat /etc/shadow命令查看shadow文件，发现操作系统存在root、ysup、yops、yluser等在用账户，不存在多余的、过期账户；2）存在多个堡垒机账户登录操作系统时共用一个账户的情况。 |
| 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； | root账户具有系统所有权限，未实现管理用户的权限分离。 |
| e）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； | 经访谈，由系统管理员root配置访问控制策略，如：/etc/passwd，/etc/profile宿主为root、权限设置为644，audit文件为700、message文件为600，其他文件权限为750，实现用户对文件的权限控制。 |
| f）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； | 由管理用户进行用户访问权限分配进行设置，依据访问控制策略,对各类文件进行访问，重要文件和目录权限均在合理范围内，用户可根据文件不同的权限进行操作。 |
| g）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。 | 执 行more /etc/selinux/config 命令，查看config文件显示 SELINUX参数为 DISABLED，即未开启强制访问控制模式。 |
| 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）执行ps -ef|grep rsyslog和ps -ef|grep auditd命令，显示rsyslog和auditd进程正在运行；2）more /etc/audit/audit.rules，显示审计内容包括：\*.info、authriv.\*、mail.\*、cron.\*、\*.emerg、uucp、news.crit、local7.\*等事件。 |
| 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； | 执行tail -20 /var/log/audit/audit.log命令，查看近20条审计日志，内容包括：时间、对象、路径、用户ID、相关的系统调用、用户执行命令等。 |
| 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）通过访问权限对审计记录进行保护，日志文件/var/log/messages、/var/log/secure、/var/log/audit/audit.log访问 权限均为600；2）审计记录本地保存，且实时备份至360本地安全大脑，保存时间满足180天以上。 |
| d）应对审计进程进行保护，防止未经授权的中断。 | 执行service auditd status命令，系统开启auditd审计保护进程，审计进程由root用户维护，经现场使用yluser用户通过service auditd stop命令尝试中断审计进程，无法将审计进程单独中断。 |
| 入侵防范 | a）应遵循最小安装的原则，仅安装需要的组件和应用程序； | 1）系统安装遵循最小化安装原则；2）执行yum list installed命令查看操作系统已安装的程序包，存在Java、oracle、SSH、天眼云镜agent等应用程序或组件，不存在与业务系统无关的组件和应用程序。 |
| b）应关闭不需要的系统服务、默认共享和高危端口； | 1）执行systemctl list-unit-files 命令，系统已关闭FTP、Telnet 等高危网络服务；2）执行netstat -pantu命令，系统关闭了135、445等高危端口，仅开启了22、1521等端口。 |
| c）应通过设定终端接入方式或网络地址范围对通过网络进行管理的管理终端进行限制； | 经核查，1）通过配置安全组策略限制仅允许通过堡垒机管理服务器；2）经核查防火墙中访问控制策略，具备堡垒机地址-服务器管理网段（10.33.0.0）的访问控制策略。 |
| d）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； | 根据GB∕T 28448-2019 《信息安全技术 网络安全等级保护测评要求》测评对象范围描述，服务器无该项要求，故判为“不适用”。 |
| e）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； | 1）经过漏洞扫描，服务器不存在高危安全漏洞；2）执行rpm -qa grep patch命令，查看系统补丁已更新至最新。 |
| f）应能够检测到对重要节点进行入侵的行为，并在发生严重入侵事件时提供报警。 | 经核查，服务器上安装有青藤云天眼云镜，对主机入侵行为进行检测，发现严重安全事件时通过钉钉告警。 |
| 恶意代码防范 | a）应采用免受恶意代码攻击的技术措施或主动免疫可信验证机制及时识别入侵和病毒行为，并将其有效阻断。 | 经核查，服务器上安装有青藤云天眼云镜，对主机恶意代码进行检测、清除，每天凌晨自动更新恶意代码特征库，经核查，具备恶意代码特征库更新记录。 |
| 可信验证 | a）可基于可信根对计算设备的系统引导程序、系统程序、重要配置参数和应用程序等进行可信验证，并在应用程序的关键执行环节进行动态可信验证，在检测到其可信性受到破坏后进行报警，并将验证结果形成审计记录送至安全管理中心。 | 未采用技术措施对计算设备的系统引导程序、系统程序、重要配置参数和通信应用程序等进行可信验证。 |
| 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； | 采用SSH协议连接操作系统，保证了鉴别信息以及管理数据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。 | 操作系统中对重要鉴别信息通过自身的加密及校验（SHA256），保证数据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； | 采用SSH协议连接操作系统，保证了鉴别信息以及管理数据在传输过程中的保密性。 |
| b）应采用密码技术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个人信息等。 | 通过系统自带的加密模块保证鉴别数据在存储过程中的保密性。 |
| 数据备份恢复 | a）应提供重要数据的本地数据备份与恢复功能； | 经核查，通过脚本每周将配置文件、代码仓库等数据备份至备份服务器中，依据需要验证备份数据的有效性。 |
| b）应提供异地实时备份功能，利用通信网络将重要数据实时备份至备份场地； | 系统无异地备份机制。 |
| c）应提供重要数据处理系统的热冗余，保证系统的高可用性。 | 服务器采用集群方式部署，保证系统的高可用性。 |
| 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； | 操作系统提供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功能。 |
| 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。 | 操作系统提供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的功能。 |

4.1.3.91. BI集群2节点2

|  |  |  |
| --- | --- | --- |
| **安全控制点** | **测评指标** | **结果记录** |
| 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）操作系统时采用用户名+SSHKey公私钥进行身份鉴别鉴别信息具有复杂度要求；2）执行cat /etc/shadow命令，查看shadow文件系统内用户身份标识唯一，不存在同名用户，且不存在空口令账号；3）经访谈，SSHKey公私钥每半年进行更换；4）查看sshd\_config配置文件中配置PasswordAuthentication no，拒绝使用密码方式进行身份鉴别。 |
| 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； | 操作系统采用用户名+SSHKey公私钥进行身份鉴别，可以防止鉴别信息被暴力破解；但未配置用户连接超时退出策略。 |
| 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； | 1）经核查，管理人员采用SSH协议连接操作系统；2）执行netatat –tpln| grep 23命令查看操作系统远程管理端口，不存在Telnet端口，防止鉴别信息在网络传输过程中的被窃听。 |
| 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。 | 未采用两种或两种以上组合的鉴别技术对用户进行身份鉴别。 |
| 访问控制 | a）应对登录的用户分配账户和权限； | 1）经访谈，通过root账户为登录的用户创建账户、分配权限；2）执行ls -l命令查看关键文件权限，均已为账户分配了相应权限，相关文件权限设置为/etc/shadow：000、/etc/passwd：644、/etc/group：644、/etc/profile：644、/etc/crontab：644、/ etc/securetty：600、/etc/ssh/sshd\_config：600。 |
| b）应重命名或删除默认账户，修改默认账户的默认口令； | 1）执行cat /etc/shadow命令查看shadow文件，操作系统中adm、lp、sync、shutdown、halt、mail、uucp、operator、games、gopher等账户均为nologin状态，存在默认账户root；2）执行more /etc/ssh/sshd\_config命令，查看“PermitRootLogin”参数设置为“yes”，即允许root远程登录；3）经访谈，root用户需通过公私钥方式进行身份鉴别。 |
| 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； | 1）执行cat /etc/shadow命令查看shadow文件，发现操作系统存在root、ysup、yops、yluser等在用账户，不存在多余的、过期账户；2）存在多个堡垒机账户登录操作系统时共用一个账户的情况。 |
| 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； | root账户具有系统所有权限，未实现管理用户的权限分离。 |
| e）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； | 经访谈，由系统管理员root配置访问控制策略，如：/etc/passwd，/etc/profile宿主为root、权限设置为644，audit文件为700、message文件为600，其他文件权限为750，实现用户对文件的权限控制。 |
| f）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； | 由管理用户进行用户访问权限分配进行设置，依据访问控制策略,对各类文件进行访问，重要文件和目录权限均在合理范围内，用户可根据文件不同的权限进行操作。 |
| g）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。 | 执 行more /etc/selinux/config 命令，查看config文件显示 SELINUX参数为 DISABLED，即未开启强制访问控制模式。 |
| 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）执行ps -ef|grep rsyslog和ps -ef|grep auditd命令，显示rsyslog和auditd进程正在运行；2）more /etc/audit/audit.rules，显示审计内容包括：\*.info、authriv.\*、mail.\*、cron.\*、\*.emerg、uucp、news.crit、local7.\*等事件。 |
| 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； | 执行tail -20 /var/log/audit/audit.log命令，查看近20条审计日志，内容包括：时间、对象、路径、用户ID、相关的系统调用、用户执行命令等。 |
| 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）通过访问权限对审计记录进行保护，日志文件/var/log/messages、/var/log/secure、/var/log/audit/audit.log访问 权限均为600；2）审计记录本地保存，且实时备份至360本地安全大脑，保存时间满足180天以上。 |
| d）应对审计进程进行保护，防止未经授权的中断。 | 执行service auditd status命令，系统开启auditd审计保护进程，审计进程由root用户维护，经现场使用yluser用户通过service auditd stop命令尝试中断审计进程，无法将审计进程单独中断。 |
| 入侵防范 | a）应遵循最小安装的原则，仅安装需要的组件和应用程序； | 1）系统安装遵循最小化安装原则；2）执行yum list installed命令查看操作系统已安装的程序包，存在Java、oracle、SSH、天眼云镜agent等应用程序或组件，不存在与业务系统无关的组件和应用程序。 |
| b）应关闭不需要的系统服务、默认共享和高危端口； | 1）执行systemctl list-unit-files 命令，系统已关闭FTP、Telnet 等高危网络服务；2）执行netstat -pantu命令，系统关闭了135、445等高危端口，仅开启了22、1521等端口。 |
| c）应通过设定终端接入方式或网络地址范围对通过网络进行管理的管理终端进行限制； | 经核查，1）通过配置安全组策略限制仅允许通过堡垒机管理服务器；2）经核查防火墙中访问控制策略，具备堡垒机地址-服务器管理网段（10.33.0.0）的访问控制策略。 |
| d）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； | 根据GB∕T 28448-2019 《信息安全技术 网络安全等级保护测评要求》测评对象范围描述，服务器无该项要求，故判为“不适用”。 |
| e）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； | 1）经过漏洞扫描，服务器不存在高危安全漏洞；2）执行rpm -qa grep patch命令，查看系统补丁已更新至最新。 |
| f）应能够检测到对重要节点进行入侵的行为，并在发生严重入侵事件时提供报警。 | 经核查，服务器上安装有青藤云天眼云镜，对主机入侵行为进行检测，发现严重安全事件时通过钉钉告警。 |
| 恶意代码防范 | a）应采用免受恶意代码攻击的技术措施或主动免疫可信验证机制及时识别入侵和病毒行为，并将其有效阻断。 | 经核查，服务器上安装有青藤云天眼云镜，对主机恶意代码进行检测、清除，每天凌晨自动更新恶意代码特征库，经核查，具备恶意代码特征库更新记录。 |
| 可信验证 | a）可基于可信根对计算设备的系统引导程序、系统程序、重要配置参数和应用程序等进行可信验证，并在应用程序的关键执行环节进行动态可信验证，在检测到其可信性受到破坏后进行报警，并将验证结果形成审计记录送至安全管理中心。 | 未采用技术措施对计算设备的系统引导程序、系统程序、重要配置参数和通信应用程序等进行可信验证。 |
| 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； | 采用SSH协议连接操作系统，保证了鉴别信息以及管理数据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。 | 操作系统中对重要鉴别信息通过自身的加密及校验（SHA256），保证数据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； | 采用SSH协议连接操作系统，保证了鉴别信息以及管理数据在传输过程中的保密性。 |
| b）应采用密码技术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个人信息等。 | 通过系统自带的加密模块保证鉴别数据在存储过程中的保密性。 |
| 数据备份恢复 | a）应提供重要数据的本地数据备份与恢复功能； | 经核查，通过脚本每周将配置文件、代码仓库等数据备份至备份服务器中，依据需要验证备份数据的有效性。 |
| b）应提供异地实时备份功能，利用通信网络将重要数据实时备份至备份场地； | 系统无异地备份机制。 |
| c）应提供重要数据处理系统的热冗余，保证系统的高可用性。 | 服务器采用集群方式部署，保证系统的高可用性。 |
| 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； | 操作系统提供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功能。 |
| 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。 | 操作系统提供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的功能。 |

4.1.3.92. XD1节点1

|  |  |  |
| --- | --- | --- |
| **安全控制点** | **测评指标** | **结果记录** |
| 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）操作系统时采用用户名+SSHKey公私钥进行身份鉴别鉴别信息具有复杂度要求；2）执行cat /etc/shadow命令，查看shadow文件系统内用户身份标识唯一，不存在同名用户，且不存在空口令账号；3）经访谈，SSHKey公私钥每半年进行更换；4）查看sshd\_config配置文件中配置PasswordAuthentication no，拒绝使用密码方式进行身份鉴别。 |
| 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； | 操作系统采用用户名+SSHKey公私钥进行身份鉴别，可以防止鉴别信息被暴力破解；但未配置用户连接超时退出策略。 |
| 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； | 1）经核查，管理人员采用SSH协议连接操作系统；2）执行netatat –tpln| grep 23命令查看操作系统远程管理端口，不存在Telnet端口，防止鉴别信息在网络传输过程中的被窃听。 |
| 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。 | 未采用两种或两种以上组合的鉴别技术对用户进行身份鉴别。 |
| 访问控制 | a）应对登录的用户分配账户和权限； | 1）经访谈，通过root账户为登录的用户创建账户、分配权限；2）执行ls -l命令查看关键文件权限，均已为账户分配了相应权限，相关文件权限设置为/etc/shadow：000、/etc/passwd：644、/etc/group：644、/etc/profile：644、/etc/crontab：644、/ etc/securetty：600、/etc/ssh/sshd\_config：600。 |
| b）应重命名或删除默认账户，修改默认账户的默认口令； | 1）执行cat /etc/shadow命令查看shadow文件，操作系统中adm、lp、sync、shutdown、halt、mail、uucp、operator、games、gopher等账户均为nologin状态，存在默认账户root；2）执行more /etc/ssh/sshd\_config命令，查看“PermitRootLogin”参数设置为“yes”，即允许root远程登录；3）经访谈，root用户需通过公私钥方式进行身份鉴别。 |
| 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； | 1）执行cat /etc/shadow命令查看shadow文件，发现操作系统存在root、ysup、yops、yluser等在用账户，不存在多余的、过期账户；2）存在多个堡垒机账户登录操作系统时共用一个账户的情况。 |
| 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； | root账户具有系统所有权限，未实现管理用户的权限分离。 |
| e）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； | 经访谈，由系统管理员root配置访问控制策略，如：/etc/passwd，/etc/profile宿主为root、权限设置为644，audit文件为700、message文件为600，其他文件权限为750，实现用户对文件的权限控制。 |
| f）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； | 由管理用户进行用户访问权限分配进行设置，依据访问控制策略,对各类文件进行访问，重要文件和目录权限均在合理范围内，用户可根据文件不同的权限进行操作。 |
| g）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。 | 执 行more /etc/selinux/config 命令，查看config文件显示 SELINUX参数为 DISABLED，即未开启强制访问控制模式。 |
| 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）执行ps -ef|grep rsyslog和ps -ef|grep auditd命令，显示rsyslog和auditd进程正在运行；2）more /etc/audit/audit.rules，显示审计内容包括：\*.info、authriv.\*、mail.\*、cron.\*、\*.emerg、uucp、news.crit、local7.\*等事件。 |
| 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； | 执行tail -20 /var/log/audit/audit.log命令，查看近20条审计日志，内容包括：时间、对象、路径、用户ID、相关的系统调用、用户执行命令等。 |
| 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）通过访问权限对审计记录进行保护，日志文件/var/log/messages、/var/log/secure、/var/log/audit/audit.log访问 权限均为600；2）审计记录本地保存，且实时备份至360本地安全大脑，保存时间满足180天以上。 |
| d）应对审计进程进行保护，防止未经授权的中断。 | 执行service auditd status命令，系统开启auditd审计保护进程，审计进程由root用户维护，经现场使用yluser用户通过service auditd stop命令尝试中断审计进程，无法将审计进程单独中断。 |
| 入侵防范 | a）应遵循最小安装的原则，仅安装需要的组件和应用程序； | 1）系统安装遵循最小化安装原则；2）执行yum list installed命令查看操作系统已安装的程序包，存在Java、oracle、SSH、天眼云镜agent等应用程序或组件，不存在与业务系统无关的组件和应用程序。 |
| b）应关闭不需要的系统服务、默认共享和高危端口； | 1）执行systemctl list-unit-files 命令，系统已关闭FTP、Telnet 等高危网络服务；2）执行netstat -pantu命令，系统关闭了135、445等高危端口，仅开启了22、1521等端口。 |
| c）应通过设定终端接入方式或网络地址范围对通过网络进行管理的管理终端进行限制； | 经核查，1）通过配置安全组策略限制仅允许通过堡垒机管理服务器；2）经核查防火墙中访问控制策略，具备堡垒机地址-服务器管理网段（10.33.0.0）的访问控制策略。 |
| d）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； | 根据GB∕T 28448-2019 《信息安全技术 网络安全等级保护测评要求》测评对象范围描述，服务器无该项要求，故判为“不适用”。 |
| e）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； | 1）经过漏洞扫描，服务器不存在高危安全漏洞；2）执行rpm -qa grep patch命令，查看系统补丁已更新至最新。 |
| f）应能够检测到对重要节点进行入侵的行为，并在发生严重入侵事件时提供报警。 | 经核查，服务器上安装有青藤云天眼云镜，对主机入侵行为进行检测，发现严重安全事件时通过钉钉告警。 |
| 恶意代码防范 | a）应采用免受恶意代码攻击的技术措施或主动免疫可信验证机制及时识别入侵和病毒行为，并将其有效阻断。 | 经核查，服务器上安装有青藤云天眼云镜，对主机恶意代码进行检测、清除，每天凌晨自动更新恶意代码特征库，经核查，具备恶意代码特征库更新记录。 |
| 可信验证 | a）可基于可信根对计算设备的系统引导程序、系统程序、重要配置参数和应用程序等进行可信验证，并在应用程序的关键执行环节进行动态可信验证，在检测到其可信性受到破坏后进行报警，并将验证结果形成审计记录送至安全管理中心。 | 未采用技术措施对计算设备的系统引导程序、系统程序、重要配置参数和通信应用程序等进行可信验证。 |
| 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； | 采用SSH协议连接操作系统，保证了鉴别信息以及管理数据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。 | 操作系统中对重要鉴别信息通过自身的加密及校验（SHA256），保证数据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； | 采用SSH协议连接操作系统，保证了鉴别信息以及管理数据在传输过程中的保密性。 |
| b）应采用密码技术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个人信息等。 | 通过系统自带的加密模块保证鉴别数据在存储过程中的保密性。 |
| 数据备份恢复 | a）应提供重要数据的本地数据备份与恢复功能； | 经核查，通过脚本每周将配置文件、代码仓库等数据备份至备份服务器中，依据需要验证备份数据的有效性。 |
| b）应提供异地实时备份功能，利用通信网络将重要数据实时备份至备份场地； | 系统无异地备份机制。 |
| c）应提供重要数据处理系统的热冗余，保证系统的高可用性。 | 服务器采用集群方式部署，保证系统的高可用性。 |
| 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； | 操作系统提供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功能。 |
| 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。 | 操作系统提供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的功能。 |

4.1.3.93. XD1节点2

|  |  |  |
| --- | --- | --- |
| **安全控制点** | **测评指标** | **结果记录** |
| 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）操作系统时采用用户名+SSHKey公私钥进行身份鉴别鉴别信息具有复杂度要求；2）执行cat /etc/shadow命令，查看shadow文件系统内用户身份标识唯一，不存在同名用户，且不存在空口令账号；3）经访谈，SSHKey公私钥每半年进行更换；4）查看sshd\_config配置文件中配置PasswordAuthentication no，拒绝使用密码方式进行身份鉴别。 |
| 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； | 操作系统采用用户名+SSHKey公私钥进行身份鉴别，可以防止鉴别信息被暴力破解；但未配置用户连接超时退出策略。 |
| 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； | 1）经核查，管理人员采用SSH协议连接操作系统；2）执行netatat –tpln| grep 23命令查看操作系统远程管理端口，不存在Telnet端口，防止鉴别信息在网络传输过程中的被窃听。 |
| 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。 | 未采用两种或两种以上组合的鉴别技术对用户进行身份鉴别。 |
| 访问控制 | a）应对登录的用户分配账户和权限； | 1）经访谈，通过root账户为登录的用户创建账户、分配权限；2）执行ls -l命令查看关键文件权限，均已为账户分配了相应权限，相关文件权限设置为/etc/shadow：000、/etc/passwd：644、/etc/group：644、/etc/profile：644、/etc/crontab：644、/ etc/securetty：600、/etc/ssh/sshd\_config：600。 |
| b）应重命名或删除默认账户，修改默认账户的默认口令； | 1）执行cat /etc/shadow命令查看shadow文件，操作系统中adm、lp、sync、shutdown、halt、mail、uucp、operator、games、gopher等账户均为nologin状态，存在默认账户root；2）执行more /etc/ssh/sshd\_config命令，查看“PermitRootLogin”参数设置为“yes”，即允许root远程登录；3）经访谈，root用户需通过公私钥方式进行身份鉴别。 |
| 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； | 1）执行cat /etc/shadow命令查看shadow文件，发现操作系统存在root、ysup、yops、yluser等在用账户，不存在多余的、过期账户；2）存在多个堡垒机账户登录操作系统时共用一个账户的情况。 |
| 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； | root账户具有系统所有权限，未实现管理用户的权限分离。 |
| e）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； | 经访谈，由系统管理员root配置访问控制策略，如：/etc/passwd，/etc/profile宿主为root、权限设置为644，audit文件为700、message文件为600，其他文件权限为750，实现用户对文件的权限控制。 |
| f）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； | 由管理用户进行用户访问权限分配进行设置，依据访问控制策略,对各类文件进行访问，重要文件和目录权限均在合理范围内，用户可根据文件不同的权限进行操作。 |
| g）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。 | 执 行more /etc/selinux/config 命令，查看config文件显示 SELINUX参数为 DISABLED，即未开启强制访问控制模式。 |
| 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）执行ps -ef|grep rsyslog和ps -ef|grep auditd命令，显示rsyslog和auditd进程正在运行；2）more /etc/audit/audit.rules，显示审计内容包括：\*.info、authriv.\*、mail.\*、cron.\*、\*.emerg、uucp、news.crit、local7.\*等事件。 |
| 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； | 执行tail -20 /var/log/audit/audit.log命令，查看近20条审计日志，内容包括：时间、对象、路径、用户ID、相关的系统调用、用户执行命令等。 |
| 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）通过访问权限对审计记录进行保护，日志文件/var/log/messages、/var/log/secure、/var/log/audit/audit.log访问 权限均为600；2）审计记录本地保存，且实时备份至360本地安全大脑，保存时间满足180天以上。 |
| d）应对审计进程进行保护，防止未经授权的中断。 | 执行service auditd status命令，系统开启auditd审计保护进程，审计进程由root用户维护，经现场使用yluser用户通过service auditd stop命令尝试中断审计进程，无法将审计进程单独中断。 |
| 入侵防范 | a）应遵循最小安装的原则，仅安装需要的组件和应用程序； | 1）系统安装遵循最小化安装原则；2）执行yum list installed命令查看操作系统已安装的程序包，存在Java、oracle、SSH、天眼云镜agent等应用程序或组件，不存在与业务系统无关的组件和应用程序。 |
| b）应关闭不需要的系统服务、默认共享和高危端口； | 1）执行systemctl list-unit-files 命令，系统已关闭FTP、Telnet 等高危网络服务；2）执行netstat -pantu命令，系统关闭了135、445等高危端口，仅开启了22、1521等端口。 |
| c）应通过设定终端接入方式或网络地址范围对通过网络进行管理的管理终端进行限制； | 经核查，1）通过配置安全组策略限制仅允许通过堡垒机管理服务器；2）经核查防火墙中访问控制策略，具备堡垒机地址-服务器管理网段（10.33.0.0）的访问控制策略。 |
| d）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； | 根据GB∕T 28448-2019 《信息安全技术 网络安全等级保护测评要求》测评对象范围描述，服务器无该项要求，故判为“不适用”。 |
| e）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； | 1）经过漏洞扫描，服务器不存在高危安全漏洞；2）执行rpm -qa grep patch命令，查看系统补丁已更新至最新。 |
| f）应能够检测到对重要节点进行入侵的行为，并在发生严重入侵事件时提供报警。 | 经核查，服务器上安装有青藤云天眼云镜，对主机入侵行为进行检测，发现严重安全事件时通过钉钉告警。 |
| 恶意代码防范 | a）应采用免受恶意代码攻击的技术措施或主动免疫可信验证机制及时识别入侵和病毒行为，并将其有效阻断。 | 经核查，服务器上安装有青藤云天眼云镜，对主机恶意代码进行检测、清除，每天凌晨自动更新恶意代码特征库，经核查，具备恶意代码特征库更新记录。 |
| 可信验证 | a）可基于可信根对计算设备的系统引导程序、系统程序、重要配置参数和应用程序等进行可信验证，并在应用程序的关键执行环节进行动态可信验证，在检测到其可信性受到破坏后进行报警，并将验证结果形成审计记录送至安全管理中心。 | 未采用技术措施对计算设备的系统引导程序、系统程序、重要配置参数和通信应用程序等进行可信验证。 |
| 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； | 采用SSH协议连接操作系统，保证了鉴别信息以及管理数据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。 | 操作系统中对重要鉴别信息通过自身的加密及校验（SHA256），保证数据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； | 采用SSH协议连接操作系统，保证了鉴别信息以及管理数据在传输过程中的保密性。 |
| b）应采用密码技术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个人信息等。 | 通过系统自带的加密模块保证鉴别数据在存储过程中的保密性。 |
| 数据备份恢复 | a）应提供重要数据的本地数据备份与恢复功能； | 经核查，通过脚本每周将配置文件、代码仓库等数据备份至备份服务器中，依据需要验证备份数据的有效性。 |
| b）应提供异地实时备份功能，利用通信网络将重要数据实时备份至备份场地； | 系统无异地备份机制。 |
| c）应提供重要数据处理系统的热冗余，保证系统的高可用性。 | 服务器采用集群方式部署，保证系统的高可用性。 |
| 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； | 操作系统提供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功能。 |
| 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。 | 操作系统提供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的功能。 |

4.1.3.94. XD1节点3

|  |  |  |
| --- | --- | --- |
| **安全控制点** | **测评指标** | **结果记录** |
| 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）操作系统时采用用户名+SSHKey公私钥进行身份鉴别鉴别信息具有复杂度要求；2）执行cat /etc/shadow命令，查看shadow文件系统内用户身份标识唯一，不存在同名用户，且不存在空口令账号；3）经访谈，SSHKey公私钥每半年进行更换；4）查看sshd\_config配置文件中配置PasswordAuthentication no，拒绝使用密码方式进行身份鉴别。 |
| 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； | 操作系统采用用户名+SSHKey公私钥进行身份鉴别，可以防止鉴别信息被暴力破解；但未配置用户连接超时退出策略。 |
| 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； | 1）经核查，管理人员采用SSH协议连接操作系统；2）执行netatat –tpln| grep 23命令查看操作系统远程管理端口，不存在Telnet端口，防止鉴别信息在网络传输过程中的被窃听。 |
| 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。 | 未采用两种或两种以上组合的鉴别技术对用户进行身份鉴别。 |
| 访问控制 | a）应对登录的用户分配账户和权限； | 1）经访谈，通过root账户为登录的用户创建账户、分配权限；2）执行ls -l命令查看关键文件权限，均已为账户分配了相应权限，相关文件权限设置为/etc/shadow：000、/etc/passwd：644、/etc/group：644、/etc/profile：644、/etc/crontab：644、/ etc/securetty：600、/etc/ssh/sshd\_config：600。 |
| b）应重命名或删除默认账户，修改默认账户的默认口令； | 1）执行cat /etc/shadow命令查看shadow文件，操作系统中adm、lp、sync、shutdown、halt、mail、uucp、operator、games、gopher等账户均为nologin状态，存在默认账户root；2）执行more /etc/ssh/sshd\_config命令，查看“PermitRootLogin”参数设置为“yes”，即允许root远程登录；3）经访谈，root用户需通过公私钥方式进行身份鉴别。 |
| 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； | 1）执行cat /etc/shadow命令查看shadow文件，发现操作系统存在root、ysup、yops、yluser等在用账户，不存在多余的、过期账户；2）存在多个堡垒机账户登录操作系统时共用一个账户的情况。 |
| 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； | root账户具有系统所有权限，未实现管理用户的权限分离。 |
| e）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； | 经访谈，由系统管理员root配置访问控制策略，如：/etc/passwd，/etc/profile宿主为root、权限设置为644，audit文件为700、message文件为600，其他文件权限为750，实现用户对文件的权限控制。 |
| f）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； | 由管理用户进行用户访问权限分配进行设置，依据访问控制策略,对各类文件进行访问，重要文件和目录权限均在合理范围内，用户可根据文件不同的权限进行操作。 |
| g）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。 | 执 行more /etc/selinux/config 命令，查看config文件显示 SELINUX参数为 DISABLED，即未开启强制访问控制模式。 |
| 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）执行ps -ef|grep rsyslog和ps -ef|grep auditd命令，显示rsyslog和auditd进程正在运行；2）more /etc/audit/audit.rules，显示审计内容包括：\*.info、authriv.\*、mail.\*、cron.\*、\*.emerg、uucp、news.crit、local7.\*等事件。 |
| 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； | 执行tail -20 /var/log/audit/audit.log命令，查看近20条审计日志，内容包括：时间、对象、路径、用户ID、相关的系统调用、用户执行命令等。 |
| 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）通过访问权限对审计记录进行保护，日志文件/var/log/messages、/var/log/secure、/var/log/audit/audit.log访问 权限均为600；2）审计记录本地保存，且实时备份至360本地安全大脑，保存时间满足180天以上。 |
| d）应对审计进程进行保护，防止未经授权的中断。 | 执行service auditd status命令，系统开启auditd审计保护进程，审计进程由root用户维护，经现场使用yluser用户通过service auditd stop命令尝试中断审计进程，无法将审计进程单独中断。 |
| 入侵防范 | a）应遵循最小安装的原则，仅安装需要的组件和应用程序； | 1）系统安装遵循最小化安装原则；2）执行yum list installed命令查看操作系统已安装的程序包，存在Java、oracle、SSH、天眼云镜agent等应用程序或组件，不存在与业务系统无关的组件和应用程序。 |
| b）应关闭不需要的系统服务、默认共享和高危端口； | 1）执行systemctl list-unit-files 命令，系统已关闭FTP、Telnet 等高危网络服务；2）执行netstat -pantu命令，系统关闭了135、445等高危端口，仅开启了22、1521等端口。 |
| c）应通过设定终端接入方式或网络地址范围对通过网络进行管理的管理终端进行限制； | 经核查，1）通过配置安全组策略限制仅允许通过堡垒机管理服务器；2）经核查防火墙中访问控制策略，具备堡垒机地址-服务器管理网段（10.33.0.0）的访问控制策略。 |
| d）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； | 根据GB∕T 28448-2019 《信息安全技术 网络安全等级保护测评要求》测评对象范围描述，服务器无该项要求，故判为“不适用”。 |
| e）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； | 1）经过漏洞扫描，服务器不存在高危安全漏洞；2）执行rpm -qa grep patch命令，查看系统补丁已更新至最新。 |
| f）应能够检测到对重要节点进行入侵的行为，并在发生严重入侵事件时提供报警。 | 经核查，服务器上安装有青藤云天眼云镜，对主机入侵行为进行检测，发现严重安全事件时通过钉钉告警。 |
| 恶意代码防范 | a）应采用免受恶意代码攻击的技术措施或主动免疫可信验证机制及时识别入侵和病毒行为，并将其有效阻断。 | 经核查，服务器上安装有青藤云天眼云镜，对主机恶意代码进行检测、清除，每天凌晨自动更新恶意代码特征库，经核查，具备恶意代码特征库更新记录。 |
| 可信验证 | a）可基于可信根对计算设备的系统引导程序、系统程序、重要配置参数和应用程序等进行可信验证，并在应用程序的关键执行环节进行动态可信验证，在检测到其可信性受到破坏后进行报警，并将验证结果形成审计记录送至安全管理中心。 | 未采用技术措施对计算设备的系统引导程序、系统程序、重要配置参数和通信应用程序等进行可信验证。 |
| 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； | 采用SSH协议连接操作系统，保证了鉴别信息以及管理数据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。 | 操作系统中对重要鉴别信息通过自身的加密及校验（SHA256），保证数据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； | 采用SSH协议连接操作系统，保证了鉴别信息以及管理数据在传输过程中的保密性。 |
| b）应采用密码技术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个人信息等。 | 通过系统自带的加密模块保证鉴别数据在存储过程中的保密性。 |
| 数据备份恢复 | a）应提供重要数据的本地数据备份与恢复功能； | 经核查，通过脚本每周将配置文件、代码仓库等数据备份至备份服务器中，依据需要验证备份数据的有效性。 |
| b）应提供异地实时备份功能，利用通信网络将重要数据实时备份至备份场地； | 系统无异地备份机制。 |
| c）应提供重要数据处理系统的热冗余，保证系统的高可用性。 | 服务器采用集群方式部署，保证系统的高可用性。 |
| 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； | 操作系统提供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功能。 |
| 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。 | 操作系统提供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的功能。 |

4.1.3.95. XD2节点3

|  |  |  |
| --- | --- | --- |
| **安全控制点** | **测评指标** | **结果记录** |
| 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）操作系统时采用用户名+SSHKey公私钥进行身份鉴别鉴别信息具有复杂度要求；2）执行cat /etc/shadow命令，查看shadow文件系统内用户身份标识唯一，不存在同名用户，且不存在空口令账号；3）经访谈，SSHKey公私钥每半年进行更换；4）查看sshd\_config配置文件中配置PasswordAuthentication no，拒绝使用密码方式进行身份鉴别。 |
| 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； | 操作系统采用用户名+SSHKey公私钥进行身份鉴别，可以防止鉴别信息被暴力破解；但未配置用户连接超时退出策略。 |
| 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； | 1）经核查，管理人员采用SSH协议连接操作系统；2）执行netatat –tpln| grep 23命令查看操作系统远程管理端口，不存在Telnet端口，防止鉴别信息在网络传输过程中的被窃听。 |
| 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。 | 未采用两种或两种以上组合的鉴别技术对用户进行身份鉴别。 |
| 访问控制 | a）应对登录的用户分配账户和权限； | 1）经访谈，通过root账户为登录的用户创建账户、分配权限；2）执行ls -l命令查看关键文件权限，均已为账户分配了相应权限，相关文件权限设置为/etc/shadow：000、/etc/passwd：644、/etc/group：644、/etc/profile：644、/etc/crontab：644、/ etc/securetty：600、/etc/ssh/sshd\_config：600。 |
| b）应重命名或删除默认账户，修改默认账户的默认口令； | 1）执行cat /etc/shadow命令查看shadow文件，操作系统中adm、lp、sync、shutdown、halt、mail、uucp、operator、games、gopher等账户均为nologin状态，存在默认账户root；2）执行more /etc/ssh/sshd\_config命令，查看“PermitRootLogin”参数设置为“yes”，即允许root远程登录；3）经访谈，root用户需通过公私钥方式进行身份鉴别。 |
| 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； | 1）执行cat /etc/shadow命令查看shadow文件，发现操作系统存在root、ysup、yops、yluser等在用账户，不存在多余的、过期账户；2）存在多个堡垒机账户登录操作系统时共用一个账户的情况。 |
| 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； | root账户具有系统所有权限，未实现管理用户的权限分离。 |
| e）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； | 经访谈，由系统管理员root配置访问控制策略，如：/etc/passwd，/etc/profile宿主为root、权限设置为644，audit文件为700、message文件为600，其他文件权限为750，实现用户对文件的权限控制。 |
| f）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； | 由管理用户进行用户访问权限分配进行设置，依据访问控制策略,对各类文件进行访问，重要文件和目录权限均在合理范围内，用户可根据文件不同的权限进行操作。 |
| g）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。 | 执 行more /etc/selinux/config 命令，查看config文件显示 SELINUX参数为 DISABLED，即未开启强制访问控制模式。 |
| 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）执行ps -ef|grep rsyslog和ps -ef|grep auditd命令，显示rsyslog和auditd进程正在运行；2）more /etc/audit/audit.rules，显示审计内容包括：\*.info、authriv.\*、mail.\*、cron.\*、\*.emerg、uucp、news.crit、local7.\*等事件。 |
| 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； | 执行tail -20 /var/log/audit/audit.log命令，查看近20条审计日志，内容包括：时间、对象、路径、用户ID、相关的系统调用、用户执行命令等。 |
| 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）通过访问权限对审计记录进行保护，日志文件/var/log/messages、/var/log/secure、/var/log/audit/audit.log访问 权限均为600；2）审计记录本地保存，且实时备份至360本地安全大脑，保存时间满足180天以上。 |
| d）应对审计进程进行保护，防止未经授权的中断。 | 执行service auditd status命令，系统开启auditd审计保护进程，审计进程由root用户维护，经现场使用yluser用户通过service auditd stop命令尝试中断审计进程，无法将审计进程单独中断。 |
| 入侵防范 | a）应遵循最小安装的原则，仅安装需要的组件和应用程序； | 1）系统安装遵循最小化安装原则；2）执行yum list installed命令查看操作系统已安装的程序包，存在Java、oracle、SSH、天眼云镜agent等应用程序或组件，不存在与业务系统无关的组件和应用程序。 |
| b）应关闭不需要的系统服务、默认共享和高危端口； | 1）执行systemctl list-unit-files 命令，系统已关闭FTP、Telnet 等高危网络服务；2）执行netstat -pantu命令，系统关闭了135、445等高危端口，仅开启了22、1521等端口。 |
| c）应通过设定终端接入方式或网络地址范围对通过网络进行管理的管理终端进行限制； | 经核查，1）通过配置安全组策略限制仅允许通过堡垒机管理服务器；2）经核查防火墙中访问控制策略，具备堡垒机地址-服务器管理网段（10.33.0.0）的访问控制策略。 |
| d）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； | 根据GB∕T 28448-2019 《信息安全技术 网络安全等级保护测评要求》测评对象范围描述，服务器无该项要求，故判为“不适用”。 |
| e）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； | 1）经过漏洞扫描，服务器不存在高危安全漏洞；2）执行rpm -qa grep patch命令，查看系统补丁已更新至最新。 |
| f）应能够检测到对重要节点进行入侵的行为，并在发生严重入侵事件时提供报警。 | 经核查，服务器上安装有青藤云天眼云镜，对主机入侵行为进行检测，发现严重安全事件时通过钉钉告警。 |
| 恶意代码防范 | a）应采用免受恶意代码攻击的技术措施或主动免疫可信验证机制及时识别入侵和病毒行为，并将其有效阻断。 | 经核查，服务器上安装有青藤云天眼云镜，对主机恶意代码进行检测、清除，每天凌晨自动更新恶意代码特征库，经核查，具备恶意代码特征库更新记录。 |
| 可信验证 | a）可基于可信根对计算设备的系统引导程序、系统程序、重要配置参数和应用程序等进行可信验证，并在应用程序的关键执行环节进行动态可信验证，在检测到其可信性受到破坏后进行报警，并将验证结果形成审计记录送至安全管理中心。 | 未采用技术措施对计算设备的系统引导程序、系统程序、重要配置参数和通信应用程序等进行可信验证。 |
| 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； | 采用SSH协议连接操作系统，保证了鉴别信息以及管理数据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。 | 操作系统中对重要鉴别信息通过自身的加密及校验（SHA256），保证数据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； | 采用SSH协议连接操作系统，保证了鉴别信息以及管理数据在传输过程中的保密性。 |
| b）应采用密码技术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个人信息等。 | 通过系统自带的加密模块保证鉴别数据在存储过程中的保密性。 |
| 数据备份恢复 | a）应提供重要数据的本地数据备份与恢复功能； | 经核查，通过脚本每周将配置文件、代码仓库等数据备份至备份服务器中，依据需要验证备份数据的有效性。 |
| b）应提供异地实时备份功能，利用通信网络将重要数据实时备份至备份场地； | 系统无异地备份机制。 |
| c）应提供重要数据处理系统的热冗余，保证系统的高可用性。 | 服务器采用集群方式部署，保证系统的高可用性。 |
| 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； | 操作系统提供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功能。 |
| 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。 | 操作系统提供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的功能。 |

