ZXVMAX-S
多维价值分析系统
安全加固指导

产品版本：V6.23

中兴通讯股份有限公司
地址：深圳市科技南路55号
邮编：518057
电话：+86-755-26771900
800-830-1118
传真：+86-755-26770801
技术支持网站：http://support.zte.com.cn
电子邮件： 800@zte.com.cn

法律声明

本产品符合关于环境保护和人身安全方面的设计要求，产品的存放、使用和弃置应遵照产品手册、相关合同或相关国法律、法规的要求进行。

如果本产品进行改进或技术变更，恕不另行专门通知。

当出现产品改进或者技术变更时，您可以通过中兴通讯技术支持网站http://support.zte.com.cn查询有关信息。

发布日期： 2024-11-07

1. 适用范围

产品安全加固的目的是“通过配置、设置、协议限制来减小攻击面”（来源于《产品安全要求总则》），使得产品免于或减小所受网络安全攻击的影响。

产品安全加固对象包括产品所使用的第三方软件（如操作系统等），以及部分自研模块。

安全合加固置是通过对加固对象中安全相关的配置项进行合理的设置，减小对象的攻击面，例如关闭不必要的端口、不必要的系统服务等；安全漏洞补丁是通过对加固对象的漏洞缺陷通过补丁升级的方式，使加固对象免予或减小遭受该漏洞带来的攻击影响，例如各类CVE漏洞、CNVD漏洞的补丁升级处理等。

本文档用于规范和指导产品安全加固配置工作，包括产品所使用的第三方软件（如操作系统等），以及部分自研模块的安全加固配置。

本文档适用于VMAX产品的安全加固配置工作。 适用于该产品所有的产品软件版本。

适用于CGSLV5或V6操作系统及国产化龙晰操作系统。

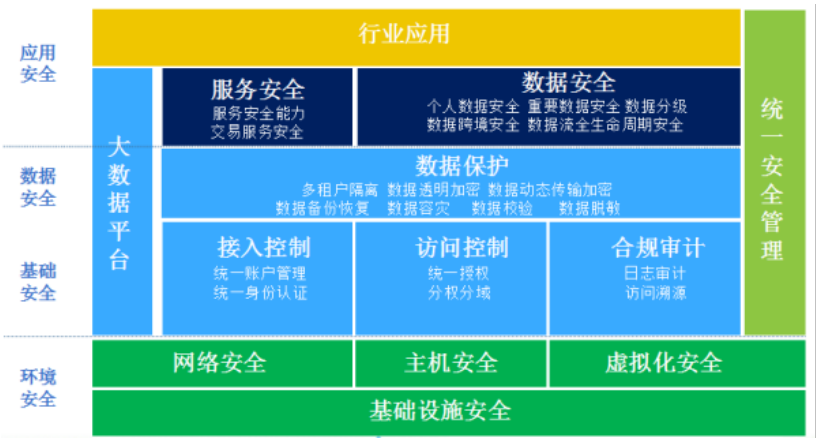
使用模板：JF-051 安全加固指南模板R1.3

2. 概述

2.1系统安全架构模型

VMAX的安全体系以数据为中心，重点考虑数据生命周期各阶段中的数据安全问题，形成了统一的安全框架，通过在数据全生命周期各环节实施安全技术和管理机制，为系统及用户数据提供安全保障。

VMAX的安全体系在VMAX自身的安全体系基础上，结合大数据平台的安全体系，形成了以数据安全机制为核心的数据安全架构，安全架构模型如下图所示：



1) 环境安全层：指VMAX系统安全运行所依赖的底层运行环境安全，包括操作系统安全、主机安全、网络安全、以及基础设施安全等。

2) 大数据平台安全层：VMAX的部分功能运行于大数据平台之上，因此大数据平台的安全性是VMAX安全性的一部分，包括：

Ø接入控制：关注于控制外部用户或者服务对集群的访问过程中的身份鉴别，包括用户账户管理模块及用户身份认证模块，这是实施大数据安全架构的基础。在访问启用群时，必须能通过服务所需要的安全认证方式；

Ø访问控制：关注于用户或者应用访问数据时，对用户的权限定义和实施过程，称为授权模块。访问控制可以限定用户是否有对某种资源的访问能力，能给不同应用提供度的访问控制能力；

Ø合规审计：审计的目的是捕获系统内的完整活动记录，且不可被更改，为用户提供安全事件的事后追溯、定位问题原因及划分事故责任的重要手段。

3) VMAX安全层：利用 数据加密、传输安全(使用标准的传输安全协议)、数据容灾、数据脱敏、存储数据安全等技术保证核心数据的安全。

4) 安全管理层:针对基础安全、数据安全、应用安全等相关功能进行统一管理，提供统一的管理界及接口，打通从用户账户、用户认证、授权、审计、数据脱敏、数据过滤等全配置及管理，并且:覆盖并打通所有主流组件，并提供监控功能。

5) 应用安全层:在保证数据安全时，应用安全是整体数据安全的一部分，但由于应用对VMAX属于第三方，因此不在VMAX安全分析中考虑

2.2 安全加固项

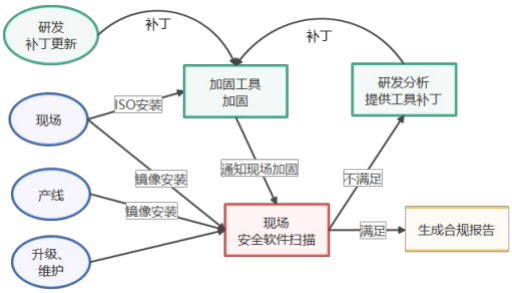
加固类型	加固项	应对风险	处理方法
账户策略	账户的安全加固体系	系统账户安全	参见第3.3章节
操作系统	操作系统安全加固	操作系统合规与漏洞	参见第3.4章节

数据库	数据安全加固体系	数据库合规与漏洞	参见第3.5章节

3. 安全加固操作

3.1 加固流程

首次开局/新建网络、升级、周期性维护等的加固流程如下图所示。



安全加固分为三个阶段：前期加固、现场加固、后期加固。

1) 前期加固：主要是出厂前的预加固，比如操作系统等，在初始版本的基础上保证将补丁安装至最新，合规配置符合基本要求等。

2) 现场加固：现场安装配置的加固，由于现场客户有自己的工具扫描，会发现一些未符合客户要求的合规项，需要在现场进行加固。

3) 后期加固：主要是后期扫描发现或者外部发现等需要处理的漏洞项。

无论是哪个阶段的安全加固，都使用相同的安全加固方案。

安全合规在如下阶段执行：

1) 早期合规：镜像文件制作时完成所有的合规工作；

2) 现场合规：由于前期未进行过合规，在现场操作；

3) 漏洞发现：由于演进发现新的漏洞或合规，需要研发提供解决方案，并由现场操作解决。

3.2 加固前的准备和检查

1、加固工具的获取：联系网服获取安全加固工具TECS-Inspector_SEC、工具使用指导书、一键安装指导书

2、通知客户以取得对应的许可或授权

3、加固前对数据进行安全备份

3.3 账户系统安全加固

在系统初始配置时，部门、操作集、角色和角色集还没有创建。应当先创建部门、操作集、角色和角色集，再进行创建用户的操作。创建用户的流程参见表2-1。

表 2-1初始配置时用户创建流程

步骤	操作	说明
1	2.1新建部门	部门是对行政部门的一个模拟，便于对用户的组织和管理。维护人员可根据需要在部门管理中创建部门，并在不同的部门中创建用户。
2	（可选）2.2新建操作集	将不同的操作权限组成一个集合，以集合的方式将操作权限分配给角色，降低权限管理的复杂性。
3	（可选）2.3新建角色	分配给该角色对网管系统中各项资源的操作权限。
4	（可选）2.4新建角色集	将不同的角色组成一个角色集，角色集所具有的权限是其下所有角色权限的集合。
5	2.5新建用户	为新用户设置用户名和密码，分配用户具有的角色或角色集，定义用户所属的部门。
6	2.6设置帐户规则	设置系统安全策略，如定制用户帐号规则、用户登录模式。

3.3.1 新建部门

摘要

部门是对行政部门的一个仿真，便于对用户的组织和管理。用户可根据需要在部门管理中创建子部门，并将创建的用户分配到各个部门下。

系统缺省情况下，系统存在一个**根部门**。该部门是最高部门，所有新建部门均是其下级子部门。

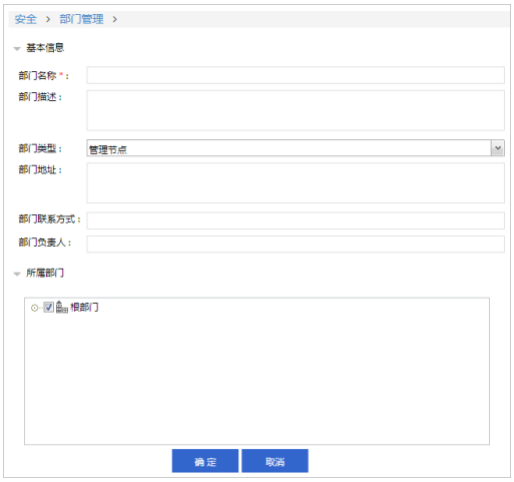
步骤

1. 在DAP系统管理窗口，选择菜单**安全→部门管理**，打开部门管理页面，如图2-1所示。

图 2-1部门管理

2. 单击**新建部门**按钮，打开部门新建页面，如图2-2所示。

图 2-2新建部门



新建部门的参数说明参见表2-2。

表 2-2新建部门的参数说明

参数名称		参数说明
基本信息	部门名称	新建部门的名称，必须输入。
	部门描述	对新建部门的详细描述信息，可选输入。
	部门类型	包括系统、部门、子部门、管理节点。
	部门地址	-
	部门联系方式	-
	部门负责人	-
所属部门		选择一个当前已存在的部门作为该新建部门的上级部门。

预定义操作集名称	操作集说明
管理员权限	管理员权限意味着对网管系统及被管网络有不受限制的完全访问权，包括对系统帐号等核心信息的修改权限，不能够对单个资源进行分配。
系统维护权限	当该权限分配给某个资源时，具备对该资源不受限制的完全访问权限，包括资源帐号等敏感信息的修改权限。
操作权限	当该权限分配给某个资源时，可对该资源进行浏览，并进行一般的配置修改，以完成开局、日常维护、故障处理等工作。但不能够修改资源的帐号等一些敏感的配置信息。
查看权限	当该权限分配给某个资源时，仅能够对该资源进行查询操作。
无权限	无权限意味着没有任何操作权限。分配了无权限的资源，用户对该资源没有任何操作权限。

3. 输入新建部门的信息以及其归属的上级部门。
4. 单击**确定**按钮，完成新部门的创建。

3.3.2 新建操作集

摘要

本节介绍如何新建一个操作集。

当系统预定义的操作集不能满足需要时，维护人员可以自定义操作集，并为该操作集选择具体可执行的操作。

相关信息

系统已经预定义了5个操作集，这些预定义的操作集无法被修改，维护人员可以直接使用，可以满足用户基本的权限分配场景。若用户还有其他的权限分配情况，可自定义操作集。

系统预定义的操作集参见表2-3。

表 2-3预定义操作集列表

预定义角色名称	角色说明
系统管理员	对网管系统及被管网络有不受限制的完全访问权，包括对系统帐号等核心信息的修改权限。
系统维护员	不具备网管安全信息维护的权限，除此之外具有对网管及被管网络的所有权限。
系统操作员	可进行一般的配置修改，不能对网管系统本身进行备份恢复等维护工作，不能修改敏感的资源配置信息。
系统监控员	可对网络信息进行浏览，如进行报表制作、数据查询等操作，但不能做配置修改操作。

