

云主机防暴力破解最佳实践

本文档旨在指导系统运维管理人员或安全检查人员进行Linux/Windows账户及远程登录相关合规性检查、安全配置指导及解决方案建议。

针对第1章节“基础系统安全加固”中的建议，已实现自动化脚本(第4章节)方便读者快速加固现有云主机，使用本文档(及相关工具)指导修改生产环境配置之前应提前进行充分测试验证，避免对生产业务造成干扰。

目录

云主机防暴力破解最佳实践.....	1
1 基础系统安全加固	4
1.1 Linux	5
1.1.1 OS-Linux-口令复杂度设置	5
1.1.2 OS-Linux-远程登录账户设置	6
1.1.3 OS-Linux-登录安全设置.....	7
1.1.4 OS-Linux-远程登录密钥对设置	8
1.1.5 OS-Linux-远程登录端口设置	9
1.1.6 OS-Linux-普通账号设置su权限.....	10
1.2 Windows.....	11
1.2.1 OS-Windows-口令复杂度设置	11
1.2.2 OS-Windows-默认账号设置.....	12
1.2.3 OS-Windows-口令锁定设置.....	14

1.2.4	OS-Windows-口令历史记录校验设置	15
1.2.5	OS-Windows-最后登录帐号设置	16
1.2.6	OS-Windows-会话超时设置.....	17
2	基础网络安全策略配置.....	18
2.1	安全组	19
2.2	Linux之iptables.....	21
2.3	Windows之防火墙.....	23
2.4	远程登录端口选择性对公网暴露.....	24
3	主机安全进阶方案	27
3.1	主机安全防护	27
3.2	云主机系统登录双因素认证	28
3.3	安全评估	31
4	加固脚本使用说明	32
4.1	Linux加固脚本.....	32
4.1.1	简介	32
4.1.2	配置备份与恢复	33
4.1.3	密码复杂度设置	34
4.1.4	SSH远程登录相关安全配置.....	34
4.1.5	history & TMOUT相关配置.....	35
4.1.6	SSH秘钥登录配置	36
4.1.7	SSH端口配置.....	37

4.1.8	su权限配置	37
4.1.9	全部加固.....	38
4.2	Windows加固脚本.....	38
4.2.1	简介	38
4.2.2	配置备份与恢复	39
4.2.3	口令复杂度设置	40
4.2.4	口令历史记录校验设置.....	40
4.2.5	口令锁定设置	41
4.2.6	系统默认账户设置	41
4.2.7	会话超时设置	42
4.2.8	最后登录账号设置	42
4.2.9	全部加固.....	43
4.3	加固脚本支持系统列表	43
4.3.1	Linux.....	43
4.3.2	Windows	44
5	解决方案咨询	44
附录1	相关产品/服务	44

1 基础系统安全加固

加固项	推荐指数
OS-Linux-口令复杂度设置	必选
OS-Linux-远程登录账户设置	必选
OS-Linux-登录安全设置	★★★★★
OS-Linux-远程登录秘钥对设置	★★★★★
OS-Linux-远程登录端口设置	★★★★
OS-Linux-普通账号设置su权限	★★★★

加固项	推荐指数
OS-Windows-口令复杂度设置	必选
OS-Windows-默认账号设置	必选
OS-Windows-口令锁定设置	★★★★★
OS-Windows-口令历史记录校验设置	★★★★
OS-Windows-最后登录帐号设置	★★★★
OS-Windows-会话超时设置	★★★

1.1 Linux

1.1.1 OS-Linux-口令复杂度设置

OS-Linux-口令复杂度设置

建议项：对于采用口令认证的设备，口令长度建议不少于**12位**，并包括**数字、小写字母、大写字母和特殊符号4类字符**。

操作指南：

1. 使用命令 “`vim /etc/pam.d/system-auth`” 修改配置文件，在文件末尾增加一下配置：

```
password requisite pam_cracklib.so retry=5 difok=3 minlen=12 lcredit=-1
```

```
ucredit=-1 dcredit=-1 ocredit=-1
```

2. Note：某些Linux版本相应的配置文件并非 `system-auth`，而是 `/etc/pam.d/common-password`，找到相应配置文件在文件末尾增加一下配置：

```
password requisite pam_cracklib.so retry=5 difok=3 minlen=12 lcredit=-1
```

```
ucredit=-1 dcredit=-1 ocredit=-1
```

3. Note：某些Linux版本并非使用 `pam_cracklib.so` 实现密码复杂度检测而是 `pam_pwquality.so`，需视具体情况在相应的配置文件 (`system-auth` 或 `common-password`) 中增加配置：

```
password requisite pam_pwquality.so retry=5 difok=3 minlen=12 lcredit=-1
```

```
ucredit=-1 dcredit=-1 ocredit=-1
```

检测方法：创建一个普通账号，为用户配置与用户名相同的口令、只包含字符或数字的

简单口令以及长度短于12的口令，查看系统是否对口令强度要求进行提示；输入带有特殊符号的复杂口令，查看系统是否可以成功设置。

判定条件：

不符合规则的密码设置不成功；

符合密码强度的密码，才可以成功设置。

补充说明：1. root账户口令设置不受口令强度要求限制，需要在设置口令时主动遵从复杂度要求，避免设置弱密码；2. 密码在满足复杂度的基础上，建议尽量避免使用常见密码(如企业内部常用密码)或使用易被猜测的串组成密码(如生日、姓名等)。

1.1.2 OS-Linux-远程登录账户设置

OS-Linux-远程登录账户设置

建议项：限制超级管理员用户远程登录；设置普通用户远程登录失败尝试次数。

操作指南：

修改vim /etc/ssh/sshd_config文件，修改：

Protocol 2 #设置SSH协议版本为

PermitRootLogin no #禁止root账户进行远程登录

MaxAuthTries 3 #可根据实际情况设置，建议[3-10]

AllowUsers usera userb userc #根据实际情况设置

重启sshd服务。

检测方法：

<p>root从远程使用SSH登录检查是否能登录成功；</p> <p>普通用户从远程使用SSH登录成功，并能su到root账户。</p>
<p>判定条件：</p> <p>root远程登录失败判定为成功；</p> <p>普通用户可以登录成功，而且可以切换到root用户判定为成功；</p> <p>普通账户和root账户输错3次密码登录被断开判定为成功。</p>
<p>补充说明：禁止root账户远程登录后，以普通账户登录系统，通过su到root账户，获得root权限，建议参考加固项-1.1.7 “OS-Linux-普通账号设置su权限” 设置能够su到root的账户。</p>

1.1.3 OS-Linux-登录安全设置

<p>OS-Linux-登录安全设置</p>
<p>建议项：配置系统历史命令操作记录和定时帐户自动登出时间。</p>
<p>操作指南：</p> <p>编辑profile文件（<code>vi /etc/profile</code>），修改HISTSIZE=1000，修改TMOUT=300（可根据情况设置，单位：秒）；在文件末位加入：<code>export HISTTIMEFORMAT="%F %T `whoami` "</code>；</p> <p>配置完成后使用source /etc/profile让配置立即生效。</p>
<p>检测方法：输入history查看历史命令是否从本条命令开始启用账户、时间记录。</p>
<p>判定条件：立即记录账户、操作时间判定为设置成功。</p>

补充说明： 启用如上配置，能够有效提升事件调查效率。

1.1.4 OS-Linux-远程登录密钥对设置

OS-Linux-远程登录密钥对设置

建议项： 限制SSH远程登录仅能通过密钥进行认证，而非口令。

操作指南：

1 如果为新建云主机场景，可以在创建时直接选择使用密钥对登录，华为云会自动进行相关配置；

2 如果为修改现有云主机SSH由密码登录方式为密钥登录方式，请按照步骤3/4/5进行配置；

3 创建密钥对，并将公钥上传至待配置的云主机(可以选择使用puttygen等工具生成公私钥对，详细步骤可参考：http://support.huaweicloud.com/usermanual-ecs/zh-cn_topic_0014250631.html)；

4 在云主机上安装公钥(以root权限执行)

```
cd /root/.ssh
```

```
cat /dir/id_rsa.pub >> authorized_keys # "/dir/id_rsa.pub" 为第3步创建的公钥
```

```
chmod 600 authorized_keys #确保文件权限正确
```

```
chmod 700 ~/.ssh
```

5 修改vim /etc/ssh/sshd_config相关配置，开启密钥登录，并重启sshd服务

RSAAuthentication yes

PubkeyAuthentication yes

PasswordAuthentication no #禁用密码登录

ChallengeResponseAuthentication no

重启sshd服务，**service sshd restart**。

检测方法：尝试用密码进行远程登录；

尝试用秘钥进行远程登录。

判定条件：密码方式登陆失败；秘钥方式登陆成功。

补充说明：如何以秘钥方式SSH登录Linux云主机，可参考

http://support.huaweicloud.com/usermanual-ecs/zh-cn_topic_0017955380.html。

1.1.5 OS-Linux-远程登录端口设置

OS-Linux-远程登录端口设置

建议项：修改默认的SSH服务端口；

操作指南：

修改 **vim /etc/ssh/sshd_config**文件，修改：

Port 2222 #修改端口是4位数以上的高端口

修改完成后重启sshd服务。

检测方法：使用默认端口SSH登录，检查是否成功；

使用新设置的端口SSH登录，检查是否成功。

判定条件：默认SSH登录不成功，新设置端口SSH登录成功，判定为设置成功。

补充说明：华为云官网安全组默认开放SSH 22号端口，修改主机的SSH端口后，需要同步修改主机所在的安全组策略配置，增加新设置端口的白名单，可参考：2.1节内容，及安全组support文档：http://support.huaweiclouds.com/usermanual-vpc/zh-cn_topic_0030969470.html。