4.1.3.96. 网点库集群节点1

|  |  |  |
| --- | --- | --- |
| **安全控制点** | **测评指标** | **结果记录** |
| 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）操作系统时采用用户名+SSHKey公私钥进行身份鉴别鉴别信息具有复杂度要求；2）执行cat /etc/shadow命令，查看shadow文件系统内用户身份标识唯一，不存在同名用户，且不存在空口令账号；3）经访谈，SSHKey公私钥每半年进行更换；4）查看sshd\_config配置文件中配置PasswordAuthentication no，拒绝使用密码方式进行身份鉴别。 |
| 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； | 操作系统采用用户名+SSHKey公私钥进行身份鉴别，可以防止鉴别信息被暴力破解；但未配置用户连接超时退出策略。 |
| 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； | 1）经核查，管理人员采用SSH协议连接操作系统；2）执行netatat –tpln| grep 23命令查看操作系统远程管理端口，不存在Telnet端口，防止鉴别信息在网络传输过程中的被窃听。 |
| 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。 | 未采用两种或两种以上组合的鉴别技术对用户进行身份鉴别。 |
| 访问控制 | a）应对登录的用户分配账户和权限； | 1）经访谈，通过root账户为登录的用户创建账户、分配权限；2）执行ls -l命令查看关键文件权限，均已为账户分配了相应权限，相关文件权限设置为/etc/shadow：000、/etc/passwd：644、/etc/group：644、/etc/profile：644、/etc/crontab：644、/ etc/securetty：600、/etc/ssh/sshd\_config：600。 |
| b）应重命名或删除默认账户，修改默认账户的默认口令； | 1）执行cat /etc/shadow命令查看shadow文件，操作系统中adm、lp、sync、shutdown、halt、mail、uucp、operator、games、gopher等账户均为nologin状态，存在默认账户root；2）执行more /etc/ssh/sshd\_config命令，查看“PermitRootLogin”参数设置为“yes”，即允许root远程登录；3）经访谈，root用户需通过公私钥方式进行身份鉴别。 |
| 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； | 1）执行cat /etc/shadow命令查看shadow文件，发现操作系统存在root、ysup、yops、yluser等在用账户，不存在多余的、过期账户；2）存在多个堡垒机账户登录操作系统时共用一个账户的情况。 |
| 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； | root账户具有系统所有权限，未实现管理用户的权限分离。 |
| e）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； | 经访谈，由系统管理员root配置访问控制策略，如：/etc/passwd，/etc/profile宿主为root、权限设置为644，audit文件为700、message文件为600，其他文件权限为750，实现用户对文件的权限控制。 |
| f）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； | 由管理用户进行用户访问权限分配进行设置，依据访问控制策略,对各类文件进行访问，重要文件和目录权限均在合理范围内，用户可根据文件不同的权限进行操作。 |
| g）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。 | 执 行more /etc/selinux/config 命令，查看config文件显示 SELINUX参数为 DISABLED，即未开启强制访问控制模式。 |
| 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）执行ps -ef|grep rsyslog和ps -ef|grep auditd命令，显示rsyslog和auditd进程正在运行；2）more /etc/audit/audit.rules，显示审计内容包括：\*.info、authriv.\*、mail.\*、cron.\*、\*.emerg、uucp、news.crit、local7.\*等事件。 |
| 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； | 执行tail -20 /var/log/audit/audit.log命令，查看近20条审计日志，内容包括：时间、对象、路径、用户ID、相关的系统调用、用户执行命令等。 |
| 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）通过访问权限对审计记录进行保护，日志文件/var/log/messages、/var/log/secure、/var/log/audit/audit.log访问 权限均为600；2）审计记录本地保存，且实时备份至360本地安全大脑，保存时间满足180天以上。 |
| d）应对审计进程进行保护，防止未经授权的中断。 | 执行service auditd status命令，系统开启auditd审计保护进程，审计进程由root用户维护，经现场使用yluser用户通过service auditd stop命令尝试中断审计进程，无法将审计进程单独中断。 |
| 入侵防范 | a）应遵循最小安装的原则，仅安装需要的组件和应用程序； | 1）系统安装遵循最小化安装原则；2）执行yum list installed命令查看操作系统已安装的程序包，存在Java、oracle、SSH、天眼云镜agent等应用程序或组件，不存在与业务系统无关的组件和应用程序。 |
| b）应关闭不需要的系统服务、默认共享和高危端口； | 1）执行systemctl list-unit-files 命令，系统已关闭FTP、Telnet 等高危网络服务；2）执行netstat -pantu命令，系统关闭了135、445等高危端口，仅开启了22、1521等端口。 |
| c）应通过设定终端接入方式或网络地址范围对通过网络进行管理的管理终端进行限制； | 经核查，1）通过配置安全组策略限制仅允许通过堡垒机管理服务器；2）经核查防火墙中访问控制策略，具备堡垒机地址-服务器管理网段（10.33.0.0）的访问控制策略。 |
| d）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； | 根据GB∕T 28448-2019 《信息安全技术 网络安全等级保护测评要求》测评对象范围描述，服务器无该项要求，故判为“不适用”。 |
| e）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； | 1）经过漏洞扫描，服务器不存在高危安全漏洞；2）执行rpm -qa grep patch命令，查看系统补丁已更新至最新。 |
| f）应能够检测到对重要节点进行入侵的行为，并在发生严重入侵事件时提供报警。 | 经核查，服务器上安装有青藤云天眼云镜，对主机入侵行为进行检测，发现严重安全事件时通过钉钉告警。 |
| 恶意代码防范 | a）应采用免受恶意代码攻击的技术措施或主动免疫可信验证机制及时识别入侵和病毒行为，并将其有效阻断。 | 经核查，服务器上安装有青藤云天眼云镜，对主机恶意代码进行检测、清除，每天凌晨自动更新恶意代码特征库，经核查，具备恶意代码特征库更新记录。 |
| 可信验证 | a）可基于可信根对计算设备的系统引导程序、系统程序、重要配置参数和应用程序等进行可信验证，并在应用程序的关键执行环节进行动态可信验证，在检测到其可信性受到破坏后进行报警，并将验证结果形成审计记录送至安全管理中心。 | 未采用技术措施对计算设备的系统引导程序、系统程序、重要配置参数和通信应用程序等进行可信验证。 |
| 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； | 采用SSH协议连接操作系统，保证了鉴别信息以及管理数据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。 | 操作系统中对重要鉴别信息通过自身的加密及校验（SHA256），保证数据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； | 采用SSH协议连接操作系统，保证了鉴别信息以及管理数据在传输过程中的保密性。 |
| b）应采用密码技术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个人信息等。 | 通过系统自带的加密模块保证鉴别数据在存储过程中的保密性。 |
| 数据备份恢复 | a）应提供重要数据的本地数据备份与恢复功能； | 经核查，通过脚本每周将配置文件、代码仓库等数据备份至备份服务器中，依据需要验证备份数据的有效性。 |
| b）应提供异地实时备份功能，利用通信网络将重要数据实时备份至备份场地； | 系统无异地备份机制。 |
| c）应提供重要数据处理系统的热冗余，保证系统的高可用性。 | 服务器采用集群方式部署，保证系统的高可用性。 |
| 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； | 操作系统提供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功能。 |
| 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。 | 操作系统提供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的功能。 |

4.1.3.97. 综合业务库集群节点1

|  |  |  |
| --- | --- | --- |
| **安全控制点** | **测评指标** | **结果记录** |
| 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）操作系统时采用用户名+SSHKey公私钥进行身份鉴别鉴别信息具有复杂度要求；2）执行cat /etc/shadow命令，查看shadow文件系统内用户身份标识唯一，不存在同名用户，且不存在空口令账号；3）经访谈，SSHKey公私钥每半年进行更换；4）查看sshd\_config配置文件中配置PasswordAuthentication no，拒绝使用密码方式进行身份鉴别。 |
| 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； | 操作系统采用用户名+SSHKey公私钥进行身份鉴别，可以防止鉴别信息被暴力破解；但未配置用户连接超时退出策略。 |
| 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； | 1）经核查，管理人员采用SSH协议连接操作系统；2）执行netatat –tpln| grep 23命令查看操作系统远程管理端口，不存在Telnet端口，防止鉴别信息在网络传输过程中的被窃听。 |
| 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。 | 未采用两种或两种以上组合的鉴别技术对用户进行身份鉴别。 |
| 访问控制 | a）应对登录的用户分配账户和权限； | 1）经访谈，通过root账户为登录的用户创建账户、分配权限；2）执行ls -l命令查看关键文件权限，均已为账户分配了相应权限，相关文件权限设置为/etc/shadow：000、/etc/passwd：644、/etc/group：644、/etc/profile：644、/etc/crontab：644、/ etc/securetty：600、/etc/ssh/sshd\_config：600。 |
| b）应重命名或删除默认账户，修改默认账户的默认口令； | 1）执行cat /etc/shadow命令查看shadow文件，操作系统中adm、lp、sync、shutdown、halt、mail、uucp、operator、games、gopher等账户均为nologin状态，存在默认账户root；2）执行more /etc/ssh/sshd\_config命令，查看“PermitRootLogin”参数设置为“yes”，即允许root远程登录；3）经访谈，root用户需通过公私钥方式进行身份鉴别。 |
| 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； | 1）执行cat /etc/shadow命令查看shadow文件，发现操作系统存在root、ysup、yops、yluser等在用账户，不存在多余的、过期账户；2）存在多个堡垒机账户登录操作系统时共用一个账户的情况。 |
| 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； | root账户具有系统所有权限，未实现管理用户的权限分离。 |
| e）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； | 经访谈，由系统管理员root配置访问控制策略，如：/etc/passwd，/etc/profile宿主为root、权限设置为644，audit文件为700、message文件为600，其他文件权限为750，实现用户对文件的权限控制。 |
| f）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； | 由管理用户进行用户访问权限分配进行设置，依据访问控制策略,对各类文件进行访问，重要文件和目录权限均在合理范围内，用户可根据文件不同的权限进行操作。 |
| g）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。 | 执 行more /etc/selinux/config 命令，查看config文件显示 SELINUX参数为 DISABLED，即未开启强制访问控制模式。 |
| 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）执行ps -ef|grep rsyslog和ps -ef|grep auditd命令，显示rsyslog和auditd进程正在运行；2）more /etc/audit/audit.rules，显示审计内容包括：\*.info、authriv.\*、mail.\*、cron.\*、\*.emerg、uucp、news.crit、local7.\*等事件。 |
| 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； | 执行tail -20 /var/log/audit/audit.log命令，查看近20条审计日志，内容包括：时间、对象、路径、用户ID、相关的系统调用、用户执行命令等。 |
| 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）通过访问权限对审计记录进行保护，日志文件/var/log/messages、/var/log/secure、/var/log/audit/audit.log访问 权限均为600；2）审计记录本地保存，且实时备份至360本地安全大脑，保存时间满足180天以上。 |
| d）应对审计进程进行保护，防止未经授权的中断。 | 执行service auditd status命令，系统开启auditd审计保护进程，审计进程由root用户维护，经现场使用yluser用户通过service auditd stop命令尝试中断审计进程，无法将审计进程单独中断。 |
| 入侵防范 | a）应遵循最小安装的原则，仅安装需要的组件和应用程序； | 1）系统安装遵循最小化安装原则；2）执行yum list installed命令查看操作系统已安装的程序包，存在Java、oracle、SSH、天眼云镜agent等应用程序或组件，不存在与业务系统无关的组件和应用程序。 |
| b）应关闭不需要的系统服务、默认共享和高危端口； | 1）执行systemctl list-unit-files 命令，系统已关闭FTP、Telnet 等高危网络服务；2）执行netstat -pantu命令，系统关闭了135、445等高危端口，仅开启了22、1521等端口。 |
| c）应通过设定终端接入方式或网络地址范围对通过网络进行管理的管理终端进行限制； | 经核查，1）通过配置安全组策略限制仅允许通过堡垒机管理服务器；2）经核查防火墙中访问控制策略，具备堡垒机地址-服务器管理网段（10.33.0.0）的访问控制策略。 |
| d）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； | 根据GB∕T 28448-2019 《信息安全技术 网络安全等级保护测评要求》测评对象范围描述，服务器无该项要求，故判为“不适用”。 |
| e）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； | 1）经过漏洞扫描，服务器不存在高危安全漏洞；2）执行rpm -qa grep patch命令，查看系统补丁已更新至最新。 |
| f）应能够检测到对重要节点进行入侵的行为，并在发生严重入侵事件时提供报警。 | 经核查，服务器上安装有青藤云天眼云镜，对主机入侵行为进行检测，发现严重安全事件时通过钉钉告警。 |
| 恶意代码防范 | a）应采用免受恶意代码攻击的技术措施或主动免疫可信验证机制及时识别入侵和病毒行为，并将其有效阻断。 | 经核查，服务器上安装有青藤云天眼云镜，对主机恶意代码进行检测、清除，每天凌晨自动更新恶意代码特征库，经核查，具备恶意代码特征库更新记录。 |
| 可信验证 | a）可基于可信根对计算设备的系统引导程序、系统程序、重要配置参数和应用程序等进行可信验证，并在应用程序的关键执行环节进行动态可信验证，在检测到其可信性受到破坏后进行报警，并将验证结果形成审计记录送至安全管理中心。 | 未采用技术措施对计算设备的系统引导程序、系统程序、重要配置参数和通信应用程序等进行可信验证。 |
| 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； | 采用SSH协议连接操作系统，保证了鉴别信息以及管理数据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。 | 操作系统中对重要鉴别信息通过自身的加密及校验（SHA256），保证数据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； | 采用SSH协议连接操作系统，保证了鉴别信息以及管理数据在传输过程中的保密性。 |
| b）应采用密码技术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个人信息等。 | 通过系统自带的加密模块保证鉴别数据在存储过程中的保密性。 |
| 数据备份恢复 | a）应提供重要数据的本地数据备份与恢复功能； | 经核查，通过脚本每周将配置文件、代码仓库等数据备份至备份服务器中，依据需要验证备份数据的有效性。 |
| b）应提供异地实时备份功能，利用通信网络将重要数据实时备份至备份场地； | 系统无异地备份机制。 |
| c）应提供重要数据处理系统的热冗余，保证系统的高可用性。 | 服务器采用集群方式部署，保证系统的高可用性。 |
| 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； | 操作系统提供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功能。 |
| 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。 | 操作系统提供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的功能。 |

4.1.3.98. 综合业务库集群节点2

|  |  |  |
| --- | --- | --- |
| **安全控制点** | **测评指标** | **结果记录** |
| 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）操作系统时采用用户名+SSHKey公私钥进行身份鉴别鉴别信息具有复杂度要求；2）执行cat /etc/shadow命令，查看shadow文件系统内用户身份标识唯一，不存在同名用户，且不存在空口令账号；3）经访谈，SSHKey公私钥每半年进行更换；4）查看sshd\_config配置文件中配置PasswordAuthentication no，拒绝使用密码方式进行身份鉴别。 |
| 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； | 操作系统采用用户名+SSHKey公私钥进行身份鉴别，可以防止鉴别信息被暴力破解；但未配置用户连接超时退出策略。 |
| 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； | 1）经核查，管理人员采用SSH协议连接操作系统；2）执行netatat –tpln| grep 23命令查看操作系统远程管理端口，不存在Telnet端口，防止鉴别信息在网络传输过程中的被窃听。 |
| 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。 | 未采用两种或两种以上组合的鉴别技术对用户进行身份鉴别。 |
| 访问控制 | a）应对登录的用户分配账户和权限； | 1）经访谈，通过root账户为登录的用户创建账户、分配权限；2）执行ls -l命令查看关键文件权限，均已为账户分配了相应权限，相关文件权限设置为/etc/shadow：000、/etc/passwd：644、/etc/group：644、/etc/profile：644、/etc/crontab：644、/ etc/securetty：600、/etc/ssh/sshd\_config：600。 |
| b）应重命名或删除默认账户，修改默认账户的默认口令； | 1）执行cat /etc/shadow命令查看shadow文件，操作系统中adm、lp、sync、shutdown、halt、mail、uucp、operator、games、gopher等账户均为nologin状态，存在默认账户root；2）执行more /etc/ssh/sshd\_config命令，查看“PermitRootLogin”参数设置为“yes”，即允许root远程登录；3）经访谈，root用户需通过公私钥方式进行身份鉴别。 |
| 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； | 1）执行cat /etc/shadow命令查看shadow文件，发现操作系统存在root、ysup、yops、yluser等在用账户，不存在多余的、过期账户；2）存在多个堡垒机账户登录操作系统时共用一个账户的情况。 |
| 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； | root账户具有系统所有权限，未实现管理用户的权限分离。 |
| e）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； | 经访谈，由系统管理员root配置访问控制策略，如：/etc/passwd，/etc/profile宿主为root、权限设置为644，audit文件为700、message文件为600，其他文件权限为750，实现用户对文件的权限控制。 |
| f）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； | 由管理用户进行用户访问权限分配进行设置，依据访问控制策略,对各类文件进行访问，重要文件和目录权限均在合理范围内，用户可根据文件不同的权限进行操作。 |
| g）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。 | 执 行more /etc/selinux/config 命令，查看config文件显示 SELINUX参数为 DISABLED，即未开启强制访问控制模式。 |
| 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）执行ps -ef|grep rsyslog和ps -ef|grep auditd命令，显示rsyslog和auditd进程正在运行；2）more /etc/audit/audit.rules，显示审计内容包括：\*.info、authriv.\*、mail.\*、cron.\*、\*.emerg、uucp、news.crit、local7.\*等事件。 |
| 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； | 执行tail -20 /var/log/audit/audit.log命令，查看近20条审计日志，内容包括：时间、对象、路径、用户ID、相关的系统调用、用户执行命令等。 |
| 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）通过访问权限对审计记录进行保护，日志文件/var/log/messages、/var/log/secure、/var/log/audit/audit.log访问 权限均为600；2）审计记录本地保存，且实时备份至360本地安全大脑，保存时间满足180天以上。 |
| d）应对审计进程进行保护，防止未经授权的中断。 | 执行service auditd status命令，系统开启auditd审计保护进程，审计进程由root用户维护，经现场使用yluser用户通过service auditd stop命令尝试中断审计进程，无法将审计进程单独中断。 |
| 入侵防范 | a）应遵循最小安装的原则，仅安装需要的组件和应用程序； | 1）系统安装遵循最小化安装原则；2）执行yum list installed命令查看操作系统已安装的程序包，存在Java、oracle、SSH、天眼云镜agent等应用程序或组件，不存在与业务系统无关的组件和应用程序。 |
| b）应关闭不需要的系统服务、默认共享和高危端口； | 1）执行systemctl list-unit-files 命令，系统已关闭FTP、Telnet 等高危网络服务；2）执行netstat -pantu命令，系统关闭了135、445等高危端口，仅开启了22、1521等端口。 |
| c）应通过设定终端接入方式或网络地址范围对通过网络进行管理的管理终端进行限制； | 经核查，1）通过配置安全组策略限制仅允许通过堡垒机管理服务器；2）经核查防火墙中访问控制策略，具备堡垒机地址-服务器管理网段（10.33.0.0）的访问控制策略。 |
| d）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； | 根据GB∕T 28448-2019 《信息安全技术 网络安全等级保护测评要求》测评对象范围描述，服务器无该项要求，故判为“不适用”。 |
| e）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； | 1）经过漏洞扫描，服务器不存在高危安全漏洞；2）执行rpm -qa grep patch命令，查看系统补丁已更新至最新。 |
| f）应能够检测到对重要节点进行入侵的行为，并在发生严重入侵事件时提供报警。 | 经核查，服务器上安装有青藤云天眼云镜，对主机入侵行为进行检测，发现严重安全事件时通过钉钉告警。 |
| 恶意代码防范 | a）应采用免受恶意代码攻击的技术措施或主动免疫可信验证机制及时识别入侵和病毒行为，并将其有效阻断。 | 经核查，服务器上安装有青藤云天眼云镜，对主机恶意代码进行检测、清除，每天凌晨自动更新恶意代码特征库，经核查，具备恶意代码特征库更新记录。 |
| 可信验证 | a）可基于可信根对计算设备的系统引导程序、系统程序、重要配置参数和应用程序等进行可信验证，并在应用程序的关键执行环节进行动态可信验证，在检测到其可信性受到破坏后进行报警，并将验证结果形成审计记录送至安全管理中心。 | 未采用技术措施对计算设备的系统引导程序、系统程序、重要配置参数和通信应用程序等进行可信验证。 |
| 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； | 采用SSH协议连接操作系统，保证了鉴别信息以及管理数据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。 | 操作系统中对重要鉴别信息通过自身的加密及校验（SHA256），保证数据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； | 采用SSH协议连接操作系统，保证了鉴别信息以及管理数据在传输过程中的保密性。 |
| b）应采用密码技术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个人信息等。 | 通过系统自带的加密模块保证鉴别数据在存储过程中的保密性。 |
| 数据备份恢复 | a）应提供重要数据的本地数据备份与恢复功能； | 经核查，通过脚本每周将配置文件、代码仓库等数据备份至备份服务器中，依据需要验证备份数据的有效性。 |
| b）应提供异地实时备份功能，利用通信网络将重要数据实时备份至备份场地； | 系统无异地备份机制。 |
| c）应提供重要数据处理系统的热冗余，保证系统的高可用性。 | 服务器采用集群方式部署，保证系统的高可用性。 |
| 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； | 操作系统提供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功能。 |
| 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。 | 操作系统提供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的功能。 |

4.1.3.99. 自动化库主库

|  |  |  |
| --- | --- | --- |
| **安全控制点** | **测评指标** | **结果记录** |
| 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）操作系统时采用用户名+SSHKey公私钥进行身份鉴别鉴别信息具有复杂度要求；2）执行cat /etc/shadow命令，查看shadow文件系统内用户身份标识唯一，不存在同名用户，且不存在空口令账号；3）经访谈，SSHKey公私钥每半年进行更换；4）查看sshd\_config配置文件中配置PasswordAuthentication no，拒绝使用密码方式进行身份鉴别。 |
| 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； | 操作系统采用用户名+SSHKey公私钥进行身份鉴别，可以防止鉴别信息被暴力破解；但未配置用户连接超时退出策略。 |
| 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； | 1）经核查，管理人员采用SSH协议连接操作系统；2）执行netatat –tpln| grep 23命令查看操作系统远程管理端口，不存在Telnet端口，防止鉴别信息在网络传输过程中的被窃听。 |
| 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。 | 未采用两种或两种以上组合的鉴别技术对用户进行身份鉴别。 |
| 访问控制 | a）应对登录的用户分配账户和权限； | 1）经访谈，通过root账户为登录的用户创建账户、分配权限；2）执行ls -l命令查看关键文件权限，均已为账户分配了相应权限，相关文件权限设置为/etc/shadow：000、/etc/passwd：644、/etc/group：644、/etc/profile：644、/etc/crontab：644、/ etc/securetty：600、/etc/ssh/sshd\_config：600。 |
| b）应重命名或删除默认账户，修改默认账户的默认口令； | 1）执行cat /etc/shadow命令查看shadow文件，操作系统中adm、lp、sync、shutdown、halt、mail、uucp、operator、games、gopher等账户均为nologin状态，存在默认账户root；2）执行more /etc/ssh/sshd\_config命令，查看“PermitRootLogin”参数设置为“yes”，即允许root远程登录；3）经访谈，root用户需通过公私钥方式进行身份鉴别。 |
| 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； | 1）执行cat /etc/shadow命令查看shadow文件，发现操作系统存在root、ysup、yops、yluser等在用账户，不存在多余的、过期账户；2）存在多个堡垒机账户登录操作系统时共用一个账户的情况。 |
| 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； | root账户具有系统所有权限，未实现管理用户的权限分离。 |
| e）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； | 经访谈，由系统管理员root配置访问控制策略，如：/etc/passwd，/etc/profile宿主为root、权限设置为644，audit文件为700、message文件为600，其他文件权限为750，实现用户对文件的权限控制。 |
| f）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； | 由管理用户进行用户访问权限分配进行设置，依据访问控制策略,对各类文件进行访问，重要文件和目录权限均在合理范围内，用户可根据文件不同的权限进行操作。 |
| g）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。 | 执 行more /etc/selinux/config 命令，查看config文件显示 SELINUX参数为 DISABLED，即未开启强制访问控制模式。 |
| 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）执行ps -ef|grep rsyslog和ps -ef|grep auditd命令，显示rsyslog和auditd进程正在运行；2）more /etc/audit/audit.rules，显示审计内容包括：\*.info、authriv.\*、mail.\*、cron.\*、\*.emerg、uucp、news.crit、local7.\*等事件。 |
| 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； | 执行tail -20 /var/log/audit/audit.log命令，查看近20条审计日志，内容包括：时间、对象、路径、用户ID、相关的系统调用、用户执行命令等。 |
| 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）通过访问权限对审计记录进行保护，日志文件/var/log/messages、/var/log/secure、/var/log/audit/audit.log访问 权限均为600；2）审计记录本地保存，且实时备份至360本地安全大脑，保存时间满足180天以上。 |
| d）应对审计进程进行保护，防止未经授权的中断。 | 执行service auditd status命令，系统开启auditd审计保护进程，审计进程由root用户维护，经现场使用yluser用户通过service auditd stop命令尝试中断审计进程，无法将审计进程单独中断。 |
| 入侵防范 | a）应遵循最小安装的原则，仅安装需要的组件和应用程序； | 1）系统安装遵循最小化安装原则；2）执行yum list installed命令查看操作系统已安装的程序包，存在Java、oracle、SSH、天眼云镜agent等应用程序或组件，不存在与业务系统无关的组件和应用程序。 |
| b）应关闭不需要的系统服务、默认共享和高危端口； | 1）执行systemctl list-unit-files 命令，系统已关闭FTP、Telnet 等高危网络服务；2）执行netstat -pantu命令，系统关闭了135、445等高危端口，仅开启了22、1521等端口。 |
| c）应通过设定终端接入方式或网络地址范围对通过网络进行管理的管理终端进行限制； | 经核查，1）通过配置安全组策略限制仅允许通过堡垒机管理服务器；2）经核查防火墙中访问控制策略，具备堡垒机地址-服务器管理网段（10.33.0.0）的访问控制策略。 |
| d）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； | 根据GB∕T 28448-2019 《信息安全技术 网络安全等级保护测评要求》测评对象范围描述，服务器无该项要求，故判为“不适用”。 |
| e）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； | 1）经过漏洞扫描，服务器不存在高危安全漏洞；2）执行rpm -qa grep patch命令，查看系统补丁已更新至最新。 |
| f）应能够检测到对重要节点进行入侵的行为，并在发生严重入侵事件时提供报警。 | 经核查，服务器上安装有青藤云天眼云镜，对主机入侵行为进行检测，发现严重安全事件时通过钉钉告警。 |
| 恶意代码防范 | a）应采用免受恶意代码攻击的技术措施或主动免疫可信验证机制及时识别入侵和病毒行为，并将其有效阻断。 | 经核查，服务器上安装有青藤云天眼云镜，对主机恶意代码进行检测、清除，每天凌晨自动更新恶意代码特征库，经核查，具备恶意代码特征库更新记录。 |
| 可信验证 | a）可基于可信根对计算设备的系统引导程序、系统程序、重要配置参数和应用程序等进行可信验证，并在应用程序的关键执行环节进行动态可信验证，在检测到其可信性受到破坏后进行报警，并将验证结果形成审计记录送至安全管理中心。 | 未采用技术措施对计算设备的系统引导程序、系统程序、重要配置参数和通信应用程序等进行可信验证。 |
| 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； | 采用SSH协议连接操作系统，保证了鉴别信息以及管理数据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。 | 操作系统中对重要鉴别信息通过自身的加密及校验（SHA256），保证数据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； | 采用SSH协议连接操作系统，保证了鉴别信息以及管理数据在传输过程中的保密性。 |
| b）应采用密码技术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个人信息等。 | 通过系统自带的加密模块保证鉴别数据在存储过程中的保密性。 |
| 数据备份恢复 | a）应提供重要数据的本地数据备份与恢复功能； | 经核查，通过脚本每周将配置文件、代码仓库等数据备份至备份服务器中，依据需要验证备份数据的有效性。 |
| b）应提供异地实时备份功能，利用通信网络将重要数据实时备份至备份场地； | 系统无异地备份机制。 |
| c）应提供重要数据处理系统的热冗余，保证系统的高可用性。 | 服务器采用集群方式部署，保证系统的高可用性。 |
| 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； | 操作系统提供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功能。 |
| 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。 | 操作系统提供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的功能。 |

4.1.3.100. 自动化库备库

|  |  |  |
| --- | --- | --- |
| **安全控制点** | **测评指标** | **结果记录** |
| 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）操作系统时采用用户名+SSHKey公私钥进行身份鉴别鉴别信息具有复杂度要求；2）执行cat /etc/shadow命令，查看shadow文件系统内用户身份标识唯一，不存在同名用户，且不存在空口令账号；3）经访谈，SSHKey公私钥每半年进行更换；4）查看sshd\_config配置文件中配置PasswordAuthentication no，拒绝使用密码方式进行身份鉴别。 |
| 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； | 操作系统采用用户名+SSHKey公私钥进行身份鉴别，可以防止鉴别信息被暴力破解；但未配置用户连接超时退出策略。 |
| 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； | 1）经核查，管理人员采用SSH协议连接操作系统；2）执行netatat –tpln| grep 23命令查看操作系统远程管理端口，不存在Telnet端口，防止鉴别信息在网络传输过程中的被窃听。 |
| 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。 | 未采用两种或两种以上组合的鉴别技术对用户进行身份鉴别。 |
| 访问控制 | a）应对登录的用户分配账户和权限； | 1）经访谈，通过root账户为登录的用户创建账户、分配权限；2）执行ls -l命令查看关键文件权限，均已为账户分配了相应权限，相关文件权限设置为/etc/shadow：000、/etc/passwd：644、/etc/group：644、/etc/profile：644、/etc/crontab：644、/ etc/securetty：600、/etc/ssh/sshd\_config：600。 |
| b）应重命名或删除默认账户，修改默认账户的默认口令； | 1）执行cat /etc/shadow命令查看shadow文件，操作系统中adm、lp、sync、shutdown、halt、mail、uucp、operator、games、gopher等账户均为nologin状态，存在默认账户root；2）执行more /etc/ssh/sshd\_config命令，查看“PermitRootLogin”参数设置为“yes”，即允许root远程登录；3）经访谈，root用户需通过公私钥方式进行身份鉴别。 |
| 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； | 1）执行cat /etc/shadow命令查看shadow文件，发现操作系统存在root、ysup、yops、yluser等在用账户，不存在多余的、过期账户；2）存在多个堡垒机账户登录操作系统时共用一个账户的情况。 |
| 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； | root账户具有系统所有权限，未实现管理用户的权限分离。 |
| e）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； | 经访谈，由系统管理员root配置访问控制策略，如：/etc/passwd，/etc/profile宿主为root、权限设置为644，audit文件为700、message文件为600，其他文件权限为750，实现用户对文件的权限控制。 |
| f）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； | 由管理用户进行用户访问权限分配进行设置，依据访问控制策略,对各类文件进行访问，重要文件和目录权限均在合理范围内，用户可根据文件不同的权限进行操作。 |
| g）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。 | 执 行more /etc/selinux/config 命令，查看config文件显示 SELINUX参数为 DISABLED，即未开启强制访问控制模式。 |
| 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）执行ps -ef|grep rsyslog和ps -ef|grep auditd命令，显示rsyslog和auditd进程正在运行；2）more /etc/audit/audit.rules，显示审计内容包括：\*.info、authriv.\*、mail.\*、cron.\*、\*.emerg、uucp、news.crit、local7.\*等事件。 |
| 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； | 执行tail -20 /var/log/audit/audit.log命令，查看近20条审计日志，内容包括：时间、对象、路径、用户ID、相关的系统调用、用户执行命令等。 |
| 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）通过访问权限对审计记录进行保护，日志文件/var/log/messages、/var/log/secure、/var/log/audit/audit.log访问 权限均为600；2）审计记录本地保存，且实时备份至360本地安全大脑，保存时间满足180天以上。 |
| d）应对审计进程进行保护，防止未经授权的中断。 | 执行service auditd status命令，系统开启auditd审计保护进程，审计进程由root用户维护，经现场使用yluser用户通过service auditd stop命令尝试中断审计进程，无法将审计进程单独中断。 |
| 入侵防范 | a）应遵循最小安装的原则，仅安装需要的组件和应用程序； | 1）系统安装遵循最小化安装原则；2）执行yum list installed命令查看操作系统已安装的程序包，存在Java、oracle、SSH、天眼云镜agent等应用程序或组件，不存在与业务系统无关的组件和应用程序。 |
| b）应关闭不需要的系统服务、默认共享和高危端口； | 1）执行systemctl list-unit-files 命令，系统已关闭FTP、Telnet 等高危网络服务；2）执行netstat -pantu命令，系统关闭了135、445等高危端口，仅开启了22、1521等端口。 |
| c）应通过设定终端接入方式或网络地址范围对通过网络进行管理的管理终端进行限制； | 经核查，1）通过配置安全组策略限制仅允许通过堡垒机管理服务器；2）经核查防火墙中访问控制策略，具备堡垒机地址-服务器管理网段（10.33.0.0）的访问控制策略。 |
| d）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； | 根据GB∕T 28448-2019 《信息安全技术 网络安全等级保护测评要求》测评对象范围描述，服务器无该项要求，故判为“不适用”。 |
| e）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； | 1）经过漏洞扫描，服务器不存在高危安全漏洞；2）执行rpm -qa grep patch命令，查看系统补丁已更新至最新。 |
| f）应能够检测到对重要节点进行入侵的行为，并在发生严重入侵事件时提供报警。 | 经核查，服务器上安装有青藤云天眼云镜，对主机入侵行为进行检测，发现严重安全事件时通过钉钉告警。 |
| 恶意代码防范 | a）应采用免受恶意代码攻击的技术措施或主动免疫可信验证机制及时识别入侵和病毒行为，并将其有效阻断。 | 经核查，服务器上安装有青藤云天眼云镜，对主机恶意代码进行检测、清除，每天凌晨自动更新恶意代码特征库，经核查，具备恶意代码特征库更新记录。 |
| 可信验证 | a）可基于可信根对计算设备的系统引导程序、系统程序、重要配置参数和应用程序等进行可信验证，并在应用程序的关键执行环节进行动态可信验证，在检测到其可信性受到破坏后进行报警，并将验证结果形成审计记录送至安全管理中心。 | 未采用技术措施对计算设备的系统引导程序、系统程序、重要配置参数和通信应用程序等进行可信验证。 |
| 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； | 采用SSH协议连接操作系统，保证了鉴别信息以及管理数据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。 | 操作系统中对重要鉴别信息通过自身的加密及校验（SHA256），保证数据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； | 采用SSH协议连接操作系统，保证了鉴别信息以及管理数据在传输过程中的保密性。 |
| b）应采用密码技术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个人信息等。 | 通过系统自带的加密模块保证鉴别数据在存储过程中的保密性。 |
| 数据备份恢复 | a）应提供重要数据的本地数据备份与恢复功能； | 经核查，通过脚本每周将配置文件、代码仓库等数据备份至备份服务器中，依据需要验证备份数据的有效性。 |
| b）应提供异地实时备份功能，利用通信网络将重要数据实时备份至备份场地； | 系统无异地备份机制。 |
| c）应提供重要数据处理系统的热冗余，保证系统的高可用性。 | 服务器采用集群方式部署，保证系统的高可用性。 |
| 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； | 操作系统提供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功能。 |
| 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。 | 操作系统提供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的功能。 |