参数名称	参数说明
角色名	角色的名称，必须输入。
角色描述信息	对角色的详细描述信息，可选输入。
资源树	定义该角色可管理的资源。
操作集信息	定义该角色对某个特定资源所拥有的操作权限。 当系统默认的操作集不能满足需求时，维护人员可以自定义操作集，具体参见“2.2新建操作集” 。

步骤

1. 在DAP系统管理窗口，选择菜单**安全→操作集**，默认显示操作集页面，如图2-3所示。

图 2-3操作集管理

2. 单击新建操作集按钮，打开操作集详情页面，如图2-4所示。

图 2-4新建操作集

3. 输入新建的**操作集名**和**操作集描述**信息。

4. 在**操作集分配情况**的操作树中，选择该操作集包含的操作内容。

5. 单击**确定**按钮，新建的操作集显示在操作集列表中。

3.3.3 新建角色

摘要

本节介绍如何创建一个新的角色，并分配给这个角色一定的资源和操作权限。

当系统预定义的角色不能满足需要时，维护人员可以自定义角色，并为该角色分配资源和操作集。

相关信息

系统预定义的角色参见表2-4，这些预定义的角色无法被修改。

表 2-4预定义角色列表

参数名称	参数说明
角色集名	角色集的名称，必须输入。
角色集描述信息	对角色集的详细描述信息，可选输入。
可供分配角色	系统中已存在的可供分配的角色。
已分配角色	已经被分配到该角色集的角色名。

步骤

1. 在DAP系统管理窗口，选择菜单**安全→角色管理**，默认显示角色管理页面，如图2-5所示。

图 2-5角色管理

2. 单击**新建角色**按钮，打开新建角色页面，如图2-6所示。

图 2-6新建角色

新建角色的参数说明参见表2-5。

表 2-5新建角色的参数说明

参数名称	参数说明
用户名	（必选）新建用户的用户名，即该用户的登录名称。用户名区分大小写，最长30个字符。
用户全名	用户的全称。
密码	用户登录时输入的口令，可以设置为空。 在用户账户规则中，可以定制密码的长度范围，具体操作参见“2.6设置帐户规则”。
确认密码	再次输入密码，必须和用户密码一致。

3. 输入角色名称和对角色的描述信息。
4. 执行如下操作，为该角色指定操作资源，并分配该资源下的操作权限。
   a. 在左侧**资源树**中选择一个资源。
   b. 在右侧**操作集信息**列表中，为该资源分配一个操作集。
   c. 重复步骤4.a~4.b，直至全部的资源节点均已分配操作集。
5. 单击**确定**按钮，完成新角色的创建。

3.3.4 新建角色集

摘要

本节介绍如何创建一个新的角色集，并为该角色集分配一定的角色。

角色集是多个角色的集合。将角色集分配给某个用户后，该用户将被赋予该角色集中所有角色的操作权限。

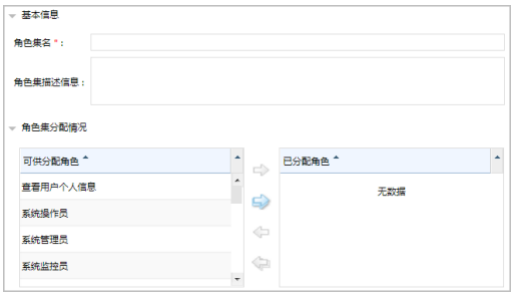
步骤

1. 在DAP系统管理窗口，选择菜单**安全→角色集管理**，默认显示角色集管理页面，如图2-7所示。

图 2-7角色集管理

2. 单击**新建角色集**按钮，打开新建角色集页面，如图2-8所示。

图 2-8新建角色集页面



新建角色集的参数说明参见表2-6。

表 2-6新建角色集的参数说明

参数名称	参数说明
用户下次登录前必须修改密码	设置用户下次登录前是否必须修改密码。 说明：如果选中该参数，则**用户不能修改密码**参数不可设置。
用户不能修改密码	设置用户能否修改密码。 说明：如果选中该参数，则**用户下次登录前必须修改密码**参数不可设置。
设置用户密码最长存留期（天）	设置用户密码最长的有效时间。以密码启用时间开始计算，如果密码启用后超过密码最长存留期，则用户需要更新密码。
设置用户密码最短存留期（天）	设置用户密码最短的有效时间。以密码启用时间开始计算，如果密码启用后未超过密码最短存留期，则用户不得更新密码。

3. 输入角色集名称、角色集的描述信息。
4. 在**可供分配角色**列表中，选择一个角色，单击按钮，将其添加到**已分配角色**。
5. 重复步骤4，直至该角色集所需包含的角色均已被添加。
6. 单击**确定**按钮，完成新角色集的创建。

3.3.5 新建用户

摘要

本节介绍如何创建一个新的用户，并为该用户分配角色集或角色。

在为新用户设置用户名和密码的同时，系统管理员还可以设置帐号、密码的有效天数，定义用户所属的部门和同一用户最多的登录数等。

说明:

如果不给用户分配角色或角色集，该用户登录后将无任何操作权限。

前提

已具有用户管理权限的用户登录ZXVMAX服务器。

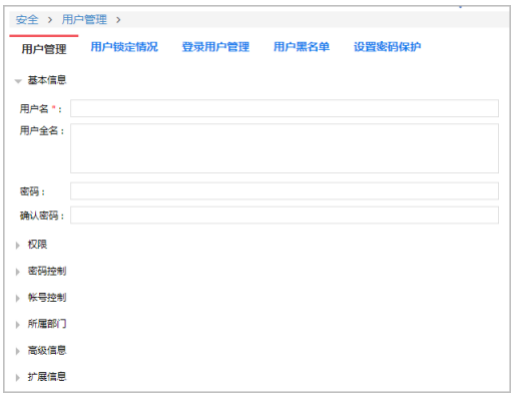
步骤

1. 在DAP系统管理窗口，选择菜单**安全→用户管理**，默认显示用户管理页面，如图2-9所示。

图 2-9用户管理

2. 单击**新建用户**按钮。在**基本信息**区域中输入新用户的**用户名**、**用户全名**、**密码**及**确认密码**，如图2-10所示。

图 2-10新建用户-基本信息



基本信息的参数说明参见表2-7。

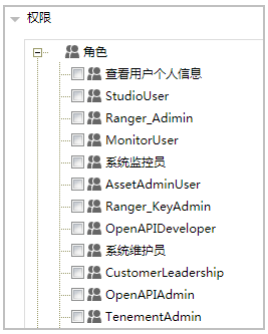
表 2-7基本信息的参数说明

参数名称	参数说明
禁用	是否禁用此帐号。 说明：如果选中此参数，则该用户无法登录系统，且**设置帐号自动禁用前最大未登录天数**参数不可设置。
设置帐号自动禁用前最大未登录天数	用户未登录天数超过此天数，则该用户会被系统自动禁用。 说明：如果选中此参数，则**禁用**参数不可设置。
设置帐号有效时间（天）	以帐号创建时间开始计算，如果用户帐号超过帐号有效时间，则该帐号失效，不能登录系统。
设置帐号暂停时间（天）	从设置帐号暂停当天开始暂停帐号的使用，超过帐号暂停时间后该帐号恢复正常使用。

3. 展开**权限**区域，为用户分配角色和角色集（可以多选），如图2-11所示。

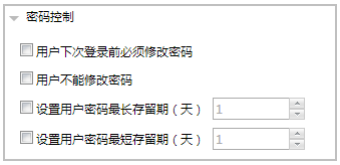
一个角色或角色集能被多个用户共享。如果当前系统中的角色或角色集不能满足需求，维护人员可以创建新的角色或角色集。具体操作可参见“2.3新建角色”和“2.4新建角色集”。

图 2-11新建用户-权限信息



4. 展开**密码控制**区域，设置该用户的密码控制策略，如图2-12所示。

图 2-12新建用户-密码控制



密码控制的参数说明参见表2-8。

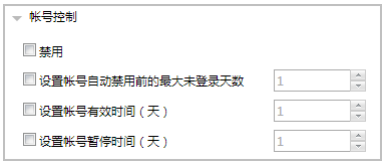
表 2-8密码控制的参数说明

参数名称	参数说明
用户描述信息	对此用户信息的描述。
电话	该用户的联系电话。

电子邮件	新建用户的电子邮件地址，必需有“@”字符，否则会提示邮件地址不合法。
同时登录数限制	设置同一用户名最多可以同时登录客户端的数目。
设置或查看工作时间	默认状态下，该用户可以在任意时段登录ZXVMAX系统。如果需要指定允许登录的时间段，可单击此按钮进行设置。
登录IP范围	默认状态下，该用户可以从任意IP地址登录ZXVMAX系统。如果需要指定允许登录的IP地址范围，可单击手工添加按钮，并设置允许该用户登录的IP地址段。

5. 展开**帐号控制**区域，设置该用户的帐号控制策略，如图2-13所示。

图 2-13新建用户-帐号控制



账号控制的参数说明参见表2-9。

表 2-9帐号控制的参数说明

参数名称	**参数说明**
最小字符长度	密码最小长度限制。
最大字符长度	密码最大长度限制。
不能与最近旧密码重复天数	新密码不能与最近几天的旧密码重复。
不能与最近旧密码重复次数	新密码不能与最近几次的旧密码重复。
密码过期前提示天数	在用户登录时，系统检查用户的密码，如果在设定的天数内即将过期，则会提示用户。
用户登录前修改过期密码	用户登录时，系统检查用户的密码，如果过期需要用户修改密码才能登录。
相同用户全名的帐号密码不同	用户全名相同的帐号的密码不能相同。
启用弱口令检测规则	是否启用弱口令检测规则。启用后，新修改的密码不能为弱口令。 弱口令的检查规则为： l密码必须包含来自以下四个类别中的三种字符：数字、小写字母、大写字母、其它字符。 l密码不能与用户名相同。 l密码不能是与用户电话号码相同。 l密码不能是用户电话号码的逆序。 l密码不能是常用词。
登录前必须修改不符合规则的密码	当启用**启用弱口令检测规则**后，用户登录时，系统检查用户的密码，如果不符合规则需要用户修改密码才能登录。