1.1.6 OS-Linux-普通账号设置 su 权限

OS-Linux-普通账号设置su权限

建议项：建议设置可以su为root的账户为制定的用户组，其它账户不能su切换至root

操作指南：

1. 编辑su文件(`vi /etc/pam.d/su`)，在文件中添加如下配置：

```
auth    required    pam_wheel.so use_id
```

并将需要的账户加入wheel组，即可完成配置。

```
#usermod -G wheel test
```

2. 某些版本Linux默认无wheel组，需要首先创建wheel组：

```
#groupadd wheel
```

再编辑su文件(`vi /etc/pam.d/su`)，在文件中添加如下配置：

```
auth    required    pam_wheel.so group=wheel
```

并将需要的账户加入wheel组，即可完成配置。

```
#usermod -G wheel test
```

检测方法：创建2个普通账户：test1和test2，test1加入wheel组，test2不加：

分别使用test1，test2远程登录后，su到root，检查是否成功。

判定条件：test1可以su到root，test2不能su到root判定为设置成功。

补充说明：测试完成后test1和test2要删除。

1.2 Windows

1.2.1 OS-Windows-口令复杂度设置

OS-Windows-口令复杂度设置

要求内容：密码长度最少12位，不能使用有键盘规律的密码（键盘规律密码：qazxsw,1qaz@WSX,1q2w3e等），且密码复杂度至少包含以下四种类别的字符中的三种：

英语大写字母 A, B, C, ... Z

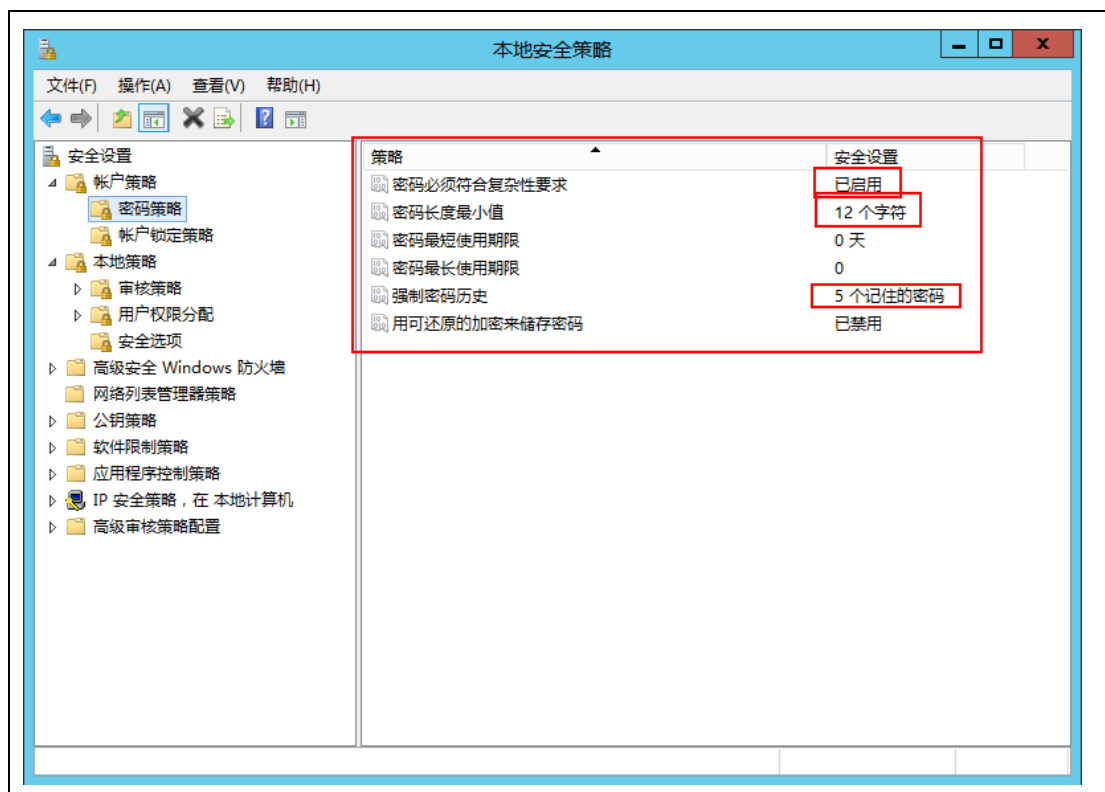
英语小写字母 a, b, c, ... z

阿拉伯数字 0, 1, 2, ... 9

非字母数字字符，如标点符号，@, #, \$, %, &, *等。

操作指南：

进入“控制面板->管理工具->本地安全策略”，在“帐户策略->密码策略”：“密码必须符合复杂性要求”选择“已启动”。并根据需要调整密码长度最小值（注意：长度为0表示不需要密码）。



检测方法：创建一个**新账号**，为用户配置与用户名相同的口令、只包含字符或数字的简单口令以及长度短于12的口令，查看系统是否对口令强度要求进行提示；输入带有特殊符号的复杂口令，查看系统是否可以成功设置。

判定条件：不符合规则的密码设置不成功，并且对口令强度要求进行提示；符合密码强度的密码，才可以成功设置。

补充说明：密码在满足复杂度的基础上，建议尽量避免使用常见密码(如企业内部常用密码)或使用易被猜测的串组成密码(如生日、姓名等)。

1.2.2 OS-Windows-默认账号设置

OS-Windows-默认账号设置

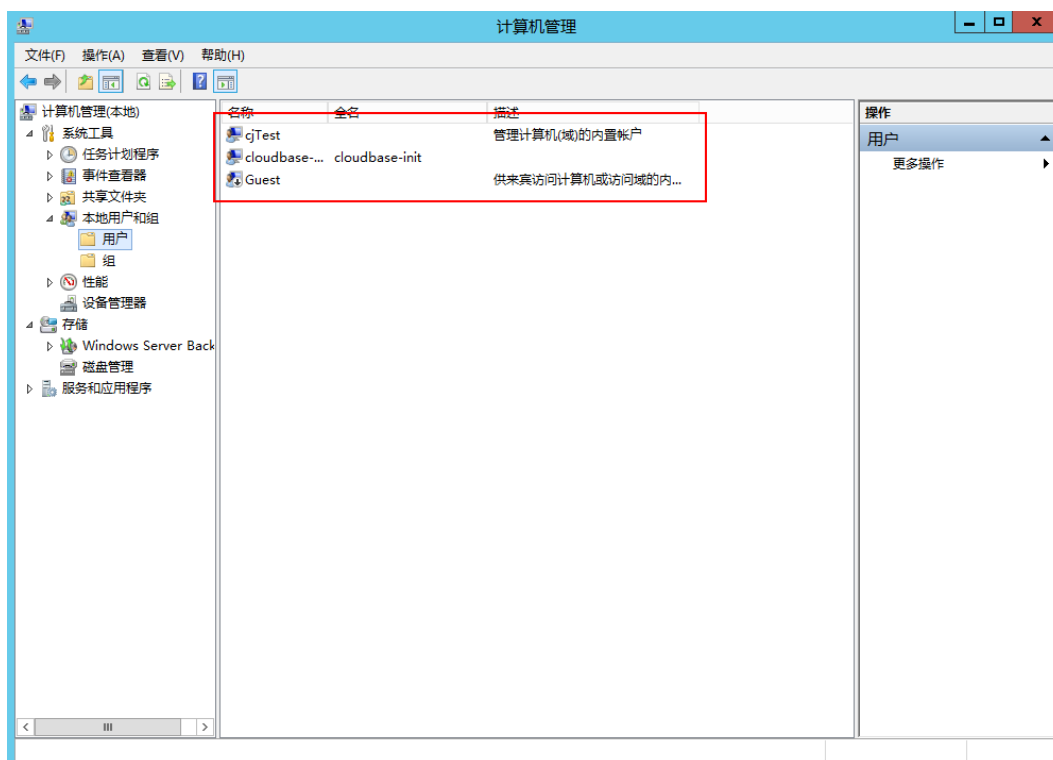
要求内容：重命名Administrator，禁用guest（来宾）帐号和其它不必要的账户；