4.1.3.101. 实名制库主库

|  |  |  |
| --- | --- | --- |
| **安全控制点** | **测评指标** | **结果记录** |
| 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）操作系统时采用用户名+SSHKey公私钥进行身份鉴别鉴别信息具有复杂度要求；2）执行cat /etc/shadow命令，查看shadow文件系统内用户身份标识唯一，不存在同名用户，且不存在空口令账号；3）经访谈，SSHKey公私钥每半年进行更换；4）查看sshd\_config配置文件中配置PasswordAuthentication no，拒绝使用密码方式进行身份鉴别。 |
| 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； | 操作系统采用用户名+SSHKey公私钥进行身份鉴别，可以防止鉴别信息被暴力破解；但未配置用户连接超时退出策略。 |
| 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； | 1）经核查，管理人员采用SSH协议连接操作系统；2）执行netatat –tpln| grep 23命令查看操作系统远程管理端口，不存在Telnet端口，防止鉴别信息在网络传输过程中的被窃听。 |
| 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。 | 未采用两种或两种以上组合的鉴别技术对用户进行身份鉴别。 |
| 访问控制 | a）应对登录的用户分配账户和权限； | 1）经访谈，通过root账户为登录的用户创建账户、分配权限；2）执行ls -l命令查看关键文件权限，均已为账户分配了相应权限，相关文件权限设置为/etc/shadow：000、/etc/passwd：644、/etc/group：644、/etc/profile：644、/etc/crontab：644、/ etc/securetty：600、/etc/ssh/sshd\_config：600。 |
| b）应重命名或删除默认账户，修改默认账户的默认口令； | 1）执行cat /etc/shadow命令查看shadow文件，操作系统中adm、lp、sync、shutdown、halt、mail、uucp、operator、games、gopher等账户均为nologin状态，存在默认账户root；2）执行more /etc/ssh/sshd\_config命令，查看“PermitRootLogin”参数设置为“yes”，即允许root远程登录；3）经访谈，root用户需通过公私钥方式进行身份鉴别。 |
| 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； | 1）执行cat /etc/shadow命令查看shadow文件，发现操作系统存在root、ysup、yops、yluser等在用账户，不存在多余的、过期账户；2）存在多个堡垒机账户登录操作系统时共用一个账户的情况。 |
| 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； | root账户具有系统所有权限，未实现管理用户的权限分离。 |
| e）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； | 经访谈，由系统管理员root配置访问控制策略，如：/etc/passwd，/etc/profile宿主为root、权限设置为644，audit文件为700、message文件为600，其他文件权限为750，实现用户对文件的权限控制。 |
| f）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； | 由管理用户进行用户访问权限分配进行设置，依据访问控制策略,对各类文件进行访问，重要文件和目录权限均在合理范围内，用户可根据文件不同的权限进行操作。 |
| g）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。 | 执 行more /etc/selinux/config 命令，查看config文件显示 SELINUX参数为 DISABLED，即未开启强制访问控制模式。 |
| 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）执行ps -ef|grep rsyslog和ps -ef|grep auditd命令，显示rsyslog和auditd进程正在运行；2）more /etc/audit/audit.rules，显示审计内容包括：\*.info、authriv.\*、mail.\*、cron.\*、\*.emerg、uucp、news.crit、local7.\*等事件。 |
| 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； | 执行tail -20 /var/log/audit/audit.log命令，查看近20条审计日志，内容包括：时间、对象、路径、用户ID、相关的系统调用、用户执行命令等。 |
| 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）通过访问权限对审计记录进行保护，日志文件/var/log/messages、/var/log/secure、/var/log/audit/audit.log访问 权限均为600；2）审计记录本地保存，且实时备份至360本地安全大脑，保存时间满足180天以上。 |
| d）应对审计进程进行保护，防止未经授权的中断。 | 执行service auditd status命令，系统开启auditd审计保护进程，审计进程由root用户维护，经现场使用yluser用户通过service auditd stop命令尝试中断审计进程，无法将审计进程单独中断。 |
| 入侵防范 | a）应遵循最小安装的原则，仅安装需要的组件和应用程序； | 1）系统安装遵循最小化安装原则；2）执行yum list installed命令查看操作系统已安装的程序包，存在Java、oracle、SSH、天眼云镜agent等应用程序或组件，不存在与业务系统无关的组件和应用程序。 |
| b）应关闭不需要的系统服务、默认共享和高危端口； | 1）执行systemctl list-unit-files 命令，系统已关闭FTP、Telnet 等高危网络服务；2）执行netstat -pantu命令，系统关闭了135、445等高危端口，仅开启了22、1521等端口。 |
| c）应通过设定终端接入方式或网络地址范围对通过网络进行管理的管理终端进行限制； | 经核查，1）通过配置安全组策略限制仅允许通过堡垒机管理服务器；2）经核查防火墙中访问控制策略，具备堡垒机地址-服务器管理网段（10.33.0.0）的访问控制策略。 |
| d）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； | 根据GB∕T 28448-2019 《信息安全技术 网络安全等级保护测评要求》测评对象范围描述，服务器无该项要求，故判为“不适用”。 |
| e）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； | 1）经过漏洞扫描，服务器不存在高危安全漏洞；2）执行rpm -qa grep patch命令，查看系统补丁已更新至最新。 |
| f）应能够检测到对重要节点进行入侵的行为，并在发生严重入侵事件时提供报警。 | 经核查，服务器上安装有青藤云天眼云镜，对主机入侵行为进行检测，发现严重安全事件时通过钉钉告警。 |
| 恶意代码防范 | a）应采用免受恶意代码攻击的技术措施或主动免疫可信验证机制及时识别入侵和病毒行为，并将其有效阻断。 | 经核查，服务器上安装有青藤云天眼云镜，对主机恶意代码进行检测、清除，每天凌晨自动更新恶意代码特征库，经核查，具备恶意代码特征库更新记录。 |
| 可信验证 | a）可基于可信根对计算设备的系统引导程序、系统程序、重要配置参数和应用程序等进行可信验证，并在应用程序的关键执行环节进行动态可信验证，在检测到其可信性受到破坏后进行报警，并将验证结果形成审计记录送至安全管理中心。 | 未采用技术措施对计算设备的系统引导程序、系统程序、重要配置参数和通信应用程序等进行可信验证。 |
| 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； | 采用SSH协议连接操作系统，保证了鉴别信息以及管理数据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。 | 操作系统中对重要鉴别信息通过自身的加密及校验（SHA256），保证数据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； | 采用SSH协议连接操作系统，保证了鉴别信息以及管理数据在传输过程中的保密性。 |
| b）应采用密码技术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个人信息等。 | 通过系统自带的加密模块保证鉴别数据在存储过程中的保密性。 |
| 数据备份恢复 | a）应提供重要数据的本地数据备份与恢复功能； | 经核查，通过脚本每周将配置文件、代码仓库等数据备份至备份服务器中，依据需要验证备份数据的有效性。 |
| b）应提供异地实时备份功能，利用通信网络将重要数据实时备份至备份场地； | 系统无异地备份机制。 |
| c）应提供重要数据处理系统的热冗余，保证系统的高可用性。 | 服务器采用集群方式部署，保证系统的高可用性。 |
| 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； | 操作系统提供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功能。 |
| 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。 | 操作系统提供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的功能。 |

4.1.3.102. 运力库主库

|  |  |  |
| --- | --- | --- |
| **安全控制点** | **测评指标** | **结果记录** |
| 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）操作系统时采用用户名+SSHKey公私钥进行身份鉴别鉴别信息具有复杂度要求；2）执行cat /etc/shadow命令，查看shadow文件系统内用户身份标识唯一，不存在同名用户，且不存在空口令账号；3）经访谈，SSHKey公私钥每半年进行更换；4）查看sshd\_config配置文件中配置PasswordAuthentication no，拒绝使用密码方式进行身份鉴别。 |
| 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； | 操作系统采用用户名+SSHKey公私钥进行身份鉴别，可以防止鉴别信息被暴力破解；但未配置用户连接超时退出策略。 |
| 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； | 1）经核查，管理人员采用SSH协议连接操作系统；2）执行netatat –tpln| grep 23命令查看操作系统远程管理端口，不存在Telnet端口，防止鉴别信息在网络传输过程中的被窃听。 |
| 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。 | 未采用两种或两种以上组合的鉴别技术对用户进行身份鉴别。 |
| 访问控制 | a）应对登录的用户分配账户和权限； | 1）经访谈，通过root账户为登录的用户创建账户、分配权限；2）执行ls -l命令查看关键文件权限，均已为账户分配了相应权限，相关文件权限设置为/etc/shadow：000、/etc/passwd：644、/etc/group：644、/etc/profile：644、/etc/crontab：644、/ etc/securetty：600、/etc/ssh/sshd\_config：600。 |
| b）应重命名或删除默认账户，修改默认账户的默认口令； | 1）执行cat /etc/shadow命令查看shadow文件，操作系统中adm、lp、sync、shutdown、halt、mail、uucp、operator、games、gopher等账户均为nologin状态，存在默认账户root；2）执行more /etc/ssh/sshd\_config命令，查看“PermitRootLogin”参数设置为“yes”，即允许root远程登录；3）经访谈，root用户需通过公私钥方式进行身份鉴别。 |
| 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； | 1）执行cat /etc/shadow命令查看shadow文件，发现操作系统存在root、ysup、yops、yluser等在用账户，不存在多余的、过期账户；2）存在多个堡垒机账户登录操作系统时共用一个账户的情况。 |
| 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； | root账户具有系统所有权限，未实现管理用户的权限分离。 |
| e）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； | 经访谈，由系统管理员root配置访问控制策略，如：/etc/passwd，/etc/profile宿主为root、权限设置为644，audit文件为700、message文件为600，其他文件权限为750，实现用户对文件的权限控制。 |
| f）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； | 由管理用户进行用户访问权限分配进行设置，依据访问控制策略,对各类文件进行访问，重要文件和目录权限均在合理范围内，用户可根据文件不同的权限进行操作。 |
| g）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。 | 执 行more /etc/selinux/config 命令，查看config文件显示 SELINUX参数为 DISABLED，即未开启强制访问控制模式。 |
| 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）执行ps -ef|grep rsyslog和ps -ef|grep auditd命令，显示rsyslog和auditd进程正在运行；2）more /etc/audit/audit.rules，显示审计内容包括：\*.info、authriv.\*、mail.\*、cron.\*、\*.emerg、uucp、news.crit、local7.\*等事件。 |
| 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； | 执行tail -20 /var/log/audit/audit.log命令，查看近20条审计日志，内容包括：时间、对象、路径、用户ID、相关的系统调用、用户执行命令等。 |
| 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）通过访问权限对审计记录进行保护，日志文件/var/log/messages、/var/log/secure、/var/log/audit/audit.log访问 权限均为600；2）审计记录本地保存，且实时备份至360本地安全大脑，保存时间满足180天以上。 |
| d）应对审计进程进行保护，防止未经授权的中断。 | 执行service auditd status命令，系统开启auditd审计保护进程，审计进程由root用户维护，经现场使用yluser用户通过service auditd stop命令尝试中断审计进程，无法将审计进程单独中断。 |
| 入侵防范 | a）应遵循最小安装的原则，仅安装需要的组件和应用程序； | 1）系统安装遵循最小化安装原则；2）执行yum list installed命令查看操作系统已安装的程序包，存在Java、oracle、SSH、天眼云镜agent等应用程序或组件，不存在与业务系统无关的组件和应用程序。 |
| b）应关闭不需要的系统服务、默认共享和高危端口； | 1）执行systemctl list-unit-files 命令，系统已关闭FTP、Telnet 等高危网络服务；2）执行netstat -pantu命令，系统关闭了135、445等高危端口，仅开启了22、1521等端口。 |
| c）应通过设定终端接入方式或网络地址范围对通过网络进行管理的管理终端进行限制； | 经核查，1）通过配置安全组策略限制仅允许通过堡垒机管理服务器；2）经核查防火墙中访问控制策略，具备堡垒机地址-服务器管理网段（10.33.0.0）的访问控制策略。 |
| d）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； | 根据GB∕T 28448-2019 《信息安全技术 网络安全等级保护测评要求》测评对象范围描述，服务器无该项要求，故判为“不适用”。 |
| e）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； | 1）经过漏洞扫描，服务器不存在高危安全漏洞；2）执行rpm -qa grep patch命令，查看系统补丁已更新至最新。 |
| f）应能够检测到对重要节点进行入侵的行为，并在发生严重入侵事件时提供报警。 | 经核查，服务器上安装有青藤云天眼云镜，对主机入侵行为进行检测，发现严重安全事件时通过钉钉告警。 |
| 恶意代码防范 | a）应采用免受恶意代码攻击的技术措施或主动免疫可信验证机制及时识别入侵和病毒行为，并将其有效阻断。 | 经核查，服务器上安装有青藤云天眼云镜，对主机恶意代码进行检测、清除，每天凌晨自动更新恶意代码特征库，经核查，具备恶意代码特征库更新记录。 |
| 可信验证 | a）可基于可信根对计算设备的系统引导程序、系统程序、重要配置参数和应用程序等进行可信验证，并在应用程序的关键执行环节进行动态可信验证，在检测到其可信性受到破坏后进行报警，并将验证结果形成审计记录送至安全管理中心。 | 未采用技术措施对计算设备的系统引导程序、系统程序、重要配置参数和通信应用程序等进行可信验证。 |
| 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； | 采用SSH协议连接操作系统，保证了鉴别信息以及管理数据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。 | 操作系统中对重要鉴别信息通过自身的加密及校验（SHA256），保证数据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； | 采用SSH协议连接操作系统，保证了鉴别信息以及管理数据在传输过程中的保密性。 |
| b）应采用密码技术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个人信息等。 | 通过系统自带的加密模块保证鉴别数据在存储过程中的保密性。 |
| 数据备份恢复 | a）应提供重要数据的本地数据备份与恢复功能； | 经核查，通过脚本每周将配置文件、代码仓库等数据备份至备份服务器中，依据需要验证备份数据的有效性。 |
| b）应提供异地实时备份功能，利用通信网络将重要数据实时备份至备份场地； | 系统无异地备份机制。 |
| c）应提供重要数据处理系统的热冗余，保证系统的高可用性。 | 服务器采用集群方式部署，保证系统的高可用性。 |
| 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； | 操作系统提供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功能。 |
| 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。 | 操作系统提供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的功能。 |

4.1.3.103. 运维终端1

|  |  |  |
| --- | --- | --- |
| **安全控制点** | **测评指标** | **结果记录** |
| 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； | 运维终端存在管理员、Guest两个账户，用户名具有唯一性，通过用户名和口令对登录用户进行身份鉴别，密码长度为8位以上，启用了密码复杂度策略，口令更换周期为90天。 |
| 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； | 运维终端设置5次无效登录锁定账户30分钟，空闲时间30分钟后启用屏幕保护。 |
| 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； | 运维终端已禁用远程连接。 |
| 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。 | 运维终端仅采用用户名和口令单一的身份鉴别技术。 |
| 访问控制 | a）应对登录的用户分配账户和权限； | 运维终端为个人办公使用，仅根据用户姓名创建管理用户，并为其分配了管理员权限。 |
| b）应重命名或删除默认账户，修改默认账户的默认口令； | 系统中默认账户已被禁用，新添加了管理用户，并将用户添加到管理员administrator组中。 |
| 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； | 运维终端根据用户姓名创建管理用户，系统中无多余、过期、共享账户。 |
| 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； | 运维终端用于个人办公，需要拥有对运维终端操作系统的所有管理权限。 |
| e）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； | 运维终端仅供个人工作使用，用户的访问控制策略在系统初始化时默认设置。 |
| f）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； | 运维终端访问控制主体为用户，客体为系统中的文件，访问控制策略为用户对系统中文件的操作权限。 |
| g）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。 | 未对重要的主体和客体设置安全标记。 |
| 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； | 运维终端配置了审核策略，内容包括：账户登陆事件、账户管理、目录服务访问、登陆事件、对象访问、策略更改、系统事件。 |
| 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； | 审计日志记录包括：日志名称、来源、事件ID、级别、用户、操作代码等。 |
| 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； | 审计记录本地保存，无法被删除或修改，并且设置为：不覆盖事件（手动清除日志）。 |
| d）应对审计进程进行保护，防止未经授权的中断。 | 审计进程受系统进程保护，不会受到未预期的中断。 |
| 入侵防范 | a）应遵循最小安装的原则，仅安装需要的组件和应用程序； | 运维终端仅安装了业务所需的应用程序，遵循了最小安装原则。 |
| b）应关闭不需要的系统服务、默认共享和高危端口； | 运维终端仅开放了业务所需的端口和系统服务，其他端口及服务均关闭。 |
| c）应通过设定终端接入方式或网络地址范围对通过网络进行管理的管理终端进行限制； | 终端已关闭远程管理功能。 |
| d）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； | 测评对象为Windows系统，不适用。 |
| e）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； | 通过电脑管家对Windows系统的补丁进行扫描以及修复，最新的补丁更新为KB5005033。 |
| f）应能够检测到对重要节点进行入侵的行为，并在发生严重入侵事件时提供报警。 | 通过360安全卫士对终端进行入侵防范，并提供告警功能。 |
| 恶意代码防范 | a）应采用免受恶意代码攻击的技术措施或主动免疫可信验证机制及时识别入侵和病毒行为，并将其有效阻断。 | 通过安装的360杀毒进行恶意代码防范以及阻断。 |
| 可信验证 | a）可基于可信根对计算设备的系统引导程序、系统程序、重要配置参数和应用程序等进行可信验证，并在应用程序的关键执行环节进行动态可信验证，在检测到其可信性受到破坏后进行报警，并将验证结果形成审计记录送至安全管理中心。 | 未采用技术措施计算设备的系统引导程序、系统程序、重要配置参数和应用程序等进行可信验证。 |
| 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； | 运维终端远程管理系统时使用HTTPS和SSH加密协议进行远程管理保证数据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。 | 通过Windows系统自带的加密模块保证鉴别数据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； | 运维终端远程管理系统时使用HTTPS和SSH加密协议进行远程管理保证数据在传输过程中的保密性。 |
| b）应采用密码技术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个人信息等。 | 通过Windows系统自带的加密模块保证鉴别数据在存储过程中的保密性。 |
| 数据备份恢复 | a）应提供重要数据的本地数据备份与恢复功能； | 系统中重要数据均在生产系统中存放，运维终端不存放重要数据。 |
| b）应提供异地实时备份功能，利用通信网络将重要数据实时备份至备份场地； | 系统中重要数据均在生产系统中存放，运维终端不存放重要数据。 |
| c）应提供重要数据处理系统的热冗余，保证系统的高可用性。 | 运维终端默认不适用。 |
| 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； | 运维终端组策略中启用了“关机清除虚拟内存页面文件”和“不显示上次登录用户名”策略。 |
| 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。 | 运维终端组策略中启用了“关机清除虚拟内存页面文件”和“不显示上次登录用户名”策略。 |

4.1.3.104. 运维终端2

|  |  |  |
| --- | --- | --- |
| **安全控制点** | **测评指标** | **结果记录** |
| 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； | 运维终端存在管理员、Guest两个账户，用户名具有唯一性，通过用户名和口令对登录用户进行身份鉴别，密码长度为8位以上，启用了密码复杂度策略，口令更换周期为90天。 |
| 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； | 运维终端设置5次无效登录锁定账户30分钟，空闲时间30分钟后启用屏幕保护。 |
| 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； | 运维终端已禁用远程连接。 |
| 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。 | 运维终端仅采用用户名和口令单一的身份鉴别技术。 |
| 访问控制 | a）应对登录的用户分配账户和权限； | 运维终端为个人办公使用，仅根据用户姓名创建管理用户，并为其分配了管理员权限。 |
| b）应重命名或删除默认账户，修改默认账户的默认口令； | 系统中默认账户已被禁用，新添加了管理用户，并将用户添加到管理员administrator组中。 |
| 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； | 运维终端根据用户姓名创建管理用户，系统中无多余、过期、共享账户。 |
| 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； | 运维终端用于个人办公，需要拥有对运维终端操作系统的所有管理权限。 |
| e）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； | 运维终端仅供个人工作使用，用户的访问控制策略在系统初始化时默认设置。 |
| f）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； | 运维终端访问控制主体为用户，客体为系统中的文件，访问控制策略为用户对系统中文件的操作权限。 |
| g）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。 | 未对重要的主体和客体设置安全标记。 |
| 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； | 运维终端配置了审核策略，内容包括：账户登陆事件、账户管理、目录服务访问、登陆事件、对象访问、策略更改、系统事件。 |
| 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； | 审计日志记录包括：日志名称、来源、事件ID、级别、用户、操作代码等。 |
| 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； | 审计记录本地保存，无法被删除或修改，并且设置为：不覆盖事件（手动清除日志）。 |
| d）应对审计进程进行保护，防止未经授权的中断。 | 审计进程受系统进程保护，不会受到未预期的中断。 |
| 入侵防范 | a）应遵循最小安装的原则，仅安装需要的组件和应用程序； | 运维终端仅安装了业务所需的应用程序，遵循了最小安装原则。 |
| b）应关闭不需要的系统服务、默认共享和高危端口； | 运维终端仅开放了业务所需的端口和系统服务，其他端口及服务均关闭。 |
| c）应通过设定终端接入方式或网络地址范围对通过网络进行管理的管理终端进行限制； | 终端已关闭远程管理功能。 |
| d）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； | 测评对象为Windows系统，不适用。 |
| e）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； | 通过电脑管家对Windows系统的补丁进行扫描以及修复，最新的补丁更新为KB5005033。 |
| f）应能够检测到对重要节点进行入侵的行为，并在发生严重入侵事件时提供报警。 | 通过360安全卫士对终端进行入侵防范，并提供告警功能。 |
| 恶意代码防范 | a）应采用免受恶意代码攻击的技术措施或主动免疫可信验证机制及时识别入侵和病毒行为，并将其有效阻断。 | 通过安装的360杀毒进行恶意代码防范以及阻断。 |
| 可信验证 | a）可基于可信根对计算设备的系统引导程序、系统程序、重要配置参数和应用程序等进行可信验证，并在应用程序的关键执行环节进行动态可信验证，在检测到其可信性受到破坏后进行报警，并将验证结果形成审计记录送至安全管理中心。 | 未采用技术措施计算设备的系统引导程序、系统程序、重要配置参数和应用程序等进行可信验证。 |
| 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； | 运维终端远程管理系统时使用HTTPS和SSH加密协议进行远程管理保证数据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。 | 通过Windows系统自带的加密模块保证鉴别数据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； | 运维终端远程管理系统时使用HTTPS和SSH加密协议进行远程管理保证数据在传输过程中的保密性。 |
| b）应采用密码技术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个人信息等。 | 通过Windows系统自带的加密模块保证鉴别数据在存储过程中的保密性。 |
| 数据备份恢复 | a）应提供重要数据的本地数据备份与恢复功能； | 系统中重要数据均在生产系统中存放，运维终端不存放重要数据。 |
| b）应提供异地实时备份功能，利用通信网络将重要数据实时备份至备份场地； | 系统中重要数据均在生产系统中存放，运维终端不存放重要数据。 |
| c）应提供重要数据处理系统的热冗余，保证系统的高可用性。 | 运维终端默认不适用。 |
| 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； | 运维终端组策略中启用了“关机清除虚拟内存页面文件”和“不显示上次登录用户名”策略。 |
| 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。 | 运维终端组策略中启用了“关机清除虚拟内存页面文件”和“不显示上次登录用户名”策略。 |

|  |  |  |  |
| --- | --- | --- | --- |
| **测评项目** |  | **测评对象** | 系统管理软件/平台 |
| **测评单位** |  | | |
| **测评地点** |  | | |
| **测评人员** |  | **配合人员** | 刘亮 |
| **测评日期** | 2023.6.16 | | |
| **测评人员签字** |  | **配合人员签字** |  |

4.1.4. 系统管理软件/平台

4.1.4.1. 阿里云控制台

|  |  |  |
| --- | --- | --- |
| **安全控制点** | **测评指标** | **结果记录** |
| 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、经现场访谈网络管理员，阿里云控制台采用用户名、口令方式+MFA动态随机码对登录用户进行身份标识和鉴别，阿里云控制台对登录用户通过真实邮箱、手机号进行验证，能够保证用户身份标识唯一； 2、经现场查看阿里云控制台RAM访问控制台-身份管理-设置菜单，用户口令长度要求为8-32位字符，由数字、大小写字母、字符三种以上组合，MFA生成6位动态随机码，首次登录时需要通过手机短信验证码，但未要求定期更换口令。 |
| 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； | 经现场查看阿里云控制台RAM访问控制台-身份管理-设置菜单，阿里云控制台启用了用户登录失败处理功能，用户一小时内连续错误登录5次需要通过拖动滑动条进行验证，并启用短信验证码进行二次验证，登录会话的过期时间为6小时。 |
| 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； | 经现场核查阿里云控制台的登录方式，阿里云控制台通过HTTPS协议进行远程管理，保证鉴别信息在网络传输过程中不被窃听。 |
| 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。 | 1、经现场访谈网络管理员，Web应用防火墙基于阿里云控制台进行身份鉴别； 2、经现场核查阿里云控制台的登录方式，阿里云控制台用户通过用户名、口令+MFA动态随机码对登录用户进行身份标识和鉴别进行身份鉴别。 |
| 访问控制 | a）应对登录的用户分配账户和权限； | 经现场查看阿里云控制台RAM访问控制台-身份管理-用户组及用户菜单，在阿里云控制台中分别为创建DBA、network-user、safe三个用户组，将三个用户组分别赋予数据库管理、网络管理及安全审计管理等权限，在控制台中按照业务需求及管理需求分别创建了相应账户，然后将管理用户根据工作职责添加到对应用户组中，进而获得相应管理权限，经现场核查，阿里云控制台中共49个账户。 |
| b）应重命名或删除默认账户，修改默认账户的默认口令； | 1、经现场访谈网络管理员及核查阿里云控制台中用户信息，阿里云控制台中管理用户为注册用户，子账户由管理用户创建，不存在默认账户；2、所有用户口令均按照复杂度策略更改。 |
| 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； | 经现场访谈网络管理员及核查阿里云控制台中用户信息，目前阿里云控制台中账户均为在职人员及业务账户，账户与人员一一对应，并且分别根据管理用户工作职责赋予工作权限，不存在多余、过期、共享账户。 |
| 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； | 经现场访谈网络管理员及核查阿里云控制台中用户权限管理，目前阿里云控制台中分别创建了系统管理员、操作用户、审计管理员、安全管理等用户，并分别赋予管理用户相应的工作权限，实现管理用户权限最小化及权限分离。 |
| e）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； | 经现场访谈网络管理员及核查阿里云控制台各管理员的权限分配情况，在阿里云控制台由管理员主账户为各管理员配置访问控制策略，访问控制策略为管理员对阿里云控制台中各功能菜单的访问及操作管理等，如：用户管理、安全服务管理、操作审计等功能菜单的操作管理。 |
| f）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； | 经现场访谈网络管理员及核查阿里云控制台各管理员的权限分配情况，阿里云控制台访问控制粒度达到主体为用户级，客体为功能菜单级。 |
| g）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。 | 经现场核查，未对重要主体和客体设置安全标记。 |
| 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； | 经现场核查阿里云控制台中操作审计功能，在阿里云控制台中启用了操作审计功能，能够对系统中用户操作内容及系统中的安全事件进行审计。 |
| 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； | 经现场核查阿里云控制台中操作审计内容，阿里云控制台操作审计记录包括：时间、用户名、事件名称、资源类型、资源名称、错误码等。 |
| 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； | 经现场核查阿里云控制台审计记录及备份设置，阿里云控制台所有用户均无权限对相关的审计记录进行删除、修改，同时管理员配置审计记录转储，每天将审计记录传输至OSS上进行存储，并保证审计记录保存时间至少为180天 。 |
| d）应对审计进程进行保护，防止未经授权的中断。 | 经现场核查阿里云控制台操作审计功能，操作审计功能为阿里公共云提供的审计服务，阿里云控制台相关的审计进程由阿里公共云负责保护，不会受到未预期的中断。 |
| 入侵防范 | a）应遵循最小安装的原则，仅安装需要的组件和应用程序； | 经核查，阿里云控制台供用户进行阿里公共云集中管理的应用系统，该测评项针对应用系统不适用。 |
| b）应关闭不需要的系统服务、默认共享和高危端口； | 经核查，阿里云控制台供用户进行阿里公共云集中管理的应用系统，该测评项针对应用系统不适用。 |
| c）应通过设定终端接入方式或网络地址范围对通过网络进行管理的管理终端进行限制； | 经核查，阿里云控制台供用户进行阿里公共云集中管理的应用系统，该测评项针对应用系统不适用。 |
| d）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； | 经现场核查阿里云控制台中配置，阿里云控制台中人机交互均采用下拉框或勾选方式实现，核查阿里云操作手册，能够对特殊字符进行了过滤，保证输入数据的有效性。 |
| e）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； | 经现场访谈管理管理员及核查阿里云控制台配置，被测系统采购阿里公共云提供的云平台服务，由阿里公共云负责对阿里云控制台进行维护管理及版本更新，阿里公共云已通过等级保护第三级测评。 |
| f）应能够检测到对重要节点进行入侵的行为，并在发生严重入侵事件时提供报警。 | 经现场访谈网络管理员及核查阿里云安全服务，在阿里公共云采购云防火墙、Web应用防火墙安全服务，云防火墙能够对网络层入侵行为进行检测，Web应用防火墙能够应用层入侵行为进行检测，发现严重入侵事件及时通过钉钉报警，经现场核查网络管理员钉钉记录，具备实时报警记录。 |
| 可信验证 | a）可基于可信根对计算设备的系统引导程序、系统程序、重要配置参数和应用程序等进行可信验证，并在应用程序的关键执行环节进行动态可信验证，在检测到其可信性受到破坏后进行报警，并将验证结果形成审计记录送至安全管理中心。 | 未基于可信根对计算设备提供可信验证。 |
| 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； | 经现场核查阿里云控制台通信方式，阿里云控制台通过HTTPS协议进行通信，保证重要数据在网络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。 | 经现场访问网络管理员及核查阿里云相关文档说明，阿里云控制台中用户鉴别信息会采用加密技术保证了重要业务数据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； | 经现场核查阿里云控制台通信方式，阿里云控制台通过HTTPS协议进行通信，保证重要数据在网络传输过程中的保密性。 |
| b）应采用密码技术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个人信息等。 | 经现场访问网络管理员及核查阿里云相关文档说明，阿里云控制台中用户鉴别信息会采用加密技术保证了重要业务数据在存储过程中的保密性。 |
| 数据备份恢复 | a）应提供重要数据的本地数据备份与恢复功能； | 经现场核查，管理员通过手动方式将阿里云控制台中配置数据进行下载备份。 |
| b）应提供异地实时备份功能，利用通信网络将重要数据实时备份至备份场地； | 公司未对重要数据提供异地备份服务。 |
| c）应提供重要数据处理系统的热冗余，保证系统的高可用性。 | 经访谈访问管理员及核查网络拓扑图，阿里云控制台冗余由阿里云负责。 |
| 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； | 经现场核查，用户退出阿里云控制台后，重新登录时，用户信息完全清除。 |
| 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。 | 经现场核查，用户退出阿里云控制台后session信息完全清除。 |
| 个人信息保护 | a）应仅采集和保存业务必需的用户个人信息； | 阿里云控制台仅用于对系统中主机资源、安全服务、数据库等进行集中管控，不用于收集用户个人信息。 |
| b）应禁止未授权访问和非法使用用户个人信息。 | 阿里云控制台仅用于对系统中主机资源、安全服务、数据库等进行集中管控，不用于收集用户个人信息。 |

4.1.4.2. 堡垒机

|  |  |  |
| --- | --- | --- |
| **安全控制点** | **测评指标** | **结果记录** |
| 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、经现场访谈堡垒机管理员及核查堡垒机，堡垒机采用用户名、口令、动态验证码进行身份标识和身份鉴别，堡垒机中用户统一接入公司AD域控，AD域控中账户统一由公司账户管理员根据员工入职创建，域控中具备用户名查重功能，创建重名用户会提示用户名已存在，确保用户身份标识具备唯一性，2、在域控中设置用户口令长度至少为8位，由数字、大写字母、字符至少两种组合，用户口令更换周期为90天，动态验证码刷新时间为30秒。 |
| 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； | 经现场核查堡垒机配置策略，堡垒机用户登录失败依赖AD域控的登录失败配置，限制用户连续错误登录10次锁定10分钟，空闲超时时间限制为3小时。 |
| 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； | 经现场核查堡垒机通信方式，管理员采用HTTPS协议对堡垒机进行远程运维管理，保证鉴别信息在网络传输过程中不被窃听。 |
| 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。 | 经现场核查堡垒机登录方式，堡垒机采用用户名、口令、动态验证码对用户进行身份鉴别。 |
| 访问控制 | a）应对登录的用户分配账户和权限； | 经现场访谈堡垒机管理员及核查堡垒机中用户管理配置，堡垒机中账户均根据域控同步至堡垒机中，在堡垒机中根据各账户工作需求为相应账户赋予不同权限，Adminstrator、liulang、yangkunyuan、chengguizhen、jax.jiang为系统管理员账户，拥有全部权限，存在系统审计员角色，如auditor、huangfusheng、qinzhuowei，拥有安全配置管理权限，其余普通用户拥有使用堡垒机权限。 |
| b）应重命名或删除默认账户，修改默认账户的默认口令； | 经现场核查堡垒机用户管理配置，堡垒机中不存在默认账户，并且用户口令已按照复杂度策略更改。 |
| 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； | 经现场访谈堡垒机管理员及核查堡垒机用户管理配置，堡垒机中账户均根据AD域控进行同步，员工离职时统一在AD域控中对该账户进行删除，堡垒机中会将该员工信息自动调整为停用状态，堡垒机中不存在多余、过期、共享账户。 |
| 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； | 经现场访谈堡垒机管理员及核查堡垒机用户管理配置，在堡垒机中根据各账户工作需求为相应账户赋予不同权限，如JMSops为系系统管理员，拥有堡垒机日常运维管理权限，qinzhuowei、huanfusheng为审计管理员，拥有审计管理权限，chenguizhen为安全管理员，拥有安全配置管理权限，其余普通用户拥有使用堡垒机权限，实现管理用户权限最小化及权限分离。 |
| e）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； | 经核查配置文件及访谈堡垒机网络管理员，堡垒机中由管理员角色账户为管理用户配置相应账号，并按照用户角色级别赋予管理用户操作权限。 |
| f）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； | 经核查配置文件及访谈堡垒机管理员，堡垒机中访问控制策略为管理用户的堡垒机中配置文件等进行配置管理及访问管理等，访问控制粒度达到主体为用户级、客体为菜单级。 |
| g）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。 | 经核查配置文件及访谈堡垒机管理员，堡垒机未对重要主体和客体设置安全标记。 |
| 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； | 经现场核查堡垒机审计功能，堡垒机启用安全审计，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。 |
| 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； | 经现场核查堡垒机中审计记录，堡垒机的登录日志包括：用户名、登录方式、认证方式、登录IP、登录城市、用户代理、MFA、原因、状态、登录日期；FTP日志包括：用户、资产、系统用户、远端地址、操作、文件名、成功、开始时间；操作日志包括：用户名、动作、资源类型、资源、远端地址、日期；改密日志包括：用户、修改者、远端地址、日期等。 |
| 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、经现场核查堡垒机中审计记录，所有用户均无权限对审计记录进行删除、修改，2、管理员在堡垒机中设置审计记录保存时间至少200天，到期自动清除，未对审计记录进行备份。 |
| d）应对审计进程进行保护，防止未经授权的中断。 | 经现场核查堡垒机中审计进程，堡垒机审计进程受系统进程保护，所有用户均无权限对审计进程进行中断。 |
| 入侵防范 | a）应遵循最小安装的原则，仅安装需要的组件和应用程序； | 经访谈堡垒机管理员及核查，堡垒机系统为厂商提供独立封装系统，不允许安装其他组件及应用程序，遵循最小安装原则。 |
| b）应关闭不需要的系统服务、默认共享和高危端口； | 经现场核查，堡垒机为供用户对服务器等进行集中管理的应用系统，故该项调整为不适用。 |
| c）应通过设定终端接入方式或网络地址范围对通过网络进行管理的管理终端进行限制； | 经现场核查，在堡垒机中添加白名单策略，仅允许10.33.130.0管理网段远程管理堡垒机。 |
| d）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； | 经现场访谈安全管理员及核查，远程管理堡垒机时仅允许管理用户使用在办公网防火墙中启用VPN隧道连接到世纪互联IDC机房中，然后对堡垒机进行远程管理。 |
| e）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； | 经现场访谈堡垒机管理员级核查堡垒机版本信息，管理员根据官网（飞致云）发布的堡垒机版本对堡垒机进行更新，目前堡垒机版本为V2.23.4，为当前发布最新版本。 |
| f）应能够检测到对重要节点进行入侵的行为，并在发生严重入侵事件时提供报警。 | 经访谈网络管理员，被测系统中部署了通过360AISA全流量威胁分析系统和360本地安全大脑将被测系统中全部流量镜像发送到360AISA全流量威胁分析系统及360本地安全大脑中进行分析监测，发现入侵事件后及时通过钉钉报警，并且能够自动阻断。 |
| 可信验证 | a）可基于可信根对计算设备的系统引导程序、系统程序、重要配置参数和应用程序等进行可信验证，并在应用程序的关键执行环节进行动态可信验证，在检测到其可信性受到破坏后进行报警，并将验证结果形成审计记录送至安全管理中心。 | 未基于可信根对计算设备提供可信验证。 |
| 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； | 经现场核查堡垒机通信方式，系统通过HTTPS协议进行通信，保证重要数据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。 | 经现场核查安全管理员，堡垒机通过厂商自身的加密技术保证用户鉴别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； | 经现场核查堡垒机通信方式，系统通过HTTPS协议进行通信，保证重要数据传输过程中的保密性。 |
| b）应采用密码技术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个人信息等。 | 经现场核查安全管理员，堡垒机通过厂商自身的加密技术保证用户鉴别信息等在存储过程中的保密性。 |
| 数据备份恢复 | a）应提供重要数据的本地数据备份与恢复功能； | 经现场访谈堡垒机管理员级核查堡垒机配置，堡垒机中管理用户信息在AD域控中进行备份保存，堡垒机中配置文件等由管理员通过手动备份方式下载至备份服务器进行备份。 |
| b）应提供异地实时备份功能，利用通信网络将重要数据实时备份至备份场地； | 经现场核查，未提供实时异地备份功能。 |
| c）应提供重要数据处理系统的热冗余，保证系统的高可用性。 | 经核查，重要数据处理系统中采用双机冗余部署，保证系统的高可用性。 |
| 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； | 经现场测试，用户退出堡垒机后，重新登录时，用户信息完全清除。 |
| 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。 | 经现场核查，用户退出阿里云控制台后session信息完全清除。 |
| 个人信息保护 | a）应仅采集和保存业务必需的用户个人信息； | 堡垒机仅用于对系统中主机资源、数据库等进行集中管控，不用于收集用户个人信息。 |
| b）应禁止未授权访问和非法使用用户个人信息。 | 堡垒机仅用于对系统中主机资源、数据库等进行集中管控，不用于收集用户个人信息。 |