6. 展开**所属部门**区域，为用户选择所属的部门，如图2-14所示。

图 2-14新建用户-所属部门

7. 展开**高级信息**区域，设置用户的附加信息、允许登录的时间段以及IP地址段等信息，如图2-15所示。

图 2-15新建用户-高级信息

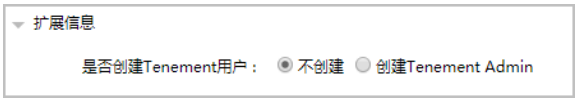
高级信息的参数说明参见表2-10。

表 2-10高级信息的参数说明

参数名称	参数说明
永不锁定	用户登录失败不受次数限制，系统不会因登录失败次数过多而锁定该用户。
永久锁定	用户连续输错次数达到**密码错误多少次锁定**设定的值后锁定用户，且不再允许该用户登录。 对于被锁定的用户，系统管理员进行手工解锁，具体操作参见“3.2查看用户锁定情况”。
暂时锁定	用户连续输错次数达到**密码错误多少次锁定**的值后锁定用户，超过**锁定后解锁时间（小时）**设定的时长后自动解锁。 对于被锁定的用户，系统管理员进行手工解锁，具体操作参见“3.2查看用户锁定情况”。
密码错误多少次锁定	用来设定系统允许的用户密码连续输错次数，到达该设定值后，系统自动锁定帐号。处于锁定状态的帐号，将不能使用。
锁定后解锁时间（小时）	如果帐号不是永久锁定类型，则锁定N小时后，帐号自动解锁。解锁后的帐号，用户可以再次使用。
帐号按IP进行锁定	用户连续输错密码，如果达到最大次数，是否只按本登录IP来锁定帐号。
admin用户不锁定	如果选中该选项，则admin用户永远不会被锁定。
不能与最近被删除帐号重名（天）	不能与最近几天被删除的帐号重复。
帐号过期前提示（天）	在用户登录时，系统检查用户的帐号，如果在设定的天数内即将过期，则会提示用户。

8. 展开**扩展信息**页面，采用默认设置，如图2-16所示。

图 2-16新建用户-扩展信息



9. 单击**确定**按钮，完成新用户的创建。

3.3.6 设置帐户规则

摘要

本节介绍如何查看或设置密码策略、帐号策略和帐号锁定规则。

步骤

1. 在DAP系统管理窗口，选择菜单**安全→帐户规则**，打开帐户规则页面，如图2-17所示。

图 2-17帐户策略-密码策略

表 2-11密码策略的参数说明

参数名称	参数说明
永不锁定	用户登录失败不受次数限制，系统不会因登录失败次数过多而锁定该用户。
永久锁定	用户连续输错次数达到**密码错误多少次锁定**设定的值后锁定用户，且不再允许该用户登录。 对于被锁定的用户，系统管理员进行手工解锁，具体操作参见“3.2查看用户锁定情况”。
暂时锁定	用户连续输错次数达到**密码错误多少次锁定**的值后锁定用户，超过**锁定后解锁时间（小时）**设定的时长后自动解锁。 对于被锁定的用户，系统管理员进行手工解锁，具体操作参见“3.2查看用户锁定情况”。
密码错误多少次锁定	用来设定系统允许的用户密码连续输错次数，到达该设定值后，系统自动锁定帐号。处于锁定状态的帐号，将不能使用。
锁定后解锁时间（小时）	如果帐号不是永久锁定类型，则锁定N小时后，帐号自动解锁。解锁后的帐号，用户可以再次使用。
帐号按IP进行锁定	用户连续输错密码，如果达到最大次数，是否只按本登录IP来锁定帐号。

admin用户不锁定	如果选中该选项，则admin用户永远不会被锁定。
不能与最近被删除帐号重名（天）	不能与最近几天被删除的帐号重复。
帐号过期前提示（天）	在用户登录时，系统检查用户的帐号，如果在设定的天数内即将过期，则会提示用户。

2. 设置用户帐号的密码策略。

3. 展开**帐号锁定规则**和**帐号策略**区域，设置用户帐号的锁定规则和策略，如图2-18所示。

图 2-18帐户策略-锁定规则

表 2-12帐号锁定和帐号策略的参数说明

参数名称	**参数说明**
永不锁定	用户登录失败不受次数限制，系统不会因登录失败次数过多而锁定该用户。
永久锁定	用户连续输错次数达到**密码错误多少次锁定**设定的值后锁定用户，且不再允许该用户登录。 对于被锁定的用户，系统管理员进行手工解锁，具体操作参见“3.2查看用户锁定情况”。
暂时锁定	用户连续输错次数达到**密码错误多少次锁定**的值后锁定用户，超过**锁定后解锁时间（小时）**设定的时长后自动解锁。 对于被锁定的用户，系统管理员进行手工解锁，具体操作参见“3.2查看用户锁定情况”。
密码错误多少次锁定	用来设定系统允许的用户密码连续输错次数，到达该设定值后，系统自动锁定帐号。处于锁定状态的帐号，将不能使用。
锁定后解锁时间（小时）	如果帐号不是永久锁定类型，则锁定N小时后，帐号自动解锁。解锁后的帐号，用户可以再次使用。
帐号按IP进行锁定	用户连续输错密码，如果达到最大次数，是否只按本登录IP来锁定帐号。
admin用户不锁定	如果选中该选项，则admin用户永远不会被锁定。
不能与最近被删除帐号重名（天）	不能与最近几天被删除的帐号重复。
帐号过期前提示（天）	在用户登录时，系统检查用户的帐号，如果在设定的天数内即将过期，则会提示用户。

4. 单击**确定**按钮，完成账户规则的设置。

3.4 操作系统安全加固

3.4.1 操作系统安全加固条目

执行的加固项	检查说明	配置确认	处理建议
OS-Linux-口令-02-【工信部/集团】检查口令生存周期要求（shadow文件）	1.检查配置文件/etc/shadow下不能存在密码过期时间小于0或者大于90天的非系统内置用户。	1、检查shadow文件： #cat /etc/shadow 2、修改账号口令生存周期： #chage -M 90 username 1）检查配置文件/etc/shadow下不能存在密码过期时间小于0或者大于90天的非系统内置用户	
OS-Linux-账号-02-【工信部/集团】检查是否删除或锁定无关账号（自动化）	删除过期账号（比如离职/转岗人员） 锁定指定用户: listen,gdm, webservd nobody nobody4 noaccess 测试账户（半自动） 共享账号（半自动） 长期不用账号(半年以上未使用，人工检查) 1、系统内置用户全部锁定 2、其它用户设置成/bin/false或/sbin/nologin 3、其它用户uuid需要大于系统内置用户的uuid	1、执行备份： #cp -p /etc/passwd /etc/passwd_bak #cp -p /etc/shadow /etc/shadow_bak 2、锁定无用帐户： 方法一： #vi /etc/shadow 在需要锁定的用户名的密码字段前面加!!，如 test:!!1QD1ju03H$LbV4vdBbpw.MY0hZ2D/Im1:14805:0:99999:7::: 方法二： #passwd -l test 3、将/etc/passwd文件中的shell域设置成/bin/false。 4、不能存在相关的测试账号，如test|ceshi|admin等。	

OS-Linux-日志-04-【工信部/集团】检查是否配置远程日志保存（自动化）	1.检查远程日志功能是否启用； 2.检查配置文件syslog.conf、rsyslog.conf、syslog-ng.conf（syslog-ng.conf文件配置存在差异需注意）的相关参数行 3.敏感审计日志确认接收到日志	/etc/syslog-ng/syslog-ng.conf、/etc/rsyslog.conf、/etc/rsyslog.conf存在配置全量日志即*.* @IP，且在敏感平台能查到资产的日志信息，则符合要求。 配置要求为*.* @IP	
OS-Linux-账号-01-【工信部/集团】检查是否按用户分配账号责任到人（自动化）	不能存在共享账号，（如厂商、test、admin、ceshi等命名账号） 从账号主目录权限限制750 1.检查设备存在非系统内置可登录账号，可登录账号数需大于等于3； 2.检查设备不存在常见的test、admin、ceshi等账号； 3.检查设备不存在常见的厂商命名账号，如xjwh、tywh等； 4.账号主目录权限限制不高于750，检查家目录（/home）；	为用户创建账号： #useradd username #创建账号 #passwd username #设置密码 修改权限： #chmod 750 directory #其中755为设置的权限，可根据实际情况设置相应的权限，directory是要更改权限的目录），/home目录下的各权限需要配置为740或者750。使用该命令为不同的用户分配不同的账号，设置不同的口令及权限信息等。	
OS-Linux-日志-02-【工信部/集团】检查日志文件权限设置（自动化）	1.检查/var/log/messages日志文件权限 2.检查/var/log/secure日志文件权限 3.检查/var/log/maillog日志文件权限 4.检查/var/log/cron日志文件权限 5.检查/var/1og/spoo1er日志文件权限 6.检查/var/1og/boot.log日志文件权限 以上文件系统默认权限为600； 7.遍历syslog.conf、rsyslog.conf、syslog-ng.conf（syslog-ng.conf文件配置存在差异需注意）日志文件存储路径下的文件权限一般为600（注意非3个文件本身权限，syslog.conf、rsyslog.conf、syslog-ng.conf3个文件是配置日志存储路径的配置参数控制文件。） 以上全部文件权限必须符合600则合规，否则不合规	1、备份需要修改的文件 2、执行下列命令，修改日志文件权限为合理值 如设置文件权限为640 #chmod 640 或者修改为600 #chmod 600 1.检查/var/log/messages日志文件权限 2.检查/var/log/secure日志文件权限 3.检查/var/log/maillog日志文件权限 4.检查/var/log/cron日志文件权限 5.检查/var/1og/spoo1er日志文件权限 6.检查/var/1og/boot.log日志文件权限 以上文件系统默认权限为600； 7.遍历syslog.conf、rsyslog.conf、syslog-ng.conf（syslog-ng.conf文件配置存在差异需注意）日志文件存储路径下的文件权限一般为600（注意非3个文件本身权限，syslog.conf、rsyslog.conf、syslog-ng.conf3个文件是配置日志存储路径的配置参数控制文件。） 以上全部文件权限必须符合600则合规，否则不合规。	
OS-Linux-日志-04-【工信部/集团】检查是否配置远程日志保存（强化）	1.检查远程日志功能是否启用； 2.检查配置文件syslog.conf、rsyslog.conf、syslog-ng.conf（syslog-ng.conf文件配置存在差异需注意）的相关参数行 3.敏感审计日志是否接收成功待确认（强化项）		
OS-Linux-口令-01-【工信部/集团】检查口令策略设置是否符合复杂度要求（自动化）	1.检查配置文件etc/login.defs的口令强度配置选项是否设置相应参数； 2.检查配置文件/etc/pam.d/system-auth的相关参数是否设置； 3.检查密码复杂度设置后是否成功设置提示（不满足密码复杂度时强制用户重新修改密码，root可强制修改密码未受参数限制）	1、执行备份： #cp -p /etc/pam.d/system-auth /etc/pam.d/system-auth_bak 或者cp -p /etc/pam.d/passwd /etc/pam.d/passwd_bak 2、配置文件/etc/login.defs，增加行PASS_MIN_LEN 8。 3、在文件/etc/pam.d/system-auth（/etc/pam.d/common-password）配置以下参数： password requisite pam_cracklib.so dcredit=-1 ucredit=-1 lcredit=-1 ocredit=- 1 minclass=3 minlen=8 enforce_for_root password sufficient pam_unix.so md5 shadow nullok try_first_pass use_authtok 是否配置了minlen=8，minclass=3。	
OS-Linux-授权-01-【工信部/集团】检查帐号文件权限设置（自动化）	1.检查/etc/passwd 、/etc/shadow 、/etc/group 三个文件的权限（自动化） 2.遍历查询/etc、安装系统后默认系统目录下所有子目录及文件写权限（自动化）	1、执行备份： #cp -p /etc/passwd /etc/passwd_bak #cp -p /etc/shadow /etc/shadow_bak #cp -p /etc/group /etc/group_bak 2、修改文件权限： #chmod 0644 /etc/passwd #chmod 0400 /etc/shadow #chmod 0644 /etc/group 3、遍历查询/etc、安装系统后默认系统目录下所有子目录及文件写权限（自动化），用户组和其他用户不存在写权限。	
OS-Linux-口令-02-【工信部/集团】检查口令生存周期要求（自动化）	1.检查配置文件/etc/login.defs的相关参数，口令生存周期大于等于1且小于等于90天 2.检查配置文件/etc/shadow下非系统内置用户的密码过期时间小于等于90天	1、执行备份： #cp -p /etc/login.defs /etc/login.defs_bak 2、修改策略设置： #vi /etc/login.defs 修改PASS_MIN_LEN的值为8，修改PASS_MAX_DAYS的值为90，按要求修改 PASS_MIN_DAYS/PASS_WARN_AGE的值，保存退出 PASS_MAX_DAYS小于等于90并且未被注释; PASS_WARN_AGE小于等于7并且未被注释; PASS_MIN_DAYS小于等于7并且未被注释;	
OS-Linux-安全补丁-01-【工信部/集团】检查是否安装OS补丁（自动化）	1.检查版本编号，确定是否为最新版本； 2.检查大补丁号，确定是否为最新版本； 3.检查不存在非必要的包 4.检查系统内核版本号，确定是否为最新版本	可以使用Online Update或Patch CD Update等方式升级系统补丁。	
OS-Linux-账号-04-【工信部/集团】检查是否设置限制su命令用户组（自动化）	设置限制使用su命令的用户组	使用命令 sudo visudo 打开sudoers文件 %admin ALL=(ALL) ALL 表示admin组的所有成员可以以任何用户的身份执行任何命令。 完全禁止某个组使用su命令，可以在文件中添加以下行： %somegroup ALL=(ALL) !/bin/su	
OS-Linux-账号-03-【工信部/集团】检查是否按角色进行帐号管理（自动化）	判断是否存在多账户组，不存在，默认合规；存在多个用户的账户组，默认判断不合规，人工问询确认多账户组是否为业务需求。 判断是否存在自己创建的用户组。	判断是否存在多个用户的账户组，不存在（即一个账户中只存在一个用户账号为合规），默认合规；存在多个用户的账户组，默认判断不合规，需人工问询确认多账户组是否为业务需求。然后由厂家人工确认是否合规。	
OS-Linux-不必要的服务-01-【工信部/集团】检查是否关闭不必要服务（自动化）	1.检查是否存在不必要的服务； 2.附表2中的“根据情况选择开放”的服务是否需要判断开启（待确认）	1、#chkconfig --list 2、禁止非必要服务：#chkconfig [service] off 开启服务为：#chkconfig [service] on 以下服务都需要关闭： amanda chargen chargen-udp cups cups-lpd daytime daytime-udp echo echo- udp eklogin ekrb5-telnet finger gssftp imap imaps ipop2 ipop3 klogin krb5- telnet kshell ktalk ntalk rexec rlogin rsh rsync talk tcpmux-server telnet tftp time-dgram time- stream uucp; 不能存在以下端口：13 37 7 9 19 25 518 113 515 67 68 69 544 543 515 2049 1270 5989 139 445。	
OS-Linux-FTP设置-01-【工信部/集团】检查FTP配置-限制用户FTP登录（自动化）	1.检查是否安装FTP服务 2.若安装FTP服务，检查是否禁止root登录FTP	1、配置文件/etc/vsftpd/vsftpd.conf或者/etc/vsftpd.conf 修改其中内容： userlist_enable=YES userlist_deny=NO 2、文件/etc/vsftpd/user_list内不能存在以下账号： root、bin、sy、listen、nuucp、sync、shutdown、lp、naoccess、adm、nobody、uucp。 （/etc/vsftpd/user_list为白名单设置，在此文件内的账户可ftp登录）	