操作指南：

进入“控制面板->管理工具->计算机管理”，在“系统工具->本地用户和组->用户”：

Administrator->右键进行重命名；

Guest帐号->属性->“账户已禁用”。



检测方法：

检查Administrator账户名称是否已更改，Guest和其它无关账户是否已停用。

判定条件： 缺省账户Administrator名称已更改；Guest帐号和其它无关账户已停用。

补充说明： 1. 修改后请谨记新账户名，原Administrator已无法登录；2. 配置后请重启系统，使用新账户名登录，否则使用可能出现异常；

1.2.3 OS-Windows-口令锁定设置

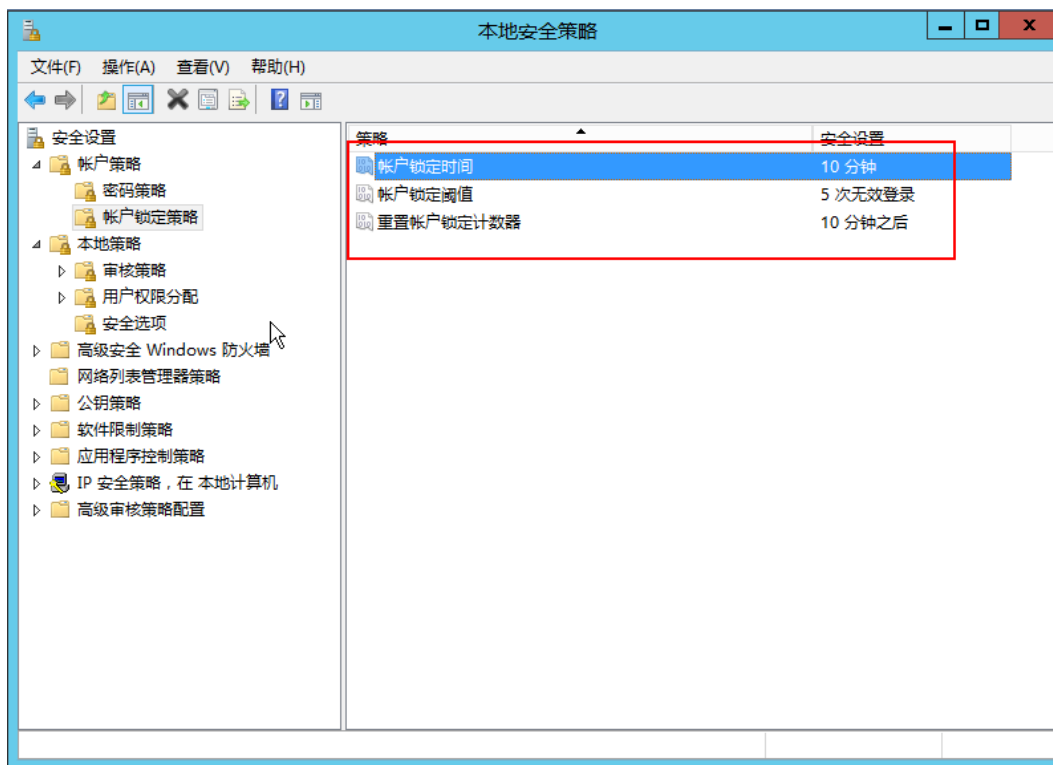
OS-Windows-口令锁定设置

要求内容：对于采用静态口令登录的主机，应配置主机当用户连续认证失败次数超过5次（不含5次），锁定该用户使用的账号。

操作指南：

进入“控制面板->管理工具->本地安全策略”，在“帐户策略->帐户锁定策略”：

“账户锁定阈值”设置为 5次，设置解锁阈值：10分钟。



检测方法：

进入“控制面板->管理工具->本地安全策略”，在“帐户策略->帐户锁定策略”：查看是否“账户锁定阈值”设置为小于等于5次，锁定时间是否已配置。

判定条件：“账户锁定阈值”设置为小于或等于5次，锁定时间配置为10分钟(或其它适

当时长)。

补充说明：设置不当可能导致账号大面积锁定，在域环境中应小心设置，

Administrator (系统管理账户) 账号本身不会被锁定。

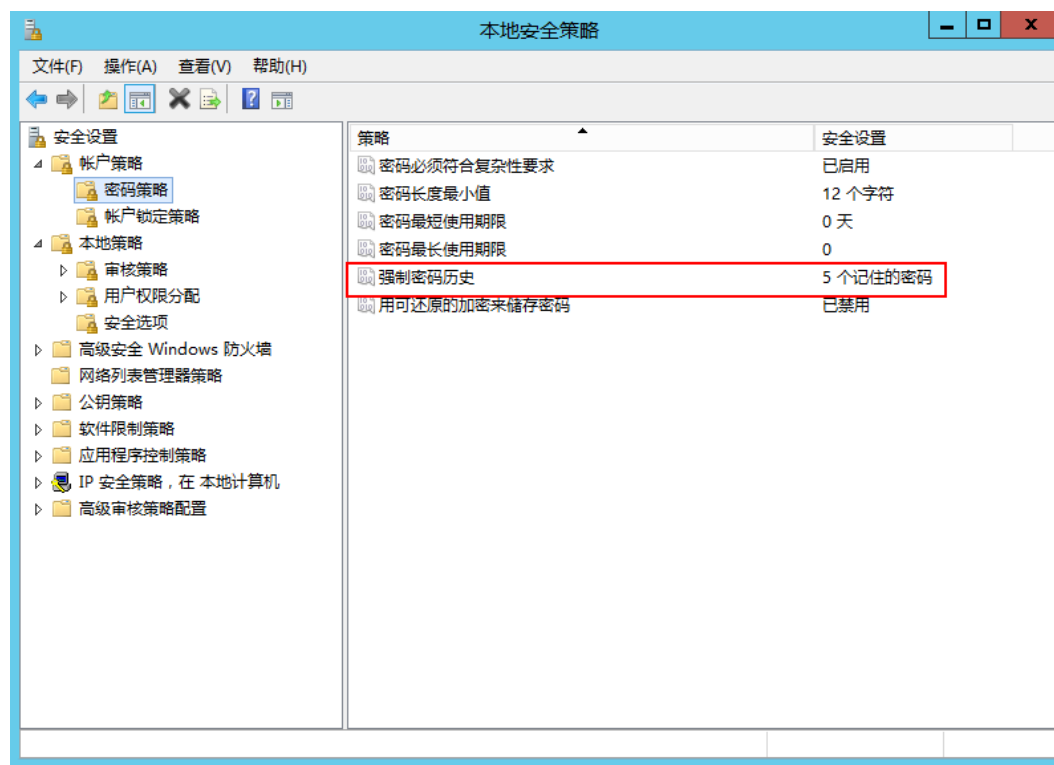
1.2.4 OS-Windows-口令历史记录校验设置

OS-Windows-口令历史记录校验设置

要求内容：对于采用静态口令登录的主机，应配置主机不能重复使用最近5次（含5次）内已使用的口令。

操作指南：

进入“控制面板->管理工具->本地安全策略”，在“帐户策略->密码策略”：“强制密码历史”设置为“记住5个密码”。



检测方法：

进入“控制面板->管理工具->本地安全策略”，在“帐户策略->密码策略”：查看是否“强制密码历史”设置为“记住5个密码”。

判定条件：“强制密码历史”设置为“记住5个密码”。

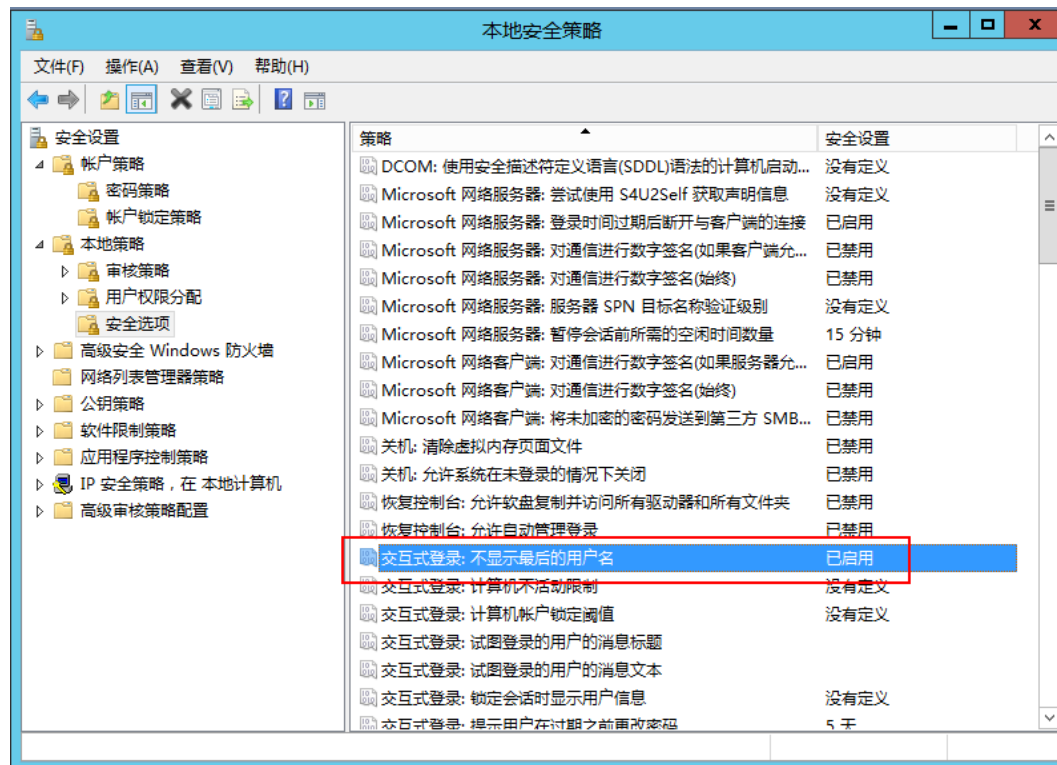
1.2.5 OS-Windows-最后登录帐号设置

OS-Windows-最后登录帐号设置

要求内容：不显示最后登录的用户名。

操作指南：

进入“控制面板->管理工具->本地安全策略”，打开“本地策略”->“安全选项”->选择“交互式登录:不显示最后的用户名”设置“已启用”。



检测方法：

进入“控制面板->管理工具->本地安全策略”，打开“本地策略”->“安全选项”->选择“交互式登录:不显示最后的用户名” 设置“已启用”。

判定条件：

相应配置项已正确配置。

1.2.6 OS-Windows-会话超时设置

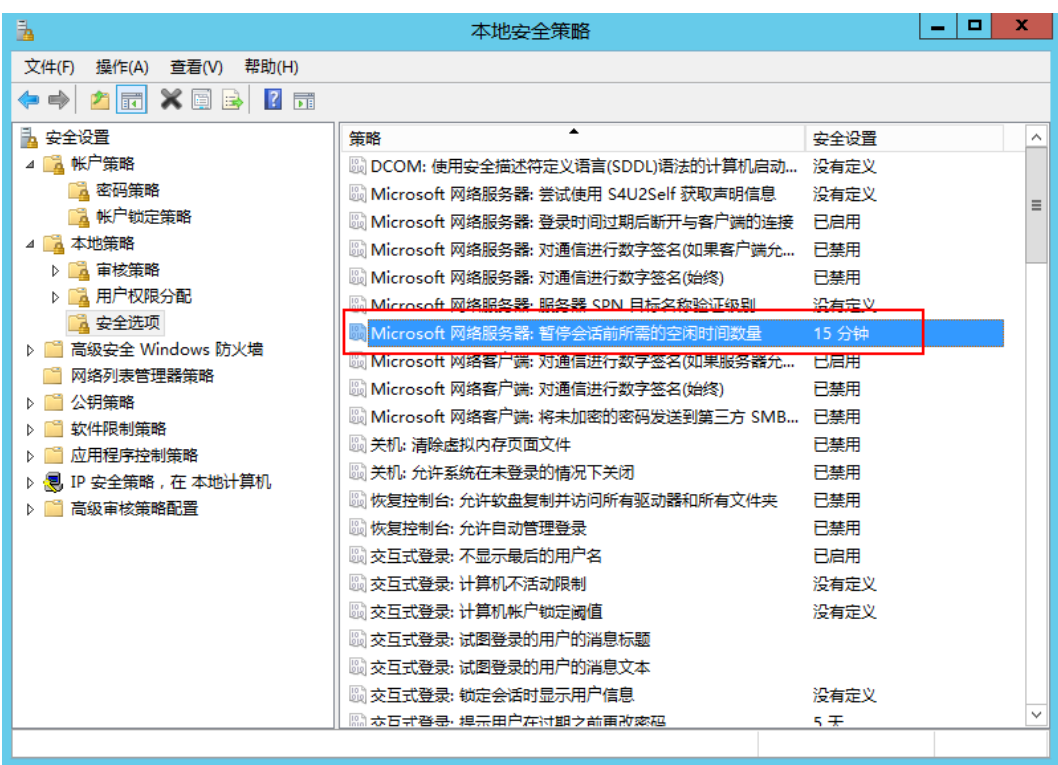
OS-Windows-会话超时设置

要求内容：对于远程登录的账户，设置不活动时，连接时间15分钟。

操作指南：

进入“控制面板—管理工具—本地安全策略”，在“本地策略—安全选项”：

“Microsoft 网络服务器” 设置为“暂停会话前所需的空闲时间” 为15分钟。

		
检测方法： 远程登录系统后闲置15分钟以上。		
判定条件： 会话自动断开为设置成功。		
补充说明： 测试时可以将15分钟的设置缩短进行测试。		

2 基础网络安全策略配置

本文档关注SSH-22，RDP-3389属于高危管理端口，一旦被攻破将可能造成极严重的损失；对于此类端口建议遵从“**最小化**”及“**默认失败**”安全原则，严格设置其访问控制策略，保证仅有业务需要的、可信的源可以访问，减小攻击面。

注：1. 以下策略建议，对于Linux仅需根据实际情况选择“安全组”或“iptables”实施访问控制策略，避免策略产生冲突；Windows系统以此类推。

加固项	推荐指数
ECS-Linux-安全组	★★★★★
OS-Linux-iptables	★★★★★
ECS-远程登录端口选择性对公网暴露- 堡垒机	★★★★★
