关键安全配置解析

— 安全运维: 风险评估

NSFOCUS

安全配置

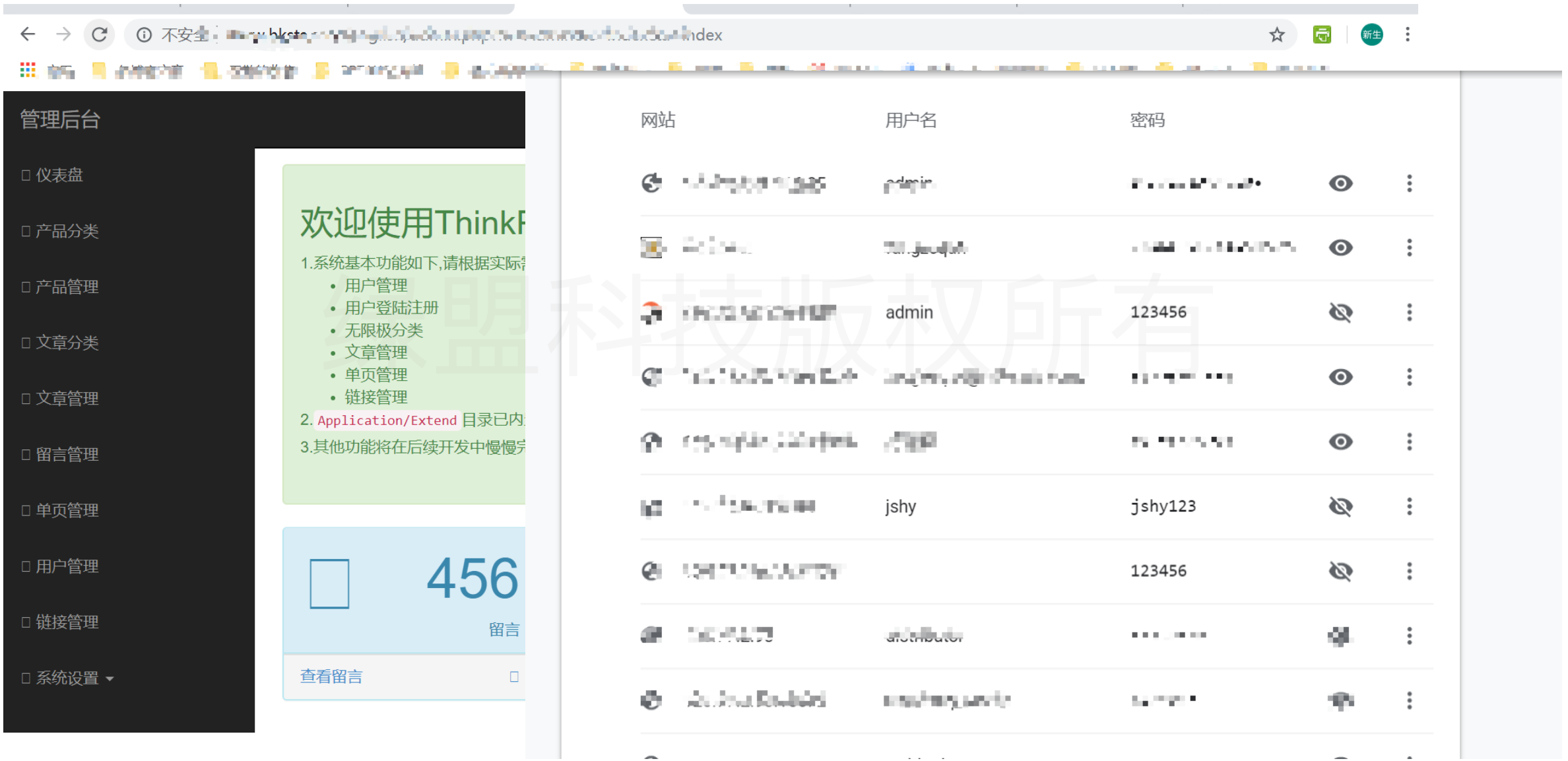
什么是安全配置

网络系统中存在服务器，路由器，防火墙，数据库等硬件与软件系统，这些系统由于设计缺陷和管理员的误操作等因素存在相当的安全隐患，安全配置旨在通过**一定的配置操作，解决或者降低这些安全隐患所带来的安全风险。**