4.1.4.3. Nginx中间件

|  |  |  |
| --- | --- | --- |
| **安全控制点** | **测评指标** | **结果记录** |
| 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； | Nginx中间件的配置管理权限由操作系统实现，不适用。 |
| 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； | Nginx中间件的配置管理权限由操作系统实现，不适用。 |
| 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； | Nginx中间件的配置管理权限由操作系统实现，不适用。 |
| 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。 | Nginx中间件的配置管理权限由操作系统实现，不适用。 |
| 访问控制 | a）应对登录的用户分配账户和权限； | Nginx中间件的配置管理权限由操作系统实现，不适用。 |
| b）应重命名或删除默认账户，修改默认账户的默认口令； | Nginx中间件的配置管理权限由操作系统实现，不适用。 |
| 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； | Nginx中间件的配置管理权限由操作系统实现，不适用。 |
| 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； | Nginx中间件的配置管理权限由操作系统实现，不适用。 |
| e）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； | Nginx中间件的配置管理权限由操作系统实现，不适用。 |
| f）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； | Nginx中间件的配置管理权限由操作系统实现，不适用。 |
| g）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。 | Nginx中间件的配置管理权限由操作系统实现，不适用。 |
| 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）启用了error.log 错误日志、access.log 网页访问日志；2）查看nginx.conf 的文件，查看error\_log和access\_log配置情况如下：error\_log logs/error.log error；access\_log logs/access.log main。 |
| 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； | 查看access.log日志，包括：msec、request\_length、request\_time、status、time\_local、http\_referer、http\_user\_agent、remote\_addr、remote\_user、request等；查看error.log，内容包括：时间、日志级别、详情等。 |
| 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）查看日志文件权限，仅root用户具有日志的管理权限，其他用户没有修改权限；2）审计记录本地保存，且实时备份至360本地安全大脑，保存时间满足180天以上。 |
| d）应对审计进程进行保护，防止未经授权的中断。 | 审计进程与中间件主进程关联，无法单独中断审计进程。 |
| 入侵防范 | a）应遵循最小安装的原则，仅安装需要的组件和应用程序； | 根据GB∕T 28448-2019 《信息安全技术 网络安全等级保护测评要求》测评对象范围描述，中间件无该项要求。 |
| b）应关闭不需要的系统服务、默认共享和高危端口； | 根据GB∕T 28448-2019 《信息安全技术 网络安全等级保护测评要求》测评对象范围描述，中间件无该项要求。 |
| c）应通过设定终端接入方式或网络地址范围对通过网络进行管理的管理终端进行限制； | 根据GB∕T 28448-2019 《信息安全技术 网络安全等级保护测评要求》测评对象范围描述，中间件无该项要求。 |
| d）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； | 根据GB∕T 28448-2019 《信息安全技术 网络安全等级保护测评要求》测评对象范围描述，中间件无该项要求。 |
| e）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； | 经漏洞扫描，未发现高危安全漏洞。 |
| f）应能够检测到对重要节点进行入侵的行为，并在发生严重入侵事件时提供报警。 | 根据GB∕T 28448-2019 《信息安全技术 网络安全等级保护测评要求》测评对象范围描述，中间件无该项要求。 |
| 可信验证 | a）可基于可信根对计算设备的系统引导程序、系统程序、重要配置参数和应用程序等进行可信验证，并在应用程序的关键执行环节进行动态可信验证，在检测到其可信性受到破坏后进行报警，并将验证结果形成审计记录送至安全管理中心。 | 根据GB∕T 28448-2019 《信息安全技术 网络安全等级保护测评要求》测评对象范围描述，中间件无该项要求。 |
| 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； | Nginx中间件的配置管理权限由操作系统实现，不适用。 |
| 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。 | Nginx中间件的配置管理权限由操作系统实现，不适用。 |
| 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； | Nginx中间件的配置管理权限由操作系统实现，不适用。 |
| b）应采用密码技术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个人信息等。 | Nginx中间件的配置管理权限由操作系统实现，不适用。 |
| 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； | Nginx中间件的配置管理权限由操作系统实现，不适用。 |
| 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。 | Nginx中间件的配置管理权限由操作系统实现，不适用。 |

4.1.4.4. Oracle数据库1

|  |  |  |
| --- | --- | --- |
| **安全控制点** | **测评指标** | **结果记录** |
| 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）数据库采用用户名/口令对用户进行身份标识、鉴别；2）数据库无法创建重名用户，用户名具有唯一性，且不存在空口令账户；3）DBA创建账户时使用密码生成器生成16位口令（数字、大写字母、小写字母和特殊字符组合）；4）执行select \* from dab\_profiles命令，未配置口令长度、复杂度、定期更换策略。 |
| 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； | 经核查，数据库未配置用户登录失败处理和超时退出策略。 |
| 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； | 运维人员登录堡垒机后采用SQL Developer软件连接数据库，防止鉴别信息在传输过程中被窃听。 |
| 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。 | 数据库未采用两种或两种以上组合的鉴别技术对用户进行身份鉴别。 |
| 访问控制 | a）应对登录的用户分配账户和权限； | 经核查，1）由管理员为登录数据库的用户创建账户、分配权限；2）目前数据库具有sys、system管理账户和只读账户。 |
| b）应重命名或删除默认账户，修改默认账户的默认口令； | 经核查，数据库默认账户sys、system无法重命名，但已修改其默认口令。 |
| 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； | 经核查，1）目前数据库仅具有sys、system等管理账户，不存在多余、过期；2）存在多个堡垒机账户登录数据库时共用一个账户的情况。 |
| 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； | 经核查，数据库未授予管理用户所需的最小权限，未实现管理用户的权限分离。 |
| e）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； | 经核查，被测数据库系统由管理员账户SYS 配置访问控制策略，已基于角色配置严格的访问控制策略，严格限制用户对系统资源的访问。 |
| f）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； | 经核查，该数据库系统已基于角色配置严格的访问控制规则，访问控制粒度主体为用户级、客体为数据库表级。 |
| g）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。 | 未对重要主体和客体进行安全标记。 |
| 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； | 经核查，通过数据库审计系统对数据库所有用户的操作行为、SQL语句等进行审计记录。 |
| 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； | 经核查，审计记录包含：SQL语句、数据库名、线程、事务号、用户名、客户端IP、操作类型、状态、执行耗时、执行时间等。 |
| 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； | 经核查，审计记录本地保存，非授权用户无权限修改、删除，避免受到未预期的删除、修改或覆盖，且审计记录每天进行备份备份，保存时间满足180天以上。 |
| d）应对审计进程进行保护，防止未经授权的中断。 | 经核查，非授权用户无法中断系统审计进程。 |
| 入侵防范 | a）应遵循最小安装的原则，仅安装需要的组件和应用程序； | 根据GB∕T 28448-2019 《信息安全技术 网络安全等级保护测评要求》测评对象范围描述，数据库无该项要求。 |
| b）应关闭不需要的系统服务、默认共享和高危端口； | 根据GB∕T 28448-2019 《信息安全技术 网络安全等级保护测评要求》测评对象范围描述，数据库无该项要求。 |
| c）应通过设定终端接入方式或网络地址范围对通过网络进行管理的管理终端进行限制； | 经核查，1）通过配置安全策略限制仅允许通过堡垒机登录服务器后本地管理数据库；2）经核查防火墙中访问控制策略，具备堡垒机地址-服务器管理网段（10.33.0.0）的访问控制策略。 |
| d）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； | 根据GB∕T 28448-2019 《信息安全技术 网络安全等级保护测评要求》测评对象范围描述，数据库无该项要求。 |
| e）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； | 经漏洞扫描，数据库不存在高危漏洞。 |
| f）应能够检测到对重要节点进行入侵的行为，并在发生严重入侵事件时提供报警。 | 根据GB∕T 28448-2019 《信息安全技术 网络安全等级保护测评要求》测评对象范围描述，数据库无该项要求。 |
| 可信验证 | a）可基于可信根对计算设备的系统引导程序、系统程序、重要配置参数和应用程序等进行可信验证，并在应用程序的关键执行环节进行动态可信验证，在检测到其可信性受到破坏后进行报警，并将验证结果形成审计记录送至安全管理中心。 | 未采用技术措施对计算设备的系统引导程序、系统程序、重要配置参数和应用程序等进行可信验证。 |
| 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； | 运维人员登录堡垒机后采用SQL Developer软件连接数据库，保证鉴别信息、管理数据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。 | 采用SHA1+salt技术对用户鉴别信息进行加密存储，保证鉴别信息在存储过程中的完整性；但未采用校验技术保证重要业务数据、用户个人信息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； | 运维人员登录堡垒机后采用SQL Developer软件连接数据库，保证鉴别信息、管理数据在传输过程中的保密性。 |
| b）应采用密码技术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个人信息等。 | 采用SHA1+salt技术对用户鉴别信息进行加密存储，保证鉴别信息在存储过程中的保密性；采用aes-128-cbc对称加密算法保证个人信息在存储过程中的保密性；但未采用密码技术保证重要业务数据在存储过程中的保密性。 |
| 数据备份恢复 | a）应提供重要数据的本地数据备份与恢复功能； | 经核查，数据库配置了本地备份策略，每天全量备份，保留近20个全量备份库文件，运维人员每季度对备份文件进行恢复测试。 |
| b）应提供异地实时备份功能，利用通信网络将重要数据实时备份至备份场地； | 无异地备份措施。 |
| c）应提供重要数据处理系统的热冗余，保证系统的高可用性。 | 经核查，数据库采用主备方式部署，保证了系统的高可用性。 |
| 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； | 经核查，数据库用户退出后自动清理鉴别信息所在的存储空间。 |
| 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。 | 经核查，数据库用户退出后自动清理敏感数据存储空间。 |
| 个人信息保护 | a）应仅采集和保存业务必需的用户个人信息； | 1）数据库存储了用户姓名、手机号、身份证号、地址等个人信息；2）公司制定了YL-1-ISMS-02《信息安全和隐私管理策略手册》，在文件中明确了用户收集规则、收集方式、收集内容等。 |
| b）应禁止未授权访问和非法使用用户个人信息。 | 1）针对用户手机号的中间4位号码进行了脱敏处理；2）通过权限控制，仅有获得授权的管理员可以查看用户个人信息，同时通过审计日志对用户的操作行为进行记录；3）用户个人信息在入库时采用aes-128-cbc对称加密算法进行加密存储；4）公司制定了YL-1-ISMS-02《信息安全和隐私管理策略手册》，在文件中明确禁止非授权访问、非法使用个人信息。 |

4.1.4.5. Oracle数据库2

|  |  |  |
| --- | --- | --- |
| **安全控制点** | **测评指标** | **结果记录** |
| 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）数据库采用用户名/口令对用户进行身份标识、鉴别；2）数据库无法创建重名用户，用户名具有唯一性，且不存在空口令账户；3）DBA创建账户时使用密码生成器生成16位口令（数字、大写字母、小写字母和特殊字符组合）；4）执行select \* from dab\_profiles命令，未配置口令长度、复杂度、定期更换策略。 |
| 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； | 经核查，数据库未配置用户登录失败处理和超时退出策略。 |
| 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； | 运维人员登录堡垒机后采用SQL Developer软件连接数据库，防止鉴别信息在传输过程中被窃听。 |
| 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。 | 数据库未采用两种或两种以上组合的鉴别技术对用户进行身份鉴别。 |
| 访问控制 | a）应对登录的用户分配账户和权限； | 经核查，1）由管理员为登录数据库的用户创建账户、分配权限；2）目前数据库具有sys、system管理账户和只读账户。 |
| b）应重命名或删除默认账户，修改默认账户的默认口令； | 经核查，数据库默认账户sys、system无法重命名，但已修改其默认口令。 |
| 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； | 经核查，1）目前数据库仅具有sys、system等管理账户，不存在多余、过期；2）存在多个堡垒机账户登录数据库时共用一个账户的情况。 |
| 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； | 经核查，数据库未授予管理用户所需的最小权限，未实现管理用户的权限分离。 |
| e）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； | 经核查，被测数据库系统由管理员账户SYS 配置访问控制策略，已基于角色配置严格的访问控制策略，严格限制用户对系统资源的访问。 |
| f）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； | 经核查，该数据库系统已基于角色配置严格的访问控制规则，访问控制粒度主体为用户级、客体为数据库表级。 |
| g）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。 | 未对重要主体和客体进行安全标记。 |
| 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； | 经核查，通过数据库审计系统对数据库所有用户的操作行为、SQL语句等进行审计记录。 |
| 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； | 经核查，审计记录包含：SQL语句、数据库名、线程、事务号、用户名、客户端IP、操作类型、状态、执行耗时、执行时间等。 |
| 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； | 经核查，审计记录本地保存，非授权用户无权限修改、删除，避免受到未预期的删除、修改或覆盖，且审计记录每天进行备份备份，保存时间满足180天以上。 |
| d）应对审计进程进行保护，防止未经授权的中断。 | 经核查，非授权用户无法中断系统审计进程。 |
| 入侵防范 | a）应遵循最小安装的原则，仅安装需要的组件和应用程序； | 根据GB∕T 28448-2019 《信息安全技术 网络安全等级保护测评要求》测评对象范围描述，数据库无该项要求。 |
| b）应关闭不需要的系统服务、默认共享和高危端口； | 根据GB∕T 28448-2019 《信息安全技术 网络安全等级保护测评要求》测评对象范围描述，数据库无该项要求。 |
| c）应通过设定终端接入方式或网络地址范围对通过网络进行管理的管理终端进行限制； | 经核查，1）通过配置安全策略限制仅允许通过堡垒机登录服务器后本地管理数据库；2）经核查防火墙中访问控制策略，具备堡垒机地址-服务器管理网段（10.33.0.0）的访问控制策略。 |
| d）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； | 根据GB∕T 28448-2019 《信息安全技术 网络安全等级保护测评要求》测评对象范围描述，数据库无该项要求。 |
| e）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； | 经漏洞扫描，数据库不存在高危漏洞。 |
| f）应能够检测到对重要节点进行入侵的行为，并在发生严重入侵事件时提供报警。 | 根据GB∕T 28448-2019 《信息安全技术 网络安全等级保护测评要求》测评对象范围描述，数据库无该项要求。 |
| 可信验证 | a）可基于可信根对计算设备的系统引导程序、系统程序、重要配置参数和应用程序等进行可信验证，并在应用程序的关键执行环节进行动态可信验证，在检测到其可信性受到破坏后进行报警，并将验证结果形成审计记录送至安全管理中心。 | 未采用技术措施对计算设备的系统引导程序、系统程序、重要配置参数和应用程序等进行可信验证。 |
| 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； | 运维人员登录堡垒机后采用SQL Developer软件连接数据库，保证鉴别信息、管理数据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。 | 采用SHA1+salt技术对用户鉴别信息进行加密存储，保证鉴别信息在存储过程中的完整性；但未采用校验技术保证重要业务数据、用户个人信息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； | 运维人员登录堡垒机后采用SQL Developer软件连接数据库，保证鉴别信息、管理数据在传输过程中的保密性。 |
| b）应采用密码技术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个人信息等。 | 采用SHA1+salt技术对用户鉴别信息进行加密存储，保证鉴别信息在存储过程中的保密性；采用aes-128-cbc对称加密算法保证个人信息在存储过程中的保密性；但未采用密码技术保证重要业务数据在存储过程中的保密性。 |
| 数据备份恢复 | a）应提供重要数据的本地数据备份与恢复功能； | 经核查，数据库配置了本地备份策略，每天全量备份，保留近20个全量备份库文件，运维人员每季度对备份文件进行恢复测试。 |
| b）应提供异地实时备份功能，利用通信网络将重要数据实时备份至备份场地； | 无异地备份措施。 |
| c）应提供重要数据处理系统的热冗余，保证系统的高可用性。 | 经核查，数据库采用主备方式部署，保证了系统的高可用性。 |
| 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； | 经核查，数据库用户退出后自动清理鉴别信息所在的存储空间。 |
| 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。 | 经核查，数据库用户退出后自动清理敏感数据存储空间。 |
| 个人信息保护 | a）应仅采集和保存业务必需的用户个人信息； | 1）数据库存储了用户姓名、手机号、身份证号、地址等个人信息；2）公司制定了YL-1-ISMS-02《信息安全和隐私管理策略手册》，在文件中明确了用户收集规则、收集方式、收集内容等。 |
| b）应禁止未授权访问和非法使用用户个人信息。 | 1）针对用户手机号的中间4位号码进行了脱敏处理；2）通过权限控制，仅有获得授权的管理员可以查看用户个人信息，同时通过审计日志对用户的操作行为进行记录；3）用户个人信息在入库时采用aes-128-cbc对称加密算法进行加密存储；4）公司制定了YL-1-ISMS-02《信息安全和隐私管理策略手册》，在文件中明确禁止非授权访问、非法使用个人信息。 |

4.1.4.6. pro-oauth-mysql

|  |  |  |
| --- | --- | --- |
| **安全控制点** | **测评指标** | **结果记录** |
| 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）数据库采用用户名/口令对用户进行身份标识、鉴别；2）执行select user,host from mysql.user命令，不存在相同的用户名；3）执行select\* from mysql.user where Pass word is null命令输入为空，无空口令账户存在；4）经访谈，DBA创建账户时使用密码生成器生成16位口令（数字、大写字母、小写字母和特殊字符组合），但数据库未配置口令无长度、复杂度、定期更换策略。 |
| 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）数据库未配置用户登录失败处理策略；2）执行show variables like %max\_connect\_errors%，返回值为：7200，即用户连接超时时间为2小时。 |
| 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； | 经核查，运维人员登录堡垒机后采用Navicat软件（采用SSL证书）连接数据库，防止鉴别信息在传输过程中被窃听。 |
| 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。 | 数据库未采用两种或两种以上组合的鉴别技术对用户进行身份鉴别。 |
| 访问控制 | a）应对登录的用户分配账户和权限； | 经核查，1）由管理员为登录数据库的用户创建账户、分配权限；2）目前数据库具有yl\_pro\_root、yl\_uat\_root等管理账户。 |
| b）应重命名或删除默认账户，修改默认账户的默认口令； | 被测数据库为采购的阿里云RDS数据库服务，阿里云RDS数据库无默认账户。 |
| 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； | 经核查，1）目前数据库仅具有yl\_pro\_root、yl\_uat\_root等管理账户，不存在多余、过期；2）存在多个堡垒机账户登录数据库时共用一个账户的情况。 |
| 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； | 经核查，未授予管理用户所需的最小权限，未实现管理用户的权限分离。 |
| e）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； | 经核查，由管理员为用户分配权限，控制用户对数据库的访问规则。 |
| f）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； | 经核查，数据库访问控制粒度达到主体为用户级，客体为数据库表级。 |
| g）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。 | 未对重要主体和客体进行安全标记。 |
| 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； | 经核查，通过阿里云SQL洞察服务对数据库所有用户的操作行为、SQL语句等进行审计记录。 |
| 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； | 经核查，审计记录包含：SQL语句、数据库名、线程、事务号、用户名、客户端IP、操作类型、状态、执行耗时、执行时间等。 |
| 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； | 经核查，审计记录本地保存，非授权用户无权限修改、删除，避免受到未预期的删除、修改或覆盖，且审计记录备份至数据库审计，保存180天。 |
| d）应对审计进程进行保护，防止未经授权的中断。 | 经核查，非授权用户无法中断系统审计进程。 |
| 入侵防范 | a）应遵循最小安装的原则，仅安装需要的组件和应用程序； | 根据GB∕T 28448-2019 《信息安全技术 网络安全等级保护测评要求》测评对象范围描述，数据库无该项要求。 |
| b）应关闭不需要的系统服务、默认共享和高危端口； | 根据GB∕T 28448-2019 《信息安全技术 网络安全等级保护测评要求》测评对象范围描述，数据库无该项要求。 |
| c）应通过设定终端接入方式或网络地址范围对通过网络进行管理的管理终端进行限制； | 经核查，1）通过堡垒机管理数据库；2）通过配置办公网防火墙策略限制仅允许办公区地址访问堡垒机。 |
| d）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； | 根据GB∕T 28448-2019 《信息安全技术 网络安全等级保护测评要求》测评对象范围描述，数据库无该项要求。 |
| e）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； | 被测数据库为采购的阿里云RDS数据库服务，由阿里云负责RDS数据库漏洞的检测、修复。 |
| f）应能够检测到对重要节点进行入侵的行为，并在发生严重入侵事件时提供报警。 | 根据GB∕T 28448-2019 《信息安全技术 网络安全等级保护测评要求》测评对象范围描述，数据库无该项要求。 |
| 可信验证 | a）可基于可信根对计算设备的系统引导程序、系统程序、重要配置参数和应用程序等进行可信验证，并在应用程序的关键执行环节进行动态可信验证，在检测到其可信性受到破坏后进行报警，并将验证结果形成审计记录送至安全管理中心。 | 未采用技术措施对计算设备的系统引导程序、系统程序、重要配置参数和应用程序等进行可信验证。 |
| 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； | 经核查，运维人员登录堡垒机后采用Navicat软件（采用SSL证书）连接数据库，保证重要数据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。 | 经核查，采用SHA1+salt技术对用户鉴别信息进行加密存储，保证鉴别信息在存储过程中的完整性；但未采用密码技术保证重要业务数据、用户个人信息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； | 经核查，运维人员登录堡垒机后采用Navicat软件（采用SSL证书）连接数据库，保证重要数据在传输过程中的保密性。 |
| b）应采用密码技术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个人信息等。 | 经核查，采用SHA1+salt技术对用户鉴别信息进行加密存储，保证鉴别信息在存储过程中的保密性；采用aes-128-cbc对称加密算法保存个人信息在存储过程中的保密性；但未采用密码技术保证重要业务数据在存储过程中的保密性。 |
| 数据备份恢复 | a）应提供重要数据的本地数据备份与恢复功能； | 经核查，数据库具有本地备份策略，每天全量备份，保留近7天的备份库，阿里云保证备份库的有效性。 |
| b）应提供异地实时备份功能，利用通信网络将重要数据实时备份至备份场地； | 无异地备份措施。 |
| c）应提供重要数据处理系统的热冗余，保证系统的高可用性。 | 经核查，数据库采用高可用版，保证了系统的高可用性。 |
| 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； | 经核查，数据库用户退出后自动清理鉴别信息所在的存储空间。 |
| 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。 | 经核查，数据库用户退出后自动清理敏感数据存储空间。 |
| 个人信息保护 | a）应仅采集和保存业务必需的用户个人信息； | 1）数据库存储了用户姓名、手机号、身份证号、地址等个人信息；2）公司制定了《个人信息保护规范》，在规范中明确了用户收集规则、收集方式、收集内容等。 |
| b）应禁止未授权访问和非法使用用户个人信息。 | 1）针对用户手机号的中间4位号码进行了脱敏处理；2）通过权限控制，仅有获得授权的管理员可以查看用户个人信息，同时通过审计日志对用户的操作行为进行记录；3）用户个人信息在入库时采用aes-128-cbc对称加密算法进行加密存储；4）公司制定了《个人信息保护规范》，在规范中明确禁止非授权访问、非法使用个人信息。 |

4.1.4.7. pro-tmp-laiqudb-mysql

|  |  |  |
| --- | --- | --- |
| **安全控制点** | **测评指标** | **结果记录** |
| 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）数据库采用用户名/口令对用户进行身份标识、鉴别；2）执行select user,host from mysql.user命令，不存在相同的用户名；3）执行select\* from mysql.user where Pass word is null命令输入为空，无空口令账户存在；4）经访谈，DBA创建账户时使用密码生成器生成16位口令（数字、大写字母、小写字母和特殊字符组合），但数据库未配置口令无长度、复杂度、定期更换策略。 |
| 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）数据库未配置用户登录失败处理策略；2）执行show variables like %max\_connect\_errors%，返回值为：7200，即用户连接超时时间为2小时。 |
| 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； | 经核查，运维人员登录堡垒机后采用Navicat软件（采用SSL证书）连接数据库，防止鉴别信息在传输过程中被窃听。 |
| 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。 | 数据库未采用两种或两种以上组合的鉴别技术对用户进行身份鉴别。 |
| 访问控制 | a）应对登录的用户分配账户和权限； | 经核查，1）由管理员为登录数据库的用户创建账户、分配权限；2）目前数据库具有yl\_pro\_root、yl\_uat\_root等管理账户。 |
| b）应重命名或删除默认账户，修改默认账户的默认口令； | 被测数据库为采购的阿里云RDS数据库服务，阿里云RDS数据库无默认账户。 |
| 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； | 经核查，1）目前数据库仅具有yl\_pro\_root、yl\_uat\_root等管理账户，不存在多余、过期；2）存在多个堡垒机账户登录数据库时共用一个账户的情况。 |
| 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； | 经核查，未授予管理用户所需的最小权限，未实现管理用户的权限分离。 |
| e）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； | 经核查，由管理员为用户分配权限，控制用户对数据库的访问规则。 |
| f）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； | 经核查，数据库访问控制粒度达到主体为用户级，客体为数据库表级。 |
| g）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。 | 未对重要主体和客体进行安全标记。 |
| 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； | 经核查，通过阿里云SQL洞察服务对数据库所有用户的操作行为、SQL语句等进行审计记录。 |
| 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； | 经核查，审计记录包含：SQL语句、数据库名、线程、事务号、用户名、客户端IP、操作类型、状态、执行耗时、执行时间等。 |
| 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； | 经核查，审计记录本地保存，非授权用户无权限修改、删除，避免受到未预期的删除、修改或覆盖，且审计记录备份至数据库审计，保存180天。 |
| d）应对审计进程进行保护，防止未经授权的中断。 | 经核查，非授权用户无法中断系统审计进程。 |
| 入侵防范 | a）应遵循最小安装的原则，仅安装需要的组件和应用程序； | 根据GB∕T 28448-2019 《信息安全技术 网络安全等级保护测评要求》测评对象范围描述，数据库无该项要求。 |
| b）应关闭不需要的系统服务、默认共享和高危端口； | 根据GB∕T 28448-2019 《信息安全技术 网络安全等级保护测评要求》测评对象范围描述，数据库无该项要求。 |
| c）应通过设定终端接入方式或网络地址范围对通过网络进行管理的管理终端进行限制； | 经核查，1）通过堡垒机管理数据库；2）通过配置办公网防火墙策略限制仅允许办公区地址访问堡垒机。 |
| d）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； | 根据GB∕T 28448-2019 《信息安全技术 网络安全等级保护测评要求》测评对象范围描述，数据库无该项要求。 |
| e）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； | 被测数据库为采购的阿里云RDS数据库服务，由阿里云负责RDS数据库漏洞的检测、修复。 |
| f）应能够检测到对重要节点进行入侵的行为，并在发生严重入侵事件时提供报警。 | 根据GB∕T 28448-2019 《信息安全技术 网络安全等级保护测评要求》测评对象范围描述，数据库无该项要求。 |
| 可信验证 | a）可基于可信根对计算设备的系统引导程序、系统程序、重要配置参数和应用程序等进行可信验证，并在应用程序的关键执行环节进行动态可信验证，在检测到其可信性受到破坏后进行报警，并将验证结果形成审计记录送至安全管理中心。 | 未采用技术措施对计算设备的系统引导程序、系统程序、重要配置参数和应用程序等进行可信验证。 |
| 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； | 经核查，运维人员登录堡垒机后采用Navicat软件（采用SSL证书）连接数据库，保证重要数据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。 | 经核查，采用SHA1+salt技术对用户鉴别信息进行加密存储，保证鉴别信息在存储过程中的完整性；但未采用密码技术保证重要业务数据、用户个人信息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； | 经核查，运维人员登录堡垒机后采用Navicat软件（采用SSL证书）连接数据库，保证重要数据在传输过程中的保密性。 |
| b）应采用密码技术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个人信息等。 | 经核查，采用SHA1+salt技术对用户鉴别信息进行加密存储，保证鉴别信息在存储过程中的保密性；采用aes-128-cbc对称加密算法保存个人信息在存储过程中的保密性；但未采用密码技术保证重要业务数据在存储过程中的保密性。 |
| 数据备份恢复 | a）应提供重要数据的本地数据备份与恢复功能； | 经核查，数据库具有本地备份策略，每天全量备份，保留近7天的备份库，阿里云保证备份库的有效性。 |
| b）应提供异地实时备份功能，利用通信网络将重要数据实时备份至备份场地； | 无异地备份措施。 |
| c）应提供重要数据处理系统的热冗余，保证系统的高可用性。 | 经核查，数据库采用高可用版，保证了系统的高可用性。 |
| 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； | 经核查，数据库用户退出后自动清理鉴别信息所在的存储空间。 |
| 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。 | 经核查，数据库用户退出后自动清理敏感数据存储空间。 |
| 个人信息保护 | a）应仅采集和保存业务必需的用户个人信息； | 1）数据库存储了用户姓名、手机号、身份证号、地址等个人信息；2）公司制定了《个人信息保护规范》，在规范中明确了用户收集规则、收集方式、收集内容等。 |
| b）应禁止未授权访问和非法使用用户个人信息。 | 1）针对用户手机号的中间4位号码进行了脱敏处理；2）通过权限控制，仅有获得授权的管理员可以查看用户个人信息，同时通过审计日志对用户的操作行为进行记录；3）用户个人信息在入库时采用aes-128-cbc对称加密算法进行加密存储；4）公司制定了《个人信息保护规范》，在规范中明确禁止非授权访问、非法使用个人信息。 |

4.1.4.8. pro-tmp-sms-mysql

|  |  |  |
| --- | --- | --- |
| **安全控制点** | **测评指标** | **结果记录** |
| 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）数据库采用用户名/口令对用户进行身份标识、鉴别；2）执行select user,host from mysql.user命令，不存在相同的用户名；3）执行select\* from mysql.user where Pass word is null命令输入为空，无空口令账户存在；4）经访谈，DBA创建账户时使用密码生成器生成16位口令（数字、大写字母、小写字母和特殊字符组合），但数据库未配置口令无长度、复杂度、定期更换策略。 |
| 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）数据库未配置用户登录失败处理策略；2）执行show variables like %max\_connect\_errors%，返回值为：7200，即用户连接超时时间为2小时。 |
| 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； | 经核查，运维人员登录堡垒机后采用Navicat软件（采用SSL证书）连接数据库，防止鉴别信息在传输过程中被窃听。 |
| 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。 | 数据库未采用两种或两种以上组合的鉴别技术对用户进行身份鉴别。 |
| 访问控制 | a）应对登录的用户分配账户和权限； | 经核查，1）由管理员为登录数据库的用户创建账户、分配权限；2）目前数据库具有yl\_pro\_root、yl\_uat\_root等管理账户。 |
| b）应重命名或删除默认账户，修改默认账户的默认口令； | 被测数据库为采购的阿里云RDS数据库服务，阿里云RDS数据库无默认账户。 |
| 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； | 经核查，1）目前数据库仅具有yl\_pro\_root、yl\_uat\_root等管理账户，不存在多余、过期；2）存在多个堡垒机账户登录数据库时共用一个账户的情况。 |
| 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； | 经核查，未授予管理用户所需的最小权限，未实现管理用户的权限分离。 |
| e）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； | 经核查，由管理员为用户分配权限，控制用户对数据库的访问规则。 |
| f）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； | 经核查，数据库访问控制粒度达到主体为用户级，客体为数据库表级。 |
| g）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。 | 未对重要主体和客体进行安全标记。 |
| 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； | 经核查，通过阿里云SQL洞察服务对数据库所有用户的操作行为、SQL语句等进行审计记录。 |
| 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； | 经核查，审计记录包含：SQL语句、数据库名、线程、事务号、用户名、客户端IP、操作类型、状态、执行耗时、执行时间等。 |
| 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； | 经核查，审计记录本地保存，非授权用户无权限修改、删除，避免受到未预期的删除、修改或覆盖，且审计记录备份至数据库审计，保存180天。 |
| d）应对审计进程进行保护，防止未经授权的中断。 | 经核查，非授权用户无法中断系统审计进程。 |
| 入侵防范 | a）应遵循最小安装的原则，仅安装需要的组件和应用程序； | 根据GB∕T 28448-2019 《信息安全技术 网络安全等级保护测评要求》测评对象范围描述，数据库无该项要求。 |
| b）应关闭不需要的系统服务、默认共享和高危端口； | 根据GB∕T 28448-2019 《信息安全技术 网络安全等级保护测评要求》测评对象范围描述，数据库无该项要求。 |
| c）应通过设定终端接入方式或网络地址范围对通过网络进行管理的管理终端进行限制； | 经核查，1）通过堡垒机管理数据库；2）通过配置办公网防火墙策略限制仅允许办公区地址访问堡垒机。 |
| d）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； | 根据GB∕T 28448-2019 《信息安全技术 网络安全等级保护测评要求》测评对象范围描述，数据库无该项要求。 |
| e）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； | 被测数据库为采购的阿里云RDS数据库服务，由阿里云负责RDS数据库漏洞的检测、修复。 |
| f）应能够检测到对重要节点进行入侵的行为，并在发生严重入侵事件时提供报警。 | 根据GB∕T 28448-2019 《信息安全技术 网络安全等级保护测评要求》测评对象范围描述，数据库无该项要求。 |
| 可信验证 | a）可基于可信根对计算设备的系统引导程序、系统程序、重要配置参数和应用程序等进行可信验证，并在应用程序的关键执行环节进行动态可信验证，在检测到其可信性受到破坏后进行报警，并将验证结果形成审计记录送至安全管理中心。 | 未采用技术措施对计算设备的系统引导程序、系统程序、重要配置参数和应用程序等进行可信验证。 |
| 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； | 经核查，运维人员登录堡垒机后采用Navicat软件（采用SSL证书）连接数据库，保证重要数据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。 | 经核查，采用SHA1+salt技术对用户鉴别信息进行加密存储，保证鉴别信息在存储过程中的完整性；但未采用密码技术保证重要业务数据、用户个人信息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； | 经核查，运维人员登录堡垒机后采用Navicat软件（采用SSL证书）连接数据库，保证重要数据在传输过程中的保密性。 |
| b）应采用密码技术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个人信息等。 | 经核查，采用SHA1+salt技术对用户鉴别信息进行加密存储，保证鉴别信息在存储过程中的保密性；采用aes-128-cbc对称加密算法保存个人信息在存储过程中的保密性；但未采用密码技术保证重要业务数据在存储过程中的保密性。 |
| 数据备份恢复 | a）应提供重要数据的本地数据备份与恢复功能； | 经核查，数据库具有本地备份策略，每天全量备份，保留近7天的备份库，阿里云保证备份库的有效性。 |
| b）应提供异地实时备份功能，利用通信网络将重要数据实时备份至备份场地； | 无异地备份措施。 |
| c）应提供重要数据处理系统的热冗余，保证系统的高可用性。 | 经核查，数据库采用高可用版，保证了系统的高可用性。 |
| 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； | 经核查，数据库用户退出后自动清理鉴别信息所在的存储空间。 |
| 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。 | 经核查，数据库用户退出后自动清理敏感数据存储空间。 |
| 个人信息保护 | a）应仅采集和保存业务必需的用户个人信息； | 1）数据库存储了用户姓名、手机号、身份证号、地址等个人信息；2）公司制定了《个人信息保护规范》，在规范中明确了用户收集规则、收集方式、收集内容等。 |
| b）应禁止未授权访问和非法使用用户个人信息。 | 1）针对用户手机号的中间4位号码进行了脱敏处理；2）通过权限控制，仅有获得授权的管理员可以查看用户个人信息，同时通过审计日志对用户的操作行为进行记录；3）用户个人信息在入库时采用aes-128-cbc对称加密算法进行加密存储；4）公司制定了《个人信息保护规范》，在规范中明确禁止非授权访问、非法使用个人信息。 |