ECS-远程登录端口选择性对公网暴露- VPN	★★★★★

加固项	推荐指数
ECS-Windows-安全组	★★★★★
OS-Windows-防火墙	★★★★★
ECS-远程登录端口选择性对公网暴露- 堡垒机	★★★★★
ECS-远程登录端口选择性对公网暴露- VPN	★★★★★

2.1 安全组

ECS-Linux-安全组
要求内容： 对于远程登录的终端，设置最小化访问控制策略（白名单），仅允许白名单内的终端登录云主机。

操作指南：

进入“华为云控制台—虚拟私有云—安全组”，找到待配置云主机所绑定的安全组，配置安全组策略：



如已参照1.1.6实践建议更改SSH端口，则在配置相应安全策略时，配置相同的端口。

该策略比较适合远端接入的IP较为固定的场景。

检测方法：

分别从白名单内、外源IP尝试SSH远程登录云主机。

判定条件：白名单内应能登录，白名单外无法登录。

补充说明：1. 如已参照1.1.6实践建议更改SSH端口，则在配置相应安全策略时，配置相同的端口。

2. 可针对有相同访问控制需求的云主机，绑定到同一安全组，方便统一管理、运维。

3. 安全组support文档：http://support.huaweicloud.com/usermanual-vpc/zh-cn_topic_0049500907.html。

ECS-Windows-安全组

内的终端登录云主机。

操作指南：

置安全组策略：

添加规则

✕

★ 方向:

入方向

出方向

★ 协议:

TCP

▼

★ 端口范围:

3389

★ 源地址:

IP地址

安全组

123.123.123.0

/

24

?

根据业务实际需求设置

确定

取消

检测方法：分别从白名单内、外源IP尝试RDP远程登录云主机。

判定条件：白名单内应能登录，白名单外无法登录。

理、运维。

cn_topic_0049500907.html。

2.2 Linux 之 iptables

OS-Linux-iptables

要求内容：对于远程登录的终端，设置最小化访问控制策略（白名单），仅允许白名单内的终端登录云主机。

操作指南：

1. 针对SSH端口(以22为例)，通过命令行顺序增加如下配置：(如是SSH登陆主机进行配置，请先阅读本节“补充说明”)

`iptables -I INPUT -p tcp --dport 22 -j DROP //【SSH-DROP】禁止所有IP访问该云主机22端口`

`iptables -I INPUT -s 123.123.123.0/24 -p tcp -dport 22 -j ACCEPT //【SSH-ACCEPT】允许123.123.123.0/24访问该云主机22端口`

2. 配置完保存，重启iptables

`service iptables save`

`service iptables restart`

3. 通过`iptables -L`命令查看当前策略，确保最终生效的策略顺序如下图所示：SSH-ACCEPT策略在前，SSH-DROP策略在后，否则由于匹配优先级原则，导致始终匹配DROP策略，SSH无法登录

```
[root@ecs-cjtest-centos-6-5 ~]# iptables -L
Chain INPUT (policy ACCEPT)
target    prot opt source                destination           tcp dpt:ssh
ACCEPT    tcp  --  123.123.123.0/24      anywhere              tcp dpt:ssh
DROP      tcp  --  anywhere              anywhere              tcp dpt:ssh

Chain FORWARD (policy ACCEPT)
target    prot opt source                destination

Chain OUTPUT (policy ACCEPT)
target    prot opt source                destination
```