安全配置

安全配置

安全配置


不安全
index
管理后台
仪表盘
产品分类
产品管理
文章分类
文章管理
留言管理
单页管理
用户管理
链接管理
系统设置
欢迎使用ThinkP
1.系统基本功能如下,请根据实际
用户管理
用户登陆注册
无限极分类
文章管理
单页管理
链接管理
2. Application/Extend 目录已内
3.其他功能将在后续开发中慢慢
456
留言
查看留言
网站
用户名
密码
admin
123456
jshy
jshy123
123456

安全配置

限制

通过一定的配置，对操作者访问系统上的资源进行一定的条件限制，如必须具有某些权限，必须处于登陆状态等。

加强

通过一定的配置，对各种访问限定条件进行加强，如登陆口令复杂度，记录日志的详细程度等。.

审计

通过一定的配置，将何时何地何人做何动作进行记录，并且存储到对应的文件中，用于事件回溯，出错排查等。

CONTENTS 目 录

01

Windows 安全配置解析

1. 安全防护机制简述
2. 安全配置分类说明
3. 核心安全配置作用及参数

NSFOCUS

1.1

安全防护机制简述

a. 认证和授权
b. 日志审计
c. 协议过滤及防火墙
d. 文件加密

安全防护机制简述 – 认证与授权

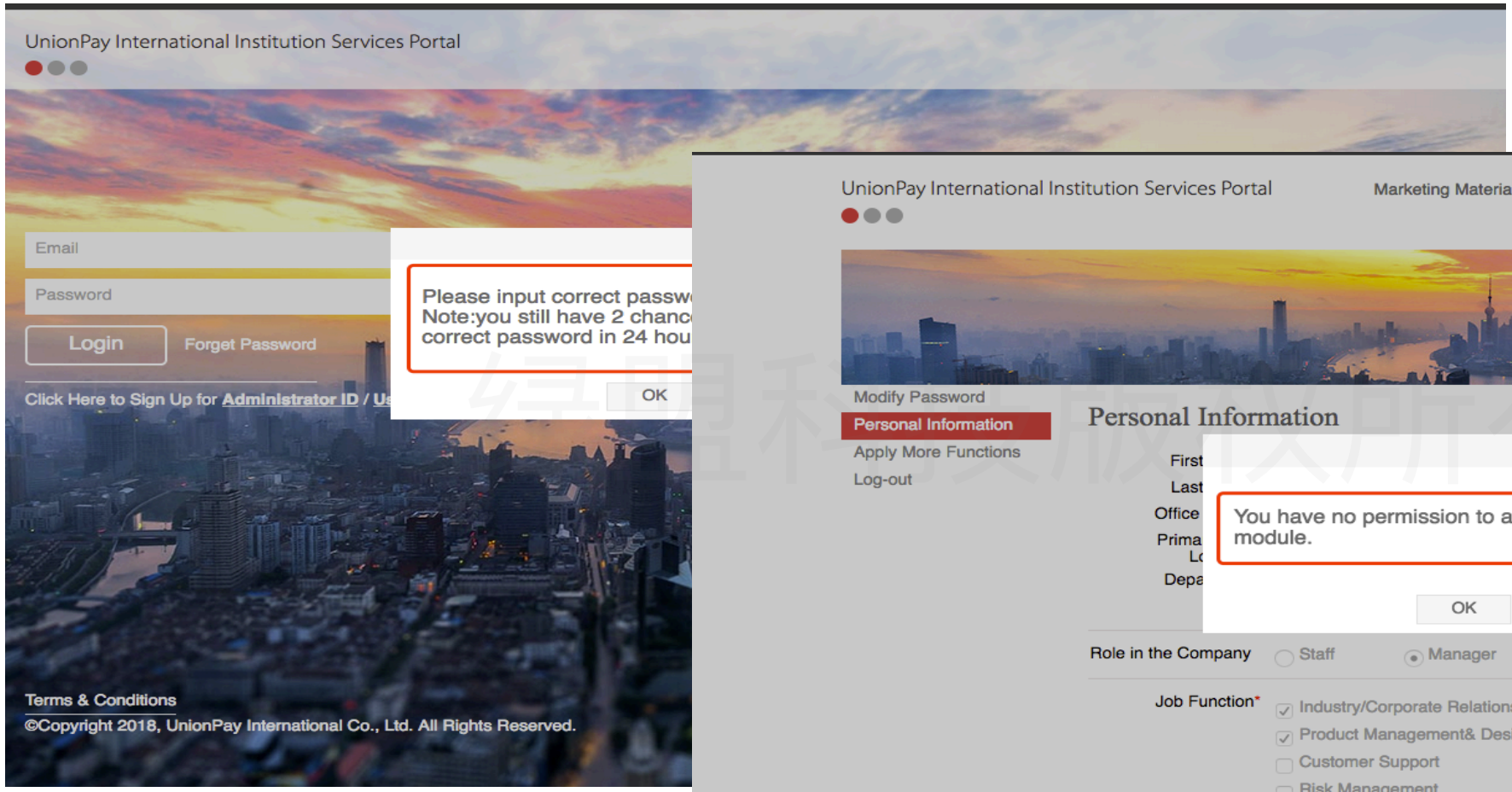
01.认证

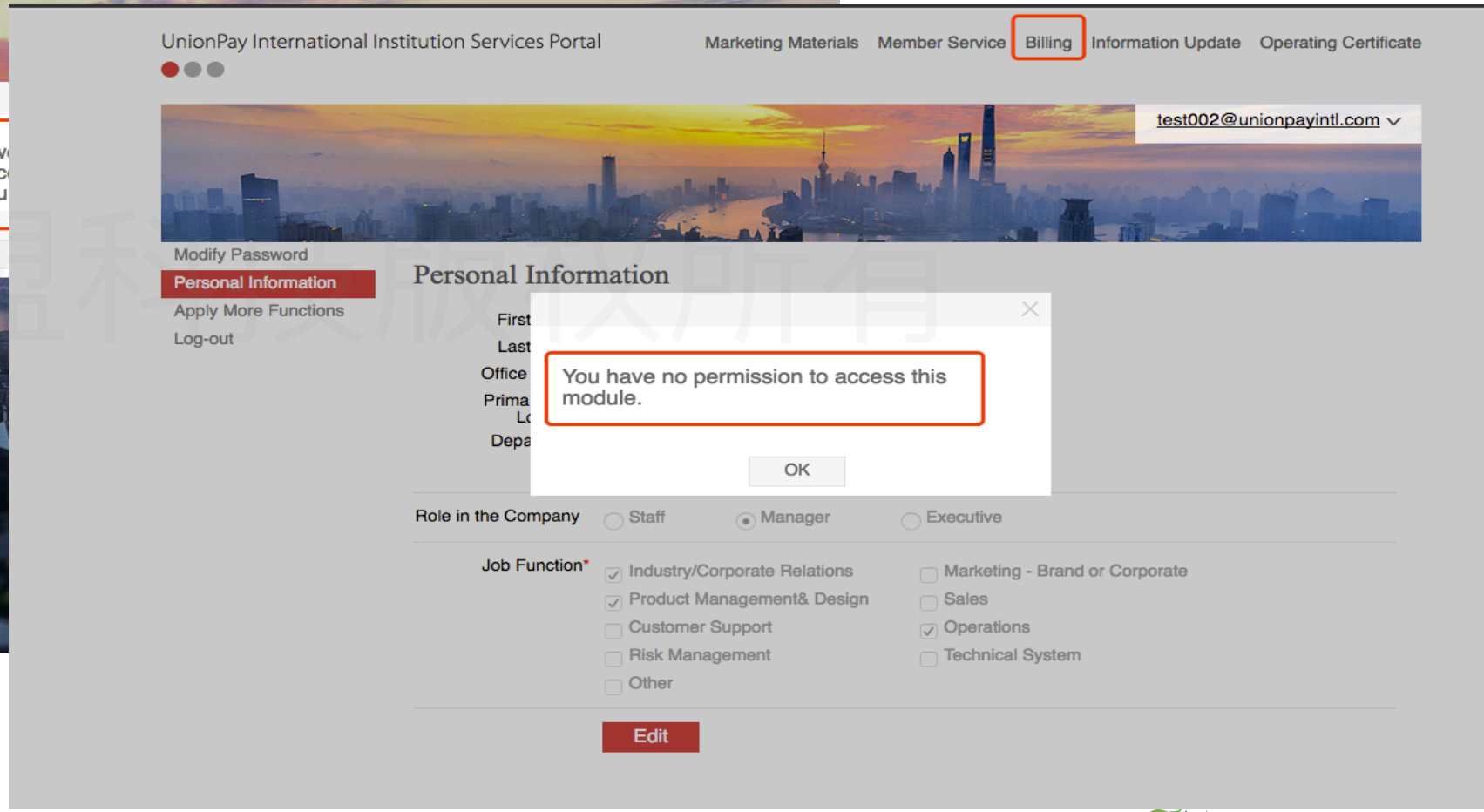
- 操作者是否具有权限访问该系统