OS-Linux-FTP设置-03-【工信部/集团】检查登录提示-更改ftp警告Banner（自动化）	1.检查是否安装FTP服务
	2.检查FTP服务类型
	3.检查配置文件是否设置相关参数
		1. 修改Pure-FTP回显信息
		Pure-ftp回显信息分为两种：
		自带回显信息：
		Pure-ftp自带回显信息没法通过更改配置来更改，只能在安装的时候选择without banner选项去掉自带BANNER信息。
		自定义回显信息：
		Pure-ftp还有自定义回显信息，配置方法如下：
		步骤1 修改pure-ftp配置文件：
		#vi /etc/pure-ftpd/pure-ftpd.conf
		找到以下行，确保该行未被注释。
		FortunesFile /usr/share/fortune/zippy
		步骤2 编辑/usr/share/fortune/zippy文件（如没有fortune文件夹或者zippy文件，则新建该文件夹或该文件）：
		#vi /usr/share/fortune/zippy
		将自定义BANNER写入其中。
		步骤3 重启服务：
		# /etc/init.d/xinetd restart
		
		2. 修改vsftp回显信息
		# vi /etc/vsftpd.conf
		ftpd_banner=” Authorized users only. All activity may be monitored and reported.”
		可根据实际需要修改该文件内容。
		重启服务：
		# /etc/init.d/xinetd restart	

OS-Linux-登录超时时间设置-01-【工信部/集团】检查是否设置登录超时（自动化）	1.检查是否设置账户登录超时登出/etc/profile 文件中TMOUT值大于0并且小于等于180或300（newstart\suse\ubuntu）	1、执行备份：
		#cp -p /etc/profile /etc/profile_bak
		#cp -p /etc/csh.cshrc /etc/csh.cshrc_bak
		2、在/etc/profile文件增加以下两行：
		#vi /etc/profile
		TMOUT=180
		export TMOUT
		改变这项设置后，重新登录才能有效	

OS-Linux-系统Banner设置-01-【工信部/集团】检查登录提示-是否设置登录成功后警告Banner（自动化）	1.检查是否更改配置文件/etc/rc.d/rc.loca1、/etc/motd、sshd_config，隐藏操作系统名称，版本号，主机名称等信息； 2.检查是否删除"/etc" 目录下的issue.net和isssue文件；	1、修改文件/etc/motd的内容，如没有该文件，则创建它。 #echo " Authorized users only. All activity may be monitored and reported " > /etc/motd 可根据实际需要修改该文件的内容。若/etc/ssh/sshd_config需要引用banner，只能配置banner /etc/motd。 2、检查已删除"/etc" 目录下的issue.net和isssue文件 同时符合以上要求则合规，否则不合规	
OS-Linux-删除潜在危险文件-01-【工信部/集团】检查帐户目录是否存在.netrc文件（自动化）	检查帐户目录是否存在.netrc文件	检查当前帐户是否存在相关文件：ls -a ~/.netrc	
OS-Linux-日志-01-【工信部/集团】检查是否记录安全事件日志（自动化）	检查是否记录安全事件日志		
OS-Linux-授权-02-【工信部/集团】检查用户缺省UMASK（自动化）	需顶格（umask前不存在空格）新增umask配置： 1.检查配置文件/etc/login.def缺省访问权限设置为750（umask为027） 2.检查全局配置文件/etc/profile缺省访问权限设置为750（umask为027）	1、执行备份： #cp -p /etc/profile /etc/profile_bak #cp -p /etc/csh.login /etc/csh.login_bak #cp -p /etc/csh.cshrc /etc/csh.cshrc_bak #cp -p /etc/bashrc /etc/bashrc_bak #cp -p /root/.bashrc /root/.bashrc_bak #cp -p /root/.cshrc /root/.cshrc_bak 2、需顶格（umask前不存在空格）新增umask配置： #vi /etc/profile #vi /etc/csh.login #vi /etc/csh.cshrc #vi /etc/bashrc #vi /root/.bashrc #vi /root/.cshrc 重新新增配置umask值为027，保存退出。	
OS-Linux-授权-03-【工信部/集团】检查FTP配置-限制FTP用户登录后能访问的目录（自动化）	1.判断是否安装FTP服务（无论FTP服务是否启动都要检查相关配置）； 2.检查具体启用的FTP服务名称; 3.在安装前提下：根据对应服务名称检查FTP对应路径配置文件，要求所有用户只在对应自身主目录下访问）	/etc/vsftpd.conf文件中存在chroot_local_user=YES和chroot_list_enable=NO或者/etc/pure-ftpd/pure-ftpd.conf中存在ChrootEveryone yes、AllowUserFXP no、AllowAnonymousFXP no；或者FTP服务未开启，以上任一条件满足即可； 参考解析：/etc/vsftpd.conf配置chroot_local_user=YES和chroot_list_enable=NO （该两个参数共同控制下配置：1.所有用户都被限制在其主目录下 2.不使用chroot_list_file指定的用户列表，没有任何“例外”用户）	
OS-Linux-远程登录-02-【工信部/集团】检查是否使用ssh替代telnet服务（自动化）	检查是否使用ssh替代telnet服务 1、打开终端,输入以下命令以检查SSH服务是否正在运行： sudo systemctl status ssh 如果看到类似“active (running)”的消息，则表示SSH服务正在运行。 2、检查Telnet服务是否已禁用。输入以下命令： sudo systemctl status telnet 如果Telnet服务未运行或已禁用，则会看到类似“inactive (dead)”的消息		
OS-Linux-日志-03-【工信部/集团】检查是否记录cron命令使用情况（自动化）	检查是否记录cron命令使用情况		
OS-Linux-远程登录-01-【工信部/集团】检查是否限制root远程登录（自动化）	1.检查是否禁止root直接远程登录； 2.检查是否开启SSH服务； 3.检查是否禁用Telnet服务； 4.检查是否存在远程登录web插件安装信息；	1、执行备份： #cp -p /etc/securetty /etc/securetty_bak #cp -p /etc/ssh/sshd_config /etc/ssh/sshd_config_bak 2、新建一个普通用户并设置高强度密码： #useradd username #passwd username 3、禁止root用户远程登录系统： #vi /etc/securetty 注释形如pts/x的行，保存退出，则禁止了root从telnet登录。 #vi /etc/ssh/sshd_config 修改PermitRootLogin设置为no并不被注释，保存退出，则禁止了root从ssh登录。 #service sshd restart	
OS-Linux-FTP设置-02-【工信部/集团】检查是否禁止匿名ftp（自动化）	1.检查是否安装FTP服务 2.检查是否禁止匿名账户FTP登录	编辑FTP配置文件/etc/vsftpd/vsftpd.conf 在配置文件中添加行： anonymous_enable=NO	