检测方法：分别从白名单内、外源IP尝试SSH远程登录该云主机。

判定条件：白名单内应能登录成功，白名单外无法登录。

补充说明：1. 如果你是远程SSH登陆的话,当你输入第一个命令后会终端SSH连接，导致

无法登录主机，建议通过华为云控制台，“远程登录”进行配置。

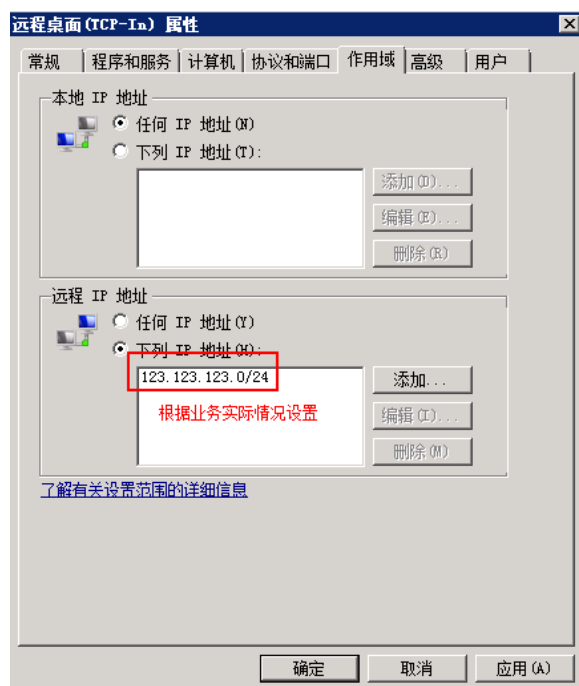
2.3 Windows 之防火墙

OS-Windows-防火墙

要求内容：对于远程登录的终端，设置最小化访问控制策略（白名单），仅允许白名单内的终端登录云主机。

操作指南：

进入“控制面板—系统和安全—Windows防火墙-高级设置-入站规则”，找到“远程桌面(TCP-in)”：修改“作用域-远程IP地址”为允许远程登录该主机的地址。



检测方法：分别从白名单内、外源IP尝试RDP远程登录该云主机。

判定条件：白名单内应能登录成功，白名单外无法登录。

补充说明：1. 如远程IP配置失误将导致无法远程登录，建议通过华为云控制台，“远程

登录”进行配置更新。

2.4 远程登录端口选择性对公网暴露

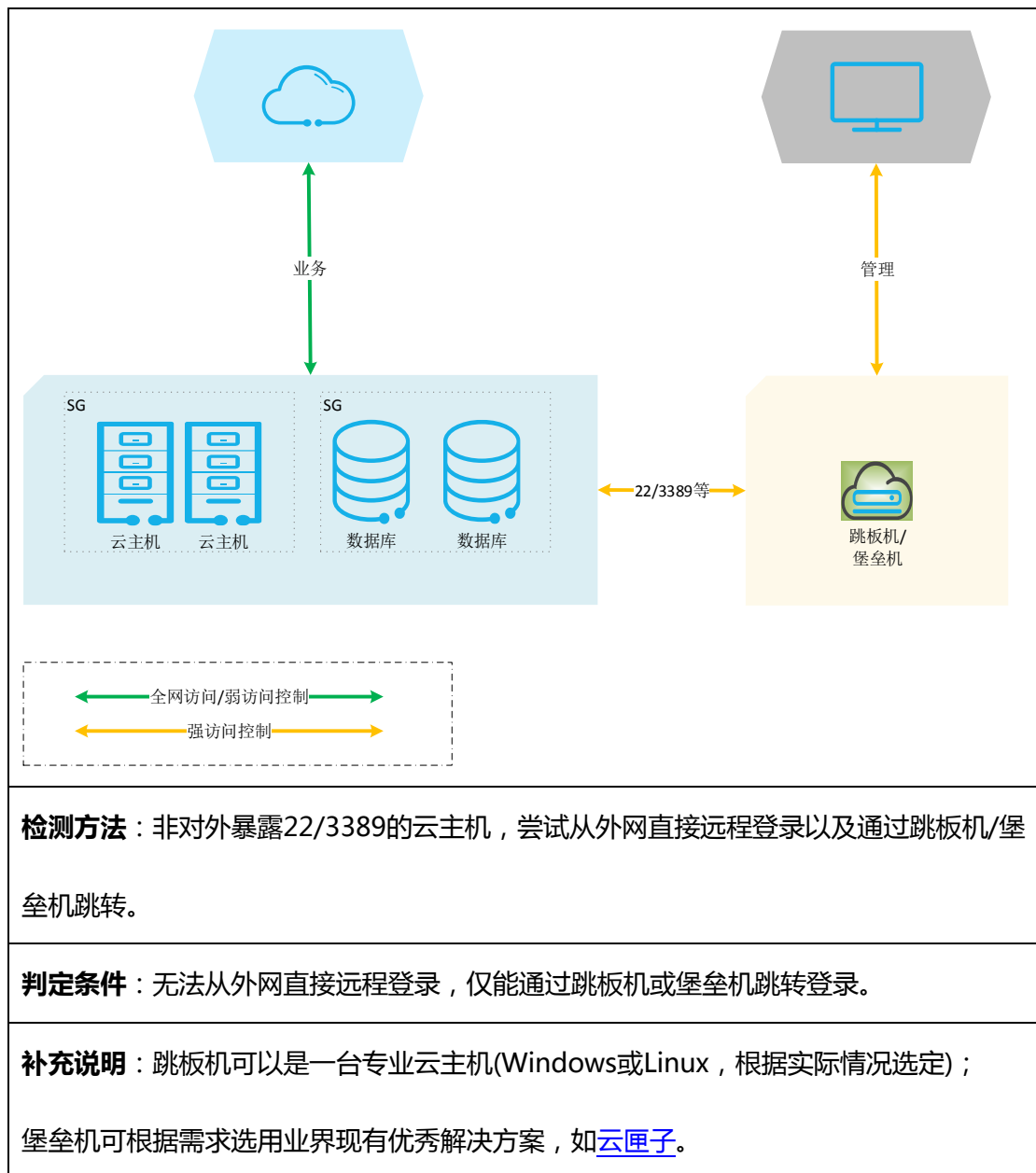
ECS-远程登录端口选择性对公网暴露-堡垒机

要求内容：仅选择必须对公网暴露SSH/RDP端口的云主机按照2.1/2.2/2.3建议设置访问控制策略，而其它ECS不对外暴露SSH/RDP端口，通过部署跳板机或堡垒机进行跳转访问、管理。

跳板机或堡垒机管理端口，建议遵从2.1思想设置访问控制策略。

操作指南：

- 1 必须对外暴露SSH/RDP端口的云主机，建议参考2.1/2.2/2.3设置访问控制策略；
 - 2 其它云主机，可参考按照如下组网建议部署跳板机或堡垒机，进行跳转访问与管理；
- 删除相应云主机所绑定的安全组中的22/3389的入方向策略。



ECS-远程登录端口选择性对公网暴露-VPN

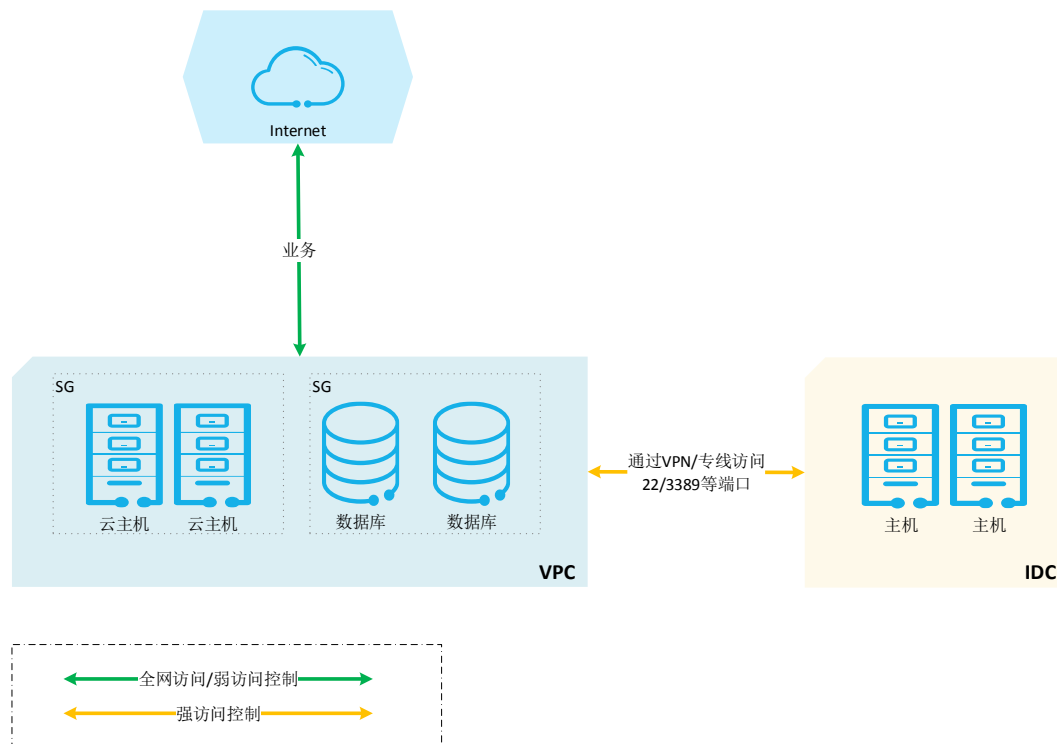
要求内容: 仅选择必须对公网暴露SSH/RDP端口的云主机按照2.1/2.2/2.3建议设置访问控制策略, 而其它ECS不对外暴露SSH/RDP端口, 通过VPN与云下系统互联。

操作指南:

1 必须对外暴露SSH/RDP端口的云主机, 建议参考2.1/2.2/2.3设置访问控制策略;