02.授权

- 操作者是否具有权限访问该系统上的某个资源

安全防护机制简述 – 认证与授权





安全防护机制简述 – 认证和授权

身份鉴别与访问控制

互动式登陆： 向域账户或者本地计算机确认用户的身份.
网络身份鉴别： 向用户试图访问的任何网络服务确认用户的身份

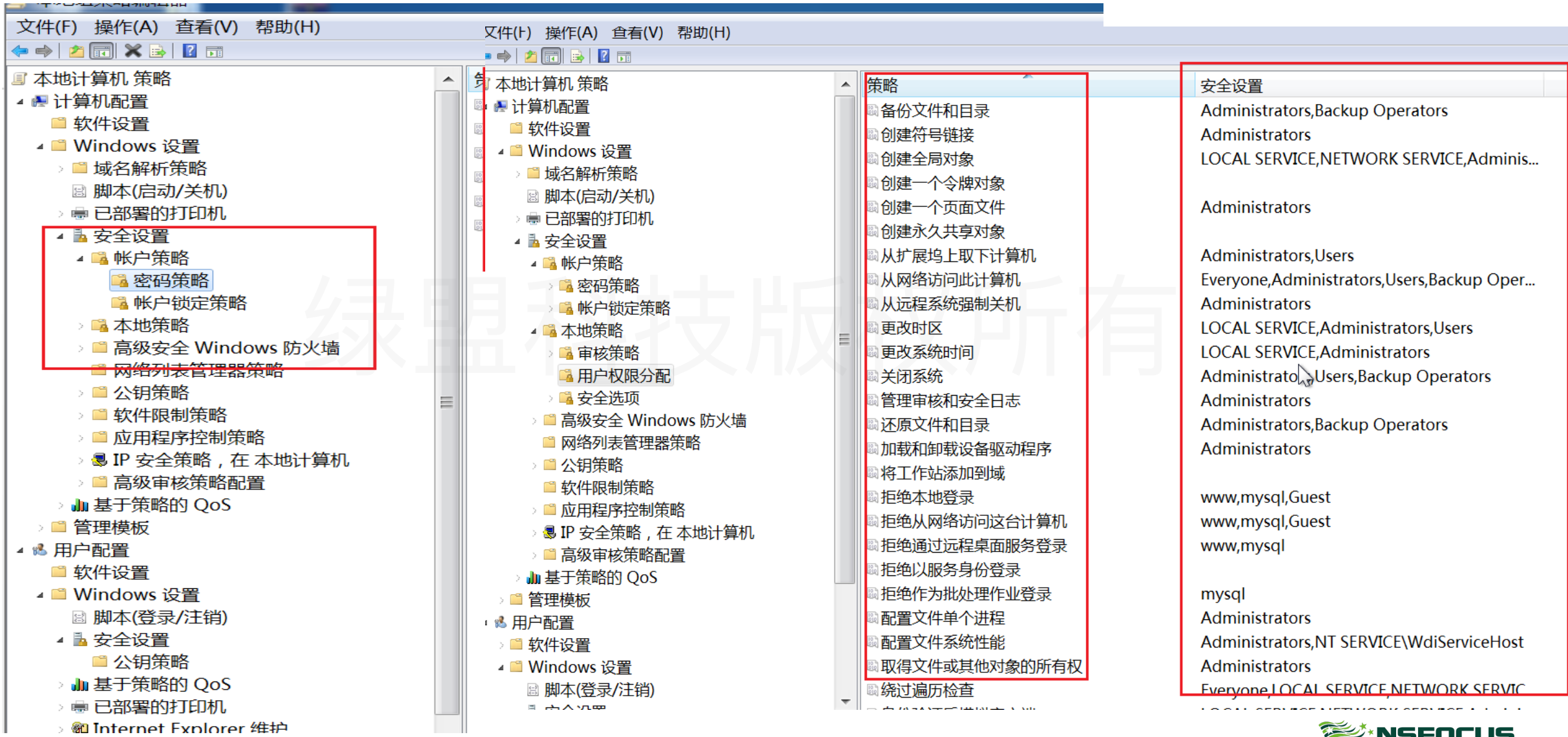
组策略

组策略将系统重要的配置功能汇集起来供管理人员使用，帮助管理员针对整个计算机或者特定用户来设置多种配置，如限制用户如何使用密码，设置账户锁定策略，哪些用户可以使用哪些程序等。

管理委派

当域中存在的系统数量较多，单一的管理员无法完全管理时，可通过管理委派将负载的域管理任务分配给多个管理员进行管理。