4.1.4.9. pro-spmibill3-opt-mysql

|  |  |  |
| --- | --- | --- |
| **安全控制点** | **测评指标** | **结果记录** |
| 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）数据库采用用户名/口令对用户进行身份标识、鉴别；2）执行select user,host from mysql.user命令，不存在相同的用户名；3）执行select\* from mysql.user where Pass word is null命令输入为空，无空口令账户存在；4）经访谈，DBA创建账户时使用密码生成器生成16位口令（数字、大写字母、小写字母和特殊字符组合），但数据库未配置口令无长度、复杂度、定期更换策略。 |
| 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）数据库未配置用户登录失败处理策略；2）执行show variables like %max\_connect\_errors%，返回值为：7200，即用户连接超时时间为2小时。 |
| 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； | 经核查，运维人员登录堡垒机后采用Navicat软件（采用SSL证书）连接数据库，防止鉴别信息在传输过程中被窃听。 |
| 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。 | 数据库未采用两种或两种以上组合的鉴别技术对用户进行身份鉴别。 |
| 访问控制 | a）应对登录的用户分配账户和权限； | 经核查，1）由管理员为登录数据库的用户创建账户、分配权限；2）目前数据库具有yl\_pro\_root、yl\_uat\_root等管理账户。 |
| b）应重命名或删除默认账户，修改默认账户的默认口令； | 被测数据库为采购的阿里云RDS数据库服务，阿里云RDS数据库无默认账户。 |
| 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； | 经核查，1）目前数据库仅具有yl\_pro\_root、yl\_uat\_root等管理账户，不存在多余、过期；2）存在多个堡垒机账户登录数据库时共用一个账户的情况。 |
| 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； | 经核查，未授予管理用户所需的最小权限，未实现管理用户的权限分离。 |
| e）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； | 经核查，由管理员为用户分配权限，控制用户对数据库的访问规则。 |
| f）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； | 经核查，数据库访问控制粒度达到主体为用户级，客体为数据库表级。 |
| g）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。 | 未对重要主体和客体进行安全标记。 |
| 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； | 经核查，通过阿里云SQL洞察服务对数据库所有用户的操作行为、SQL语句等进行审计记录。 |
| 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； | 经核查，审计记录包含：SQL语句、数据库名、线程、事务号、用户名、客户端IP、操作类型、状态、执行耗时、执行时间等。 |
| 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； | 经核查，审计记录本地保存，非授权用户无权限修改、删除，避免受到未预期的删除、修改或覆盖，且审计记录备份至数据库审计，保存180天。 |
| d）应对审计进程进行保护，防止未经授权的中断。 | 经核查，非授权用户无法中断系统审计进程。 |
| 入侵防范 | a）应遵循最小安装的原则，仅安装需要的组件和应用程序； | 根据GB∕T 28448-2019 《信息安全技术 网络安全等级保护测评要求》测评对象范围描述，数据库无该项要求。 |
| b）应关闭不需要的系统服务、默认共享和高危端口； | 根据GB∕T 28448-2019 《信息安全技术 网络安全等级保护测评要求》测评对象范围描述，数据库无该项要求。 |
| c）应通过设定终端接入方式或网络地址范围对通过网络进行管理的管理终端进行限制； | 经核查，1）通过堡垒机管理数据库；2）通过配置办公网防火墙策略限制仅允许办公区地址访问堡垒机。 |
| d）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； | 根据GB∕T 28448-2019 《信息安全技术 网络安全等级保护测评要求》测评对象范围描述，数据库无该项要求。 |
| e）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； | 被测数据库为采购的阿里云RDS数据库服务，由阿里云负责RDS数据库漏洞的检测、修复。 |
| f）应能够检测到对重要节点进行入侵的行为，并在发生严重入侵事件时提供报警。 | 根据GB∕T 28448-2019 《信息安全技术 网络安全等级保护测评要求》测评对象范围描述，数据库无该项要求。 |
| 可信验证 | a）可基于可信根对计算设备的系统引导程序、系统程序、重要配置参数和应用程序等进行可信验证，并在应用程序的关键执行环节进行动态可信验证，在检测到其可信性受到破坏后进行报警，并将验证结果形成审计记录送至安全管理中心。 | 未采用技术措施对计算设备的系统引导程序、系统程序、重要配置参数和应用程序等进行可信验证。 |
| 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； | 经核查，运维人员登录堡垒机后采用Navicat软件（采用SSL证书）连接数据库，保证重要数据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。 | 经核查，采用SHA1+salt技术对用户鉴别信息进行加密存储，保证鉴别信息在存储过程中的完整性；但未采用密码技术保证重要业务数据、用户个人信息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； | 经核查，运维人员登录堡垒机后采用Navicat软件（采用SSL证书）连接数据库，保证重要数据在传输过程中的保密性。 |
| b）应采用密码技术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个人信息等。 | 经核查，采用SHA1+salt技术对用户鉴别信息进行加密存储，保证鉴别信息在存储过程中的保密性；采用aes-128-cbc对称加密算法保存个人信息在存储过程中的保密性；但未采用密码技术保证重要业务数据在存储过程中的保密性。 |
| 数据备份恢复 | a）应提供重要数据的本地数据备份与恢复功能； | 经核查，数据库具有本地备份策略，每天全量备份，保留近7天的备份库，阿里云保证备份库的有效性。 |
| b）应提供异地实时备份功能，利用通信网络将重要数据实时备份至备份场地； | 无异地备份措施。 |
| c）应提供重要数据处理系统的热冗余，保证系统的高可用性。 | 经核查，数据库采用高可用版，保证了系统的高可用性。 |
| 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； | 经核查，数据库用户退出后自动清理鉴别信息所在的存储空间。 |
| 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。 | 经核查，数据库用户退出后自动清理敏感数据存储空间。 |
| 个人信息保护 | a）应仅采集和保存业务必需的用户个人信息； | 1）数据库存储了用户姓名、手机号、身份证号、地址等个人信息；2）公司制定了《个人信息保护规范》，在规范中明确了用户收集规则、收集方式、收集内容等。 |
| b）应禁止未授权访问和非法使用用户个人信息。 | 1）针对用户手机号的中间4位号码进行了脱敏处理；2）通过权限控制，仅有获得授权的管理员可以查看用户个人信息，同时通过审计日志对用户的操作行为进行记录；3）用户个人信息在入库时采用aes-128-cbc对称加密算法进行加密存储；4）公司制定了《个人信息保护规范》，在规范中明确禁止非授权访问、非法使用个人信息。 |

4.1.4.10. pro-spmibill3-piece-mysql

|  |  |  |
| --- | --- | --- |
| **安全控制点** | **测评指标** | **结果记录** |
| 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）数据库采用用户名/口令对用户进行身份标识、鉴别；2）执行select user,host from mysql.user命令，不存在相同的用户名；3）执行select\* from mysql.user where Pass word is null命令输入为空，无空口令账户存在；4）经访谈，DBA创建账户时使用密码生成器生成16位口令（数字、大写字母、小写字母和特殊字符组合），但数据库未配置口令无长度、复杂度、定期更换策略。 |
| 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）数据库未配置用户登录失败处理策略；2）执行show variables like %max\_connect\_errors%，返回值为：7200，即用户连接超时时间为2小时。 |
| 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； | 经核查，运维人员登录堡垒机后采用Navicat软件（采用SSL证书）连接数据库，防止鉴别信息在传输过程中被窃听。 |
| 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。 | 数据库未采用两种或两种以上组合的鉴别技术对用户进行身份鉴别。 |
| 访问控制 | a）应对登录的用户分配账户和权限； | 经核查，1）由管理员为登录数据库的用户创建账户、分配权限；2）目前数据库具有yl\_pro\_root、yl\_uat\_root等管理账户。 |
| b）应重命名或删除默认账户，修改默认账户的默认口令； | 被测数据库为采购的阿里云RDS数据库服务，阿里云RDS数据库无默认账户。 |
| 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； | 经核查，1）目前数据库仅具有yl\_pro\_root、yl\_uat\_root等管理账户，不存在多余、过期；2）存在多个堡垒机账户登录数据库时共用一个账户的情况。 |
| 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； | 经核查，未授予管理用户所需的最小权限，未实现管理用户的权限分离。 |
| e）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； | 经核查，由管理员为用户分配权限，控制用户对数据库的访问规则。 |
| f）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； | 经核查，数据库访问控制粒度达到主体为用户级，客体为数据库表级。 |
| g）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。 | 未对重要主体和客体进行安全标记。 |
| 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； | 经核查，通过阿里云SQL洞察服务对数据库所有用户的操作行为、SQL语句等进行审计记录。 |
| 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； | 经核查，审计记录包含：SQL语句、数据库名、线程、事务号、用户名、客户端IP、操作类型、状态、执行耗时、执行时间等。 |
| 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； | 经核查，审计记录本地保存，非授权用户无权限修改、删除，避免受到未预期的删除、修改或覆盖，且审计记录备份至数据库审计，保存180天。 |
| d）应对审计进程进行保护，防止未经授权的中断。 | 经核查，非授权用户无法中断系统审计进程。 |
| 入侵防范 | a）应遵循最小安装的原则，仅安装需要的组件和应用程序； | 根据GB∕T 28448-2019 《信息安全技术 网络安全等级保护测评要求》测评对象范围描述，数据库无该项要求。 |
| b）应关闭不需要的系统服务、默认共享和高危端口； | 根据GB∕T 28448-2019 《信息安全技术 网络安全等级保护测评要求》测评对象范围描述，数据库无该项要求。 |
| c）应通过设定终端接入方式或网络地址范围对通过网络进行管理的管理终端进行限制； | 经核查，1）通过堡垒机管理数据库；2）通过配置办公网防火墙策略限制仅允许办公区地址访问堡垒机。 |
| d）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； | 根据GB∕T 28448-2019 《信息安全技术 网络安全等级保护测评要求》测评对象范围描述，数据库无该项要求。 |
| e）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； | 被测数据库为采购的阿里云RDS数据库服务，由阿里云负责RDS数据库漏洞的检测、修复。 |
| f）应能够检测到对重要节点进行入侵的行为，并在发生严重入侵事件时提供报警。 | 根据GB∕T 28448-2019 《信息安全技术 网络安全等级保护测评要求》测评对象范围描述，数据库无该项要求。 |
| 可信验证 | a）可基于可信根对计算设备的系统引导程序、系统程序、重要配置参数和应用程序等进行可信验证，并在应用程序的关键执行环节进行动态可信验证，在检测到其可信性受到破坏后进行报警，并将验证结果形成审计记录送至安全管理中心。 | 未采用技术措施对计算设备的系统引导程序、系统程序、重要配置参数和应用程序等进行可信验证。 |
| 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； | 经核查，运维人员登录堡垒机后采用Navicat软件（采用SSL证书）连接数据库，保证重要数据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。 | 经核查，采用SHA1+salt技术对用户鉴别信息进行加密存储，保证鉴别信息在存储过程中的完整性；但未采用密码技术保证重要业务数据、用户个人信息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； | 经核查，运维人员登录堡垒机后采用Navicat软件（采用SSL证书）连接数据库，保证重要数据在传输过程中的保密性。 |
| b）应采用密码技术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个人信息等。 | 经核查，采用SHA1+salt技术对用户鉴别信息进行加密存储，保证鉴别信息在存储过程中的保密性；采用aes-128-cbc对称加密算法保存个人信息在存储过程中的保密性；但未采用密码技术保证重要业务数据在存储过程中的保密性。 |
| 数据备份恢复 | a）应提供重要数据的本地数据备份与恢复功能； | 经核查，数据库具有本地备份策略，每天全量备份，保留近7天的备份库，阿里云保证备份库的有效性。 |
| b）应提供异地实时备份功能，利用通信网络将重要数据实时备份至备份场地； | 无异地备份措施。 |
| c）应提供重要数据处理系统的热冗余，保证系统的高可用性。 | 经核查，数据库采用高可用版，保证了系统的高可用性。 |
| 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； | 经核查，数据库用户退出后自动清理鉴别信息所在的存储空间。 |
| 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。 | 经核查，数据库用户退出后自动清理敏感数据存储空间。 |
| 个人信息保护 | a）应仅采集和保存业务必需的用户个人信息； | 1）数据库存储了用户姓名、手机号、身份证号、地址等个人信息；2）公司制定了《个人信息保护规范》，在规范中明确了用户收集规则、收集方式、收集内容等。 |
| b）应禁止未授权访问和非法使用用户个人信息。 | 1）针对用户手机号的中间4位号码进行了脱敏处理；2）通过权限控制，仅有获得授权的管理员可以查看用户个人信息，同时通过审计日志对用户的操作行为进行记录；3）用户个人信息在入库时采用aes-128-cbc对称加密算法进行加密存储；4）公司制定了《个人信息保护规范》，在规范中明确禁止非授权访问、非法使用个人信息。 |

4.1.4.11. pro-dc-mysql

|  |  |  |
| --- | --- | --- |
| **安全控制点** | **测评指标** | **结果记录** |
| 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）数据库采用用户名/口令对用户进行身份标识、鉴别；2）执行select user,host from mysql.user命令，不存在相同的用户名；3）执行select\* from mysql.user where Pass word is null命令输入为空，无空口令账户存在；4）经访谈，DBA创建账户时使用密码生成器生成16位口令（数字、大写字母、小写字母和特殊字符组合），但数据库未配置口令无长度、复杂度、定期更换策略。 |
| 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）数据库未配置用户登录失败处理策略；2）执行show variables like %max\_connect\_errors%，返回值为：7200，即用户连接超时时间为2小时。 |
| 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； | 经核查，运维人员登录堡垒机后采用Navicat软件（采用SSL证书）连接数据库，防止鉴别信息在传输过程中被窃听。 |
| 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。 | 数据库未采用两种或两种以上组合的鉴别技术对用户进行身份鉴别。 |
| 访问控制 | a）应对登录的用户分配账户和权限； | 经核查，1）由管理员为登录数据库的用户创建账户、分配权限；2）目前数据库具有yl\_pro\_root、yl\_uat\_root等管理账户。 |
| b）应重命名或删除默认账户，修改默认账户的默认口令； | 被测数据库为采购的阿里云RDS数据库服务，阿里云RDS数据库无默认账户。 |
| 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； | 经核查，1）目前数据库仅具有yl\_pro\_root、yl\_uat\_root等管理账户，不存在多余、过期；2）存在多个堡垒机账户登录数据库时共用一个账户的情况。 |
| 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； | 经核查，未授予管理用户所需的最小权限，未实现管理用户的权限分离。 |
| e）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； | 经核查，由管理员为用户分配权限，控制用户对数据库的访问规则。 |
| f）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； | 经核查，数据库访问控制粒度达到主体为用户级，客体为数据库表级。 |
| g）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。 | 未对重要主体和客体进行安全标记。 |
| 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； | 经核查，通过阿里云SQL洞察服务对数据库所有用户的操作行为、SQL语句等进行审计记录。 |
| 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； | 经核查，审计记录包含：SQL语句、数据库名、线程、事务号、用户名、客户端IP、操作类型、状态、执行耗时、执行时间等。 |
| 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； | 经核查，审计记录本地保存，非授权用户无权限修改、删除，避免受到未预期的删除、修改或覆盖，且审计记录备份至数据库审计，保存180天。 |
| d）应对审计进程进行保护，防止未经授权的中断。 | 经核查，非授权用户无法中断系统审计进程。 |
| 入侵防范 | a）应遵循最小安装的原则，仅安装需要的组件和应用程序； | 根据GB∕T 28448-2019 《信息安全技术 网络安全等级保护测评要求》测评对象范围描述，数据库无该项要求。 |
| b）应关闭不需要的系统服务、默认共享和高危端口； | 根据GB∕T 28448-2019 《信息安全技术 网络安全等级保护测评要求》测评对象范围描述，数据库无该项要求。 |
| c）应通过设定终端接入方式或网络地址范围对通过网络进行管理的管理终端进行限制； | 经核查，1）通过堡垒机管理数据库；2）通过配置办公网防火墙策略限制仅允许办公区地址访问堡垒机。 |
| d）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； | 根据GB∕T 28448-2019 《信息安全技术 网络安全等级保护测评要求》测评对象范围描述，数据库无该项要求。 |
| e）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； | 被测数据库为采购的阿里云RDS数据库服务，由阿里云负责RDS数据库漏洞的检测、修复。 |
| f）应能够检测到对重要节点进行入侵的行为，并在发生严重入侵事件时提供报警。 | 根据GB∕T 28448-2019 《信息安全技术 网络安全等级保护测评要求》测评对象范围描述，数据库无该项要求。 |
| 可信验证 | a）可基于可信根对计算设备的系统引导程序、系统程序、重要配置参数和应用程序等进行可信验证，并在应用程序的关键执行环节进行动态可信验证，在检测到其可信性受到破坏后进行报警，并将验证结果形成审计记录送至安全管理中心。 | 未采用技术措施对计算设备的系统引导程序、系统程序、重要配置参数和应用程序等进行可信验证。 |
| 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； | 经核查，运维人员登录堡垒机后采用Navicat软件（采用SSL证书）连接数据库，保证重要数据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。 | 经核查，采用SHA1+salt技术对用户鉴别信息进行加密存储，保证鉴别信息在存储过程中的完整性；但未采用密码技术保证重要业务数据、用户个人信息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； | 经核查，运维人员登录堡垒机后采用Navicat软件（采用SSL证书）连接数据库，保证重要数据在传输过程中的保密性。 |
| b）应采用密码技术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个人信息等。 | 经核查，采用SHA1+salt技术对用户鉴别信息进行加密存储，保证鉴别信息在存储过程中的保密性；采用aes-128-cbc对称加密算法保存个人信息在存储过程中的保密性；但未采用密码技术保证重要业务数据在存储过程中的保密性。 |
| 数据备份恢复 | a）应提供重要数据的本地数据备份与恢复功能； | 经核查，数据库具有本地备份策略，每天全量备份，保留近7天的备份库，阿里云保证备份库的有效性。 |
| b）应提供异地实时备份功能，利用通信网络将重要数据实时备份至备份场地； | 无异地备份措施。 |
| c）应提供重要数据处理系统的热冗余，保证系统的高可用性。 | 经核查，数据库采用高可用版，保证了系统的高可用性。 |
| 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； | 经核查，数据库用户退出后自动清理鉴别信息所在的存储空间。 |
| 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。 | 经核查，数据库用户退出后自动清理敏感数据存储空间。 |
| 个人信息保护 | a）应仅采集和保存业务必需的用户个人信息； | 1）数据库存储了用户姓名、手机号、身份证号、地址等个人信息；2）公司制定了《个人信息保护规范》，在规范中明确了用户收集规则、收集方式、收集内容等。 |
| b）应禁止未授权访问和非法使用用户个人信息。 | 1）针对用户手机号的中间4位号码进行了脱敏处理；2）通过权限控制，仅有获得授权的管理员可以查看用户个人信息，同时通过审计日志对用户的操作行为进行记录；3）用户个人信息在入库时采用aes-128-cbc对称加密算法进行加密存储；4）公司制定了《个人信息保护规范》，在规范中明确禁止非授权访问、非法使用个人信息。 |

4.1.4.12. pro-spmibill-2-mysql

|  |  |  |
| --- | --- | --- |
| **安全控制点** | **测评指标** | **结果记录** |
| 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）数据库采用用户名/口令对用户进行身份标识、鉴别；2）执行select user,host from mysql.user命令，不存在相同的用户名；3）执行select\* from mysql.user where Pass word is null命令输入为空，无空口令账户存在；4）经访谈，DBA创建账户时使用密码生成器生成16位口令（数字、大写字母、小写字母和特殊字符组合），但数据库未配置口令无长度、复杂度、定期更换策略。 |
| 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）数据库未配置用户登录失败处理策略；2）执行show variables like %max\_connect\_errors%，返回值为：7200，即用户连接超时时间为2小时。 |
| 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； | 经核查，运维人员登录堡垒机后采用Navicat软件（采用SSL证书）连接数据库，防止鉴别信息在传输过程中被窃听。 |
| 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。 | 数据库未采用两种或两种以上组合的鉴别技术对用户进行身份鉴别。 |
| 访问控制 | a）应对登录的用户分配账户和权限； | 经核查，1）由管理员为登录数据库的用户创建账户、分配权限；2）目前数据库具有yl\_pro\_root、yl\_uat\_root等管理账户。 |
| b）应重命名或删除默认账户，修改默认账户的默认口令； | 被测数据库为采购的阿里云RDS数据库服务，阿里云RDS数据库无默认账户。 |
| 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； | 经核查，1）目前数据库仅具有yl\_pro\_root、yl\_uat\_root等管理账户，不存在多余、过期；2）存在多个堡垒机账户登录数据库时共用一个账户的情况。 |
| 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； | 经核查，未授予管理用户所需的最小权限，未实现管理用户的权限分离。 |
| e）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； | 经核查，由管理员为用户分配权限，控制用户对数据库的访问规则。 |
| f）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； | 经核查，数据库访问控制粒度达到主体为用户级，客体为数据库表级。 |
| g）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。 | 未对重要主体和客体进行安全标记。 |
| 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； | 经核查，通过阿里云SQL洞察服务对数据库所有用户的操作行为、SQL语句等进行审计记录。 |
| 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； | 经核查，审计记录包含：SQL语句、数据库名、线程、事务号、用户名、客户端IP、操作类型、状态、执行耗时、执行时间等。 |
| 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； | 经核查，审计记录本地保存，非授权用户无权限修改、删除，避免受到未预期的删除、修改或覆盖，且审计记录备份至数据库审计，保存180天。 |
| d）应对审计进程进行保护，防止未经授权的中断。 | 经核查，非授权用户无法中断系统审计进程。 |
| 入侵防范 | a）应遵循最小安装的原则，仅安装需要的组件和应用程序； | 根据GB∕T 28448-2019 《信息安全技术 网络安全等级保护测评要求》测评对象范围描述，数据库无该项要求。 |
| b）应关闭不需要的系统服务、默认共享和高危端口； | 根据GB∕T 28448-2019 《信息安全技术 网络安全等级保护测评要求》测评对象范围描述，数据库无该项要求。 |
| c）应通过设定终端接入方式或网络地址范围对通过网络进行管理的管理终端进行限制； | 经核查，1）通过堡垒机管理数据库；2）通过配置办公网防火墙策略限制仅允许办公区地址访问堡垒机。 |
| d）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； | 根据GB∕T 28448-2019 《信息安全技术 网络安全等级保护测评要求》测评对象范围描述，数据库无该项要求。 |
| e）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； | 被测数据库为采购的阿里云RDS数据库服务，由阿里云负责RDS数据库漏洞的检测、修复。 |
| f）应能够检测到对重要节点进行入侵的行为，并在发生严重入侵事件时提供报警。 | 根据GB∕T 28448-2019 《信息安全技术 网络安全等级保护测评要求》测评对象范围描述，数据库无该项要求。 |
| 可信验证 | a）可基于可信根对计算设备的系统引导程序、系统程序、重要配置参数和应用程序等进行可信验证，并在应用程序的关键执行环节进行动态可信验证，在检测到其可信性受到破坏后进行报警，并将验证结果形成审计记录送至安全管理中心。 | 未采用技术措施对计算设备的系统引导程序、系统程序、重要配置参数和应用程序等进行可信验证。 |
| 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； | 经核查，运维人员登录堡垒机后采用Navicat软件（采用SSL证书）连接数据库，保证重要数据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。 | 经核查，采用SHA1+salt技术对用户鉴别信息进行加密存储，保证鉴别信息在存储过程中的完整性；但未采用密码技术保证重要业务数据、用户个人信息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； | 经核查，运维人员登录堡垒机后采用Navicat软件（采用SSL证书）连接数据库，保证重要数据在传输过程中的保密性。 |
| b）应采用密码技术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个人信息等。 | 经核查，采用SHA1+salt技术对用户鉴别信息进行加密存储，保证鉴别信息在存储过程中的保密性；采用aes-128-cbc对称加密算法保存个人信息在存储过程中的保密性；但未采用密码技术保证重要业务数据在存储过程中的保密性。 |
| 数据备份恢复 | a）应提供重要数据的本地数据备份与恢复功能； | 经核查，数据库具有本地备份策略，每天全量备份，保留近7天的备份库，阿里云保证备份库的有效性。 |
| b）应提供异地实时备份功能，利用通信网络将重要数据实时备份至备份场地； | 无异地备份措施。 |
| c）应提供重要数据处理系统的热冗余，保证系统的高可用性。 | 经核查，数据库采用高可用版，保证了系统的高可用性。 |
| 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； | 经核查，数据库用户退出后自动清理鉴别信息所在的存储空间。 |
| 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。 | 经核查，数据库用户退出后自动清理敏感数据存储空间。 |
| 个人信息保护 | a）应仅采集和保存业务必需的用户个人信息； | 1）数据库存储了用户姓名、手机号、身份证号、地址等个人信息；2）公司制定了《个人信息保护规范》，在规范中明确了用户收集规则、收集方式、收集内容等。 |
| b）应禁止未授权访问和非法使用用户个人信息。 | 1）针对用户手机号的中间4位号码进行了脱敏处理；2）通过权限控制，仅有获得授权的管理员可以查看用户个人信息，同时通过审计日志对用户的操作行为进行记录；3）用户个人信息在入库时采用aes-128-cbc对称加密算法进行加密存储；4）公司制定了《个人信息保护规范》，在规范中明确禁止非授权访问、非法使用个人信息。 |

4.1.4.13. pro-spmibill07-mysql

|  |  |  |
| --- | --- | --- |
| **安全控制点** | **测评指标** | **结果记录** |
| 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）数据库采用用户名/口令对用户进行身份标识、鉴别；2）执行select user,host from mysql.user命令，不存在相同的用户名；3）执行select\* from mysql.user where Pass word is null命令输入为空，无空口令账户存在；4）经访谈，DBA创建账户时使用密码生成器生成16位口令（数字、大写字母、小写字母和特殊字符组合），但数据库未配置口令无长度、复杂度、定期更换策略。 |
| 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）数据库未配置用户登录失败处理策略；2）执行show variables like %max\_connect\_errors%，返回值为：7200，即用户连接超时时间为2小时。 |
| 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； | 经核查，运维人员登录堡垒机后采用Navicat软件（采用SSL证书）连接数据库，防止鉴别信息在传输过程中被窃听。 |
| 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。 | 数据库未采用两种或两种以上组合的鉴别技术对用户进行身份鉴别。 |
| 访问控制 | a）应对登录的用户分配账户和权限； | 经核查，1）由管理员为登录数据库的用户创建账户、分配权限；2）目前数据库具有yl\_pro\_root、yl\_uat\_root等管理账户。 |
| b）应重命名或删除默认账户，修改默认账户的默认口令； | 被测数据库为采购的阿里云RDS数据库服务，阿里云RDS数据库无默认账户。 |
| 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； | 经核查，1）目前数据库仅具有yl\_pro\_root、yl\_uat\_root等管理账户，不存在多余、过期；2）存在多个堡垒机账户登录数据库时共用一个账户的情况。 |
| 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； | 经核查，未授予管理用户所需的最小权限，未实现管理用户的权限分离。 |
| e）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； | 经核查，由管理员为用户分配权限，控制用户对数据库的访问规则。 |
| f）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； | 经核查，数据库访问控制粒度达到主体为用户级，客体为数据库表级。 |
| g）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。 | 未对重要主体和客体进行安全标记。 |
| 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； | 经核查，通过阿里云SQL洞察服务对数据库所有用户的操作行为、SQL语句等进行审计记录。 |
| 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； | 经核查，审计记录包含：SQL语句、数据库名、线程、事务号、用户名、客户端IP、操作类型、状态、执行耗时、执行时间等。 |
| 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； | 经核查，审计记录本地保存，非授权用户无权限修改、删除，避免受到未预期的删除、修改或覆盖，且审计记录备份至数据库审计，保存180天。 |
| d）应对审计进程进行保护，防止未经授权的中断。 | 经核查，非授权用户无法中断系统审计进程。 |
| 入侵防范 | a）应遵循最小安装的原则，仅安装需要的组件和应用程序； | 根据GB∕T 28448-2019 《信息安全技术 网络安全等级保护测评要求》测评对象范围描述，数据库无该项要求。 |
| b）应关闭不需要的系统服务、默认共享和高危端口； | 根据GB∕T 28448-2019 《信息安全技术 网络安全等级保护测评要求》测评对象范围描述，数据库无该项要求。 |
| c）应通过设定终端接入方式或网络地址范围对通过网络进行管理的管理终端进行限制； | 经核查，1）通过堡垒机管理数据库；2）通过配置办公网防火墙策略限制仅允许办公区地址访问堡垒机。 |
| d）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； | 根据GB∕T 28448-2019 《信息安全技术 网络安全等级保护测评要求》测评对象范围描述，数据库无该项要求。 |
| e）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； | 被测数据库为采购的阿里云RDS数据库服务，由阿里云负责RDS数据库漏洞的检测、修复。 |
| f）应能够检测到对重要节点进行入侵的行为，并在发生严重入侵事件时提供报警。 | 根据GB∕T 28448-2019 《信息安全技术 网络安全等级保护测评要求》测评对象范围描述，数据库无该项要求。 |
| 可信验证 | a）可基于可信根对计算设备的系统引导程序、系统程序、重要配置参数和应用程序等进行可信验证，并在应用程序的关键执行环节进行动态可信验证，在检测到其可信性受到破坏后进行报警，并将验证结果形成审计记录送至安全管理中心。 | 未采用技术措施对计算设备的系统引导程序、系统程序、重要配置参数和应用程序等进行可信验证。 |
| 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； | 经核查，运维人员登录堡垒机后采用Navicat软件（采用SSL证书）连接数据库，保证重要数据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。 | 经核查，采用SHA1+salt技术对用户鉴别信息进行加密存储，保证鉴别信息在存储过程中的完整性；但未采用密码技术保证重要业务数据、用户个人信息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； | 经核查，运维人员登录堡垒机后采用Navicat软件（采用SSL证书）连接数据库，保证重要数据在传输过程中的保密性。 |
| b）应采用密码技术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个人信息等。 | 经核查，采用SHA1+salt技术对用户鉴别信息进行加密存储，保证鉴别信息在存储过程中的保密性；采用aes-128-cbc对称加密算法保存个人信息在存储过程中的保密性；但未采用密码技术保证重要业务数据在存储过程中的保密性。 |
| 数据备份恢复 | a）应提供重要数据的本地数据备份与恢复功能； | 经核查，数据库具有本地备份策略，每天全量备份，保留近7天的备份库，阿里云保证备份库的有效性。 |
| b）应提供异地实时备份功能，利用通信网络将重要数据实时备份至备份场地； | 无异地备份措施。 |
| c）应提供重要数据处理系统的热冗余，保证系统的高可用性。 | 经核查，数据库采用高可用版，保证了系统的高可用性。 |
| 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； | 经核查，数据库用户退出后自动清理鉴别信息所在的存储空间。 |
| 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。 | 经核查，数据库用户退出后自动清理敏感数据存储空间。 |
| 个人信息保护 | a）应仅采集和保存业务必需的用户个人信息； | 1）数据库存储了用户姓名、手机号、身份证号、地址等个人信息；2）公司制定了《个人信息保护规范》，在规范中明确了用户收集规则、收集方式、收集内容等。 |
| b）应禁止未授权访问和非法使用用户个人信息。 | 1）针对用户手机号的中间4位号码进行了脱敏处理；2）通过权限控制，仅有获得授权的管理员可以查看用户个人信息，同时通过审计日志对用户的操作行为进行记录；3）用户个人信息在入库时采用aes-128-cbc对称加密算法进行加密存储；4）公司制定了《个人信息保护规范》，在规范中明确禁止非授权访问、非法使用个人信息。 |

4.1.4.14. pro-spmnbill-mysql

|  |  |  |
| --- | --- | --- |
| **安全控制点** | **测评指标** | **结果记录** |
| 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）数据库采用用户名/口令对用户进行身份标识、鉴别；2）执行select user,host from mysql.user命令，不存在相同的用户名；3）执行select\* from mysql.user where Pass word is null命令输入为空，无空口令账户存在；4）经访谈，DBA创建账户时使用密码生成器生成16位口令（数字、大写字母、小写字母和特殊字符组合），但数据库未配置口令无长度、复杂度、定期更换策略。 |
| 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）数据库未配置用户登录失败处理策略；2）执行show variables like %max\_connect\_errors%，返回值为：7200，即用户连接超时时间为2小时。 |
| 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； | 经核查，运维人员登录堡垒机后采用Navicat软件（采用SSL证书）连接数据库，防止鉴别信息在传输过程中被窃听。 |
| 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。 | 数据库未采用两种或两种以上组合的鉴别技术对用户进行身份鉴别。 |
| 访问控制 | a）应对登录的用户分配账户和权限； | 经核查，1）由管理员为登录数据库的用户创建账户、分配权限；2）目前数据库具有yl\_pro\_root、yl\_uat\_root等管理账户。 |
| b）应重命名或删除默认账户，修改默认账户的默认口令； | 被测数据库为采购的阿里云RDS数据库服务，阿里云RDS数据库无默认账户。 |
| 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； | 经核查，1）目前数据库仅具有yl\_pro\_root、yl\_uat\_root等管理账户，不存在多余、过期；2）存在多个堡垒机账户登录数据库时共用一个账户的情况。 |
| 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； | 经核查，未授予管理用户所需的最小权限，未实现管理用户的权限分离。 |
| e）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； | 经核查，由管理员为用户分配权限，控制用户对数据库的访问规则。 |
| f）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； | 经核查，数据库访问控制粒度达到主体为用户级，客体为数据库表级。 |
| g）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。 | 未对重要主体和客体进行安全标记。 |
| 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； | 经核查，通过阿里云SQL洞察服务对数据库所有用户的操作行为、SQL语句等进行审计记录。 |
| 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； | 经核查，审计记录包含：SQL语句、数据库名、线程、事务号、用户名、客户端IP、操作类型、状态、执行耗时、执行时间等。 |
| 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； | 经核查，审计记录本地保存，非授权用户无权限修改、删除，避免受到未预期的删除、修改或覆盖，且审计记录备份至数据库审计，保存180天。 |
| d）应对审计进程进行保护，防止未经授权的中断。 | 经核查，非授权用户无法中断系统审计进程。 |
| 入侵防范 | a）应遵循最小安装的原则，仅安装需要的组件和应用程序； | 根据GB∕T 28448-2019 《信息安全技术 网络安全等级保护测评要求》测评对象范围描述，数据库无该项要求。 |
| b）应关闭不需要的系统服务、默认共享和高危端口； | 根据GB∕T 28448-2019 《信息安全技术 网络安全等级保护测评要求》测评对象范围描述，数据库无该项要求。 |
| c）应通过设定终端接入方式或网络地址范围对通过网络进行管理的管理终端进行限制； | 经核查，1）通过堡垒机管理数据库；2）通过配置办公网防火墙策略限制仅允许办公区地址访问堡垒机。 |
| d）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； | 根据GB∕T 28448-2019 《信息安全技术 网络安全等级保护测评要求》测评对象范围描述，数据库无该项要求。 |
| e）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； | 被测数据库为采购的阿里云RDS数据库服务，由阿里云负责RDS数据库漏洞的检测、修复。 |
| f）应能够检测到对重要节点进行入侵的行为，并在发生严重入侵事件时提供报警。 | 根据GB∕T 28448-2019 《信息安全技术 网络安全等级保护测评要求》测评对象范围描述，数据库无该项要求。 |
| 可信验证 | a）可基于可信根对计算设备的系统引导程序、系统程序、重要配置参数和应用程序等进行可信验证，并在应用程序的关键执行环节进行动态可信验证，在检测到其可信性受到破坏后进行报警，并将验证结果形成审计记录送至安全管理中心。 | 未采用技术措施对计算设备的系统引导程序、系统程序、重要配置参数和应用程序等进行可信验证。 |
| 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； | 经核查，运维人员登录堡垒机后采用Navicat软件（采用SSL证书）连接数据库，保证重要数据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。 | 经核查，采用SHA1+salt技术对用户鉴别信息进行加密存储，保证鉴别信息在存储过程中的完整性；但未采用密码技术保证重要业务数据、用户个人信息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； | 经核查，运维人员登录堡垒机后采用Navicat软件（采用SSL证书）连接数据库，保证重要数据在传输过程中的保密性。 |
| b）应采用密码技术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个人信息等。 | 经核查，采用SHA1+salt技术对用户鉴别信息进行加密存储，保证鉴别信息在存储过程中的保密性；采用aes-128-cbc对称加密算法保存个人信息在存储过程中的保密性；但未采用密码技术保证重要业务数据在存储过程中的保密性。 |
| 数据备份恢复 | a）应提供重要数据的本地数据备份与恢复功能； | 经核查，数据库具有本地备份策略，每天全量备份，保留近7天的备份库，阿里云保证备份库的有效性。 |
| b）应提供异地实时备份功能，利用通信网络将重要数据实时备份至备份场地； | 无异地备份措施。 |
| c）应提供重要数据处理系统的热冗余，保证系统的高可用性。 | 经核查，数据库采用高可用版，保证了系统的高可用性。 |
| 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； | 经核查，数据库用户退出后自动清理鉴别信息所在的存储空间。 |
| 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。 | 经核查，数据库用户退出后自动清理敏感数据存储空间。 |
| 个人信息保护 | a）应仅采集和保存业务必需的用户个人信息； | 1）数据库存储了用户姓名、手机号、身份证号、地址等个人信息；2）公司制定了《个人信息保护规范》，在规范中明确了用户收集规则、收集方式、收集内容等。 |
| b）应禁止未授权访问和非法使用用户个人信息。 | 1）针对用户手机号的中间4位号码进行了脱敏处理；2）通过权限控制，仅有获得授权的管理员可以查看用户个人信息，同时通过审计日志对用户的操作行为进行记录；3）用户个人信息在入库时采用aes-128-cbc对称加密算法进行加密存储；4）公司制定了《个人信息保护规范》，在规范中明确禁止非授权访问、非法使用个人信息。 |