检查是否设置口令生存周期	1.检查配置文件/etc/shadow下不能存在密码过期时间小于0或者大于90天的非系统内置用户。	1、检查shadow文件： #cat /etc/shadow 2、修改账号口令生存周期： #chage -M 90 username 1）检查配置文件/etc/shadow下不能存在密码过期时间小于0或者大于90天的非系统内置用户	
关闭telnet服务	检查是否使用ssh替代telnet服务 1、打开终端,输入以下命令以检查SSH服务是否正在运行： sudo systemctl status ssh 如果看到类似“active (running)”的消息，则表示SSH服务正在运行。 2、检查Telnet服务是否已禁用。输入以下命令： sudo systemctl status telnet 如果Telnet服务未运行或已禁用，则会看到类似“inactive (dead)”的消息	sed -i "s/^.*disable.*$/disable = yes/" /etc/xinetd.d/telnet systemctl restart xinetd >> "$logPath"/compliance.log systemctl disable xinetd systemctl stop xinetd rpm -e telnet-server--nodeps	
禁止icmp重定向	临时禁用ICMP重定向： sudo sysctl -w net.ipv4.conf.all.send_redirects=0 只针对某个网络接口禁用ICMP重定向，例如eth0： sudo sysctl -w net.ipv4.conf.eth0.send_redirects=0 使更改永久生效，编辑/etc/sysctl.conf文件并添加以下行： net.ipv4.conf.all.send_redirects = 0 或者针对某个网络接口： net.ipv4.conf.eth0.send_redirects = 0 保存并关闭文件。 应用更改，运行以下命令： sudo sysctl -p 这样就成功地在Linux操作系统中禁止了ICMP重定向	sed -i "/net.ipv4.conf.all.accept_redirects/d" /etc/sysctl.conf echo "net.ipv4.conf.all.accept_redirects=0" >> /etc/sysctl.conf	
检查是否配置远程日志保存	1.检查远程日志功能是否启用； 2.检查配置文件syslog.conf、rsyslog.conf、syslog-ng.conf（syslog-ng.conf文件配置存在差异需注意）的相关参数行 3.敏感审计日志确认接收到日志	/etc/syslog-ng/syslog-ng.conf、/etc/rsyslog.conf、/etc/rsyslog.conf存在配置全量日志即 *.* @IP，且在敏感平台能查到资产的日志信息，则符合要求。 配置要求为*.* @IP	

检查登录提示-更改ftp警告Banner	1.检查是否安装FTP服务
	2.检查FTP服务类型
	3.检查配置文件是否设置相关参数
		1. 修改Pure-FTP回显信息
		Pure-ftp回显信息分为两种：
		自带回显信息：
		Pure-ftp自带回显信息没法通过更改配置来更改，只能在安装的时候选择without banner选项去掉自带BANNER信息。
		自定义回显信息：
		Pure-ftp还有自定义回显信息，配置方法如下：
		步骤1 修改pure-ftp配置文件：
		#vi /etc/pure-ftpd/pure-ftpd.conf
		找到以下行，确保该行未被注释。
		FortunesFile /usr/share/fortune/zippy
		步骤2 编辑/usr/share/fortune/zippy文件（如没有fortune文件夹或者zippy文件，则新建该文件夹或该文件）：
		#vi /usr/share/fortune/zippy
		将自定义BANNER写入其中。
		步骤3 重启服务：
		# /etc/init.d/xinetd restart
		
		2. 修改vsftp回显信息
		# vi /etc/vsftpd.conf
		ftpd_banner=” Authorized users only. All activity may be monitored and reported.”
		可根据实际需要修改该文件内容。
		重启服务：
		# /etc/init.d/xinetd restart	

检查口令策略设置是否符合复杂度要求、检查口令锁定策略、检查口令重复次数限制	1.检查配置文件etc/login.defs的口令强度配置选项是否设置相应参数； 2.检查配置文件/etc/pam.d/system-auth的相关参数是否设置； 3.检查密码复杂度设置后是否成功设置提示（不满足密码复杂度时强制用户重新修改密码，root可强制修改密码未受参数限制）	1、执行备份： #cp -p /etc/pam.d/system-auth /etc/pam.d/system-auth_bak 或者cp -p /etc/pam.d/passwd /etc/pam.d/passwd_bak 2、配置文件/etc/login.defs，增加行PASS_MIN_LEN 8。 3、在文件/etc/pam.d/system-auth（/etc/pam.d/common-password）配置以下参数： password requisite pam_cracklib.so dcredit=-1 ucredit=-1 lcredit=-1 ocredit=- 1 minclass=3 minlen=8 enforce_for_root password sufficient pam_unix.so md5 shadow nullok try_first_pass use_authtok 是否配置了minlen=8，minclass=3。	
检查登录提示-是否设置ssh警告Banner	编辑/etc/ssh/sshd_config文件，将参数设置为如下值： /etc/issue.net	运行以下命令并验证输出匹配结果： #grep “^Banner “/etc/ssh/sshd_config /etc/issue.net	
检查登录提示-是否设置登录成功后警告Banner	1.检查是否更改配置文件/etc/rc.d/rc.loca1、/etc/motd、sshd_config，隐藏操作系统名称，版本号，主机名称等信息； 2.检查是否删除"/etc" 目录下的issue.net和isssue文件；	1、修改文件/etc/motd的内容，如没有该文件，则创建它。 #echo " Authorized users only. All activity may be monitored and reported " > /etc/motd 可根据实际需要修改该文件的内容。若/etc/ssh/sshd_config需要引用banner，只能配置banner /etc/motd。 2、检查已删除"/etc" 目录下的issue.net和isssue文件 同时符合以上要求则合规，否则不合规	
检查登录提示-是否更改telnet警告Banner	1.检查是否存在不必要的服务； 2.附表2中的“根据情况选择开放”的服务是否需要判断开启（待确认）	1、#chkconfig --list 2、禁止非必要服务：#chkconfig [service] off 开启服务为：#chkconfig [service] on 以下服务都需要关闭： amanda chargen chargen-udp cups cups-lpd daytime daytime-udp echo echo- udp eklogin ekrb5-telnet finger gssftp imap imaps ipop2 ipop3 klogin krb5- telnet kshell ktalk ntalk rexec rlogin rsh rsync talk tcpmux-server telnet tftp time-dgram time- stream uucp; 不能存在以下端口：13 37 7 9 19 25 518 113 515 67 68 69 544 543 515 2049 1270 5989 139 445。	
检查是否设置登录超时	1、检查/etc/profile文件中是否设置TMOUT 2、检查 /etc/csh.cshrc是否设置autologout	cat /etc/profile|grep TMOUT cat /etc/csh.cshrc|grep autologout	
检查是否删除或锁定无关账号	删除过期账号（比如离职/转岗人员） 锁定指定用户: listen,gdm, webservd nobody nobody4 noaccess 测试账户（半自动） 共享账号（半自动） 长期不用账号(半年以上未使用，人工检查) 1、系统内置用户全部锁定 2、其它用户设置成/bin/false或/sbin/nologin 3、其它用户uuid需要大于系统内置用户的uuid	1、执行备份： #cp -p /etc/passwd /etc/passwd_bak #cp -p /etc/shadow /etc/shadow_bak 2、锁定无用帐户： 方法一： #vi /etc/shadow 在需要锁定的用户名的密码字段前面加!!，如 test:!!1QD1ju03H$LbV4vdBbpw.MY0hZ2D/Im1:14805:0:99999:7::: 方法二： #passwd -l test 3、将/etc/passwd文件中的shell域设置成/bin/false。 4、不能存在相关的测试账号，如test|ceshi|admin等。	

设置FTP用户登录后对文件、目录的存取权限	1.判断是否安装FTP服务（无论FTP服务是否启动都要检查相关配置）； 2.检查具体启用的FTP服务名称; 3.在安装前提下：根据对应服务名称检查FTP对应路径配置文件，要求所有用户只在对应自身主目录下访问）	/etc/vsftpd.conf文件中存在chroot_local_user=YES和chroot_list_enable=NO或者/etc/pure-ftpd/pure-ftpd.conf中存在ChrootEveryone yes、AllowUserFXP no、AllowAnonymousFXP no； 或者FTP服务未开启，以上任一条件满足即可； 参考解析：/etc/vsftpd.conf配置chroot_local_user=YES和chroot_list_enable=NO （该两个参数共同控制下配置：1.所有用户都被限制在其主目录下 2.不使用chroot_list_file指定的用户列表，没有任何“例外”用户）其他 ls_recurse_enable=YES local_umask=022 anon_umask=022 nopriv_user=ftpnobody userlist_enable=YES userlist_deny=NO anonymous_enable=NO	
限制用户FTP登录	1.检查是否安装FTP服务 2.若安装FTP服务，检查是否禁止root登录FTP	1、配置文件/etc/vsftpd/vsftpd.conf或者/etc/vsftpd.conf 修改其中内容： userlist_enable=YES userlist_deny=NO 2、文件/etc/vsftpd/user_list内不能存在以下账号： root、bin、sy、listen、nuucp、sync、shutdown、lp、naoccess、adm、nobody、uucp。 （/etc/vsftpd/user_list为白名单设置，在此文件内的账户可ftp登录）	
检查是否配置定时自动屏幕锁定	检查配置定时自动屏幕锁定	gconftool-2 --direct --config-source xml:readwrite:/etc/gconf/gconf.xml.mandatory --set --type=bool /apps/gnome-screensaver/idle_activation_enabled true gconftool-2 --direct --config-source xml:readwrite:/etc/gconf/gconf.xml.mandatory --set --type=int /apps/gnome-screensaver/idle_delay 15 gconftool-2 --direct --config-source xml:readwrite:/etc/gconf/gconf.xml.mandatory --set --type=string /apps/gnome-screensaver/mode blank-only gconftool-2 --direct --config-source xml:readwrite:/etc/gconf/gconf.xml.mandatory --set --type=bool /apps/gnome-screensaver/lock_enabled true	
检查口令最小长度	1.检查配置文件etc/login.defs的口令强度配置选项是否设置相应参数； 2.检查配置文件/etc/pam.d/system-auth的相关参数是否设置； 3.检查密码复杂度设置后是否成功设置提示（不满足密码复杂度时强制用户重新修改密码，root可强制修改密码未受参数限制）	1、执行备份： #cp -p /etc/pam.d/system-auth /etc/pam.d/system-auth_bak 或者cp -p /etc/pam.d/passwd /etc/pam.d/passwd_bak 2、配置文件/etc/login.defs，增加行PASS_MIN_LEN 8。 3、在文件/etc/pam.d/system-auth（/etc/pam.d/common-password）配置以下参数： password requisite pam_cracklib.so dcredit=-1 ucredit=-1 lcredit=-1 ocredit=- 1 minclass=3 minlen=8 enforce_for_root password sufficient pam_unix.so md5 shadow nullok try_first_pass use_authtok 是否配置了minlen=8，minclass=3。	
检查是否修改snmp默认团体字	SNMP（简单网络管理协议）的默认团体字（community string）通常是 "public"。这是一个众所周知的默认值，用于只读访问。然而，在生产环境中，为了安全考虑，通常会更改这个默认值	cat /etc/snmp/snmpd.conf| grep "com2sec"	grep -v "#" |grep "public"	
操作系统Linux目录文件权限安全基线要求项		file_permissions.sh	
Linux远程登录安全基线要求项-root用户远程登录限制	1.检查是否禁止root直接远程登录； 2.检查是否开启SSH服务； 3.检查是否禁用Telnet服务； 4.检查是否存在远程登录web插件安装信息；	1、执行备份： #cp -p /etc/securetty /etc/securetty_bak #cp -p /etc/ssh/sshd_config /etc/ssh/sshd_config_bak 2、新建一个普通用户并设置高强度密码： #useradd username #passwd username 3、禁止root用户远程登录系统： #vi /etc/securetty 注释形如pts/x的行，保存退出，则禁止了root从telnet登录。 #vi /etc/ssh/sshd_config 修改PermitRootLogin设置为no并不被注释，保存退出，则禁止了root从ssh登录。 #service sshd restart	
操作系统Linux SSH安全连接要求	1、检查是否使用ssh替代telnet服务 2、检查Telnet服务是否已禁用。	1、检查SSH服务是否正在运行： sudo systemctl status ssh 如果看到类似“active (running)”的消息，则表示SSH服务正在运行。 2、检查Telnet服务是否已禁用 sudo systemctl status telnet 如果Telnet服务未运行或已禁用，则会看到类似“inactive (dead)”的消息	
core dump 状态安全基线要求项	禁用全局core dump：默认情况下，应禁用全局core dump功能。这可以通过在/etc/security/limits.conf文件中添加以下行来实现： * hard core 0 这将限制所有用户（包括root）创建core文件的大小为0，从而禁用此功能。 限制特定用户的core dump权限：如果需要为特定用户或应用程序启用core dump，应在/etc/security/limits.conf中为这些用户设置限制。例如： user_name hard core unlimited 允许名为user_name的用户创建不受大小限制的core文件。 配置core文件的位置：为了更好地控制和保护core文件，应将其保存在一个受限制的目录中。这可以通过编辑/proc/sys/kernel/core_pattern文件来完成。如： echo "|/usr/bin/coredumpctl %e.%p" > /proc/sys/kernel/core_pattern 这将使所有core文件通过systemd-coredump服务管理，并存储在系统默认位置。	cat /etc/security/limits.conf|grep core	
操作系统Linux用户口令设置安全基线要求项-口令最长使用天数	1.检查配置文件etc/login.defs的口令强度配置选项是否设置相应参数； 2.检查配置文件/etc/pam.d/system-auth的相关参数是否设置； 3.检查密码复杂度设置后是否成功设置提示（不满足密码复杂度时强制用户重新修改密码，root可强制修改密码未受参数限制）	1、执行备份： #cp -p /etc/pam.d/system-auth /etc/pam.d/system-auth_bak 或者cp -p /etc/pam.d/passwd /etc/pam.d/passwd_bak 2、配置文件/etc/login.defs，增加行PASS_MIN_LEN 8。 3、在文件/etc/pam.d/system-auth（/etc/pam.d/common-password）配置以下参数： password requisite pam_cracklib.so dcredit=-1 ucredit=-1 lcredit=-1 ocredit=- 1 minclass=3 minlen=8 enforce_for_root password sufficient pam_unix.so md5 shadow nullok try_first_pass use_authtok 是否配置了minlen=8，minclass=3。	
检查主机访问控制	检查主机访问控制	检查 /etc/hosts.allow、/etc/hosts.deny配置文件是中否设置访问控制	
检查是否限制root远程登录	检查限制root远程登录	检查 /etc/ssh/sshd_config配置文件中的PermitRootLogin是否设置为 no	