2 其它云主机，可参考按照如下组网建议使用VPN或专线，与云下系统互联(如IDC)；

配置相应安全组策略，放通云下系统IP端可访问云主机22/3389端口；



产品推荐：

华为云[VPN](#)，[专线\(DC\)](#)

检测方法：非对外暴露22/3389的云主机，尝试从外网直接远程登录以及通过IDC内网主机进行登录。

判定条件：无法从外网直接远程登录，仅能通过IDC内网主机进行登录。

补充说明：为部署VPN或专线业务，需要云下系统(如IDC)具备相应的设备或系统(如防火墙设备)与华为云上VPC建立VPN隧道，详情请见产品页面或咨询客服。

3 主机安全进阶方案

3.1 主机安全防护

ECS-Linux-主机安全防护
要求内容： 使用主机安全产品，对SSH爆破进行检测和防御。
使用场景： 对关键云主机(如公网可访问的云主机)，部署业界现有的主机安全产品，对暴力破解攻击进行防御。 同时此类主机安全产品还能提供弱口令扫描、异地登录检测、主机漏洞检测、恶意程序检测等特性，全面增加云主机安全性。 产品推荐： 华为云 主机安全服务HSS ， 服务器安全狗(Linux版)
补充说明： 1. 产品详细特性、部署、配置等信息请见产品页面或咨询客服。

ECS-Windows-主机安全防护
要求内容： 使用主机安全产品，对RDP爆破进行检测和防御。
使用场景： 对关键云主机(如公网可访问的云主机)，部署业界现有的主机安全产品，对暴力破解攻击进行防御。 同时此类主机安全产品还能提供弱口令扫描、异地登录检测、主机漏洞检测、恶意程序检测等特性，全面增加云主机安全性。

产品推荐：

[服务器安全狗\(Windows版\)-华为云专用版](#)

补充说明：1. 产品详细特性、部署、配置等信息请见产品页面或咨询客服；2. 华为主机安全服务HSS(基础版&专业版当前暂仅支持Linux，相应Windows版本即将上线，敬请期待)。

3.2 云主机系统登录双因素认证

ECS-Linux-系统登录双因素认证

要求内容：使用更加安全的双因素身份认证方式，提高远程访问Linux操作系统的安全。

使用场景：可提供两种认证方式，动态口令认证和推送认证。

动态口令认证：远程登录时，需要输入由手机令牌或硬件令牌产生的动态口令，才能登录成功。



推送认证：远程登录时，输入“push”，绑定的手机会收到授权信息，点击“√”或摇一摇手机才能登录成功，否则登录失败。



产品推荐：

[Linux系统登录保护助手](#)

检测方法：尝试SSH远程登录该云主机。

判定条件：需进行相应的认证后(动态口令认证和推送认证)才能登录。

补充说明：1. 产品详细部署、配置请见产品页面或咨询客服；

ECS-Windows-系统登录双因素认证

要求内容：使用更加安全的双因素身份认证方式，提高远程访问Windows操作系统的安全。

使用场景：两种可选认证方式，分别为动态口令认证和推送认证。

动态口令认证：登录时，输入用户名和密码后，提示“安全认证，输入口令”需要输入手机令牌或硬件令牌产生的动态口令，如下图：



推送认证：登录时，输入用户名和密码后，提示“等待推送恢复中.....”，绑定的手机会收到授权信息，点击“√”或摇一摇手机才能登录成功，否则登录失败，如下图：



产品推荐：

[Windows系统登录保护助手](#)

检测方法：尝试RDP远程登录该云主机。

判定条件：需进行相应的认证后(动态口令认证和推送认证)才能登录。

补充说明：1. 产品详细部署、配置请见产品页面或咨询客服；

3.3 安全评估

ECS-安全评估

要求内容：建议周期性对业务站点进行安全评估，及时规避弱口令安全风险。

使用场景：

业务系统常有变更、扩容等场景，经常会引入新账户，或修改已有账户口令；人员操作失误、或安全意识低，可能引入弱口令风险；

建议周期性，或重大变更后，使用“专家式”安全评估服务，对业务系统进行整体评

估，及时发现、解决弱口令问题；

另外，此类服务还能够提供常见Web漏洞(SQL注入、XSS等)等其它评估项，多角度审视业务系统安全性。

对于常规自动化安全检查常见，可使用华为云Web漏洞扫描服务，覆盖常见OWASP

TOP10漏洞检测，以及弱密码扫描。

服务推荐：

[安全体检服务](#)、[Web漏洞扫描](#)

补充说明：1. 产品详细部署、配置请见产品页面或咨询客服。

4 加固脚本使用说明

4.1 Linux 加固脚本

4.1.1 简介

```
#####
#                                     Menu                                     #
#      1:ALL                          #
#      2:Set Password Complexity Requirements                             #
#      3:Set Remote Login Configuration(SSH)                             #
#      4:Set Shell History and TMOUT                                       #
#      5:Set Key Login(SSH)                                                #
#      6:Set SSH Port                                                       #
#      7:Set Su User                                                        #
#      8:Recover Configuration                                             #
#      9:Exit                                                                #
#####
Please choice[1-9]:
```

如上图所示，Linux版加固脚本提供1.1章节中涉及的所有加固项配置功能，及配置备份与恢复功能。

4.1.2 配置备份与恢复

备份：脚本在首次执行时会将系统配置保存于脚本所在目录下的backup目录下（如下图），以便后续需要恢复配置时使用。再次运行脚本时，将不会再进行备份，除非原备份目录被删除。

Note：当OS type检测为unknown时，请谨慎使用该脚本。

```
[root@ecs-cjtest-centos7-4 ~]# sh main.sh
OS type is centos
Auto backup successfully

#####
#                                     Menu                                     #
#                                     #                                     #
# 1:ALL                             #                                     #
# 2:Set Password Complexity Requirements #                                     #
# 3:Set Remote Login Configuration(SSH) #                                     #
# 4:Set Shell History and TMOUT        #                                     #
# 5:Set Key Login(SSH)                 #                                     #
# 6:Set SSH Port                       #                                     #
# 7:Set Su User                        #                                     #
# 8:Recover Configuration              #                                     #
# 9:Exit                              #                                     #
#####
Please choice[1-9]:
```

```
[root@ecs-cjtest-centos7-4 ~]# ls | grep backup
backup
[root@ecs-cjtest-centos7-4 ~]# sh main.sh
OS type is centos
Backup file already exist, to avoid overwriting these files, backup will not perform again

#####
#                                     Menu                                     #
#                                     #                                     #
# 1:ALL                             #                                     #
# 2:Set Password Complexity Requirements #                                     #
# 3:Set Remote Login Configuration(SSH) #                                     #
# 4:Set Shell History and TMOUT        #                                     #
# 5:Set Key Login(SSH)                 #                                     #
# 6:Set SSH Port                       #                                     #
# 7:Set Su User                        #                                     #
# 8:Recover Configuration              #                                     #
# 9:Exit                              #                                     #
#####
Please choice[1-9]:
```

恢复：如有需要恢复配置时，请运行脚本，选择‘8’进行配置恢复；配置恢复后，可能需要SSH服务，请按照提示手动进行重启。

Note：针对加固项7“Set su user”，配置恢复功能，无法恢复用户所属group，需

要手动恢复。

```
[root@ecs-cjtest-centos7-4 ~]# sh main.sh
OS type is centos
Backup file already exist, to avoid overwriting these files, backup will not perform again

#####
#                               Menu                               #
#####
#      1:ALL                    #
#      2:Set Password Complexity Requirements                    #
#      3:Set Remote Login Configuration(SSh)                    #
#      4:Set Shell History and TMOUT                            #
#      5:Set Key Login(SSh)                                     #
#      6:Set SSh Port                                           #
#      7:Set Su User                                             #
#      8:Recover Configuration                                  #
#      9:Exit                                                    #
#####
Please choice[1-9]:8
Recover success
Please restart SSh service manually by using 'service sshd restart' or '/etc/init.d/ssh restart'
[root@ecs-cjtest-centos7-4 ~]#
```

4.1.3 密码复杂度设置

选择 '2' 进行密码复杂度配置，脚本会根据实践文档建议自动进行配置(口令长度建议不少于**12位**，并包括**数字、小写字母、大写字母和特殊符号4类字符**)；如需自定义配置，请按照1.1.1节步骤手动进行配置。

```
[root@ecs-cjtest-centos7-4 ~]# sh main.sh
OS type is centos
Backup file already exist, to avoid overwriting these files, backup will not perform again

#####
#                               Menu                               #
#####
#      1:ALL                    #
#      2:Set Password Complexity Requirements                    #
#      3:Set Remote Login Configuration(SSh)                    #
#      4:Set Shell History and TMOUT                            #
#      5:Set Key Login(SSh)                                     #
#      6:Set SSh Port                                           #
#      7:Set Su User                                             #
#      8:Recover Configuration                                  #
#      9:Exit                                                    #
#####
Please choice[1-9]:2
#####
set password complexity requirements
[success]
[root@ecs-cjtest-centos7-4 ~]#
```