4.1.4.15. pro-spmibill02-mysql

|  |  |  |
| --- | --- | --- |
| **安全控制点** | **测评指标** | **结果记录** |
| 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）数据库采用用户名/口令对用户进行身份标识、鉴别；2）执行select user,host from mysql.user命令，不存在相同的用户名；3）执行select\* from mysql.user where Pass word is null命令输入为空，无空口令账户存在；4）经访谈，DBA创建账户时使用密码生成器生成16位口令（数字、大写字母、小写字母和特殊字符组合），但数据库未配置口令无长度、复杂度、定期更换策略。 |
| 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）数据库未配置用户登录失败处理策略；2）执行show variables like %max\_connect\_errors%，返回值为：7200，即用户连接超时时间为2小时。 |
| 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； | 经核查，运维人员登录堡垒机后采用Navicat软件（采用SSL证书）连接数据库，防止鉴别信息在传输过程中被窃听。 |
| 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。 | 数据库未采用两种或两种以上组合的鉴别技术对用户进行身份鉴别。 |
| 访问控制 | a）应对登录的用户分配账户和权限； | 经核查，1）由管理员为登录数据库的用户创建账户、分配权限；2）目前数据库具有yl\_pro\_root、yl\_uat\_root等管理账户。 |
| b）应重命名或删除默认账户，修改默认账户的默认口令； | 被测数据库为采购的阿里云RDS数据库服务，阿里云RDS数据库无默认账户。 |
| 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； | 经核查，1）目前数据库仅具有yl\_pro\_root、yl\_uat\_root等管理账户，不存在多余、过期；2）存在多个堡垒机账户登录数据库时共用一个账户的情况。 |
| 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； | 经核查，未授予管理用户所需的最小权限，未实现管理用户的权限分离。 |
| e）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； | 经核查，由管理员为用户分配权限，控制用户对数据库的访问规则。 |
| f）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； | 经核查，数据库访问控制粒度达到主体为用户级，客体为数据库表级。 |
| g）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。 | 未对重要主体和客体进行安全标记。 |
| 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； | 经核查，通过阿里云SQL洞察服务对数据库所有用户的操作行为、SQL语句等进行审计记录。 |
| 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； | 经核查，审计记录包含：SQL语句、数据库名、线程、事务号、用户名、客户端IP、操作类型、状态、执行耗时、执行时间等。 |
| 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； | 经核查，审计记录本地保存，非授权用户无权限修改、删除，避免受到未预期的删除、修改或覆盖，且审计记录备份至数据库审计，保存180天。 |
| d）应对审计进程进行保护，防止未经授权的中断。 | 经核查，非授权用户无法中断系统审计进程。 |
| 入侵防范 | a）应遵循最小安装的原则，仅安装需要的组件和应用程序； | 根据GB∕T 28448-2019 《信息安全技术 网络安全等级保护测评要求》测评对象范围描述，数据库无该项要求。 |
| b）应关闭不需要的系统服务、默认共享和高危端口； | 根据GB∕T 28448-2019 《信息安全技术 网络安全等级保护测评要求》测评对象范围描述，数据库无该项要求。 |
| c）应通过设定终端接入方式或网络地址范围对通过网络进行管理的管理终端进行限制； | 经核查，1）通过堡垒机管理数据库；2）通过配置办公网防火墙策略限制仅允许办公区地址访问堡垒机。 |
| d）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； | 根据GB∕T 28448-2019 《信息安全技术 网络安全等级保护测评要求》测评对象范围描述，数据库无该项要求。 |
| e）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； | 被测数据库为采购的阿里云RDS数据库服务，由阿里云负责RDS数据库漏洞的检测、修复。 |
| f）应能够检测到对重要节点进行入侵的行为，并在发生严重入侵事件时提供报警。 | 根据GB∕T 28448-2019 《信息安全技术 网络安全等级保护测评要求》测评对象范围描述，数据库无该项要求。 |
| 可信验证 | a）可基于可信根对计算设备的系统引导程序、系统程序、重要配置参数和应用程序等进行可信验证，并在应用程序的关键执行环节进行动态可信验证，在检测到其可信性受到破坏后进行报警，并将验证结果形成审计记录送至安全管理中心。 | 未采用技术措施对计算设备的系统引导程序、系统程序、重要配置参数和应用程序等进行可信验证。 |
| 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； | 经核查，运维人员登录堡垒机后采用Navicat软件（采用SSL证书）连接数据库，保证重要数据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。 | 经核查，采用SHA1+salt技术对用户鉴别信息进行加密存储，保证鉴别信息在存储过程中的完整性；但未采用密码技术保证重要业务数据、用户个人信息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； | 经核查，运维人员登录堡垒机后采用Navicat软件（采用SSL证书）连接数据库，保证重要数据在传输过程中的保密性。 |
| b）应采用密码技术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个人信息等。 | 经核查，采用SHA1+salt技术对用户鉴别信息进行加密存储，保证鉴别信息在存储过程中的保密性；采用aes-128-cbc对称加密算法保存个人信息在存储过程中的保密性；但未采用密码技术保证重要业务数据在存储过程中的保密性。 |
| 数据备份恢复 | a）应提供重要数据的本地数据备份与恢复功能； | 经核查，数据库具有本地备份策略，每天全量备份，保留近7天的备份库，阿里云保证备份库的有效性。 |
| b）应提供异地实时备份功能，利用通信网络将重要数据实时备份至备份场地； | 无异地备份措施。 |
| c）应提供重要数据处理系统的热冗余，保证系统的高可用性。 | 经核查，数据库采用高可用版，保证了系统的高可用性。 |
| 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； | 经核查，数据库用户退出后自动清理鉴别信息所在的存储空间。 |
| 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。 | 经核查，数据库用户退出后自动清理敏感数据存储空间。 |
| 个人信息保护 | a）应仅采集和保存业务必需的用户个人信息； | 1）数据库存储了用户姓名、手机号、身份证号、地址等个人信息；2）公司制定了《个人信息保护规范》，在规范中明确了用户收集规则、收集方式、收集内容等。 |
| b）应禁止未授权访问和非法使用用户个人信息。 | 1）针对用户手机号的中间4位号码进行了脱敏处理；2）通过权限控制，仅有获得授权的管理员可以查看用户个人信息，同时通过审计日志对用户的操作行为进行记录；3）用户个人信息在入库时采用aes-128-cbc对称加密算法进行加密存储；4）公司制定了《个人信息保护规范》，在规范中明确禁止非授权访问、非法使用个人信息。 |

4.1.4.16. pro-spmibill03-mysql

|  |  |  |
| --- | --- | --- |
| **安全控制点** | **测评指标** | **结果记录** |
| 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）数据库采用用户名/口令对用户进行身份标识、鉴别；2）执行select user,host from mysql.user命令，不存在相同的用户名；3）执行select\* from mysql.user where Pass word is null命令输入为空，无空口令账户存在；4）经访谈，DBA创建账户时使用密码生成器生成16位口令（数字、大写字母、小写字母和特殊字符组合），但数据库未配置口令无长度、复杂度、定期更换策略。 |
| 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）数据库未配置用户登录失败处理策略；2）执行show variables like %max\_connect\_errors%，返回值为：7200，即用户连接超时时间为2小时。 |
| 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； | 经核查，运维人员登录堡垒机后采用Navicat软件（采用SSL证书）连接数据库，防止鉴别信息在传输过程中被窃听。 |
| 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。 | 数据库未采用两种或两种以上组合的鉴别技术对用户进行身份鉴别。 |
| 访问控制 | a）应对登录的用户分配账户和权限； | 经核查，1）由管理员为登录数据库的用户创建账户、分配权限；2）目前数据库具有yl\_pro\_root、yl\_uat\_root等管理账户。 |
| b）应重命名或删除默认账户，修改默认账户的默认口令； | 被测数据库为采购的阿里云RDS数据库服务，阿里云RDS数据库无默认账户。 |
| 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； | 经核查，1）目前数据库仅具有yl\_pro\_root、yl\_uat\_root等管理账户，不存在多余、过期；2）存在多个堡垒机账户登录数据库时共用一个账户的情况。 |
| 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； | 经核查，未授予管理用户所需的最小权限，未实现管理用户的权限分离。 |
| e）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； | 经核查，由管理员为用户分配权限，控制用户对数据库的访问规则。 |
| f）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； | 经核查，数据库访问控制粒度达到主体为用户级，客体为数据库表级。 |
| g）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。 | 未对重要主体和客体进行安全标记。 |
| 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； | 经核查，通过阿里云SQL洞察服务对数据库所有用户的操作行为、SQL语句等进行审计记录。 |
| 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； | 经核查，审计记录包含：SQL语句、数据库名、线程、事务号、用户名、客户端IP、操作类型、状态、执行耗时、执行时间等。 |
| 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； | 经核查，审计记录本地保存，非授权用户无权限修改、删除，避免受到未预期的删除、修改或覆盖，且审计记录备份至数据库审计，保存180天。 |
| d）应对审计进程进行保护，防止未经授权的中断。 | 经核查，非授权用户无法中断系统审计进程。 |
| 入侵防范 | a）应遵循最小安装的原则，仅安装需要的组件和应用程序； | 根据GB∕T 28448-2019 《信息安全技术 网络安全等级保护测评要求》测评对象范围描述，数据库无该项要求。 |
| b）应关闭不需要的系统服务、默认共享和高危端口； | 根据GB∕T 28448-2019 《信息安全技术 网络安全等级保护测评要求》测评对象范围描述，数据库无该项要求。 |
| c）应通过设定终端接入方式或网络地址范围对通过网络进行管理的管理终端进行限制； | 经核查，1）通过堡垒机管理数据库；2）通过配置办公网防火墙策略限制仅允许办公区地址访问堡垒机。 |
| d）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； | 根据GB∕T 28448-2019 《信息安全技术 网络安全等级保护测评要求》测评对象范围描述，数据库无该项要求。 |
| e）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； | 被测数据库为采购的阿里云RDS数据库服务，由阿里云负责RDS数据库漏洞的检测、修复。 |
| f）应能够检测到对重要节点进行入侵的行为，并在发生严重入侵事件时提供报警。 | 根据GB∕T 28448-2019 《信息安全技术 网络安全等级保护测评要求》测评对象范围描述，数据库无该项要求。 |
| 可信验证 | a）可基于可信根对计算设备的系统引导程序、系统程序、重要配置参数和应用程序等进行可信验证，并在应用程序的关键执行环节进行动态可信验证，在检测到其可信性受到破坏后进行报警，并将验证结果形成审计记录送至安全管理中心。 | 未采用技术措施对计算设备的系统引导程序、系统程序、重要配置参数和应用程序等进行可信验证。 |
| 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； | 经核查，运维人员登录堡垒机后采用Navicat软件（采用SSL证书）连接数据库，保证重要数据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。 | 经核查，采用SHA1+salt技术对用户鉴别信息进行加密存储，保证鉴别信息在存储过程中的完整性；但未采用密码技术保证重要业务数据、用户个人信息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； | 经核查，运维人员登录堡垒机后采用Navicat软件（采用SSL证书）连接数据库，保证重要数据在传输过程中的保密性。 |
| b）应采用密码技术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个人信息等。 | 经核查，采用SHA1+salt技术对用户鉴别信息进行加密存储，保证鉴别信息在存储过程中的保密性；采用aes-128-cbc对称加密算法保存个人信息在存储过程中的保密性；但未采用密码技术保证重要业务数据在存储过程中的保密性。 |
| 数据备份恢复 | a）应提供重要数据的本地数据备份与恢复功能； | 经核查，数据库具有本地备份策略，每天全量备份，保留近7天的备份库，阿里云保证备份库的有效性。 |
| b）应提供异地实时备份功能，利用通信网络将重要数据实时备份至备份场地； | 无异地备份措施。 |
| c）应提供重要数据处理系统的热冗余，保证系统的高可用性。 | 经核查，数据库采用高可用版，保证了系统的高可用性。 |
| 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； | 经核查，数据库用户退出后自动清理鉴别信息所在的存储空间。 |
| 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。 | 经核查，数据库用户退出后自动清理敏感数据存储空间。 |
| 个人信息保护 | a）应仅采集和保存业务必需的用户个人信息； | 1）数据库存储了用户姓名、手机号、身份证号、地址等个人信息；2）公司制定了《个人信息保护规范》，在规范中明确了用户收集规则、收集方式、收集内容等。 |
| b）应禁止未授权访问和非法使用用户个人信息。 | 1）针对用户手机号的中间4位号码进行了脱敏处理；2）通过权限控制，仅有获得授权的管理员可以查看用户个人信息，同时通过审计日志对用户的操作行为进行记录；3）用户个人信息在入库时采用aes-128-cbc对称加密算法进行加密存储；4）公司制定了《个人信息保护规范》，在规范中明确禁止非授权访问、非法使用个人信息。 |

|  |  |  |  |
| --- | --- | --- | --- |
| **测评项目** |  | **测评对象** | 业务应用软件/平台 |
| **测评单位** |  | | |
| **测评地点** |  | | |
| **测评人员** |  | **配合人员** | 刘亮 |
| **测评日期** | 2023.6.15-2023.6.16 | | |
| **测评人员签字** |  | **配合人员签字** |  |

4.1.5. 业务应用软件/平台

4.1.5.1. JMS综合物流平台系统

|  |  |  |
| --- | --- | --- |
| **安全控制点** | **测评指标** | **结果记录** |
| 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.Jms综合物流平台用户信息均通过极兔速递有限公司PS（人力资源管理系统）同步获取，Jms综合物流平台本身无用户注册功能，具有两种登录方式，一种是账号+密码登录+滑块验证码，一种是微信扫码登录（通过微信授权接口对准入用户进行确认，包含普通用户微信或企业微信）； 2.用户名为登录人员的员工编号，用户员工编号于用户手机号绑定，通过创建同名用户的方式测试，同一编号的账户不允许创建，用户名唯一； 3.系统中用户密码策略在底层开发文件中定义，配置为密码长度最少8位，需要至少4种组合（字母大小写、数字、特殊符号），策略不允许连续三个相同字符的密码，通过测试，在用户未按策略要求配置密码时，会弹出提示信息，要求用户正确配置相关信息； 4.通过测试，在系统中创建新用户时，管理员通过重置密码功能为新用户提供随机密码，要求用户首次登录必须修改密码，用户密码60天更换一次，未按要求变更密码会锁定用户登录功能。通过微信扫码登录的用户，用户权限（登陆、绑定、解绑、重置密码）由JMS基础资料-用户管理模块管理，未授权用户无法登录。 |
| 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、JMS综合物流平台系统启用了登录失败处理功能，策略配置为用户密码5分钟内连续输入错误5次，锁定账户5分钟； 2、测试人员使用正确的用户名、错误的口令连续多次登录系统，在登录错误第一次后会弹出图形验证码，登录错误5次会显示用户锁定，需联系管理员解锁； 3.通过查看，系统用户Token时间设置为两小时失效，用户两小时内无操作自动退出登录。 |
| 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； | JMS综合物流平台系统仅开启了443端口进行远程连接访问，只允许通过HTTPS协议进行通信，采购并使用了商业证书服务，能够防止鉴别信息在网络传输过程中被窃听。 |
| 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。 | 1、JMS综合物流平台系统用户正常登录系统（IP地址地区）无双因素验证； 2、用户在异地或常用IP地址变更的情况下登录系统，需通过用户名+密码+滑块验证码+动态短信验证的方式进行身份鉴别。 |
| 访问控制 | a）应对登录的用户分配账户和权限； | 1.Jms综合物流平台在访问控制方面采用RBAC访问控制架构，系统通过PS（人力资源管理系统）同步获取用户信息，用户权限通过 OA系统申请并由直属上级领导确认后，由管理员手动为用户赋予对应的角色权限，权限可以细化至功能按钮级； 2.系统中目前有各类角色7387类，包括各类业务用户角色、普通用户角色、开发人员角色、运维角色、测试角色、部门管理角色等，系统中现有用户1533809个，其中活跃用户为349781，其他用户均为停用状态； 3.用户在PS系统创建用户时，必须填写员工编号、性别、证件类型、身份证号、所属网点、所属部门、岗位、手机号等信息，同时相关信息也会推送至JMS系统，通过现场查看，所用用户均对应相应的员工编号，系统中不存在匿名账户，超级管理员账户admin为默认账户，由公司客户渠道总监管理，并已按策略要求配置复杂密码。 |
| b）应重命名或删除默认账户，修改默认账户的默认口令； | Jms综合物流平台中只有一个默认账户admin管理员账户，账户目前已按照密码策略配置复杂密码，由公司客户渠道总监管理。 |
| 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； | 1.通过查看，目前Jms综合物流平台中所有在用用户均为真实使用的用户，通过员工编号进行标识对应，无多余或过期账户存在。系统中管理员角色包括配置管理员、系统管理员等相关管理角色及用户。 2.Jms综合物流平台中针对离职用户的处理方式是在系统中调整在职状态为“离职”，相关用户不可登录系统。 3.系统中针对临时用户的处理方式是给予用户最低权限，按照业务需求，用户通过提工单的方式请求权限，通过管理人员确认后，由系统管理员为其赋予相应权限。在共享账户方面，目前由客户渠道总监负责超级管理账号admin的管理，账号的使用需等到客户渠道总监的授权，同时重要操作均有管理人员陪同确认。 4.通过现场查看，系统中目前无多余或过期账户。 |
| 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； | 1.通过查看，系统中的所有管理用户，如配置管理员、系统管理员、普通用户均只拥有完成自己承担任务所需的最小权限； 2.通过测试，所有管理用户均不具备业务操作权限，且管理用户分为系统管理员、配置管理员等管理角色，未发现独立的安全审计员角色。 3.通过测试，配置管理员、普通用户的实际权限与其职责相符，为完成其承担任务所需的最小权限，系统管理员具备安全审计员的权限。 4.目前系统中未配置独立的安全审计员角色，由系统管理员承担了系统运维、事件审计等工作内容，未形成不同管理用户之间相互制约的关系，未实现用户权限分离。 |
| e）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.Jms综合物流平台采用RBAC架构，采用用户对应系统功能模块的方式对用户访问资源进行授权。 2.管理员负责配置访问控制策略，依据用户部门、工作内容统一分配用户角色、权限，并赋予用户使用的权限。 3.访问控制策略为主体用户客体功能按键级。 4.通过现场查看，非管理用户不能访问与权限管理相关的功能。 |
| f）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； | Jms综合物流平台采用RBAC架构，访问控制策略为主体用户级，客体为功能按键级。 |
| g）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、JMS综合物流平台系统未依据安全策略对重要账户和重要信息设置安全标记； 2、JMS综合物流平台系统未依据安全标记控制账户对有安全标记信息资源的访问。 |
| 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、JMS综合物流平台系统针对不同业务模块分别提供了多种日志审计模块，包括用户登录日志、系统管理日志、设备登录日志、操作日志、消息日志、设备修改日志、导出日志、接口日志、异常日志等； 2、通过现场查看，相关审计日志能够覆盖系统所有模块及用户，包含了用户所有重要操作行为及业务操作等。 |
| 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； | 1、JMS综合物流平台系统重要安全日志包括用户登录日志、系统管理日志、设备登录日志、任务操作日志、设备修改日志、接口异常日志等。 2、通过现场查看，日志情况如下：用户登录日志：用户编号、用户姓名、所属网点、部门、岗位、登录端、应用类型、登录时间、IP地址、登录地址；系统管理日志：所属平台、所属模块、基本表明、操作类型、关联信息、操作描述、操作用户编号、操作用户姓名、操作网点、时间； 任务操作日志：WEB端名称、操作界面、操作类型、操作内容、操作时间、操作人、操作账号；设备登录日志：应用、IMEI、SN、用户编号、用户姓名、所属网点、供应商、登录时间、登录IP； 接口异常日志：接口名称、关键字、接收方、开始时间、结束时间、异常描述、请求报文、相应报文、请求时间； 设备修改日志：设备名称、操作类型、操作时间、操作人等。 |
| 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.Jms综合物流平台审计日志存储与应用服务器及数据库服务器，在应用层面管理员只有对记录查看的权限，无法做其他操作； 2.通过现场查看，审计日志实时进行保存，可追溯至180天前的记录。数据库每周一次全备，两次增量备份，每季度进行数据恢复测试。 |
| d）应对审计进程进行保护，防止未经授权的中断。 | 1.通过现场查看，Jms综合物流平台审计进程与应用服务之间有依存关系，服务启动审计进程启动，服务停止进程同步停止； 2.通过访谈、查看网络拓扑、查看系统所部署的阿里云平台资源池，确认Jms综合物流平台采用集群方式部署，出现系统安全情况，能够保证系统业务与日志不会中断，同时，公司与阿里云、IDC签署了SLA协议，由服务供应商保障系统基础环境的可用性。 |
| 入侵防范 | a）应遵循最小安装的原则，仅安装需要的组件和应用程序； | 通过现场访谈、查看，JMS综合物流平台系统的安装遵循最小安装的原则，不存在仍在开发或未经安全测试的功能模块。 |
| b）应关闭不需要的系统服务、默认共享和高危端口； | Jms综合物流平台为应用系统，此项不适用。 |
| c）应通过设定终端接入方式或网络地址范围对通过网络进行管理的管理终端进行限制； | JMS综合物流平台系统用户面向本部及全国的各及服务商，目前使用用户共有1340578个，无法对访问范围细化至用户级别，目前应用层面通过平台的身份鉴别机制对用户的访问进行限制。 |
| d）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； | 1.公司制定了YL-2-ISMS-41《应用安全开发指引》，针对数据有效性校验进行了要求； 2.现场对Jms综合物流平台重要业务模块的输入窗口、上传窗口进行测试，确认针对手机号、身份证号、姓名、单号等重要输入窗口均具有有效性校验，针对上传窗口均使用白名单机制，基于业务所需对上传文件的格式、大小、文件类型进行了限制，要求上传文件格式为xls、doc等，最多2M，图片格式为jpg、png，最多10M。 |
| e）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； | 通过漏洞扫描、渗透测试，Jms综合物流平台及所属应用服务器、中间件、数据库服务器相关高风险漏洞已修复。 |
| f）应能够检测到对重要节点进行入侵的行为，并在发生严重入侵事件时提供报警。 | Jms综合物流平台为应用系统，此项不适用。 |
| 可信验证 | a）可基于可信根对计算设备的系统引导程序、系统程序、重要配置参数和应用程序等进行可信验证，并在应用程序的关键执行环节进行动态可信验证，在检测到其可信性受到破坏后进行报警，并将验证结果形成审计记录送至安全管理中心。 | Jms综合物流平台未基于可信根对计算设备的系统引导程序、系统程序、重要配置参数和应用程序等进行可信验证。 |
| 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； | JMS综合物流平台系统启用了证书服务，通过HTTPS协议保证系统中鉴别数据、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。 | JMS综合物流平台系统针对用户鉴别信息在存储时采用md5+salt的方式保护数据的完整性。通过现场查看，存储重要业务数据、重要审计数据、重要配置数据和重要个人信息等数据库表中未发现完整性校验字段，未对部分重要数据在存储过程中的完整性进行保护。 |
| 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； | JMS综合物流平台系统启用了证书服务，通过HTTPS协议保证系统鉴别数据、重要业务数据和重要个人信息等在传输过程中的保密性。 |
| b）应采用密码技术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个人信息等。 | 1、通过现场查看，平台中针对入库个人数据，如：内外部人员身份证号码、照片、收件人手机号、员工手机号等，均采用aes-128-cbc对称加密算法进行了加密处理； 2、未对鉴别数据、重要业务数据进行存储加密。 |
| 数据备份恢复 | a）应提供重要数据的本地数据备份与恢复功能； | JMS综合物流平台系统重要数据存储在数据库中，云上数据库每天全量备份，保留近7个备份库文件，阿里云保证备份库的有效性；IDC机房数据库每天全量备份，保留近20个备份库文件，运维人员每季度对备份文件进行恢复测试。 |
| b）应提供异地实时备份功能，利用通信网络将重要数据实时备份至备份场地； | JMS综合物流平台系统无异地备份措施。 |
| c）应提供重要数据处理系统的热冗余，保证系统的高可用性。 | JMS综合物流平台系统涉及的服务器、数据库均采用冗余方式部署，保证了系统的高可用性。 |
| 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； | 通过现场查看、测试，JMS综合物流平台系统用户在手动退出系统后，再次登录系统需输入账号、密码，同时在系统代码中配置用户 Session时间为120分钟，能够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。 |
| 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。 | 通过现场查看、测试，JMS综合物流平台系统用户在手动退出系统后，再次登录系统需输入账号、密码，同时在系统代码中配置用户 Session时间为120分钟，能够保证敏感数据所在的存储空间被释放或重新分配前得到完全清除。 |
| 个人信息保护 | a）应仅采集和保存业务必需的用户个人信息； | 1、JMS综合物流平台系统用户由管理员手动创建，系统内依据业务需求会存储用户姓名、手机号、身份证号、地址等个人信息。 2、公司制定了YL-1-ISMS-02《信息安全和隐私管理策略手册》，在规范中明确了用户个人信息收集规则、收集方式、收集内容等。 |
| b）应禁止未授权访问和非法使用用户个人信息。 | 1、JMS综合物流平台系统针对用户手机号进行了脱敏处理，对手机号中间4位号码进行了脱敏处理，在数据维护方面，针对用户数据的访问只有获得授权的管理员可以查看，同时通过审计日志对用户的操作行为进行记录，个人数据信息在入库时采用压缩加密的方式进行保护。 2、公司制定了YL-1-ISMS-02《信息安全和隐私管理策略手册》，在手册中明确了个人信息在收集、传输、存储、使用、共享、销毁等方面的管理要求及技术实现方式。 |

4.1.5.2. 极兔速递小程序

|  |  |  |
| --- | --- | --- |
| **安全控制点** | **测评指标** | **结果记录** |
| 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； | 极兔速递小程序是面向用户提供快递邮寄、查看等功能的应用程序，包含了微信小程序、支付宝小程序、抖音小程序、百度小程序，用户登录分别通过微信授权登录或手机号+验证码、支付宝授权登录或手机号+验证码、抖音手机号授权登录或手机号+验证码、百度账号授权登录或手机号+验证码等方式进行登录，用户信息如微信用户名、支付宝账户名、手机号、用户昵称等分别通过业务接口推送至JMS综合物流平台系统。 |
| 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； | 极兔速递小程序通过调取微信用户令牌信息+手机号授权的方式、支付宝授权登录或手机号+验证码、抖音手机号授权登录或手机号+验证码、百度账号授权登录或手机号+验证码等方式对登录用户进行验证，在登录失败处理方面，用户登录小程序必须接受手机号授权，否则无法登录，不涉及登录失败方面的场景，目前因用户体验原因未启用超时自动退出功能，用户如需退出，可手动操作退出系统。 |
| 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； | 极兔速递小程序目前通过HTTPS协议进行通信，采购并使用了商业证书服务，能够防止鉴别信息在网络传输过程中被窃听。 |
| 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。 | 极兔速递小程序采用微信授权或手机号+短信验证码、支付宝授权登录或手机号+验证码、抖音手机号授权登录或手机号+验证码、百度账号授权登录或手机号+验证码等方式进行登录，用户在提交订单后付款时会通过微信支付、支付宝支付等程序进行费用支付，由微信支付程序或支付宝支付程序对用户付款进行二次确认，如采用密码、生物识别等方式，百度小程序、抖音小程序可以在线上下单，需要在线下付款。 |
| 访问控制 | a）应对登录的用户分配账户和权限； | 极兔速递小程序用户包括两种类型，分别为个人用户及大批量业务用户，两类用户只区别在小程序使用功能的不同，相关用户只有业务操作权限，用户均为自主管理。 |
| b）应重命名或删除默认账户，修改默认账户的默认口令； | 极兔速递小程序用户均通过自主注册的方式创建自身系统登录账号，用户可对自己账户信息进行修改，系统中没有默认账户。 |
| 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； | 1.目前极兔速递小程序用户均为通过微信、支付宝、抖音、百度等小程序授权用户，用户分为普通用户、大客户用户两类； 2.小程序用户除用户主动提出清除用户信息，系统不会主动删除或停用用户。 |
| 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； | 极兔速递小程序中用户分为普通用户及大客户用户两类，在程序方面用户只有对自身业务操作的权限，系统中无单独的管理用户。 |
| e）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； | 极兔速递小程序采用用户对应系统功能模块的方式对用户访问资源进行授权。小程序用户只能对页面展示中的功能点进行查看、使用，访问控制策略为主体用户客体文件、数据库表级。 |
| f）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； | 极兔速递小程序用户访问控制设定为文件、数据库表级。 |
| g）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。 | 极兔速递小程序未采用相应技术手段对主体、客体设置安全标记，未采用MAC强制访问控制策略。 |
| 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； | 极兔速递小程序针对用户登陆启用了日志审计功能，通过JMS综合物流平台-综合业务-用户管理-用户登录日志模块，能够查看用户的登录信息，用户业务操作（下单、退单等）日志统一记录于系统数据库中，审计日志能够覆盖小程序所有模块及用户，包含了用户所有重要操作行为及业务操作等 |
| 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； | 极兔速递小程序依托于JMS综合物流平台系统对业务用户、管理用户的重要操作行为、安全事件等进行日志审计，JMS综合物流平台系统重要安全日志包括用户登录日志、系统管理日志、设备登录日志、任务操作日志、设备修改日志、接口异常日志等。用户登录日志：用户编号、用户姓名、所属网点、部门、岗位、登录端、应用类型、登录时间、IP地址、登录地址；系统管理日志：所属平台、所属模块、基本表明、操作类型、关联信息、操作描述、操作用户编号、操作用户姓名、操作网点、时间；任务操作日志：WEB端名称、操作界面、操作类型、操作内容、操作时间、操作人、操作账号；设备登录日志：应用、IMEI、SN、用户编号、用户姓名、所属网点、供应商、登录时间、登录IP；接口异常日志：接口名称、关键字、接收方、开始时间、结束时间、异常描述、请求报文、相应报文、请求时间；设备修改日志：设备名称、操作类型、操作时间、操作人等。 |
| 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； | 极兔速递小程序审计日志存储与应用服务器及数据库服务器，在应用层面管理员只有对记录查看的权限，无法做其他操作；审计日志实时进行保存，通过现场查看，可追溯至2022年10月，大于180天。数据库每周一次全备，两次增量备份，每季度进行数据恢复测试。 |
| d）应对审计进程进行保护，防止未经授权的中断。 | 1.极兔速递小程序依托于Jms综合物流平台对业务用户、管理用户的重要操作行为、安全事件等进行日志审计，Jms综合物流平台审计进程与应用服务之间有依存关系，服务启动审计进程启动，服务停止进程同步停止； 2.极兔速递小程序及Jms综合物流平台均采用集群方式部署，出现系统安全情况，可已保证系统业务与日志不会中断。 |
| 入侵防范 | a）应遵循最小安装的原则，仅安装需要的组件和应用程序； | 通过现场访谈、查看，极兔速递小程序的安装遵循最小安装的原则，不存在仍在开发或未经安全测试的功能模块。 |
| b）应关闭不需要的系统服务、默认共享和高危端口； | 极兔速递小程序不适用此项测评要求。 |
| c）应通过设定终端接入方式或网络地址范围对通过网络进行管理的管理终端进行限制； | 极兔速递小程序通过微信小程序服务的方式提供业务服务，此项不适用。 |
| d）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； | 通过对极兔速递小程序的输入窗口、上传窗口进行测试，确认针对手机号、姓名、单号等均具有有效性校验，针对上传窗口均使用白名单机制，基于业务所需对上传文件的格式、大小、文件类型进行了限制。 |
| e）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； | 通过漏洞扫描、渗透测试，极兔快递小程序及所属应用服务器、中间件、数据库服务器高风险漏洞均已修复。 |
| f）应能够检测到对重要节点进行入侵的行为，并在发生严重入侵事件时提供报警。 | 极兔速递小程序不适用此项测评要求。 |
| 可信验证 | a）可基于可信根对计算设备的系统引导程序、系统程序、重要配置参数和应用程序等进行可信验证，并在应用程序的关键执行环节进行动态可信验证，在检测到其可信性受到破坏后进行报警，并将验证结果形成审计记录送至安全管理中心。 | 极兔速递小程序未基于可信根对计算设备的系统引导程序、系统程序、重要配置参数和应用程序等进行可信验证。 |
| 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； | 极兔速递小程序启用了证书服务，通过HTTPS协议保证系统中鉴别数据、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。 | 极兔速递小程序针对用户鉴别信息在存储时采用md5+salt的方式保护数据的完整性。通过现场查看，存储重要业务数据、重要审计数据、重要配置数据和重要个人信息等数据库表中未发现完整性校验字段，未对部分重要数据在存储过程中的完整性进行保护。 |
| 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； | 极兔速递小程序启用了证书服务，通过HTTPS协议保证系统鉴别数据、重要业务数据和重要个人信息等在传输过程中的保密性。 |
| b）应采用密码技术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个人信息等。 | 1、通过现场查看，极兔速递小程序所属JMS平台中针对入库个人数据，如：内外部人员身份证号码、照片、收件人手机号、员工手机号等，均采用aes-128-cbc对称加密算法进行了加密处理； 2、未对鉴别数据、重要业务数据进行存储加密。 |
| 数据备份恢复 | a）应提供重要数据的本地数据备份与恢复功能； | 系统重要数据存储在数据库中，云上数据库每天全量备份，保留近7个备份库文件，阿里云保证备份库的有效性；IDC机房数据库每天全量备份，保留近20个备份库文件，运维人员每季度对备份文件进行恢复测试。 |
| b）应提供异地实时备份功能，利用通信网络将重要数据实时备份至备份场地； | 无异地备份措施。 |
| c）应提供重要数据处理系统的热冗余，保证系统的高可用性。 | 极兔速递小程序涉及的服务器、数据库均采用冗余方式部署，保证了系统的高可用性。 |
| 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； | 极兔速递小程序用户可通过手动退出或注销账号的方式退出登录，手动退出或注销后能够清除用户鉴别信息。 |
| 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。 | 极兔速递小程序用户可通过手动退出或注销账号的方式退出登录，手动退出或注销后能够清除用户敏感数据信息。 |
| 个人信息保护 | a）应仅采集和保存业务必需的用户个人信息； | 1、极兔速递小程序在使用时会按照程序业务需求收集用户姓名、手机号、身份证号、地址、OpenID、UnionID、设备信息、微信信息等个人信息。 2、公司制定了《隐私政策》，并在用户登录前要求用户确认，在政策第一节“我们如何收集您的个人信息”中对用户信息收集的方法、信息类型在规范中明确了用户收集规则、收集方式、收集内容等进行了详细说明。 细说明。 |
| b）应禁止未授权访问和非法使用用户个人信息。 | 1、极兔速递小程序针对用户手机号进行了脱敏处理，对手机号中间4位号码进行了脱敏处理，在数据维护方面，针对用户数据的访问只有获得授权的管理员可以查看，同时通过审计日志对用户的操作行为进行记录，个人数据信息在入库时采用压缩加密的方式进行保护。 2、公司制定了《隐私政策》，在隐私政策第二、三、四、五中说明了对用户信息的使用、存储保护、对外提供、访问管理等方式方法，在第六、七、八节中，明确了对儿童信息、信息转移方面的具体处理方法。 |