检查用户缺省UMASK	需顶格（umask前不存在空格）新增umask配置： 1.检查配置文件/etc/login.def缺省访问权限设置为750（umask为027） 2.检查全局配置文件/etc/profile缺省访问权限设置为750（umask为027）	1、执行备份： #cp -p /etc/profile /etc/profile_bak #cp -p /etc/csh.login /etc/csh.login_bak #cp -p /etc/csh.cshrc /etc/csh.cshrc_bak #cp -p /etc/bashrc /etc/bashrc_bak #cp -p /root/.bashrc /root/.bashrc_bak #cp -p /root/.cshrc /root/.cshrc_bak 2、需顶格（umask前不存在空格）新增umask配置： #vi /etc/profile #vi /etc/csh.login #vi /etc/csh.cshrc #vi /etc/bashrc #vi /root/.bashrc #vi /root/.cshrc 重新新增配置umask值为027，保存退出。	
检查是否设置重复登录失败后锁定时间限制	检查是否设置重复登录失败后锁定时间限制	cat /etc/pam.d/system-auth|grep deny	
操作系统中不允许存在网络嗅探类的工具	是否安装了在网络嗅探类的工具	rpm -qa |egrep 'Tcpdump|Gdb|strace|dexdump|cpp|tcpdump|ethereal|wireshark'	
检查是否开启命令及登录失败记录	检查开启命令及登录失败记录	cat /etc/login.defs|grep LASTLOG_ENAB cat /etc/login.defs|grep FAILLOG_ENAB	
检查是否关闭不必要服务	1.检查是否存在不必要的服务； 2.附表2中的“根据情况选择开放”的服务是否需要判断开启（待确认）	1、#chkconfig --list 2、禁止非必要服务：#chkconfig [service] off 开启服务为：#chkconfig [service] on 以下服务都需要关闭： amanda chargen chargen-udp cups cups-lpd daytime daytime-udp echo echo-udp eklogin ekrb5-telnet finger gssftp imap imaps ipop2 ipop3 klogin krb5-telnet kshell ktalk ntalk rexec rlogin rsh rsync talk tcpmux-server telnet tftp time-dgram time-stream uucp; 不能存在以下端口：13 37 7 9 19 25 518 113 515 67 68 69 544 543 515 2049 1270 5989 139 445。	
检查口令长度及构成字符要求	1.检查配置文件etc/login.defs的口令强度配置选项是否设置相应参数； 2.检查配置文件/etc/pam.d/system-auth的相关参数是否设置； 3.检查密码复杂度设置后是否成功设置提示（不满足密码复杂度时强制用户重新修改密码，root可强制修改密码未受参数限制）	1、执行备份： #cp -p /etc/pam.d/system-auth /etc/pam.d/system-auth_bak 或者cp -p /etc/pam.d/passwd /etc/pam.d/passwd_bak 2、配置文件/etc/login.defs，增加行PASS_MIN_LEN 8。 3、在文件/etc/pam.d/system-auth（/etc/pam.d/common-password）配置以下参数： password requisite pam_cracklib.so dcredit=-1 ucredit=-1 lcredit=-1 ocredit=-1 minclass=3 minlen=8 enforce_for_root password sufficient pam_unix.so md5 shadow nullok try_first_pass use_authtok 是否配置了minlen=8，minclass=3。	
检查是否可以对日志数量进行配置	检查日志数量进行设置	cat /etc/logrotate.d|grep rotate cat /etc/logrotate.d|grep size	
禁止使用Tunnel设备	禁止使用Tunnel设备	cat /etc/ssh/sshd_config|grep PermitTunnel 检查值是否为 no	
是否开启selinux	开启selinux	cat /etc/selinux/config|grep SELINUX 检查值是否为permissive	
支持配置sshd服务端未认证连接最大并发量	检查配置sshd服务端未认证连接最大并发量	cat /etc/ssh/sshd_config|grep MaxStartups 检查是否设置并发最大值	
重复登录失败后锁定时间限制	重复登录失败后锁定时间限制	检查文件/etc/pam.d/password-auth" "/etc/pam.d/system-auth"中是否存在unlock_time=900 even_deny_root设置	
检查历史命令设置	HISTFILESIZE是一个环境变量，它控制着bash shell历史文件（通常为~/.bash_history）中可以保存的命令行历史记录条目的数量	/etc/profile 中是否存在HISTFILESIZE设置，如HISTFILESIZE=5	
检查是否关闭IP伪装和绑定多IP功能	检查关闭IP伪装和绑定多IP功能	cat /etc/host.conf |grep multi 是否为 off cat /etc/host.conf |grep nospoof 是否为 on	
检查账户认证失败次数限制	检查账户认证失败次数限制	/etc/pam.d/system-auth配置文件 是否存在“required pam_tally2.so deny=5 unlock_time=600”	
检查是否使用PAM认证模块禁止wheel组之外的用户su为root	检查使用PAM认证模块禁止wheel组之外的用户su为root	/etc/pam.d/su配置文件 是否存在“auth required pam_wheel.so use_uid"	
检查安全事件日志配置	检查记录安全事件日志	在/etc/syslog.conf配置文件中是否已配置 "*.err;auth.info /var/adm/messages"	
检查是否记录su日志	检查记录su日志	在/etc/syslog.conf配置文件中是否已配置 "authpriv.*"	
检查日志文件权限设置	检查日志文件权限设置	检查 /etc/syslog.conf配置文件权限是否为640	

具体加固操作联系网服获取：

《大数据安全加固TECS-Inspector_SEC工具使用指导书》

《大数据安全加固TECS-Inspector_SEC工具一键安装指导书》

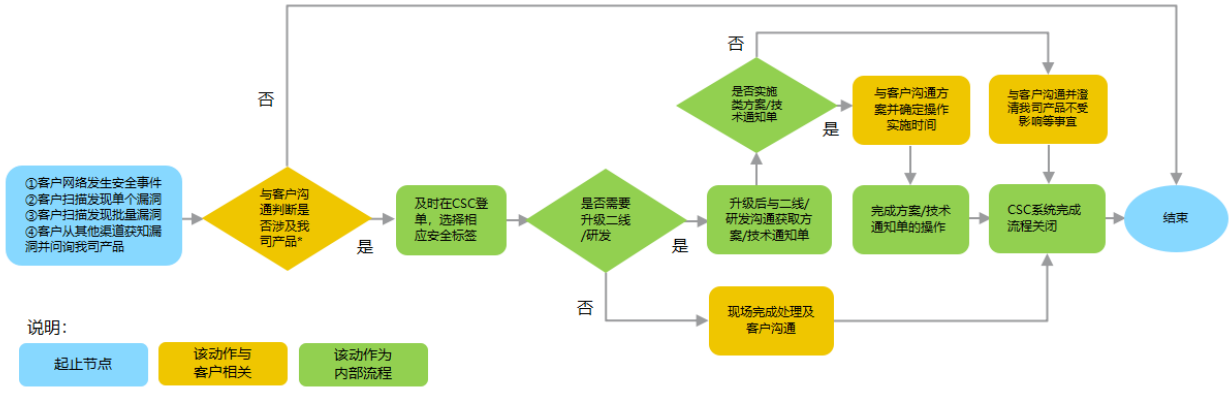
3.5 数据库安全加固

加固项	检查说明	
密码过期策略	1.检查GBASE所有管理节点配置文件/opt/gbase/gcluster/config/gbase_8a_gcluster.cnf中password_life_time参数	控制密码的有效期，达到有效期后用户密码自动过期。用户密码过期后，允许用户登录，在执行 SQL 时提示用