4.1.4 SSH 远程登录相关安全配置

选择 '3' 进行SSH远程登录相关安全配置，脚本会自动配置SSH协议为2，然后根据

用户输入配置“是否禁止root登录”、“允许登录的用户”等配置。

Note：禁止root登录前，请确保已经有至少一个普通用户可用于远程登录；执行此加

固项后需重启SSH服务。

```
[root@ecs-cjtest-centos7-4 ~]# sh main.sh
OS type is centos
Backup file already exist, to avoid overwriting these files, backup will not perform again

#####
#                               Menu                               #
#                               #                                   #
# 1:ALL                         #                                   #
# 2:Set Password Complexity Requirements #                                   #
# 3:Set Remote Login Configuration{SSH} #                                   #
# 4:Set Shell History and TMOUT        #                                   #
# 5:Set Key Login{SSH}                 #                                   #
# 6:Set SSH Port                       #                                   #
# 7:Set Su User                        #                                   #
# 8:Recover Configuration              #                                   #
# 9:Exit                              #                                   #
#####
Please choice[1-9]:3
#####
set remote user login
[Success: Set SSH Protocol to 2]
disable root remote login?[y/n](Please make sure you have created at least one another account):y
[success]
set max login tries?[y/n]:y
please input the max login tires(recommend to 3-10):3
[success]
set allow users?[y/n]:y
Currentlly AllowUsers is:
please input allow users,for example: test1 test2 test3, it will overwrite the current configuration :test
[success]
Please restart SSH service manully by using 'service sshd restart' or '/etc/init.d/ssh restart'
[root@ecs-cjtest-centos7-4 ~]#
```

4.1.5 history & TMOUT 相关配置

选择‘4’进行history & TMOUT配置，脚本会根据最佳实践建议自动配置HISTSIZE

和HISTTIMEFORMAT，然后根据用户输入配置会话超时时间。

```
[root@ecs-cjtest-centos7-4 ~]# sh main.sh
OS type is centos
Backup file already exist, to avoid overwriting these files, backup will not perform again

#####
#                                     Menu                                     #
#                                     #                                     #
#      1:ALL                          #                                     #
#      2:Set Password Complexity Requirements                             #
#      3:Set Remote Login Configuration(SSH)                             #
#      4:Set Shell History and TMOUT                                       #
#      5:Set Key Login(SSH)                                                #
#      6:Set SSH Port                                                       #
#      7:Set Su User                                                        #
#      8:Recover Configuration                                             #
#      9:Exit                                                                #
#####
Please choice[1-9]:4
#####
set history
set history size, format, and TMOUT?[y/n]:y
HISTSIZE has been set to 1000
HISTTIMEFORMAT has been set to "%F %T `whoami`"
set shell TMOUT?[300-600]seconds:300
[success]
[root@ecs-cjtest-centos7-4 ~]#
```

4.1.6 SSH 秘钥登录配置

选择 ‘5’ 进行SSH秘钥登录配置，脚本会根据最佳实践建议自动配置SSH配置文件，然后根据用户输入注入相应的公钥。

Note：在进行该项加固前，请务必主备好可用的公私钥对，详细生成方法见1.1.4

节；执行此加固项后需重启SSH服务。

```
[root@ecs-cjtest-centos7-4 ~]# sh main.sh
OS type is centos
Backup file already exist, to avoid overwriting these files, backup will not perform again

#####
#                                     Menu                                     #
#                                     #                                     #
#      1:ALL                          #                                     #
#      2:Set Password Complexity Requirements                             #
#      3:Set Remote Login Configuration(SSH)                             #
#      4:Set Shell History and TMOUT                                       #
#      5:Set Key Login(SSH)                                                #
#      6:Set SSH Port                                                       #
#      7:Set Su User                                                        #
#      8:Recover Configuration                                             #
#      9:Exit                                                                #
#####
Please choice[1-9]:5
#####
set login key
set login key?[y/n]y
Please input the directory of the public key file(such as /root/.id_rsa.pub): /root/test.pub
[Success: you can login using Root with the right private key after restarting SSH service]
Please restart SSH service manually by using 'service sshd restart' or '/etc/init.d/ssh restart'
[root@ecs-cjtest-centos7-4 ~]# service sshd restart
Redirecting to /bin/systemctl restart sshd.service
[root@ecs-cjtest-centos7-4 ~]#
```

4.1.7 SSH 端口配置

选择 ‘6’ 进行SSH服务端口配置，脚本会根据用户输入配置相应的端口，当用户输入的端口已被占用时，脚本会给出提示，要求用户重新选择。

Note：执行此加固项后需重启SSH服务。

```
[root@ecs-cjtest-centos7-4 ~]# sh main.sh
OS type is centos
Backup file already exist, to avoid overwriting these files, backup will not perform again

#####
#                               Menu                               #
#                               #                                   #
#       1:ALL                    #                                   #
#       2:Set Password Complexity Requirements                    #                                   #
#       3:Set Remote Login Configuration(SSH)                    #                                   #
#       4:Set Shell History and TMOUT                             #                                   #
#       5:Set Key Login(SSH)                                       #                                   #
#       6:Set SSH Port                                             #                                   #
#       7:Set Su User                                              #                                   #
#       8:Recover Configuration                                    #                                   #
#       9:Exit                                                      #                                   #
#####
Please choice[1-9]:6
#####
set ssh port
change ssh port?[y/n]:y
please input the new ssh port(recommend to larger than 1000, please make sure the port is not in used):25
The port 25 is already in used, try again
#####
set ssh port
change ssh port?[y/n]:y
please input the new ssh port(recommend to larger than 1000, please make sure the port is not in used):22222
[success]
[success]
Please restart SSH service manually by using 'service sshd restart' or '/etc/init.d/ssh restart'
[root@ecs-cjtest-centos7-4 ~]#
```

4.1.8 su 权限配置

选择 ‘7’ 进行su权限配置，脚本会根据用户输入配置相应的用户拥有su权限。

Note：执行此加固项前请确保相应的用户已经创建成功；执行后，相应用户会加入

wheel组；恢复配置功能，无法恢复用户所属group，需要手动恢复。

```
[root@ecs-cjtest-centos7-4 ~]# sh main.sh
OS type is centos
Backup file already exist, to avoid overwriting these files, backup will not perform again

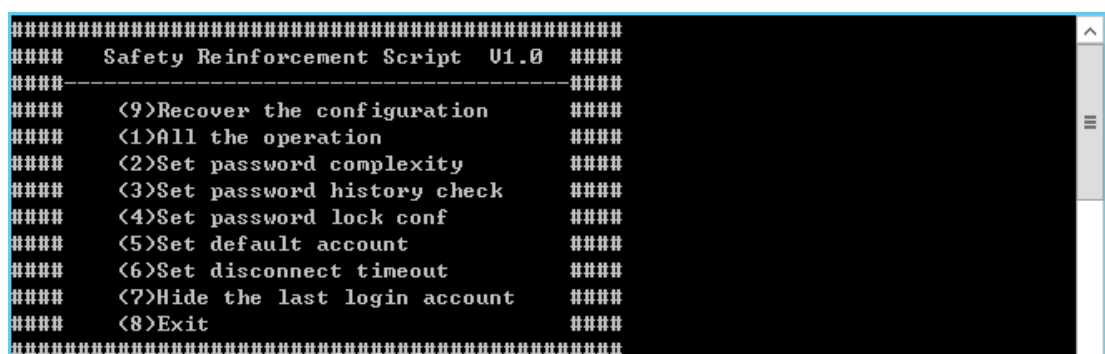
#####
#                               Menu                               #
#                               #
#       1:ALL                   #
#       2:Set Password Complexity Requirements                   #
#       3:Set Remote Login Configuration(SSH)                   #
#       4:Set Shell History and TMOUT                           #
#       5:Set Key Login(SSH)                                     #
#       6:Set SSH Port                                           #
#       7:Set Su User                                            #
#       8:Recover Configuration                                  #
#       9:Exit                                                   #
#####
Please choice[1-9]:7
#####
Set which user can su to root
set su conf[y/n]:y
please input the user:test
[success]
[root@ecs-cjtest-centos7-4 ~]#
```

4.1.9 全部加固

选择 ‘1’ 进行全部加固，脚本会自动按2-7顺序执行加固动作，如上文描述，部分参数需要用户手动输入。

4.2 Windows 加固脚本

4.2.1 简介



```
#####
####  Safety Reinforcement Script  V1.0  ####
####-----####
####  <9>Recover the configuration          ####
####  <1>All the operation                  ####
####  <2>Set password complexity           ####
####  <3>Set password history check        ####
####  <4>Set password lock conf            ####
####  <5>Set default account                ####
####  <6>Set disconnect timeout             ####
####  <7>Hide the last login account        ####
####  <8>Exit                              ####
#####
```