4.1.5.3. PDA系统

|  |  |  |
| --- | --- | --- |
| **安全控制点** | **测评指标** | **结果记录** |
| 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； | PDA设备包括内场、外场，内场使用人员为网点人员与转运中心操作人员，主要功能有到出一体、循环袋建包、装车发件、卸车到件、问题件、建包、拆包、自动集包、收入发、收入建、退件签收、航空发件、航空到件、收件、入仓、出仓、封发车、到解车；外场使用人员为快递员，主要功能包括常用操作（收件、新建运单、出仓、签收、扫码转寄、留仓件、快件跟踪、95短号、短信发送），扫描操作（到出一体、退件签收、问题件、装车发件、卸车到件、盘库、打印、转邮、一键到出、收入发、收入建）；辅助操作（客户管理（大客户单位）工服抽查）；查询操作（待出仓查询、运费查询、违禁品查询、公告查询、备案查询、驿站异常信息、收派签统计、派件统计、短信统计、筛单区域、残单查询）。 用户通过员工编号+密码的方式进行登录，用户信息统一由JMS-基础资料模块创建，用户不能自己申请账户，登录用户均有自己独立的员工编号，与自己的手机绑定，PDA用户创建时会分配一个8位包含英文大写+数字的密码，用户首次登录需手动修改密码，通过查看提示，要求密码8-16位，包含英文字母和数字，密码策略内置于代码中，JMS系统中无对PDA用户的密码策略配置页面，无密码定期更换功能。 |
| 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、通过现场测试，用户使用手持PDA设备登录失败一次后弹出提示文字，登录失败5次锁定账户，每次输入错误均会弹出图形验证码，连续5次失败后锁定用户，锁定后需要通过JMS系统进行手动解锁。 2、PDA系统密码策略内置于程序代码中，通过人工查看，配置了用户Token信息24小时过期，24小时无操作会要求再次进行登录验证。 |
| 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； | 经现场查看，场内PDA通信采用专用WIFI与JMS平台同步信息，场外PDA通过手机卡与JMS通信，JMS平台启用了证书协议，需通过HTTPS协议进行通信。 |
| 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。 | 经现场查看，PDA无双因素验证机制。 |
| 访问控制 | a）应对登录的用户分配账户和权限； | 1、统一由JMS平台管理员为PDA使用用户配置权限，通过基础资料模块-权限管理- APP操作角色对PDA设备使用用户配置具体角色，目前相关用户包括集散点操作员、收派员、网点操作员、分拨操作员等业务角色。用户管理通过JMS平台管理员具体配置。 2、系统中PDA设备通过SN码进行标识，设备再出现故障不能使用时，会标记为停用状态。 |
| b）应重命名或删除默认账户，修改默认账户的默认口令； | 1、PDA使用用户由管理员统一创建，用户没有注册权限。 2、用户首次登录随机分配一个长度8位，大写英文字母+数字组合的口令，用户首次登录要求必须重新创建密码，要求密码8-16位，至少两种组合。 |
| 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； | 1、离职用户会通过OA系统统一推送至JMS系统，JMS通过计划任务方式设置用户状态为非正常状态，通过现场测试，离职或无权限登录用户在登录设备时会提示登录失败，无法登录。 2、用户均通过独立的员工号标识，临时人员也会由JMS系统创建临时员工编号。 3、系统中过期账户均由管理员设为禁用状态。 |
| 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； | 1、通过查看基础资料模块-权限管理-APP操作角色中PDA设备使用用户角色情况，目前配置角色包括集散点操作员、收派员、网点操作员、分拨操作员等业务角色。用户管理统一通过JMS平台管理员具体配置，无单独的安全审计员。 2、通过现场测试，不同角色用户只能展示所属角色业务所需内容，未授权功能不在用户界面中展示。 |
| e）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、PDA设备采用用户对应系统功能模块的方式对用户访问资源进行授权。 2、JMS系统管理员负责配置PDA系统访问控制策略，依据用户部门、工作内容统一分配用户角色、权限，并赋予用户使用的权限。 3、访问控制策略为主体用户客体功能按键级。 4、通过现场查看，非管理用户不能访问与权限管理相关的功能。 |
| f）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； | PDA系统访问控制策略为主体用户级，客体为功能按键级。 |
| g）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、PDA系统未依据安全策略对重要账户和重要信息设置安全标记； 2、PDA系统物流平台未依据安全标记控制账户对有安全标记信息资源的访问。 |
| 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、PDA用户日志包括本地日志（位于PDA设备自身，记录了PDA的具体操作日志）及交互日志。 2、PDA使用人员在出现交互数据与JMS系统不匹配的情况下，通过手动日志上传功能上本地日志传至阿里云oss中，由总部开发人员查看日志，判断数据情况，在JMS平台同步PDA交互数据；PDA交互日志记录了设备登录时间、登录用户信息、数据操作时间、数据上传时间、操作类型等信息； 3.设备上传的本地日志及交互日志均统一打包记录于阿里云oss中进行保存。 |
| 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； | 1、PDA系统涉及了两类日志，分别为本地日志及交互日志； 2、具体日志内容如下： 本地日志：用户名、登录时间、操作内容、系统时间、操作时间； 交互日志：设备登录时间、登录用户信息、数据操作时间、数据上传时间、操作类型。 |
| 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、PDA中不展示日志信息，只保存相关日志记录，用户在系统中无法查看相关信息，相关日志信息统一保存在阿里云oss中； 2、日志信息通过oss保存，在oss中日志只允许读取，用户无修改、删除权限； 3、oss中日志永久保存，资源空间不足时会通知管理员增加存储资源，通过上机查看，可追溯至2022年1月的日志信息。 |
| d）应对审计进程进行保护，防止未经授权的中断。 | PDA系统没有独立的审计进程，系统基于安卓技术开发，内置极兔PDA程序，默认系统启动所有相关功能均开启，在管理后台配置了用户退出输入密码策略、用户安装新APP输入密码策略以及不允许开启调试模式等策略，能够防止用户对设备系统恶意操作。 |
| 入侵防范 | a）应遵循最小安装的原则，仅安装需要的组件和应用程序； | 通过现场访谈、查看，PDA系统的安装遵循最小安装的原则，不存在仍在开发或未经安全测试的功能模块。 |
| b）应关闭不需要的系统服务、默认共享和高危端口； | PDA系统为APP应用系统，此项不适用。 |
| c）应通过设定终端接入方式或网络地址范围对通过网络进行管理的管理终端进行限制； | PDA系统为APP应用系统，此项不适用。 |
| d）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； | 通过对PDA系统的输入窗口、上传窗口进行测试，确认针对手机号、单号等均具有有效性校验，针对上传窗口均使用白名单机制，基于业务所需对上传文件的格式、大小、文件类型进行了限制。 |
| e）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； | 通过漏洞扫描、APP测试，PDA系统及所属应用服务器、中间件、数据库服务器等未发现高风险漏洞。 |
| f）应能够检测到对重要节点进行入侵的行为，并在发生严重入侵事件时提供报警。 | PDA系统为APP应用系统，此项不适用。 |
| 可信验证 | a）可基于可信根对计算设备的系统引导程序、系统程序、重要配置参数和应用程序等进行可信验证，并在应用程序的关键执行环节进行动态可信验证，在检测到其可信性受到破坏后进行报警，并将验证结果形成审计记录送至安全管理中心。 | PDA系统未基于可信根对计算设备的系统引导程序、系统程序、重要配置参数和应用程序等进行可信验证。 |
| 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； | PDA系统启用了证书服务，通过HTTPS协议保证系统中鉴别数据、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。 | PDA系统针对用户鉴别信息在存储时采用md5+salt的方式保护数据的完整性。通过现场查看，存储重要业务数据、重要审计数据、重要配置数据和重要个人信息等数据库表中未发现完整性校验字段，未对部分重要数据在存储过程中的完整性进行保护。 |
| 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； | PDA系统启用了证书服务，通过HTTPS协议保证系统鉴别数据、重要业务数据和重要个人信息等在传输过程中的保密性。 |
| b）应采用密码技术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个人信息等。 | 1、通过现场查看，PDA系统所属JMS平台中针对入库个人数据，如：内外部人员身份证号码、照片、收件人手机号、员工手机号等，均采用aes-128-cbc对称加密算法进行了加密处理； 2、未对鉴别数据、重要业务数据进行存储加密。 |
| 数据备份恢复 | a）应提供重要数据的本地数据备份与恢复功能； | 系统重要数据存储在数据库中，云上数据库每天全量备份，保留近7个备份库文件，阿里云保证备份库文件的有效性；IDC机房数据库每天全量备份，保留近20个备份库文件，运维人员每季度对备份文件进行恢复测试。 |
| b）应提供异地实时备份功能，利用通信网络将重要数据实时备份至备份场地； | 无异地备份措施。 |
| c）应提供重要数据处理系统的热冗余，保证系统的高可用性。 | PDA系统涉及的服务器、数据库均采用集群方式部署，保证了系统的高可用性。 |
| 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； | PDA系统中用户Token信息失效时间配置为24小时，24小时用户无操作注销用户登录信息，能够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。 |
| 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。 | PDA系统中用户Token信息失效时间配置为24小时，24小时用户无操作注销用户登录信息，能够保证敏感数据所在的存储空间被释放或重新分配前得到完全清除。 |
| 个人信息保护 | a）应仅采集和保存业务必需的用户个人信息； | 1、快递员在使用PDA设备收发快件时，会通过扫码获取用户个人信息，包括用户名（虚拟或真实）、手机号（中间4位脱敏），快递员因业务需要与用户通话时，通过扫描条行码获取用户脱敏后的手机号，与用户通过95短号进行通信。 2、公司制定了YL-1-ISMS-02《信息安全和隐私管理策略手册》，并在用户登录前要求用户确认，在政策第一节“我们如何收集您的个人信息”中对用户信息收集的方法、信息类型在规范中明确了用户收集规则、收集方式、收集内容等进行了详细说明。 |
| b）应禁止未授权访问和非法使用用户个人信息。 | 1、用户手机号统一存储在JMS平台数据库中，数据库针对用户手机号进行了加密+脱敏处理，因业务需要需展示用户真实手机号时，在获取页面点击确认按钮进行确认，并记录至日志中。同时针对用户数据的访问只有获得授权的管理员可以查看，同时通过审计日志对用户的操作行为进行记录，同时个人数据信息在入库时采用压缩加密的方式进行保护。 2、公司制定了YL-1-ISMS-02《信息安全和隐私管理策略手册》，在手册第二、三、四、五中说明了对用户信息的使用、存储保护、对外提供、访问管理等方式方法，在第六、七、八节中，明确了对儿童信息、信息转移方面的具体处理方法。 |

|  |  |  |  |
| --- | --- | --- | --- |
| **测评项目** |  | **测评对象** | 数据资源 |
| **测评单位** |  | | |
| **测评地点** |  | | |
| **测评人员** |  | **配合人员** | 刘亮 |
| **测评日期** | 2023.6.15-2023.6.16 | | |
| **测评人员签字** |  | **配合人员签字** |  |

4.1.6. 数据资源

4.1.6.1. 鉴别数据

|  |  |  |
| --- | --- | --- |
| **安全控制点** | **测评指标** | **结果记录** |
| 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； | 采用HTTPS加密传输协议保证鉴别数据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。 | 采用MD5+salt校验技术保证鉴别数据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； | 采用HTTPS加密传输协议保证鉴别数据在传输过程中的保密性。 |
| b）应采用密码技术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个人信息等。 | 未采用加密技术保证鉴别数据在存储过程中的保密性。 |
| 数据备份恢复 | a）应提供重要数据的本地数据备份与恢复功能； | 测评对象为鉴别数据，不适用。 |
| b）应提供异地实时备份功能，利用通信网络将重要数据实时备份至备份场地； | 测评对象为鉴别数据，不适用。 |
| c）应提供重要数据处理系统的热冗余，保证系统的高可用性。 | 测评对象为鉴别数据，不适用。 |
| 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； | 测评对象为鉴别数据，不适用。 |
| 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。 | 测评对象为鉴别数据，不适用。 |
| 个人信息保护 | a）应仅采集和保存业务必需的用户个人信息； | 测评对象为鉴别数据，不适用。 |
| b）应禁止未授权访问和非法使用用户个人信息。 | 测评对象为鉴别数据，不适用。 |

4.1.6.2. 重要业务数据

|  |  |  |
| --- | --- | --- |
| **安全控制点** | **测评指标** | **结果记录** |
| 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； | 采用HTTPS加密传输协议保证业务数据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。 | 未采用校验技术保证业务数据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； | 采用HTTPS加密传输协议保证业务数据在传输过程中的保密性。 |
| b）应采用密码技术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个人信息等。 | 未采用加密技术保证业务数据在存储过程中的保密性。 |
| 数据备份恢复 | a）应提供重要数据的本地数据备份与恢复功能； | 业务数据存储在数据库中，数据库具有本地备份策略，云上数据库每天全量备份， |
| b）应提供异地实时备份功能，利用通信网络将重要数据实时备份至备份场地； | 无异地备份措施。 |
| c）应提供重要数据处理系统的热冗余，保证系统的高可用性。 | 测评对象为重要业务数据，不适用。 |
| 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； | 测评对象为重要业务数据，不适用。 |
| 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。 | 测评对象为重要业务数据，不适用。 |
| 个人信息保护 | a）应仅采集和保存业务必需的用户个人信息； | 测评对象为重要业务数据，不适用。 |
| b）应禁止未授权访问和非法使用用户个人信息。 | 测评对象为重要业务数据，不适用。 |

4.1.6.3. 主要配置数据

|  |  |  |
| --- | --- | --- |
| **安全控制点** | **测评指标** | **结果记录** |
| 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； | 采用HTTPS加密传输协议保证配置数据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。 | 未采用校验技术保证配置数据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； | 测评对象为重要配置数据，不适用。 |
| b）应采用密码技术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个人信息等。 | 测评对象为重要配置数据，不适用。 |
| 数据备份恢复 | a）应提供重要数据的本地数据备份与恢复功能； | 重要配置数据存储在数据库中，数据库具有本地备份策略，云上数据库每天全量备份，备份库保留7天，阿里云保证备份库的有效性；IDC机房数据库每天全量备份，备份库保留20天，运维人员每季度进行恢复测试。 |
| b）应提供异地实时备份功能，利用通信网络将重要数据实时备份至备份场地； | 测评对象为重要配置数据，不适用。 |
| c）应提供重要数据处理系统的热冗余，保证系统的高可用性。 | 测评对象为重要配置数据，不适用。 |
| 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； | 测评对象为重要配置数据，不适用。 |
| 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。 | 测评对象为重要配置数据，不适用。 |
| 个人信息保护 | a）应仅采集和保存业务必需的用户个人信息； | 测评对象为重要配置数据，不适用。 |
| b）应禁止未授权访问和非法使用用户个人信息。 | 测评对象为重要配置数据，不适用。 |

4.1.6.4. 重要个人信息

|  |  |  |
| --- | --- | --- |
| **安全控制点** | **测评指标** | **结果记录** |
| 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； | 采用HTTPS加密传输协议保证个人信息数据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。 | 未采用校验技术保证个人信息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； | 采用HTTPS加密传输协议保证个人信息在传输过程中的保密性。 |
| b）应采用密码技术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个人信息等。 | 采用aes-128-cbc对称加密算法保证个人信息在存储过程中的保密性。 |
| 数据备份恢复 | a）应提供重要数据的本地数据备份与恢复功能； | 个人信息存储在数据库中，数据库具有本地备份策略，云上数据库每天全量备份， |
| b）应提供异地实时备份功能，利用通信网络将重要数据实时备份至备份场地； | 测评对象为重要个人信息，不适用。 |
| c）应提供重要数据处理系统的热冗余，保证系统的高可用性。 | 测评对象为重要个人信息，不适用。 |
| 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； | 测评对象为重要个人信息，不适用。 |
| 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。 | 测评对象为重要个人信息，不适用。 |
| 个人信息保护 | a）应仅采集和保存业务必需的用户个人信息； | 测评对象为重要个人信息，不适用。 |
| b）应禁止未授权访问和非法使用用户个人信息。 | 测评对象为重要个人信息，不适用。 |

4.1.6.5. 重要审计数据

|  |  |  |
| --- | --- | --- |
| **安全控制点** | **测评指标** | **结果记录** |
| 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； | 采用HTTPS加密传输协议保证审计数据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。 | 未采用校验技术保证审计数据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； | 测评对象为重要审计数据，不适用。 |
| b）应采用密码技术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个人信息等。 | 测评对象为重要审计数据，不适用。 |
| 数据备份恢复 | a）应提供重要数据的本地数据备份与恢复功能； | 审计数据存储在数据库中，数据库具有本地备份策略，云上数据库每天全量备份， |
| b）应提供异地实时备份功能，利用通信网络将重要数据实时备份至备份场地； | 测评对象为重要审计数据，不适用。 |
| c）应提供重要数据处理系统的热冗余，保证系统的高可用性。 | 测评对象为重要审计数据，不适用。 |
| 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； | 测评对象为重要审计数据，不适用。 |
| 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。 | 测评对象为重要审计数据，不适用。 |
| 个人信息保护 | a）应仅采集和保存业务必需的用户个人信息； | 测评对象为重要审计数据，不适用。 |
| b）应禁止未授权访问和非法使用用户个人信息。 | 测评对象为重要审计数据，不适用。 |

4.2. 云计算安全扩展要求部分

|  |  |  |  |
| --- | --- | --- | --- |
| **测评项目** |  | **测评对象** | 系统管理软件/平台 |
| **测评单位** |  | | |
| **测评地点** |  | | |
| **测评人员** |  | **配合人员** | 刘亮 |
| **测评日期** | 2023.6.16 | | |
| **测评人员签字** |  | **配合人员签字** |  |

4.2.1. 系统管理软件/平台

4.2.1.1. 阿里云控制台1

|  |  |  |
| --- | --- | --- |
| **安全控制点** | **测评指标** | **结果记录** |
| 身份鉴别 | a）当远程管理云计算平台中设备时，管理终端和云计算平台之间应建立双向身份验证机制。 | 经现场核查，管理终端和云计算平台之间未建立双向身份验证机制。 |
| 访问控制 | a）应保证当虚拟机迁移时，访问控制策略随其迁移； | 客户为云服务客户，系统部署在阿里公共云上，云计算安全由阿里云负责，阿里公共云已经通过等级保护第三级测评。 |
| b）应允许云服务客户设置不同虚拟机之间的访问控制策略。 | 在阿里云控制台中用户能够根据业务需求为虚拟服务器添加安全组，并且能够配置安全组策略，实现虚拟机之间的访问控制。 |
| 入侵防范 | a）应能检测虚拟机之间的资源隔离失效，并进行告警； | 客户为云服务客户，系统部署在阿里公共云上，云计算安全由阿里云负责，阿里云已经通过等级保护第三级测评。 |
| b）应能检测非授权新建虚拟机或者重新启用虚拟机，并进行告警； | 客户为云服务客户，系统部署在阿里公共云上，云计算安全由阿里云负责，阿里云已经通过等级保护第三级测评。 |
| c）应能够检测恶意代码感染及在虚拟机间蔓延的情况，并进行告警。 | 客户为云服务客户，系统部署在阿里公共云上，云计算安全由阿里云负责，阿里云已经通过等级保护第三级测评。 |
| 镜像和快照保护 | a）应针对重要业务系统提供加固的操作系统镜像或操作系统安全加固服务； | 客户为云服务客户，系统部署在阿里公共云上，云计算安全由阿里云负责，阿里云已经通过等级保护第三级测评。 |
| b）应提供虚拟机镜像、快照完整性校验功能，防止虚拟机镜像被恶意篡改； | 客户为云服务客户，系统部署在阿里公共云上，云计算安全由阿里云负责，阿里云已经通过等级保护第三级测评。 |
| c）应采取密码技术或其他技术手段防止虚拟机镜像、快照中可能存在的敏感资源被非法访问。 | 客户为云服务客户，系统部署在阿里公共云上，云计算安全由阿里云负责，阿里云已经通过等级保护第三级测评。 |
| 数据完整性和保密性 | a）应确保云服务客户数据、用户个人信息等存储于中国境内，如需出境应遵循国家相关规定； | 系统中所有数据均存储在阿里云华东二区（上海），在中国境内。 |
| b）应确保只有在云服务客户授权下，云服务商或第三方才具有云服务客户数据的管理权限； | 客户为云服务客户，系统部署在阿里公共云上，云计算安全由阿里云负责，阿里云已经通过等级保护第三级测评。 |
| c）应使用校验码或密码技术确保虚拟机迁移过程中重要数据的完整性，并在检测到完整性受到破坏时采取必要的恢复措施； | 客户为云服务客户，系统部署在阿里公共云上，云计算安全由阿里云负责，阿里云已经通过等级保护第三级测评。 |
| d）应支持云服务客户部署密钥管理解决方案，保证云服务客户自行实现数据的加解密过程。 | 客户为云服务客户，系统部署在阿里公共云上，云计算安全由阿里云负责，阿里云已经通过等级保护第三级测评。 |
| 数据备份恢复 | a）云服务客户应在本地保存其业务数据的备份； | 云租户能够通过自定义的方式选择重要业务数据的备份方式，备份周期等，同时公司在世纪互联IDC机房中配置备份策略，将重要数据备份至IDC机房中。 |
| b）应提供查询云服务客户数据及备份存储位置的能力； | 客户为云服务客户，系统部署在阿里公共云上，云计算安全由阿里云负责，阿里云已经通过等级保护第三级测评。 |
| c）云服务商的云存储服务应保证云服务客户数据存在若干个可用的副本，各副本之间的内容应保持一致； | 客户为云服务客户，系统部署在阿里公共云上，云计算安全由阿里云负责，阿里云已经通过等级保护第三级测评。 |
| d）应为云服务客户将业务系统及数据迁移到其他云计算平台和本地系统提供技术手段，并协助完成迁移过程。 | 客户为云服务客户，系统部署在阿里公共云上，云计算安全由阿里云负责，阿里云已经通过等级保护第三级测评。 |
| 剩余信息保护 | a）应保证虚拟机所使用的内存和存储空间回收时得到完全清除； | 客户为云服务客户，系统部署在阿里公共云上，云计算安全由阿里云负责，阿里云已经通过等级保护第三级测评。 |
| b）云服务客户删除业务应用数据时，云计算平台应将云存储中所有副本删除。 | 客户为云服务客户，系统部署在阿里公共云上，云计算安全由阿里云负责，阿里云已经通过等级保护第三级测评。 |

4.3. 移动互联安全扩展要求部分

|  |  |  |  |
| --- | --- | --- | --- |
| **测评项目** |  | **测评对象** | 系统管理软件/平台 |
| **测评单位** |  | | |
| **测评地点** |  | | |
| **测评人员** |  | **配合人员** | 刘亮 |
| **测评日期** | 2023.6.16 | | |
| **测评人员签字** |  | **配合人员签字** |  |

4.3.1. 系统管理软件/平台

4.3.1.1. PDA系统1

|  |  |  |
| --- | --- | --- |
| **安全控制点** | **测评指标** | **结果记录** |
| 移动终端管控 | a）应保证移动终端安装、注册并运行终端管理客户端软件； | 1.PDA设备的集中管理通过JMS综合物流平台系统-智能设备模块-巴枪管控进行控制管理； 2.PDA设备在出场时OS版本内置极兔助手程序，使用用户首次使用需通过PDA登录极兔助手，通过员工编号+密码的方式验证身份，开展具体工作。 3.设备首次接入JMS综合物流平台系统时，需要在极兔助手中确认注册，将所属网点、型号、sn号、imei、mac信息同步至JMS平台，JMS平台通过智能设备模块-巴枪管控-设备登记模块记录设备信息，通过此模块可修改设备具体信息。 |
| b）移动终端应接受移动终端管理服务端的设备生命周期管理、设备远程控制，如：远程锁定、远程擦除等。 | 1.管理员通过JMS综合物流平台系统-智能设备模块-巴枪管控-策略管理模块，可以对PDA设备进行安全控制管理，如：密码安全（解锁密码）、功能限制（禁止使用原生浏览器、禁止修改系统时间和日期、禁止开启开发者选项、USB调试、禁止恢复出厂设置）、扫描头设置（禁止系统扫描）、安全桌面（用户退出系统的密码规则）、未知密码（下载未知来源软件的密码规则）； 2.管理员通过JMS综合物流平台系统-智能设备模块-巴枪管控-设备管理可以控制设备的锁屏密码清除、远程锁定设备、远程恢复设备出厂。 |
| 移动应用管控 | a）应具有选择应用软件安装、运行的功能； | PDA设备是定制化开发的专用设备，设备自身支持第三方软件的下载、安装、运行，管理员通过JMS平台-智能设备模块-巴枪管控-设备管理可以对设备软件安装、运行进行控制。 |
| b）应只允许指定证书签名的应用软件安装和运行； | 1.PDA设备中内置极兔助手程序，极兔助手程序中推送的相关应用是通过JMS平台手动同步的程序，极兔助手中相关应用不需要密码就能够安装，通过其他软件安装的相关应用均需输入安装密码。 2.安装后的第三方软件不能够在极兔桌面展示，需要退出极兔桌面进入供应商桌面进行使用，在退出极兔桌面时需输入单独的退出密码（与用户登录密码不同）。 |
| c）应具有软件白名单功能，应能根据白名单控制应用软件安装、运行。 | 1.极兔助手中相关应用为默认白名单软件，其他来源安装的软件均不在极兔桌面中展示； 2.在使用以安装的第三方软件时，需输入退出密码退出极兔桌面。 |

5. 安全管理中心测评表

|  |  |  |  |
| --- | --- | --- | --- |
| **测评项目** |  | **测评对象** | 安全管理中心 |
| **测评单位** |  | | |
| **测评地点** |  | | |
| **测评人员** |  | **配合人员** | 周强 |
| **测评日期** | 2023.6.19 | | |
| **测评人员签字** |  | **配合人员签字** |  |

5.1. 安全通用要求部分

5.1.1. 安全管理中心

|  |  |  |
| --- | --- | --- |
| **安全控制点** | **测评指标** | **结果记录** |
| 系统管理 | a）应对系统管理员进行身份鉴别，只允许其通过特定的命令或操作界面进行系统管理操作，并对这些操作进行审计； | 在阿里云控制台、堡垒机、天眼云镜等管理系统、360本地安全大脑、数据库安全审计系统中通过用户名、口令的方式进行身份鉴别，并且单独创建系统管理员账号，可以通过独立操作界面进行系统的管理操作，并能够对用户操作行为进行审计记录。 |
| b）应通过系统管理员对系统的资源和运行进行配置、控制和管理，包括用户身份、系统资源配置、系统加载和启动、系统运行的异常处理、数据和设备的备份与恢复等。 | 在阿里云控制台、堡垒机、天眼云镜、360本地安全大脑等管理系统、、数据库安全审计系统中系统管理员可以对系统的访问控制权限进行分配管理，对业务系统的部署和运维进行管理，对系统的入侵和异常进行处理，并可对数据进行备份等操作。 |
| 审计管理 | a）应对审计管理员进行身份鉴别，只允许其通过特定的命令或操作界面进行安全审计操作，并对这些操作进行审计； | 在阿里云控制台、堡垒机、天眼云镜、360本地安全大脑、数据库安全审计系统等管理系统中单独创建审计管理员账户，审计管理员通过用户名、口令的方式进行身份鉴别，可以通过操作界面进行系统的管理操作，并可对用户的登录行为、操作行为以及系统的安全事件包括sql语句、入侵事件等进行审计。 |
| b）应通过审计管理员对审计记录应进行分析，并根据分析结果进行处理，包括根据安全审计策略对审计记录进行存储、管理和查询等。 | 在阿里云控制台、堡垒机、天眼云镜等管理系统、360本地安全大脑、数据库安全审计系统中通过审计管理员对审计记录进行审计，审计权限包括对审计记录的存储、管理以及查询，并提供数据导出以及生成报表的能力。 |
| 安全管理 | a）应对安全管理员进行身份鉴别，只允许其通过特定的命令或操作界面进行安全管理操作，并对这些操作进行审计； | 经现场核查，阿里云控制台、堡垒机、天眼云镜、360本地安全大脑、数据库安全审计系统等管理系统中配置安全管理员角色用户，通过用户名、口令的方式进行身份鉴别，可以通过操作界面进行系统的管理操作，并对用户的登录行为、操作行为以及系统的安全事件包括sql语句、入侵事件等进行审计。 |
| b）应通过安全管理员对系统中的安全策略进行配置，包括安全参数的设置，主体、客体进行统一安全标记，对主体进行授权，配置可信验证策略等。 | 未通过安全管理员对系统主体、客体进行安全标记以及可信验证。 |
| 集中管控 | a）应划分出特定的管理区域，对分布在网络中的安全设备或安全组件进行管控； | 经现场核查，被测系统中单独划分了带外管理区，对分布在网络中的安全设备及安全服务等进行集中管控。 |
| b）应能够建立一条安全的信息传输路径，对网络中的安全设备或安全组件进行管理； | 经现场核查，被测系统采用SSH协议对网络设备进行远程管理，采用HTTPS加密通道对安全设备进行管理。 |
| c）应对网络链路、安全设备、网络设备和服务器等的运行状况进行集中监测； | 经现场访谈及核查，被测系统中部署了360本地安全大脑阿里云控制台、天眼云镜系统，对安全设备、网络设备、服务器的运行状况及通信链路等进行集中监测。 |
| d）应对分散在各个设备上的审计数据进行收集汇总和集中分析，并保证审计记录的留存时间符合法律法规要求； | 经现场核查及访谈，在阿里云控制台上启用操作审计，将阿里公共云的审计日志进行集中汇总、分析；服务器、网络设备、安全设备中审计记录集中汇总至360本地安全大脑中进行汇总、分析，审计记录保存时间满足180天以上。 |
| e）应对安全策略、恶意代码、补丁升级等安全相关事项进行集中管理； | 经现场核查及访谈，通过阿里公共云业务区恶意代码及补丁升级等均由阿里云负责升级维护，世纪互联IDC机房中安全策略、恶意代码、补丁升级等均由信息安全工程师负责维护。 |
| f）应能对网络中发生的各类安全事件进行识别、报警和分析。 | 经现场核查及访谈，被测系统中部署360全流量分析及360本地安全大脑、青藤云天眼云镜等安全设备，对网络中发生的各类安全事件进行识别、分析，发生严重事件提供钉钉报警。 |

|  |  |  |  |
| --- | --- | --- | --- |
| **测评项目** |  | **测评对象** | 安全管理中心 |
| **测评单位** |  | | |
| **测评地点** |  | | |
| **测评人员** |  | **配合人员** | 周强 |
| **测评日期** | 2023.6.19 | | |
| **测评人员签字** |  | **配合人员签字** |  |

5.2. 云计算安全扩展要求部分

5.2.1. 安全管理中心

|  |  |  |
| --- | --- | --- |
| **安全控制点** | **测评指标** | **结果记录** |
| 集中管控 | a）应能对物理资源和虚拟资源按照策略做统一管理调度与分配； | 客户为云租户，云计算安全由阿里云负责，阿里公共云已经通过等级保护第三级测评。 |
| b）应保证云计算平台管理流量与云服务客户业务流量分离； | 客户为云租户，云计算安全由阿里云负责，阿里公共云已经通过等级保护第三级测评。 |
| c）应根据云服务商和云服务客户的职责划分，收集各自控制部分的审计数据并实现各自的集中审计； | 经现场访谈及核查，客户为云租户，阿里云控制台中仅能够采集云租户账号所属的安全服务及安全资源相关的审计记录。 |
| d）应根据云服务商和云服务客户的职责划分，实现各自控制部分，包括虚拟化网络、虚拟机、虚拟化安全设备等的运行状况的集中监测。 | 客户为云租户，在阿里云采购了云监控服务，通过云监控服务仅能够对云租户采购的安全服务及虚拟资源等进行集中监控。 |

6. 安全管理制度测评表

|  |  |  |  |
| --- | --- | --- | --- |
| **测评项目** |  | **测评对象** | 安全管理制度 |
| **测评单位** |  | | |
| **测评地点** |  | | |
| **测评人员** |  | **配合人员** | 周强 |
| **测评日期** | 2023.6.16 | | |
| **测评人员签字** |  | **配合人员签字** |  |

6.1. 安全通用要求部分

6.1.1. 安全管理制度

|  |  |  |
| --- | --- | --- |
| **安全控制点** | **测评指标** | **结果记录** |
| 安全策略 | a）应制定网络安全工作的总体方针和安全策略，阐明机构安全工作的总体目标、范围、原则和安全框架等。 | 经现场检查，极兔速递有限公司制定了YL-1-ISMS-02《信息安全和隐私管理策略手册》，文件明确了网络安全工作的总体方针和策略，内容包括了信息安全的目标、范围、原则、框架等。 |
| 管理制度 | a）应对安全管理活动中的各类管理内容建立安全管理制度； | 经现场检查，极兔速递有限公司对安全管理活动中的各类管理内容建立了相应的安全管理体系和安全管理制度，如：YL-1-ISMS-02《信息安全和隐私管理策略手册》、YL-2-ISMS-10《信息资产分类分级管理制度》、YL-2-ISMS-31《信息安全事件管理制度》、YL-1-ISMS-03《信息安全和隐私管理组织架构与职责》等，内容覆盖了制度管理、机构管理、人员管理、系统建设管理和运维管理等方面的各类安全管理活动。 |
| b）应对管理人员或操作人员执行的日常管理操作建立操作规程； | 经现场检查，极兔速递有限公司对安全管理人员和操作人员的日常管理建立了操作规程，已形成YL-2-PD-29《Java安全编程规范》、YL-2-PO-20《IT变更管理流程》、YL-2-ISMS-41《应用安全开发指引》、YL-2-PO-18《网络与系统安全管理规范》等重要操作的操作规程。 |
| c）应形成由安全策略、管理制度、操作规程、记录表单等构成的全面的安全管理制度体系。 | 经现场检查，极兔速递有限公司申请通过了ISO27001《信息安全管理体系认证》、ISO27701《隐私信息管理体系认证》，并形成了由安全策略、管理制度、操作规程、记录表单构成较全面的安全管理制度体系。 |
| 制定和发布 | a）应指定或授权专门的部门或人员负责安全管理制度的制定； | 经现场检查，极兔速递有限公司制定了YL-1-ISMS-02《信息安全和隐私管理策略手册》，明确了由信息安全组负责管理体系文件的制定、修订，并由信息安全组负责落实。 |
| b）安全管理制度应通过正式、有效的方式发布，并进行版本控制。 | 经现场检查，极兔速递有限公司制定了YL-1-ISMS-02《信息安全和隐私管理策略手册》，明确了安全管理制度的流程和规范，规定了安全管理制度的制定流程、发布程序、发布范围等各项要求，安全管理制度由高层领导批准后通过ONES系统正式发布。 |
| 评审和修订 | a）应定期对安全管理制度的合理性和适用性进行论证和审定，对存在不足或需要改进的安全管理制度进行修订。 | 经现场检查，极兔速递有限公司在YL-1-ISMS-02《信息安全和隐私管理策略手册》中规定至少每年一次对安全管理制度的合理性适用性进行检查和审定，经过查验，公司已对需要改进的安全管理制度进行修订，形成了修订版本记录表格。 |

7. 安全管理机构测评表

|  |  |  |  |
| --- | --- | --- | --- |
| **测评项目** |  | **测评对象** | 安全管理机构 |
| **测评单位** |  | | |
| **测评地点** |  | | |
| **测评人员** |  | **配合人员** | 周强 |
| **测评日期** | 2023.6.16 | | |
| **测评人员签字** |  | **配合人员签字** |  |

7.1. 安全通用要求部分

7.1.1. 安全管理机构

|  |  |  |
| --- | --- | --- |
| **安全控制点** | **测评指标** | **结果记录** |
| 岗位设置 | a）应成立指导和管理网络安全工作的委员会或领导小组，其最高领导由单位主管领导担任或授权； | 经现场检查，极兔速递有限公司制定了YL-1-ISMS-03《信息安全和隐私管理组织架构与职责》，明确了信息安全和隐私管理决策委员会和信息安全组的人员构成情况和工作职责，委员会的最高领导由CEO耿仙朋担任，信息安全组组长由信息安全部门负责人黄福胜担任。 |
| b）应设立网络安全管理工作的职能部门，设立安全主管、安全管理各个方面的负责人岗位，并定义各负责人的职责； | 制定了YL-1-ISMS-03《信息安全和隐私管理组织架构与职责》，明确网络安全管理工作的决策部门为信息安全和隐私管理决策委员会，网络安全管理工作的职能部门为信息安全组，同时设置数据安全及隐私保护负责人、产品负责人、研发负责人、人事负责人、平台运维负责人等岗位，并且对各负责人工作职责进行详细描述，如：数据安全及隐私保护负责人工作职责为全面统筹实施组织内部的信息安全、数据安全、个人信息保护工作，对信息安全、数据安全、个人隐私保护负直接责任，组织制定数据安全、个人隐私保护工作计划并督促落实等。 |
| c）应设立系统管理员、审计管理员和安全管理员等岗位，并定义部门及各个工作岗位的职责。 | 经访谈安全管理员及查验YL-1-ISMS-03《信息安全和隐私管理组织架构与职责》，公司设置了系统运维工程师、信息安全工程师等岗位，并在制度文件中对各岗位工作职责进行明确描述，如：系统运维工程师主要负系统日常运行维护工作，包括：网络设备、安全设备、服务器和用户终端，信息安全工程师主要负责安全制度落实，整体安全管理、安全审计管理等。 |
| 人员配备 | a）应配备一定数量的系统管理员、审计管理员和安全管理员等； | 经现场检查，极兔速递有限公司配备了一定数量的系统运维工程师、信息安全工程师，数量满足业务需要和相互制约的要求，同时提供了管理人员清单。 |
| b）应配备专职安全管理员，不可兼任。 | 经现场检查，极兔速递有限公司设立了专职的安全管理人员，目前由信息安全工程师（张吉祥）担任专职安全管理员。 |
| 授权和审批 | a）应根据各个部门和岗位的职责明确授权审批事项、审批部门和批准人等； | 经现场检查，极兔速递有限公司采用信息化管理，通过OA系统进行流程审批，在系统中根据各个部门和岗位的职责明确授权审批事项、审批部门和批准人。 |
| b）应针对系统变更、重要操作、物理访问和系统接入等事项建立审批程序，按照审批程序执行审批过程，对重要活动建立逐级审批制度； | 在OA系统中针对系统变更、重要操作、物理访问和系统接入等事项建立审批程序，对于财务经费报批等重要活动建立了逐级审批制度。 |
| c）应定期审查审批事项，及时更新需授权和审批的项目、审批部门和审批人等信息。 | 经现场检查，极兔速递有限公司由信息科技部负责每月审查审批事项，及时在OA系统上更新需授权和审批的项目、审批部门和审批人等信息。 |
| 沟通和合作 | a）应加强各类管理人员、组织内部机构和网络安全管理部门之间的合作与沟通，定期召开协调会议，共同协作处理网络安全问题； | 经现场检查，极兔速递有限公司定期组织管理人员之间、组织内部机构和网络安全管理部门之间进行合作与沟通，并留存有相关会议记录表单记录。 |
| b）应加强与网络安全职能部门、各类供应商、业界专家及安全组织的合作与沟通； | 经现场检查，极兔速递有限公司与上海市青浦区网安支队、国家邮政局、拼多多、阿里云等机构保持有密切的沟通合作机制，并保留有相关会议纪要文件。 |
| c）应建立外联单位联系列表，包括外联单位名称、合作内容、联系人和联系方式等信息。 | 经现场检查，极兔速递有限公司已建立外部单位联系表，与上海市青浦区网安支队、国家邮政局、拼多多等监管单位及客户单位保持联系交流，外联单包括单位名称、联系人、联系电话等信息。 |
| 审核和检查 | a）应定期进行常规安全检查，检查内容包括系统日常运行、系统漏洞和数据备份等情况； | 经现场访谈安全管理员，公司运维组通过阿里云控制台、天眼云镜、360本地安全大脑等对系统日常运行情况进行实时监控，通过漏洞扫描设备定期对服务器、网络设备、安全设备等进行漏洞扫描，运维组成员定期登录备份服务器对备份数据进行完整性检查等，经现场核查，阿里云控制台、天眼云镜、360本地安全大脑运行正常，运维人员提供漏洞扫描报告及巡检记录等。 |
| b）应定期进行全面安全检查，检查内容包括现有安全技术措施的有效性、安全配置与安全策略的一致性、安全管理制度的执行情况等； | 经现场检查，极兔速递有限公司制定了《安全需求基线》、《信息安全及隐私保护有效性度量检查表》等检查表格，每个季度根据检查表格进行安全检查，检查内容包括：安全基线配置一致性、信息安全目标完成度、管理制度落实等。 |
| c）应制定安全检查表格实施安全检查，汇总安全检查数据，形成安全检查报告，并对安全检查结果进行通报。 | 经现场检查，极兔速递有限公司制定了《安全需求基线》、《信息安全及隐私保护有效性度量检查表》，安全管理员根据检查表格进行全面安全检查，经现场核查，公司于2022年3月23日-3月30日进行内审，并形成管理体系内审报告。 |

8. 安全管理人员测评表

|  |  |  |  |
| --- | --- | --- | --- |
| **测评项目** |  | **测评对象** | 安全管理人员 |
| **测评单位** |  | | |
| **测评地点** |  | | |
| **测评人员** |  | **配合人员** | 周强 |
| **测评日期** | 2023.6.19 | | |
| **测评人员签字** |  | **配合人员签字** |  |