密码重用控制	1.检查GBASE所有管理节点配置文件/opt/gbase/gcluster/config/gbase_8a_gcluster.cnf中password_reuse_time和password_reuse_max参数	密码重复使用时最短间隔天数。超过了才能重复使用。默认0不限制。
登录重试次数	1.检查GBASE所有管理节点配置文件/opt/gbase/gcluster/config/gbase_8a_gcluster.cnf中login_attempt_max参数	参数控制尝试登陆的密码错误次数，超过了会将账号锁定，默认为0不限制次数
密码复杂度策略	1.检查GBASE所有管理节点配置文件/opt/gbase/gcluster/config/gbase_8a_gcluster.cnf中password_format_option参数	密码的组合要求，默认值为 0，表示无复杂度要求。组合中可包含数字（1）、小写字符（2）、大写字符（4） 1：表示必须包含数字。 2：表示必须包含小写字母。 4：表示必须包含大写字母。 8：表示必须包含其它字符。 16：表示不能和用户名相同。 要限定组合时配置为上述值的和，可以任意组合。例如：限定包含所有种类字符为（1+2+4+8=15）。 注意：从9.5.2.44版本开始，该参数改变为0-4，表示从4种组合种最少选择几种。比如3，表示最少要从数字，
密码最短长度策略	1.检查GBASE所有管理节点配置文件/opt/gbase/gcluster/config/gbase_8a_gcluster.cnf中password_min_length参数	限制用户密码最小长度，默认0不限制
审计日志开关	1.检查GBASE所有管理节点配置文件/opt/gbase/gcluster/config/gbase_8a_gcluster.cnf中audit_log参数	控制是的开启审计日志，默认值为0关闭
审计日志的记录策略	登录数据库执行select * from gbase.audit_policy	支持指定不同操作记录 INSERT,DELETE,UPDATE,LOAD,CREATE_USER,CREATE_DB,CREATE_TABLE,CRE 不指定表示记录所有，默认没有创建规则 执行创建审计策略create audit policy audit_ALL 执行删除审计策略drop audit policy audit_ALL
审计日志的存储方式	1.检查GBASE所有管理节点配置文件/opt/gbase/gcluster/config/gbase_8a_gcluster.cnf中log_output参数	配置审计日志记录存储在表中或文本文件中，默认值为file
数据库用户密码加密方式	1.检查GBASE所有管理节点配置文件/opt/gbase/gcluster/config/gbase_8a_gcluster.cnf中gbase_caching_sha2_password参数	支持sha256的用户密码加密， 0，不开启 默认值 1， 开启，之后创建用户和设置密码时，会用sha256进行加密

3.6其它安全加固

通过主动扫描、被动监测、安全披露、社区协助等发现的新的安全问题，如涉及 中兴通讯产品，目前通过IEC系统上报解决。

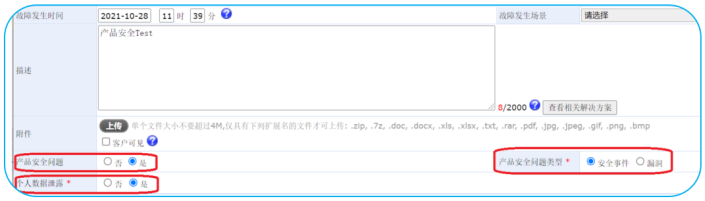


***我司产品：**包括我司自研产品以及我司发货并负责维护的外购件产品。

1、产品安全问题登单路径：

http://csc.zte.com.cn--客户请求管理--受理--客户故障/客户问题及投诉，请不要登记客户协助请求。

2、产品安全事件登记客户故障单：选择产品安全标签为**是**，问题类型选择产品**安全事件**，系统会邮件通知产品安全事件响应团队；同时需要选择是否涉及个人数据泄露，如果涉及个人数据泄露，系统会邮件通知个人数据泄露响应团队。



3、产品安全漏洞登记客户问题单：选择产品安全标签为**是**，问题类型选择产品安全**漏洞**，选择漏洞分类，并将漏洞扫描报告做为附件上传。

4、CSC单据跟踪：现场工程师登记产品安全问题后，系统会发送通知邮件，知会相关领域的安全负责人。现场工程师应及时通过申请升级将问题升级到网服二线团队处理。网服二线团队可以通过升级研发故障中心到产品研发团队获取进一步支持。必要时现场工程师还应知会项目组/工服处/办事处产品安全经理，通过组建MOA等方式加入相关人员推动问题快速处理。

5、单据修正：CSC单据升级到二线或三线后，处理工程师需要根据单据信息与一线沟通，如确认非产品安全事件或漏洞，应及时修正单据，通过编辑详细菜单取消安全标签的勾选。如发现实际是产品安全事件或漏洞，但一线没有正确填报的，也应及时修正单据，通过编辑详细菜单增加产品安全标签的勾选。

6、闭环跟踪：现场工程师应与网服、研发支持团队保持沟通，在正式发布实施方案、实施技术通知单后根据本项目涉及产品波及分析及客户沟通，按时完成相关操作，形成闭环。
漏洞单关闭时，需在解决方案中填写治理记录，如：本次上报漏洞X个，已解决X个，备案X个，无影响或不涉及的澄清X个，尚遗留X个漏洞未解决，已经与客户充分沟通确认。漏洞较多时，可以上传附件举证处置情况。

***产品安全漏洞：**包括客户通过漏洞扫描、渗透测试以及其他方式发现的漏洞，导致安全基线扫描不通过的不符合项或客户要求必须修复的不符合项。

3.7 加固后检查

3.7.1 账户系统共安全加固检查

在日常维护中，通常部门、操作集、角色和角色集已经创建完成。系统管理员可以通过查询已登录用户、查看锁定用户等操作，了解系统的安全情况，并可以通过设置用户黑名单等操作来杜绝一些潜在的安全隐患。

3.7.1.1 查询已登录用户

摘要

查询当前登录用户的信息，包括登录用户的名称、登录IP地址、登录时间。维护人员也可以将其他已登录用户强制退出。

步骤

1. 在DAP系统管理窗口，选择菜单**安全→登录用户管理**，查看当前登录用户的信息，如图 3-1所示。

图 3-1登录用户管理

2. 单击**刷新**按钮，重新向服务器获取登录用户的信息。
3. （可选）如果需要将一个当前登录的用户强制退出，执行如下操作。
   a. 选择一个当前登录用户，单击**强制退出**按钮，系统弹出**确认**对话框。
   b. 单击**确认**按钮。

3.7.1.2 查看用户锁定情况

摘要

系统管理员可以查看用户锁定情况，并对用户进行解锁操作。

当用户帐号规则中设置了帐号锁定的条件（即密码连续输错次数），如果用户密码输入错误次数达到了设置的密码错误次数，用户帐号将被锁定。

步骤

1. 在DAP系统管理窗口，选择菜单**安全→用户锁定情况**，查看用户锁定情况，如图 3-2所示。

图 3-2查看用户锁定情况

2. （可选）如果需要解锁某个用户，选中该用户，单击**解锁**按钮，并在弹出的**确认**对话框中单击**是**按钮。

3.7.1.3 设置用户黑名单

摘要

本节介绍如何设置用户黑名单，进入黑名单的用户将不允许登录ZXVMAX系统。

说明：

只有拥有**系统管理员**角色的用户才能执行如下操作。

前提

以拥有**系统管理员**角色的用户已登录客户端。

步骤

1. 在DAP系统管理窗口，选择菜单**安全→用户黑名单**，查看黑名单的用户信息，如图 3-3所示。

图 3-3用户黑名单

2. 在左侧用户列表中选择需要添加至黑名单的用户，单击，将其添加至**黑名单用户**列。

3. 单击**确定**按钮。

3.7.2 操作系统安全加固检查

参考《大数据安全加固TECS-Inspector_SEC工具使用指导书》中的任务执行章节

或参考3.4.1安全加固条目

3.7.3 数据库安全加固检查

参考3.5章节中说明进行检查

4. 回退

4.1 操作系统安全加固回退

参考《大数据安全加固TECS-Inspector_SEC工具使用指导书》中的回退章节

4.2 数据库安全加固回退

参考3.5章节中说明进行反向操作进行回退

5. 默认安全配置项

5.1 账户系统默认安全加固项

加固项参见3.3章节，默认设置如下表：

5.1.1 密码策略

参数名	默认值
最小密码字符长度	8
最大密码字符长度	20
不能与最近**次重复	启用，不能与最近3次重复
启用强密码检测	启用
密码与用户名不能包含连续字符相同	选中复选框，设置连续字符数，系统自动检测密码，禁止密码包含与用户名相同的连续字符数。取值范围1~16。
允许包含空格	选中复选框，密码允许包含空格
首次登录时必须修改密码	启用

密码最大有效期	60天
过期提示	启用，过期前3天提示

5.1.2 账号锁定规则

参数名	默认值
锁定规则	暂时锁定
锁定后解锁时间	1440分钟
锁定密码错误输入次数	3次

5.1.3 用户最长在线时间

参数名	默认值
用户最长在线时间	30分钟。30分钟无操作则自动退出

5.2 操作系统默认安全加固项

由于操作系统版本的差异，在新安装设备必须通过工具进行安全加固检查，具体参见由TECS-Inspector_SEC安全加固工具进行检查设置。

建议的默认加固项如下表：

执行的加固项	说明
OS-Linux-口令-02-【工信部/集团】检查口令生存周期要求（shadow文件）	1.检查配置文件/etc/shadow下不能存在密码过期时间小于0或者大于90天的非系统内置用户。默认设置(与操作系统版本号有关)
OS-Linux-账号-02-【工信部/集团】检查是否删除或锁定无关账号（自动化）	删除过期账号（比如离职/转岗人员） 锁定指定用户: listen,gdm, webservd nobody nobody4 noaccess 测试账户（半自动） 共享账号（半自动） 长期不用账号(半年以上未使用，人工检查)
OS-Linux-日志-04-【工信部/集团】检查是否配置远程日志保存（自动化）	检查远程日志功能是否启用； 默认不启用，需要手动配置IP
OS-Linux-账号-01-【工信部/集团】检查是否按用户分配账号责任到人（自动化）	不能存在共享账号，（如厂商、test、admin、ceshi等命名账号） 从账号主目录权限限制750
OS-Linux-日志-02-【工信部/集团】检查日志文件权限设置（自动化）	检查日志文件权限设置，默认未设置
OS-Linux-日志-04-【工信部/集团】检查是否配置远程日志保存（强化）	检查远程日志功能是否启用； 默认不启用，需要手动配置IP
OS-Linux-口令-01-【工信部/集团】检查口令策略设置是否符合复杂度要求（自动化）	检查口令策略设置是否符合复杂度要求 默认设置
OS-Linux-授权-01-【工信部/集团】检查帐号文件权限设置（自动化）	1.检查/etc/passwd 、/etc/shadow 、/etc/group 三个文件的权限（自动化） 2.遍历查询/etc、安装系统后默认系统目录下所有子目录及文件写权限（自动化） 默认支持
OS-Linux-口令-02-【工信部/集团】检查口令生存周期要求（自动化）	1.检查配置文件/etc/login.defs的相关参数，口令生存周期大于等于1且小于等于90天 2.检查配置文件/etc/shadow下非系统内置用户的密码过期时间小于等于90天 默认支持
OS-Linux-安全补丁-01-【工信部/集团】检查是否安装OS补丁（自动化）	1.检查版本编号，确定是否为最新版本； 2.检查大补丁号，确定是否为最新版本； 3.检查不存在非必要的包 4.检查系统内核版本号，确定是否为最新版本
OS-Linux-账号-04-【工信部/集团】检查是否设置限制su命令用户组（自动化）	设置限制使用su命令的用户组 非默认设置
OS-Linux-账号-03-【工信部/集团】检查是否按角色进行帐号管理（自动化）	判断是否存在多账户组，不存在，默认合规；存在多个用户的账户组，默认判断不合规，人工问询确认多账户组是否为业务需求。 判断是否存在自己创建的用户组。 非默认设置
OS-Linux-不必要的服务-01-【工信部/集团】检查是否关闭不必要服务（自动化）	1.检查是否存在不必要的服务； 2.附表2中的“根据情况选择开放”的服务是否需要判断开启（待确认） 非默认设置
OS-Linux-FTP设置-01-【工信部/集团】检查FTP配置-限制用户FTP登录（自动化）	1.检查是否安装FTP服务 2.若安装FTP服务，检查是否禁止root登录FTP 默认未安装
OS-Linux-FTP设置-03-【工信部/集团】检查登录提示-更改ftp警告Banner（自动化）	1.检查是否安装FTP服务 2.检查FTP服务类型 3.检查配置文件是否设置相关参数 默认未安装
OS-Linux-登录超时时间设置-01-【工信部/集团】检查是否设置登录超时（自动化）	1.检查是否设置账户登录超时登出/etc/profile 文件中TMOUT值大于0并且小于等于180或300（newstart\suse\ubuntu） 默认设置5分钟