如上图所示，Windows版加固脚本提供1.2章节中涉及的所有加固项配置功能，及配置备份与恢复功能。

Note：脚本执行后需重启系统使配置生效。


```
#####
####  Safety Reinforcement Script  V1.0  ####
#####-----#####
####  (9)Recover the configuration      ####
####  (1)All the operation              ####
####  (2)Set password complexity       ####
####  (3)Set password history check    ####
####  (4)Set password lock conf        ####
####  (5)Set default account           ####
####  (6)Set disconnect timeout        ####
####  (7)Hide the last login account    ####
####  (8)Exit                          ####
#####
System policy files have been backed up under C:\policy.cfg, and this backup file
can be used if you need a recovery policy
Please enter the option:9
任务成功结束。
有关详细信息，请参阅日志 %windir%\security\logs\scserv.log。
Please enter the option:
```

4.2.3 口令复杂度设置

选择 ‘2’ 进行口令复杂度配置，脚本会根据实践文档建议自动进行配置；如需自定义配置，请按照1.2.1节步骤手动进行配置。

```
#####
####  Safety Reinforcement Script  V1.0  ####
#####-----#####
####  (9)Recover the configuration      ####
####  (1)All the operation              ####
####  (2)Set password complexity       ####
####  (3)Set password history check    ####
####  (4)Set password lock conf        ####
####  (5)Set default account           ####
####  (6)Set disconnect timeout        ####
####  (7)Hide the last login account    ####
####  (8)Exit                          ####
#####
System policy files have been backed up under C:\policy.cfg, and this backup file
can be used if you need a recovery policy
Please enter the option:2
The minimum length of the password is 12 characters and the password complexity
is checked.
Please enter the option: _
```

4.2.4 口令历史记录校验设置

选择 ‘3’ 进行口令历史记录校验配置，脚本会根据实践文档建议自动进行配置；如需自定义配置，请按照1.2.4节步骤手动进行配置。


```
#####
####  Safety Reinforcement Script  V1.0  ####
#####-----#####
####  <9>Recover the configuration          ####
####  <1>All the operation                  ####
####  <2>Set password complexity           ####
####  <3>Set password history check        ####
####  <4>Set password lock conf            ####
####  <5>Set default account                ####
####  <6>Set disconnect timeout            ####
####  <7>Hide the last login account       ####
####  <8>Exit                              ####
#####
System policy files have been backed up under C:\policy.cfg, and this backup file
can be used if you need a recovery policy
Please enter the option:3
Password history check setting is enabled, and the password is not the same with
in 5 times.
Please enter the option: _
```

4.2.5 口令锁定设置

选择 ‘4’ 进行口令锁定配置，脚本会根据实践文档建议自动进行配置；如需自定义配置，请按照1.2.3节步骤手动进行配置。

```
#####
####  Safety Reinforcement Script  V1.0  ####
#####-----#####
####  <9>Recover the configuration          ####
####  <1>All the operation                  ####
####  <2>Set password complexity           ####
####  <3>Set password history check        ####
####  <4>Set password lock conf            ####
####  <5>Set default account                ####
####  <6>Set disconnect timeout            ####
####  <7>Hide the last login account       ####
####  <8>Exit                              ####
#####
System policy files have been backed up under C:\policy.cfg, and this backup file
can be used if you need a recovery policy
Please enter the option:4
Password lock setting is completed, password input is locked after 5 failures, a
nd unlock time is 10 minutes.
Please enter the option: _
```

4.2.6 系统默认账户设置

选择 ‘5’ 进行系统默认账户配置，脚本会根据实践文档建议自动进行配置，以及根据用户输入重命名管理员账户，详见1.2.2节。

Note：脚本执行后，请务必记住管理员账户名，否则将无法登录系统。

```
#####
####  Safety Reinforcement Script  V1.0  ####
#####-----#####
####  (9)Recover the configuration      ####
####  (1)All the operation              ####
####  (2)Set password complexity        ####
####  (3)Set password history check     ####
####  (4)Set password lock conf         ####
####  (5)Set default account            ####
####  (6)Set disconnect timeout         ####
####  (7)Hide the last login account    ####
####  (8)Exit                           ####
#####
System policy files have been backed up under C:\policy.cfg, and this backup file
can be used if you need a recovery policy
Please enter the option:5
[*]Notice[*],Keep in mind the name of the new administrator account!
Please Input New Administrator Name:cjTest
[*]Notice[*],Default account consolidation completion,Please keep in mind!
Please enter the option:
```

4.2.7 会话超时设置

选择 ‘6’ 进行会话超时配置，脚本会根据实践文档建议自动进行配置；如需自定义配置，请按照1.2.6节步骤手动进行配置。

```
#####
####  Safety Reinforcement Script  V1.0  ####
#####-----#####
####  (9)Recover the configuration      ####
####  (1)All the operation              ####
####  (2)Set password complexity        ####
####  (3)Set password history check     ####
####  (4)Set password lock conf         ####
####  (5)Set default account            ####
####  (6)Set disconnect timeout         ####
####  (7)Hide the last login account    ####
####  (8)Exit                           ####
#####
System policy files have been backed up under C:\policy.cfg, and this backup file
can be used if you need a recovery policy
Please enter the option:6
Completion of session reinforcement:Set disconnect timeout.
Please enter the option:
```

4.2.8 最后登录账号设置

选择 ‘7’ 进行最后登录账号配置，脚本会根据实践文档建议自动进行配置；如需自定义配置，请按照1.2.5节步骤手动进行配置。

```
#####
####  Safety Reinforcement Script  V1.0  ####
#####-----#####
####  <9>Recover the configuration          ####
####  <1>All the operation                  ####
####  <2>Set password complexity           ####
####  <3>Set password history check        ####
####  <4>Set password lock conf            ####
####  <5>Set default account                ####
####  <6>Set disconnect timeout            ####
####  <7>Hide the last login account       ####
####  <8>Exit                              ####
#####
System policy files have been backed up under C:\policy.cfg, and this backup file
can be used if you need a recovery policy
Please enter the option:7
Completion of session reinforcement:Hide the last login account.
Please enter the option: _
```

4.2.9 全部加固

选择 ‘1’ 进行全部加固，脚本会自动按2-7顺序执行加固动作，如上文描述，部分参数需要用户手动输入。

4.3 加固脚本支持系统列表

Note：以下系统均基于华为公有云公有镜像验证，非此场景，请在测试环境充分验证后，再操作生产环境。

4.3.1 Linux

CentOS：6.3 64bit、6.5 64 bit、6.8 64bit、6.9 64bit、7.0 64bit、7.1 64bit、7.2

64bit、7.3 64bit、7.4 64bit

Ubuntu：14.04 32/64bit、16.04 64bit

Debian：7.5.0 32bit、7.5.0 64bit、8.2 64bit、8.8.0 64bit、9.0.0 64bit

Fedora：24 64bit、25 64bit

Suse Enterprise：11 SP4 64bit、12 SP1 64bit、12 SP2 64bit

OpenSUSE : 13.2 64bit、42.2 64bit

EulerOS : 2.2 64bit

4.3.2 Windows

2016 DC 64bit(EN)、2016 DC 64bit、2016 Standard 64bit(EN)、2016 Standard 64bit、2012 R2 Standard 64bit、2012 R2 Standard 64bit(EN)、2012 R2 DC 64bit、2012 R2 DC 64bit(EN)、2008 WEB R2 64bit、2008 R2 Standard 64bit、2008 R2 Standard 64bit(EN)、2008 R2 Enterprise 64bit、2008 R2 Enterprise 64bit(EN)、2008 R2 DC 64bit、2008 Enterprise SP2 64bit

5 解决方案咨询

为了您能获得更好的服务，请访问以下[咨询页面](#)，选择合适的方式联系华为云，华为云专家会在三个工作日内联系您，为您提供咨询、解决方案等服务，感谢您对华为云的支持！

附录 1：相关产品/服务

产品/服务名称	分类	链接	相关章节
弹性云服务器 (ECS)	IaaS	http://www.huaweicloud.com/product/ecs.html	全文
安全组、虚拟私	IaaS	http://www.huaweicloud.com/product/vpc	2.1/2.4

有云(VPC)		.html	
虚拟专用网络 (VPN)	IaaS	http://www.huaweicloud.com/product/vpn.html	2.4
云专线DC	IaaS	http://www.huaweicloud.com/product/dc.html	2.4
主机安全服务 (HSS)	主机安全	http://www.huaweicloud.com/product/hss.html	3.1
安全体检服务 (SAS)	安全管理	http://www.huaweicloud.com/product/sas.html	3.3
Web漏洞扫描 (WebScan)	安全管理	http://www.huaweicloud.com/product/webscan.html	3.3
服务器安全狗	主机安全	Windows版： https://app.huaweicloud.com/product/41b3f256080e4142877d8d3b158b2302 Linux版： https://app.huaweicloud.com/product/ff0b4e533e5a41c5afc84580a7fb7f1f	3.1
系统登录保护助手	双因素认证	Windows版： https://app.huaweicloud.com/product/46748b4ad8054b56b33d19d7c27c0349 Linux版：	3.2

		https://app.huaweicloud.com/product/f3938413943a453f884ddf279a5d7cb2	
云匣子	安全管理	https://app.huaweicloud.com/seller/48b5438cbf57416bb3a949fef7c9e51d	2.4