安全防护机制简述 – 认证和授权



NSFOCUS

安全防护机制简述 – 日志审计

Windows日志

安全日志

系统日志

SetUp日志

……

应用程序与服务日志

硬件日志

Internet Explorer日志

Micosoft日志

……

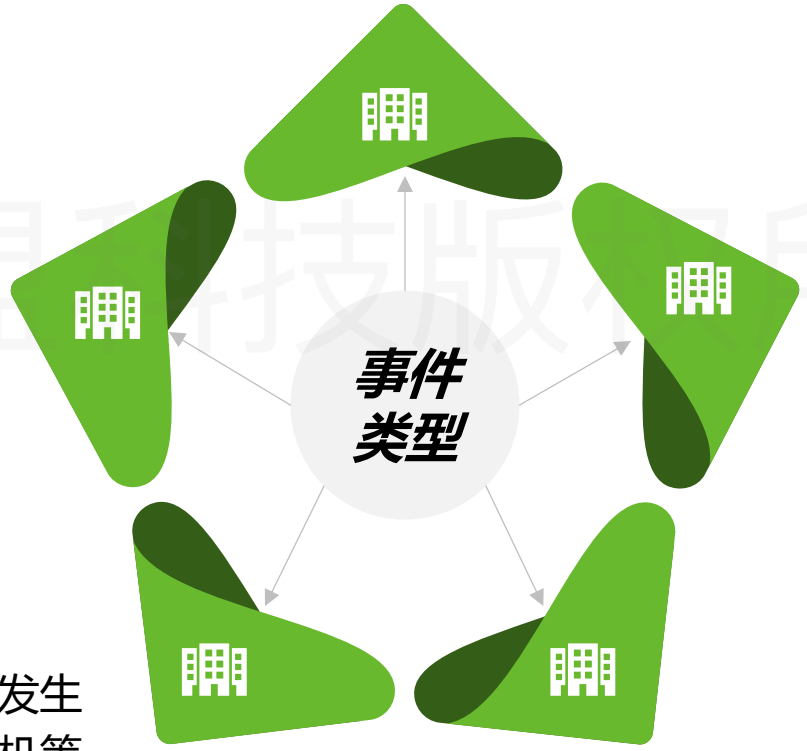
安全防护机制简述 – 日志审计

成功审核（Success audit）

记录用户登陆/注销、对象访问、特权使用、账户管理、策略更改、详细跟踪、账户登陆等事件

错误（Error）

用户应该知道的重要的问题，通常是功能和数据的丢失



失败审核(Failure audit)