OS-Linux-系统Banner设置-01-【工信部/集团】检查登录提示-是否设置登录成功后警告Banner（自动化）	1.检查是否更改配置文件/etc/rc.d/rc.local、/etc/motd、sshd_config，隐藏操作系统名称，版本号，主机名称等信息； 2.检查是否删除"/etc" 目录下的issue.net和issue文件； 非默认设置
OS-Linux-删除潜在危险文件-01-【工信部/集团】检查帐户目录是否存在.netrc文件（自动化）	检查帐户目录是否存在.netrc文件 非默认设置
OS-Linux-日志-01-【工信部/集团】检查是否记录安全事件日志（自动化）	检查是否记录安全事件日志 非默认设置
OS-Linux-授权-02-【工信部/集团】检查用户缺省UMASK（自动化）	需顶格（umask前不存在空格）新增umask配置： 1.检查配置文件/etc/login.def缺省访问权限设置为750（umask为027） 2.检查全局配置文件/etc/profile缺省访问权限设置为750（umask为027） 非默认设置
OS-Linux-授权-03-【工信部/集团】检查FTP配置-限制FTP用户登录后能访问的目录（自动化）	1.判断是否安装FTP服务（无论FTP服务是否启动都要检查相关配置）； 2.检查具体启用的FTP服务名称; 3.在安装前提下：根据对应服务名称检查FTP对应路径配置文件，要求所有用户只在对应自身主目录下访问） 默认不安装
OS-Linux-远程登录-02-【工信部/集团】检查是否使用ssh替代telnet服务（自动化）	检查是否使用ssh替代telnet服务 默认不安装Telnet
OS-Linux-日志-03-【工信部/集团】检查是否记录cron命令使用情况（自动化）	检查是否记录cron命令使用情况 默认支持
OS-Linux-远程登录-01-【工信部/集团】检查是否限制root远程登录（自动化）	1.检查是否禁止root直接远程登录；默认禁止 2.检查是否开启SSH服务；默认开启 3.检查是否禁用Telnet服务；默认禁用 4.检查是否存在远程登录web插件安装信息；默认不安装
OS-Linux-FTP设置-02-【工信部/集团】检查是否禁止匿名ftp（自动化）	1.检查是否安装FTP服务 2.检查是否禁止匿名账户FTP登录 默认不安装
检查是否设置口令生存周期	1.检查配置文件/etc/shadow下不能存在密码过期时间小于0或者大于90天的非系统内置用户。 非默认设置
关闭telnet服务	检查是否使用ssh替代telnet服务 默认使用ssh,不启用telnet服务
禁止icmp重定向	临时禁用ICMP重定向： sudo sysctl -w net.ipv4.conf.all.send_redirects=0 默认禁止
检查是否配置远程日志保存	1.检查远程日志功能是否启用； 2.检查配置文件syslog.conf、rsyslog.conf、syslog-ng.conf（syslog-ng.conf文件配置存在差异需注意）的相关参数行 3.敏感审计日志确认接收到日志 非默认设置
检查登录提示-更改ftp警告Banner	1.检查是否安装FTP服务 2.检查FTP服务类型 3.检查配置文件是否设置相关参数 默认不启用FTP服务
检查口令策略设置是否符合复杂度要求、检查口令锁定策略、检查口令重复次数限制	1.检查配置文件etc/login.defs的口令强度配置选项是否设置相应参数； 2.检查配置文件/etc/pam.d/system-auth的相关参数是否设置； 3.检查密码复杂度设置后是否成功设置提示（不满足密码复杂度时强制用户重新修改密码，root可强制修改密码未受参数限制） 新操作系统默认支持
检查登录提示-是否设置ssh警告Banner	编辑/etc/ssh/sshd_config文件，将参数设置为如下值： /etc/issue.net 非默认设置
检查登录提示-是否设置登录成功后警告Banner	1.检查是否更改配置文件/etc/rc.d/rc.local、/etc/motd、sshd_config，隐藏操作系统名称，版本号，主机名称等信息； 2.检查是否删除"/etc" 目录下的issue.net和issue文件； 非默认设置
检查登录提示-是否更改telnet警告Banner	1.检查是否存在不必要的服务； 2.附表2中的“根据情况选择开放”的服务是否需要判断开启（待确认） 默认不存在
检查是否设置登录超时	1、检查/etc/profile文件中是否设置TMOUT 2、检查 /etc/csh.cshrc是否设置autologout 默认设置5分钟
检查是否删除或锁定无关账号	删除过期账号（比如离职/转岗人员） 锁定指定用户: listen,gdm, webservd nobody nobody4 noaccess 测试账户（半自动） 共享账号（半自动） 长期不用账号(半年以上未使用，人工检查)
设置FTP用户登录后对文件、目录的存取权限	1.判断是否安装FTP服务（无论FTP服务是否启动都要检查相关配置）； 2.检查具体启用的FTP服务名称; 3.在安装前提下：根据对应服务名称检查FTP对应路径配置文件，要求所有用户只在对应自身主目录下访问） 默认不安装FTP服务
限制用户FTP登录	1.检查是否安装FTP服务 2.若安装FTP服务，检查是否禁止root登录FTP 默认不安装FTP服务
检查是否配置定时自动屏幕锁定	检查配置定时自动屏幕锁定 默认5分钟自动锁定
检查口令最小长度	1.检查配置文件etc/login.defs的口令强度配置选项是否设置相应参数； 2.检查配置文件/etc/pam.d/system-auth的相关参数是否设置； 3.检查密码复杂度设置后是否成功设置提示（不满足密码复杂度时强制用户重新修改密码，root可强制修改密码未受参数限制） 默认14字符
检查是否修改snmp默认团体字	SNMP（简单网络管理协议）的默认团体字（community string）通常是"public"。这是一个众所周知的默认值，用于只读访问。然而，在生产环境中，为了安全考虑，通常会更改这个默认值 默认为public
操作系统Linux目录文件权限安全基线要求项	非默认设置

Linux远程登录安全基线要求项-root用户远程登录限制	1.检查是否禁止root直接远程登录；默认禁止 2.检查是否开启SSH服务；默认开启 3.检查是否禁用Telnet服务；默认禁用 4.检查是否存在远程登录web插件安装信息；默认不安装
操作系统Linux SSH安全连接要求	1、检查是否使用ssh替代telnet服务 2、检查Telnet服务是否已禁用。 默认禁用Telnet
core dump 状态安全基线要求项	禁用全局core dump：默认情况下，禁用全局core dump功能。
操作系统Linux用户口令设置安全基线要求项-口令最长使用天数	1.检查配置文件etc/login.defs的口令强度配置选项是否设置相应参数； 2.检查配置文件/etc/pam.d/system-auth的相关参数是否设置； 3.检查密码复杂度设置后是否成功设置提示（不满足密码复杂度时强制用户重新修改密码，root可强制修改密码未受参数限制） 非默认设置
检查主机访问控制	检查主机访问控制 非默认设置
检查是否限制root远程登录	检查限制root远程登录，默认限制
检查用户缺省UMASK	需顶格（umask前不存在空格）新增umask配置： 1.检查配置文件/etc/login.def缺省访问权限设置为750（umask为027） 2.检查全局配置文件/etc/profile缺省访问权限设置为750（umask为027） 非默认设置
检查是否设置重复登录失败后锁定时间限制	检查是否设置重复登录失败后锁定时间限制，默认5分钟限制
操作系统中不允许存在网络嗅探类的工具	是否安装了在网络嗅探类的工具，默认不安装
检查是否开启命令及登录失败记录	检查开启命令及登录失败记录，默认支持
检查是否关闭不必要服务	1.检查是否存在不必要的服务； 2.附表2中的“根据情况选择开放”的服务是否需要判断开启（待确认） 默认 无不必要服务
检查口令长度及构成字符要求	1.检查配置文件etc/login.defs的口令强度配置选项是否设置相应参数； 2.检查配置文件/etc/pam.d/system-auth的相关参数是否设置； 3.检查密码复杂度设置后是否成功设置提示（不满足密码复杂度时强制用户重新修改密码，root可强制修改密码未受参数限制） 默认限制
检查是否可以对日志数量进行配置	检查日志数量进行设置 非默认设置
禁止使用Tunnel设备	禁止使用Tunnel设备 非默认设置
是否开启selinux	开启selinux 默认开启
支持配置sshd服务端未认证连接最大并发量	检查配置sshd服务端未认证连接最大并发量 非默认设置
重复登录失败后锁定时间限制	重复登录失败后锁定时间限制 非默认设置
检查历史命令设置	HISTFILESIZE是一个环境变量，它控制着bash shell历史文件（通常为~/.bash_history）中可以保存的命令行历史记录条目的数量 非默认设置
检查是否关闭IP伪装和绑定多IP功能	检查关闭IP伪装和绑定多IP功能 非默认设置
检查账户认证失败次数限制	检查账户认证失败次数限制 非默认设置
检查是否使用PAM认证模块禁止wheel组之外的用户su为root	检查使用PAM认证模块禁止wheel组之外的用户su为root 非默认设置
检查安全事件日志配置	检查记录安全事件日志，默认记录
检查是否记录su日志	检查记录su日志，默认记录
检查日志文件权限设置	检查日志文件权限设置，非默认设置

5.3 数据库默认安全加固项

加固项参见3.5章节，默认设置如下表：

加固项	默认设置
密码过期策略	password_life_time配置为 0
密码重用控制	password_reuse_max配置为0 password_reuse_time配置为0
登录重试次数	login_attempt_max配置为0
密码复杂度策略	password_format_option配置为3
密码最短长度策略	password_min_length配置为8
审计日志开关	audit_log配置为1
审计日志的记录策略	执行创建审计策略create audit policy audit_ALL

审计日志的存储方式	log_output配置为file
数据库用户密码加密方式	gbase_caching_sha2_password配置为1