8.1. 安全通用要求部分

8.1.1. 安全管理人员

|  |  |  |
| --- | --- | --- |
| **安全控制点** | **测评指标** | **结果记录** |
| 人员录用 | a）应指定或授权专门的部门或人员负责人员录用； | 经现场检查，极兔速递有限公司指定人资行政部负责人员招聘、录用等工作。 |
| b）应对被录用人员的身份、安全背景、专业资格或资质等进行审查，对其所具有的技术技能进行考核； | 经现场检查，极兔速递有限公司《招聘管理制度》中规定，人员录用时，雇佣了背调公司对被录用人员进行背景调查，在面试中采用技术考试的方式，对其所具有的技术技能进行考核。 |
| c）应与被录用人员签署保密协议，与关键岗位人员签署岗位责任协议。 | 经现场检查，极兔速递有限公司要求新员工签订劳动合同，同时签订《保密承诺书》、《保密与知识产权保护协议》、《竞业禁止协议》，未与关键岗位人员签署岗位责任协议。 |
| 人员离岗 | a）应及时终止离岗人员的所有访问权限，取回各种身份证件、钥匙、徽章等以及机构提供的软硬件设备； | 经现场检查，极兔速递有限公司在《内部人员信息安全与隐私管理制度》和《人力资源安全基线》中明确规定，员工应提前一个月提出离职申请，在领导审批后，由运维人员回收离职员工账号，行政人员回收离职员工身份证件、钥匙、电脑等公司提供的软硬件设备。 |
| b）应办理严格的调离手续，并承诺调离后的保密义务后方可离开。 | 经现场访谈，极兔速递有限公司人员离岗时，由运维和行政人员确认原岗位使用的各类信息是否已完成交接或被关闭，并确保保管的工作资料、信息资产及各类计算机设备已全部交回，经核查具备人员离职交接单。 |
| 安全意识教育和培训 | a）应对各类人员进行安全意识教育和岗位技能培训，并告知相关的安全责任和惩戒措施； | 经现场检查，极兔速递有限公司《培训制度》和YL-2-HR-09《信息安全和隐私奖惩管理制度》中规定公司对各类人员进行安全教育培训，经核实，在腾讯乐享上进行线上课程学习，且明确了相关安全责任和惩戒措施，提供了《信息安全违规行为与处罚等级对应表》。 |
| b）应针对不同岗位制定不同的培训计划，对安全基础知识、岗位操作规程等进行培训； | 经现场检查，极兔速递有限公司针对不同岗位，如产品、研发等，制定了不同的培训计划，公司人员通过腾讯乐享完成对安全基础知识、岗位操作规程的学习，通过查看腾讯乐享中员工培训记录情况，所有员工均参加相应培训。 |
| c）应定期对不同岗位的人员进行技能考核。 | 经现场检查，极兔速递有限公司未定期对不同岗位的人员进行技能考核。 |
| 外部人员访问管理 | a）应在外部人员物理访问受控区域前先提出书面申请，批准后由专人全程陪同，并登记备案； | 经现场检查，极兔速递有限公司YL-2-ISMS-16《第三方人员信息安全和隐私管理制度》中规定，外部人员访问受控区域时，必须由接待人必须全程陪同，并告知有关安全管理规定。 |
| b）应在外部人员接入受控网络访问系统前先提出书面申请，批准后由专人开设账户、分配权限，并登记备案； | 经现场检查，极兔速递有限公司YL-2-ISMS-16《第三方人员信息安全和隐私管理制度》中对外部人员及第三方人员的接入访问进行了明确规定，未经许可，不允许外部访问人员进行系统接入，外部人员接入受控网络访问系统前由受访部门人员先提出OA申请，批准后由专人开设账户、分配权限。 |
| c）外部人员离场后应及时清除其所有的访问权限； | 经现场检查，极兔速递有限公司规定外部人员离场后由运维人员及时清除其所有的访问权限。 |
| d）获得系统访问授权的外部人员应签署保密协议，不得进行非授权操作，不得复制和泄露任何敏感信息。 | 经现场检查，极兔速递有限公司具有与获得系统访问权限的第三方人员签署《第三方人员保密承诺函》。 |

9. 安全建设管理测评表

|  |  |  |  |
| --- | --- | --- | --- |
| **测评项目** |  | **测评对象** | 安全建设管理 |
| **测评单位** |  | | |
| **测评地点** |  | | |
| **测评人员** |  | **配合人员** | 周强 |
| **测评日期** | 2023.6.16-2023.6.19 | | |
| **测评人员签字** |  | **配合人员签字** |  |

9.1. 安全通用要求部分

9.1.1. 安全建设管理

|  |  |  |
| --- | --- | --- |
| **安全控制点** | **测评指标** | **结果记录** |
| 定级和备案 | a）应以书面的形式说明保护对象的安全保护等级及确定等级的方法和理由； | 1、《信息系统安全等级保护定级报告》中明确了系统的安全保护等级为第三级（S3A3）；2、《信息系统安全等级保护定级报告》中说明了该系统定为第三级的方法和理由。 |
| b）应组织相关部门和有关安全技术专家对定级结果的合理性和正确性进行论证和审定； | 1、公司组织了专家评审会，针对该系统定级结果的合理性和正确性进行了论证和评审；2、形成了《专家评审意见》。 |
| c）应保证定级结果经过相关部门的批准； | 1、定级结果已得到公司信息安全领导小组的审批；2、具有审批记录。 |
| d）应将备案材料报主管部门和相应公安机关备案。 | 1、已将备案材料上报给上海市公安局进行备案；2、已获得上海市公安局出具的备案证明。 |
| 安全方案设计 | a）应根据安全保护等级选择基本安全措施，依据风险分析的结果补充和调整安全措施； | 1、该系统每年进行等保测评工作，测评机构对系统安全防护措施进行核查，提出了《问题清单及整改意见》；2、公司已按照《问题清单及整改意见》进行整改，对于目前无法及时整改的问题进行了风险评估。 |
| b）应根据保护对象的安全保护等级及与其他级别保护对象的关系进行安全整体规划和安全方案设计，设计内容应包含密码技术相关内容，并形成配套文件； | 公司目前暂无安全整体规划和安全方案设计文件。 |
| c）应组织相关部门和有关安全专家对安全整体规划及其配套文件的合理性和正确性进行论证和审定，经过批准后才能正式实施。 | 公司目前暂无安全整体规划和安全方案设计文件。 |
| 产品采购和使用 | a）应确保网络安全产品采购和使用符合国家的有关规定； | 1、在JT/88-A-AM-2021-001《采购管理制度V.2》中明确了产品采购的要求和产品采购流程；2、经核查，防火墙、web应用防火墙等安全设备具有销售许可证。 |
| b）应确保密码产品与服务的采购和使用符合国家密码管理主管部门的要求； | 系统使用了GlobalSign nv-sa证书，未满足国家密码管理部门的要求。 |
| c）应预先对产品进行选型测试，确定产品的候选范围，并定期审定和更新候选产品名单。 | 1、产品采购时，由使用部门提起申请，经采购部进行产品选型测试，最终确定产品候选范围；2、具有选型测试记录和产品候选清单。 |
| 自行软件开发 | a）应将开发环境与实际运行环境物理分开，测试数据和测试结果受到控制； | 1、系统开发环境部署在阿里公共云，生产环境分别部署在阿里公共云及世纪互联IDC机房中，其中阿里公共云开发环境与阿里公共云生产环境部分部署在不同VPC中，彼此之间不能互相通信；2、测试数据由测试人员负责管理，禁止非授权使用。 |
| b）应制定软件开发管理制度，明确说明开发过程的控制方法和人员行为准则； | 1、制定了软件开发方面的管理制度，如：YL-2-ISMS-41《应用安全开发指引》、YL-2-ISMS-42《安全测试管理规范》、YL-2-PD-30《开源代码管理规范》等；2、制度内容覆盖开发过程管控要求、人员开发准则等。 |
| c）应制定代码编写安全规范，要求开发人员参照规范编写代码； | 系统开发过程中，开发人员需根据YL-2-PD-29《JAVA安全编程规范》的相关要求编写代码。 |
| d）应具备软件设计的相关文档和使用指南，并对文档使用进行控制； | 经现场访谈安全管理员，JMS综合物流平台系统中相关设计文档及使用指南均在ONES系统中归档保存，经现场核查ONES系统中相关文档，具备软件设计文档及用户使用指南。 |
| e）应保证在软件开发过程中对安全性进行测试，在软件安装前对可能存在的恶意代码进行检测； | 经现场访谈安全管理员，JMS综合物流平台系统中每次版本迭代时均由安全测试人员进行安全测试，经现场核查，具备系统安全测试报告。 |
| f）应对程序资源库的修改、更新、发布进行授权和批准，并严格进行版本控制； | 经现场访谈安全管理员，JMS综合物流平台系统相关代码库均通过gitlib进行控制，代码库的合并、更新、发布均由管理员进行控制管理。 |
| g）应保证开发人员为专职人员，开发人员的开发活动受到控制、监视和审查。 | 1、经访谈，开发人员均为专职人员；2、YL-2-ISMS-41《应用安全开发指引》中对开发人员行为进行了规定，并由项目经理进行监督。 |
| 外包软件开发 | a）应在软件交付前检测其中可能存在的恶意代码； | 被测系统为自行开发，不涉及外包软件开发，故调整为不适用。 |
| b）应保证开发单位提供软件设计文档和使用指南； | 被测系统为自行开发，不涉及外包软件开发，故调整为不适用。 |
| c）应保证开发单位提供软件源代码，并审查软件中可能存在的后门和隐蔽信道。 | 被测系统为自行开发，不涉及外包软件开发，故调整为不适用。 |
| 工程实施 | a）应指定或授权专门的部门或人员负责工程实施过程的管理； | 授权产品经理负责工程实施过程的管理。 |
| b）应制定安全工程实施方案控制工程实施过程； | 经现场访谈安全管理员，公司针对系统版本迭代会建立产品迭代方案，在产品迭代方案中针对工程实施过程进行详细说明，经现场核查，具备产品迭代方案。 |
| c）应通过第三方工程监理控制项目的实施过程。 | 被测系统为自行开发，不适用。 |
| 测试验收 | a）应制订测试验收方案，并依据测试验收方案实施测试验收，形成测试验收报告； | 经现场访谈安全管理员，JMS综合物流平台系统版本迭代完成后会进行结项评分，包括主导部门，协助部门（技术架构、安全、UE团队、数据应用、移动团队）等均需参加评分，最终会根据项目结项评级落实项目验收，经现场核查，具备项目《结项评级表》。 |
| b）应进行上线前的安全性测试，并出具安全测试报告，安全测试报告应包含密码应用安全性测试相关内容。 | 经现场访谈安全管理员，系统上线前和每次迭代前均进行了安全测试，经现场核查，公司提供系统安全测试报告。 |
| 系统交付 | a）应制定交付清单，并根据交付清单对所交接的设备、软件和文档等进行清点； | 经现场访谈安全管理员及核查，在ONES系统中具备系统交付汇总材料，包含：设备清单、软件记录、建设文档材料等。 |
| b）应对负责运行维护的技术人员进行相应的技能培训； | 1、开发人员已对系统运行维护人员进行相应的技能培训；2、具有培训记录。 |
| c）应提供建设过程文档和运行维护文档。 | 经现场核查，在ones系统中具备系统建设文档、运行维护文档等。 |
| 等级测评 | a）应定期进行等级测评，发现不符合相应等级保护标准要求的及时整改； | 1、系统每年进行一次等级保护测评，针对不符合项进行了相应的整改；2、具有等保测评报告和整改记录。 |
| b）应在发生重大变更或级别发生变化时进行等级测评； | 被测系统目前未发生重大变更或级别发生变化，后续若遇到发生重大变更的情况，将依据相关法律法规重新进行等级测评。 |
| c）应确保测评机构的选择符合国家有关规定。 | 本次测评选择了具备测评资质的进行等级测评，符合国家相关规定。 |
| 服务供应商选择 | a）应确保服务供应商的选择符合国家的有关规定； | 公司选择了阿里云、世纪互联等供应商，符合国家的有关规定。 |
| b）应与选定的服务供应商签订相关协议，明确整个服务供应链各方需履行的网络安全相关义务； | 公司与阿里云、世纪互联签订了安全服务协议，明确了提供的技术支持和服务承诺等。 |
| c）应定期监督、评审和审核服务供应商提供的服务，并对其变更服务内容加以控制。 | 1、具有安全服务商提交的安全服务报告；2、对安全服务商提供的服务进行了审核。 |

|  |  |  |  |
| --- | --- | --- | --- |
| **测评项目** |  | **测评对象** | 安全建设管理 |
| **测评单位** |  | | |
| **测评地点** |  | | |
| **测评人员** |  | **配合人员** | 周强 |
| **测评日期** | 2023.6.16-2023.6.19 | | |
| **测评人员签字** |  | **配合人员签字** |  |

9.2. 云计算安全扩展要求部分

9.2.1. 安全建设管理

|  |  |  |
| --- | --- | --- |
| **安全控制点** | **测评指标** | **结果记录** |
| 云服务商选择 | a）应选择安全合规的云服务商，其所提供的云计算平台应为其所承载的业务应用系统提供相应等级的安全保护能力； | 公司选择的云服务商为阿里云，系统部署在阿里公共云上，阿里公共云通过了网络安全等级保护第三级测评，能够为其所承载的业务应用系统提供相应等级的安全保护能力。 |
| b）应在服务水平协议中规定云服务的各项服务内容和具体技术指标； | 1、已与阿里云签订了服务协议；2、协议中对实例型号、配置、服务期限等均进行了说明。 |
| c）应在服务水平协议中规定云服务商的权限与责任，包括管理范围、职责划分、访问授权、隐私保护、行为准则、违约责任等； | 1、与阿里云签订了服务协议；2、协议中规定了云服务商的权限与责任，包括管理范围、职责划分、访问授 权、隐私保护、行为准则、违约责任等。 |
| d）应在服务水平协议中规定服务合约到期时，完整提供云服务客户数据，并承诺相关数据在云计算平台上清除； | 1、与阿里云签订了服务协议；2、协议中规定了：当服务期届满、服务提前终止或发生欠费时，阿里云仅在一定的缓冲期内继续存储用户业务数据，逾期阿里云将删除所有用户业务数据，包括所有缓存或者备份的副本，不再保留任何用户业务数据。 |
| e）应与选定的云服务商签署保密协议，要求其不得泄露云服务客户数据。 | 1、与阿里云签订的服务协议中包含保密条款；2、保密条款规定数据归云服务客户所有，阿里云不得以任何理由泄露云服务客户的数据。 |
| 供应链管理 | a）应确保供应商的选择符合国家有关规定； | 客户为云租户，云计算安全由阿里云负责，阿里公共云已经通过等级保护第三级测评，符合国家的有关规定。 |
| b）应将供应链安全事件信息或安全威胁信息及时传达到云服务客户； | 客户为云租户，云计算安全由阿里云负责，阿里公共云已经通过等级保护第三级测评，符合国家的有关规定。 |
| c）应将供应商的重要变更及时传达到云服务客户，并评估变更带来的安全风险，采取措施对风险进行控制。 | 客户为云租户，云计算安全由阿里云负责，阿里公共云已经通过等级保护第三级测评，符合国家的有关规定。 |

|  |  |  |  |
| --- | --- | --- | --- |
| **测评项目** |  | **测评对象** | 安全建设管理 |
| **测评单位** |  | | |
| **测评地点** |  | | |
| **测评人员** |  | **配合人员** | 周强 |
| **测评日期** | 2023.6.16-2023.6.19 | | |
| **测评人员签字** |  | **配合人员签字** |  |

9.3. 移动互联安全扩展要求部分

9.3.1. 安全建设管理

|  |  |  |
| --- | --- | --- |
| **安全控制点** | **测评指标** | **结果记录** |
| 移动应用软件采购 | a）应保证移动终端安装、运行的应用软件来自可靠分发渠道或使用可靠证书签名； | 经核查、PDA系统为自行开发，不涉及移动应用软件采购，故调整为不适用。 |
| b）应保证移动终端安装、运行的应用软件由指定的开发者开发。 | 经核查、PDA系统为自行开发，不涉及移动应用软件采购，故调整为不适用。 |
| 移动应用软件开发 | a）应对移动业务应用软件开发者进行资格审查； | 公司对开发人员进行入职面试、笔试，要求相关人员具有多年行业经验方能通过入职面试，相关人员已通过公司技能通职业技能培训在线教学。 |
| b）应保证开发移动业务应用软件的签名证书合法性。 | 公司开发的PDA系统依据Android开发要求进行开发，要求所有的程序经过数字签名才能安装，如果没有可用的数字签名，安卓系统将不许安装运行此程序签名基本信息包括：密钥库类型: JKS密钥库提供方: SUN 发布者: CN=云路信息科技, OU=云路信息科技, O=云路信息科技, L=云路信息科技, ST=云路信息科技序列号: 5c88cd2c有效期开始日期: Tue Sep 24 18:28:34 CST 2019, 截止日期: Wed Sep 11 18:28:34 CST 2069签名算法名称: SHA256withRSA。 |

10. 安全运维管理测评表

|  |  |  |  |
| --- | --- | --- | --- |
| **测评项目** |  | **测评对象** | 安全运维管理 |
| **测评单位** |  | | |
| **测评地点** |  | | |
| **测评人员** |  | **配合人员** | 周强 |
| **测评日期** | 2023.6.19 | | |
| **测评人员签字** |  | **配合人员签字** |  |

10.1. 安全通用要求部分

10.1.1. 安全运维管理

|  |  |  |
| --- | --- | --- |
| **安全控制点** | **测评指标** | **结果记录** |
| 环境管理 | a）应指定专门的部门或人员负责机房安全，对机房出入进行管理，定期对机房供配电、空调、温湿度控制、消防等设施进行维护管理； | 该系统部署在世纪互联IDC机房和阿里公共云机房，阿里公共云已通过等级保护第三级测评，IDC机房由世纪互联负责运行维护，对机房出入进行管理，每天对机房供配电、空调、温湿度控制、消防等设施进行维护管理； |
| b）应建立机房安全管理制度，对有关物理访问、物品带进出和环境安全等方面的管理作出规定； | 该系统部署在世纪互联IDC机房和阿里公共云机房，阿里公共云已通过等级保护第三级测评，IDC机房由世纪互联负责运行维护，世纪互联建立了机房安全方面的管理制度，对物理机房访问、物品进出、环境安全等进行了明确规定，且具有人员访问登记表、设备出入登记表和机房设施巡检记录等文件。 |
| c）应不在重要区域接待来访人员，不随意放置含有敏感信息的纸档文件和移动介质等。 | 1、建立了YL-2-AD-17《办公环境物理安全管理制度》，第3.8章节“来访人员管理”中规定对于重要或特殊访客，先引导来访人员到指定区域；对于一般访客（主要为面试候选人），接待人员在确认信息后，及时通知面试官；访客原则不能单独进入办公区域，需要人员全程陪同。2、第3.7章节“办公桌面管理”中规定员工应做好重要资料保存工作，不得随意摆放保密文件，不得随意泄露，要收集并放置在指定位置。 |
| 资产管理 | a）应编制并保存与保护对象相关的资产清单，包括资产责任部门、重要程度和所处位置等内容； | 1、公司编制了系统资产清单；2、清单内容包括：设备名称、操作系统版本、数量、中间件/应用软件、IP地址等信息。 |
| b）应根据资产的重要程度对资产进行标识管理，根据资产的价值选择相应的管理措施； | 1、公司建立了YL-2-ISMS-10《信息资产分类分级管理制度》，对资产标识方法进行了规范，将信息资产分类实物资产、软件资产、企业数据资产、人员资产等；2、通过《固定资产管理制度》、YL-2-ISMS-11《数据资产密级划分、标识及处置管理制度》、YL-2-HR-08《内部人员信息安全和隐私管理制度》等对不同的资产进行管理。 |
| c）应对信息分类与标识方法作出规定，并对信息的使用、传输和存储等进行规范化管理。 | 1、公司建立了YL-2-ISMS-10《信息资产分类分级管理制度》，明确了信息资产的分类原则、分级原则以及标识方法；2、建立了YL-2-ISMS-11《数据资产密级划分、标识及处理管理制度》，对不同数据资产的保存、传输、下载等进行了规定。 |
| 介质管理 | a）应将介质存放在安全的环境中，对各类介质进行控制和保护，实行存储环境专人管理，并根据存档介质的目录清单定期盘点； | 1、公司建立了YL-2-ISMS-27《存储介质安全管理制度》，第2.3.3章节“存储介质保管”中规定涉密存储介质应存放在安全的环境中，做到防盗、防磁、防火、防潮、防止损坏，对脱机存放的各类存储介质由专人负责进行检查、控制和保护，以防止被盗、被毁、被修改以及信息的非法泄露；2、由公司统一安排时间对员工的资产情况进行盘点，形成了盘点记录。 |
| b）应对介质在物理传输过程中的人员选择、打包、交付等情况进行控制，并对介质的归档和查询等进行登记记录。 | 1、公司建立了YL-2-ISMS-27《存储介质安全管理制度》，第2.3章节对存储介质的使用、保管、维修、传输、报废、回收及反复利用等情况进行了规定；2、通过OA系统对介质申请、归档及查询进行登记记录，由行政部通过资产表对介质发放、归档等信息进行维护，资产表包括：编号、名称、资产组、使用部门、状态、规格型号、单独核算、使用人、计量单位、资产使用位置、入库日期、数量、资产类型、所属部门、资产来源等内容。 |
| 设备维护管理 | a）应对各种设备（包括备份和冗余设备）、线路等指定专门的部门或人员定期进行维护管理； | 1、系统部署在世纪互联IDC机房及阿里公共云，机房的各种设备及线路均由机房管理人员进行维护；2、公司内部各种设备（配套设施、软硬件等）的定期维护和管理由平台运维部负责。 |
| b）应建立配套设施、软硬件维护方面的管理制度，对其维护进行有效的管理，包括明确维护人员的责任、维修和服务的审批、维修过程的监督控制等； | 公司建立了《固定资产管理规定》，明确了运维部的职责和权限，并对固定资产的领用和登记、调拨转移、维修维养、出售、报废处置、清查盘点等进行了规定。 |
| c）信息处理设备应经过审批才能带离机房或办公地点，含有存储介质的设备带出工作环境时其中重要数据应加密； | 1、公司建立了YL-2-ISMS-14《公司机房管理制度》，第2.2.2章节“操作管理”中规定未经机房管理人员允许，禁止私自将设备或配件迁入/迁出机房；2、IT设备进出IDC机房时，需写邮件至机房管理人员，进行审核报备并登记；3、建立了YL-2-ISMS-27《存储介质安全管理记录》，第2.3.6章节“存储介质传输规定”中要求针对保存涉密数据的存储介质传输，应指定经过管理层授权的专人进行，保证良好的包装以免物理破损。 |
| d）含有存储介质的设备在报废或重用前，应进行完全清除或被安全覆盖，保证该设备上的敏感数据和授权软件无法被恢复重用。 | 公司建立了YL-2-ISMS-27《存储介质安全管理制度》，第2.3.7章节“存储介质报废”中规定允许按照资产管理相关制度处置报废储存介质，但至少应考虑以下几类风险：违反软件许可协议、未授权的散播机密信息、未授权的泄露商业机密、版权和其它知识产权；并分别对桌面类可消磁的存储介质、不可消磁的存储介质、机房类存储介质、涉密存储介质建立了相应的销毁方法。 |
| 漏洞和风险管理 | a）应采取必要的措施识别安全漏洞和隐患，对发现的安全漏洞和隐患及时进行修补或评估可能的影响后进行修补； | 1、信息科技部安全运维组日常进行安全测试、渗透测试、风险评估等工作，并形成报告；2、公司组织第三方安全众测对安全漏洞进行收集及预警；由安全运维组负责响应发布的漏洞预警，并进行系统的漏洞修补工作。 |
| b）应定期开展安全测评，形成安全测评报告，采取措施应对发现的安全问题。 | 公司按照等级保护相关规定每年对系统开展一次等级保护测评，针对测评过程中发现的问题进行及时整改。 |
| 网络和系统安全管理 | a）应划分不同的管理员角色进行网络和系统的运维管理，明确各个角色的责任和权限； | 公司设立了运维工程师、信息安全工程师等岗位，并在制度文件中对各岗位工作职责进行明确描述。 |
| b）应指定专门的部门或人员进行账户管理，对申请账户、建立账户、删除账户等进行控制； | 1、公司建立了《系统账号权限管理规范》，规定由OA系统管理员负责OA系统账号权限申请流程，审批通过后对员工OA账号创建、权限分配、权限变更、权限删除工作；2、由部门负责人负责OA系统“账号权限申请流程”的审核、会签工作，核实审核申请人所申请的权限是否与其岗位一致，确保申请权限的合理性、必要性和符合职责分工要求。 |
| c）应建立网络和系统安全管理制度，对安全策略、账户管理、配置管理、日志管理、日常操作、升级与打补丁、口令更新周期等方面作出规定； | 公司建立了《系统账号权限管理规范》、YL-2-ISMS-12《口令及访问管理制度》、YL-2-ISMS-23《安全日志管理制度》、YL-2-PO-18《网络与系统安全管理规范》分别对系统账号管理、安全配置要求、日志统一化管理、系统补丁及安全漏洞、口令更新、网络隔离策略等方面做出规定。 |
| d）应制定重要设备的配置和操作手册，依据手册对设备进行安全配置和优化配置等； | 经现场核查，在FAQ运维知识库中具备重要设备的配置和操作手册等，如：F5&WAF常规操作、MySQL操作手册、gitlib仓库操作手册、JMS应用操作手册等。 |
| e）应详细记录运维操作日志，包括日常巡检工作、运行维护记录、参数的设置和修改等内容； | 经现场访谈安全管理员，管理员运维操作日志分别在堡垒机、服务器、安全设备中进行详细记录，同时将审计记录上传至360本地安全大脑进行备份保存，经现场核查，堡垒机、服务器、安全设备中对用户操作行为，参数设置等均进行详细记录。 |
| f）应指定专门的部门或人员对日志、监测和报警数据等进行分析、统计，及时发现可疑行为； | 通过360本地安全大脑对设备、出口及系统日志等进行监控，由安全运维组对其检测报警数据进行管理，并将任务分配给具体人员进行处理。 |
| g）应严格控制变更性运维，经过审批后才可改变连接、安装系统组件或调整配置参数，操作过程中应保留不可更改的审计日志，操作结束后应同步更新配置信息库； | 1、公司建立了YL-2-PO-20《IT变更管理流程》，规定针对任何可能影响IT服务进行的增加、修改活删除活动；2、变更前由变更负责人通过OA系统填写《系统变更申请表》制定变更计划和影响评估，经过评审后，在正式变更之前对系统进行备份并通知变更方，准备工作完成后根据变更步骤进行变更。 |
| h）应严格控制运维工具的使用，经过审批后才可接入进行操作，操作过程中应保留不可更改的审计日志，操作结束后应删除工具中的敏感数据； | 1、公司规定仅由安全运维组人员远程连接堡垒机对系统进行运行维护；2、堡垒机记录了运维人员操作过程中的审计日志，且日志不可更改。 |
| i）应严格控制远程运维的开通，经过审批后才可开通远程运维接口或通道，操作过程中应保留不可更改的审计日志，操作结束后立即关闭接口或通道； | 1、系统运维地点以办公区域为主，如确有必要，根据YL-2-PO-18《网络和系统安全管理制度》第2.3.5章节“远程接入和第三方网络接入”中规定员工远程办公只能通过公司VPN拨入，一律禁止私自调整网络安全策略违规临时接入远程维护；2、远程接入网络的行为应有比较详细的日志记录，包含但不局限于VPN账号登录信息、访问资源信息、网络操作行为信息等。 |
| j）应保证所有与外部的连接均得到授权和批准，应定期检查违反规定无线上网及其他违反网络安全策略的行为。 | 经核查，在边界防火墙中配置可访问外部网络白名单策略，对与外部网络通信进行控制，并通过360AISA全流量威胁分析系统及360本地安全大脑对访问外部网络行为进行检测、记录等。 |
| 恶意代码防范管理 | a）应提高所有用户的防恶意代码意识，对外来计算机或存储设备接入系统前进行恶意代码检查等； | 1、公司建立了YL-2-PO-22《办公电脑使用与管理制度》，第2.3.5.1章节“病毒防护”中规定公司所有办公电脑都必须安全制定的杀毒软件，任何部门和个人不得随意停用、卸载；2、第2.3.5.3章节“移动设备管理”中规定外来人员需将移动设备接入公司内部网络使用时，需经过安全运维组确认并检测设备安全性，对于符合安全规定的的设备才能准许接入；3、员工可通过ONES项目管理平台进行制度的查看，要求全体员工了解病毒的危害，进而提高全员防病毒意识。 |
| b）应定期验证防范恶意代码攻击的技术措施的有效性。 | 1、公司建立了YL-2-PO-22《办公电脑使用与管理制度》，第2.3.5.1章节“病毒防护”中规定客户端从官方网站每24小时自动执行一次病毒库更新；2、经现场查看，病毒库最新更新时间为2022.11.8。 |
| 配置管理 | a）应记录和保存基本配置信息，包括网络拓扑结构、各个设备安装的软件组件、软件组件的版本和补丁信息、各个设备或软件组件的配置参数等； | 由公司安全运维组对信息系统的网络拓扑结构、设备安装的组件、组件版本号及软件配置信息进行记录和保存。 |
| b）应将基本配置信息改变纳入变更范畴，实施对配置信息改变的控制，并及时更新基本配置信息库。 | 公司已将信息系统基本配置信息的修改纳入系统变更的管理制度范畴内，通过OA系统提交申请进行配置信息的变更。 |
| 密码管理 | a）应遵循密码相关国家标准和行业标准； | 系统使用了GlobalSign nv-sa证书，未满足国家标准的要求。 |
| b）应使用国家密码管理主管部门认证核准的密码技术和产品。 | 系统使用了GlobalSign nv-sa证书，未经过密码主管部门的认证。 |
| 变更管理 | a）应明确变更需求，变更前根据变更需求制定变更方案，变更方案经过评审、审批后方可实施； | 公司建立了YL-2-PO-20《IT变更管理流程》，第2.3.3章节规定在变更实施前变更负责人通过OA系统填写《系统变更申请表》，制定变更计划和影响评估，并明确详细的变更步骤，变更小组进行评审后才可执行。 |
| b）应建立变更的申报和审批控制程序，依据程序控制所有的变更，记录变更实施过程； | 1、公司制定了YL-2-PO-20《IT变更管理流程》，建立了变更程序，并将变更程序划分为变更判断、变更计划、变更测试、变更准备、执行、变更观察及验证等方面；2、经现场核查，公司具备项目变更流程、变更申请表等。 |
| c）应建立中止变更并从失败变更中恢复的程序，明确过程控制方法和人员职责，必要时对恢复过程进行演练。 | 公司建立了《系统变更申请表》，存在系统回滚计划，需要采取备份等方式，确保在变更失败或变更取消等情况下，系统能顺利的回退到原来系统的状态；同时回退计划在资源允许的情况下，需对其进行必要的演练。 |
| 备份与恢复管理 | a）应识别需要定期备份的重要业务信息、系统数据及软件系统等； | 经现场访谈，JMS综合化物理平台系统中重要配置数据、重要业务数据、鉴别数据、个人信息、代码程序等均需要进行备份。 |
| b）应规定备份信息的备份方式、备份频度、存储介质、保存期等； | 公司建立了YL-2-PO-19《数据备份与恢复管理制度》，第2.3章节“备份策略”中对数据库、日志的备份方式、备份频率、数据保留周期等进行了规定，经核查，网络设备、安全设备等重要配置数据每天进行一次备份，永久保存，重要业务数据、鉴别数据、个人信息等均存储在数据库中，每天对数据进行全量备份，保留20个备份文件，代码程序由研发人员实时上传至gitlib库中进行备份，永久保存。 |
| c）应根据数据的重要性和数据对系统运行的影响，制定数据的备份策略和恢复策略、备份程序和恢复程序等。 | 1、公司建立了YL-2-PO-19《数据备份与恢复管理制度》，第2.3章节“备份策略”中针对Oracle数据库、PolarDB数据库、日志制定了备份策略；2、第2.4章节“备份管理流程”中明确了备份系统的日常维护、备份失败处理机制以及数据备份申请流程；3、第2.5章节“数据恢复申请方式”中对数据恢复方式和数据申请流程做出规定。 |
| 安全事件处置 | a）应及时向安全管理部门报告所发现的安全弱点和可疑事件； | 公司建立了YL-2-ISMS-31《信息安全事件管理制度》，第2.5.3章节“上报流程”中明确，通过安全监控、员工上报、反馈、投诉、审核、发现等途径获得信息安全事件时，首先判断事件类型，再通过公司邮箱、电话等方式及时向相关人员上报。 |
| b）应制定安全事件报告和处置管理制度，明确不同安全事件的报告、处置和响应流程，规定安全事件的现场处理、事件报告和后期恢复的管理职责等； | 1、公司建立了YL-2-ISMS-31《信息安全事件管理制度》，第2.2章节“职责分工”中明确了与安全事件有关的信息安全组、综合管理部、公司各部门、公司所有员工的工作职责；2、第2.3章节“信息安全事件分类”中根据信息安全事件发生的原因、表现等将信息安全事件分为网络攻击事件、有害程序事件、信息泄露事件和信息内容安全事件四类，并分别对这四类信息安全事件的上报、响应、处理、升级、总结等进行了规定。 |
| c）应在安全事件报告和响应处理过程中，分析和鉴定事件产生的原因，收集证据，记录处理过程，总结经验教训； | 1、公司建立了YL-2-ISMS-31《信息安全事件管理制度》，第2.5.3章节“流程说明”中明确了在信息安全事件发生后，由安全应急处理人员对安全事件涉及的相关业务系统、模块运行状况进行问题排查，保留记录，填写安全事件处理过程及相关记录；2、事件处理完成后，安全事件调查人启动事件原因调查工作，对事件原因进行分析，确定安全事件责任人并形成调查报告，最终由安全应急处理人就事件原因、事件经过、处理决定、改进意见等内容形成信息安全事件报告。 |
| d）对造成系统中断和造成信息泄漏的重大安全事件应采用不同的处理程序和报告程序。 | 公司建立了YL-2-ISMS-31《信息安全事件管理制度》，将信息安全事件分为网络攻击事件、有害程序事件、信息泄露事件和信息内容安全事件四大类，并将这四大类安全事件进一步进行分级，针对不同级别的安全事件，分别建立了上报、响应、处理、升级等程序。 |
| 应急预案管理 | a）应规定统一的应急预案框架，包括启动预案的条件、应急组织构成、应急资源保障、事后教育和培训等内容； | 公司建立了《网络安全事件应急预案》，在第五章正文中包括网络安全事件应急工作要求、信息监测与报告、预警处理与预警发布、先期处理、应急处理、应急结束、监测与演练等内容。 |
| b）应制定重要事件的应急预案，包括应急处理流程、系统恢复流程等内容； | 公司针对DDoS攻击、恶意代码安全事件、运维堡垒机系统故障、个人数据泄露、其他突发事件等重要事件进行了分级，并制定了相应的应急处置流程、应急培训与演练等。 |
| c）应定期对系统相关的人员进行应急预案培训，并进行应急预案的演练； | 1、公司规定由信息安全组协调有关部门进行定期演练，并在应急预案演练之前对相关人员进行应急预案培训，确保每个应急响应人员能够了解各自的角色职责和应急处置流程；2、经现场核查，公司针对双11大促制定应急预案，并具备演练记录。 |
| d）应定期对原有的应急预案重新评估，修订完善。 | 经访谈安全管理员，每年会对应急预案框架及重点应急事件预案进行评估及完善，经现场核查，本年度对应急保障人员名单进行更新。 |
| 外包运维管理 | a）应确保外包运维服务商的选择符合国家的有关规定； | 被测系统为自行运维管理，不涉及外包运维管理，故调整为不适用。 |
| b）应与选定的外包运维服务商签订相关的协议，明确约定外包运维的范围、工作内容； | 被测系统为自行运维管理，不涉及外包运维管理，故调整为不适用。 |
| c）应保证选择的外包运维服务商在技术和管理方面均应具有按照等级保护要求开展安全运维工作的能力，并将能力要求在签订的协议中明确； | 被测系统为自行运维管理，不涉及外包运维管理，故调整为不适用。 |
| d）应在与外包运维服务商签订的协议中明确所有相关的安全要求，如可能涉及对敏感信息的访问、处理、存储要求，对IT 基础设施中断服务的应急保障要求等。 | 被测系统为自行运维管理，不涉及外包运维管理，故调整为不适用。 |

|  |  |  |  |
| --- | --- | --- | --- |
| **测评项目** |  | **测评对象** | 安全运维管理 |
| **测评单位** |  | | |
| **测评地点** |  | | |
| **测评人员** |  | **配合人员** | 周强 |
| **测评日期** | 2023.6.19 | | |
| **测评人员签字** |  | **配合人员签字** |  |

10.2. 云计算安全扩展要求部分

10.2.1. 安全运维管理

|  |  |  |
| --- | --- | --- |
| **安全控制点** | **测评指标** | **结果记录** |
| 云计算环境管理 | a）云计算平台的运维地点应位于中国境内，境外对境内云计算平台实施运维操作应遵循国家相关规定。 | 系统部分服务器部署在阿里云华东1区（上海），云计算平台的运维地点位于中国境内。 |

|  |  |  |  |
| --- | --- | --- | --- |
| **测评项目** |  | **测评对象** | 安全运维管理 |
| **测评单位** |  | | |
| **测评地点** |  | | |
| **测评人员** |  | **配合人员** | 周强 |
| **测评日期** | 2023.6.19 | | |
| **测评人员签字** |  | **配合人员签字** |  |

10.3. 移动互联安全扩展要求部分

10.3.1. 安全运维管理

|  |  |  |
| --- | --- | --- |
| **安全控制点** | **测评指标** | **结果记录** |
| 配置管理 | a）应建立合法无线接入设备和合法移动终端配置库，用于对非法无线接入设备和非法移动终端的识别。 | 1.各分拨中心PDA设备均通过各分拨中心无线AC进行统一接入，设备接入AC通过MAC绑定的方式进行准入控制，未绑定MAC地址设备无法连接分拨中心无线网络；2.快递员使用的PDA设备通过手机卡访问互联网，在JMS综合物流平台系统中绑定了所有PDA设备的sn号，并对设备相关信息进行记录，如：所属网点、型号、sn号、imei、mac等信息。 |