失败的审核安全登陆尝试，例如用户试图访问网络驱动器失败

警告（Warning）

不是直接的、主要的，但是会导致将来问题发生的问题，例如磁盘空间不足或者未找到打印机等

信息（Information）

应用程序，驱动程序或者服务的成功操作事件

安全防护机制简述 – 日志审计

什么是日志审计

指通过一定的安全配置，使得操作系统记录系统上发生的各类关键事件

为什么需要日志审计

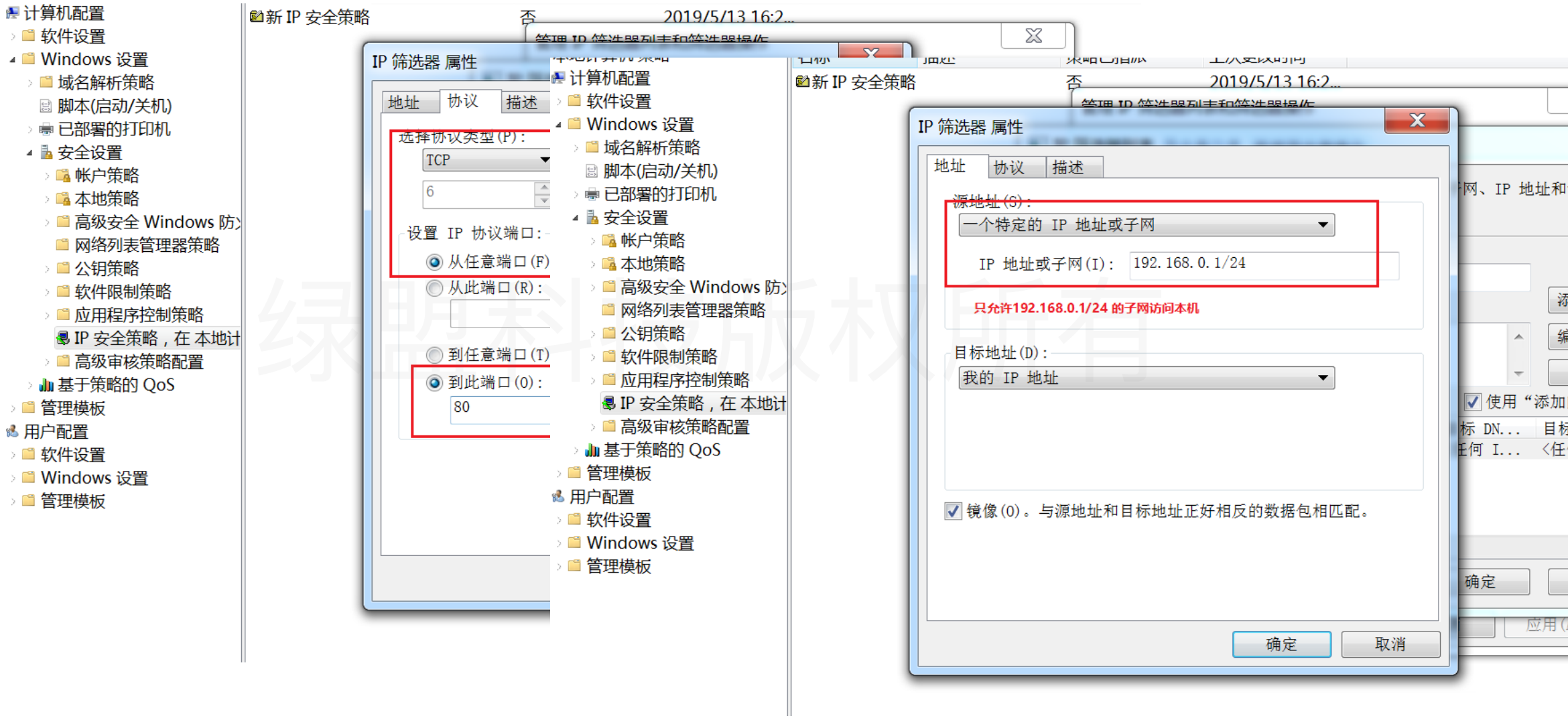
通过日志审计，可以通过记录的日志对系统运行中的错误进行快速定位与排查，也可用于入侵事件的回溯等。

安全防护机制简述 – 协议过滤及防火墙

什么是协议过滤

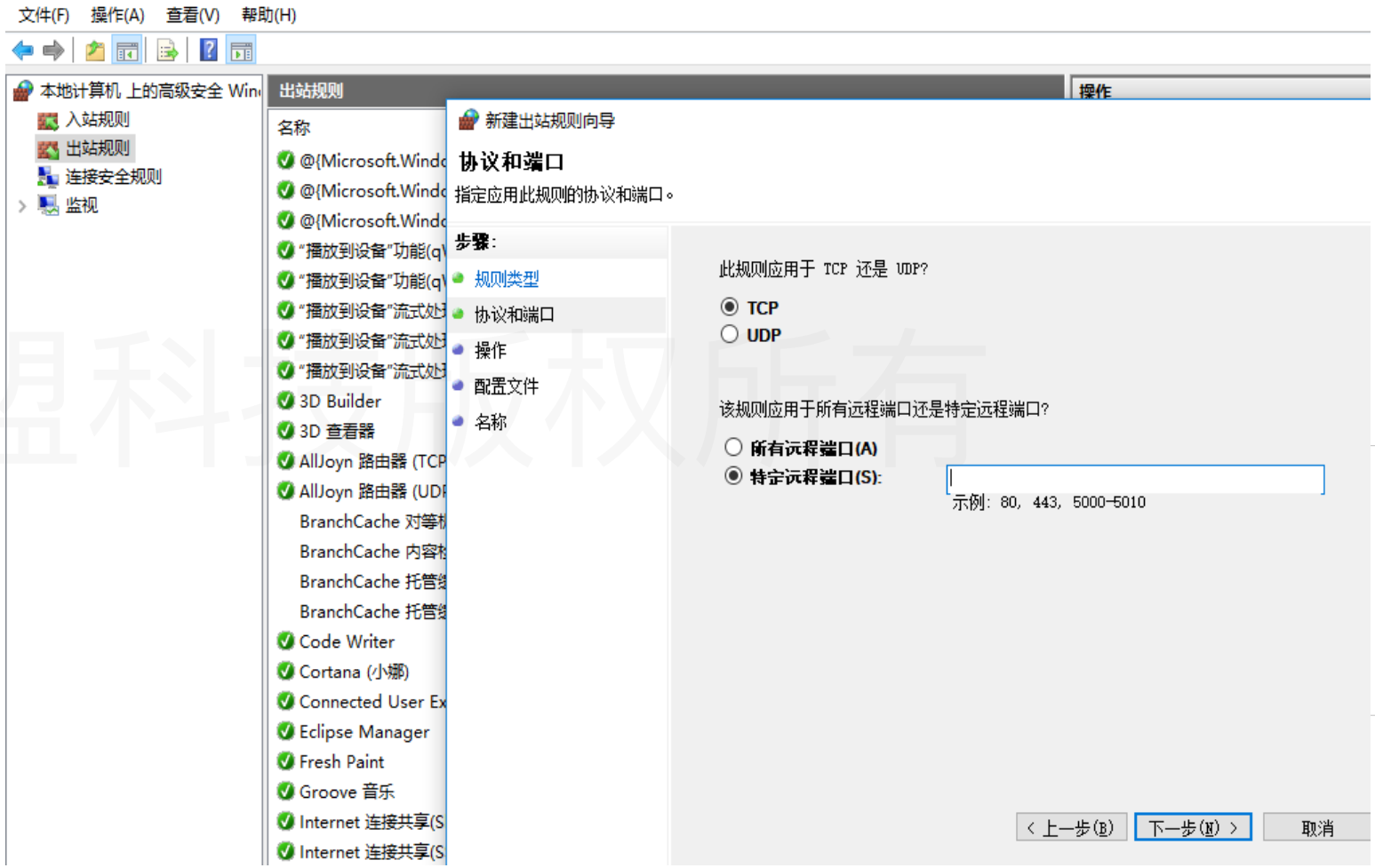
可通过一定的安全配置，设置操作系统只接受或者拒绝特定端口特定协议的流量，并且可限定特定的IP地址的访问。

安全防护机制简述 – 协议过滤及防火墙



安全防护机制简述 – 协议过滤及防火墙

主要的过滤功能



安全防护机制简述 – 协议过滤及防火墙

为什么需要协议过滤与防火墙过滤

Windows中每一项服务都对应相应的端口，而黑客大多是通过端口进行入侵的，关闭一些端口可以防止黑客的入侵。

为了方便用户，Windows默认安装了许多我们暂时不用的服务，在系统资源相对紧张的情况下，额外的服务会导致系统资源紧张，引起系统的不稳定，它还会为黑客的远程入侵提供了多种途径

安全防护机制简述 – 协议过滤及防火墙

Microsc

Microsoft \

发布日期：2017 年 3

版本：1.0

执行摘要

此安全更新程序修复
殊设计的消息，那么

【安全公告】CVE-2019-0708远程桌面服务远程代码执行漏洞

2019-05-15 11:26:14　来源：蓝队云

漏洞信息：

2019年5月14日微软官方发布安全补丁，修复了Windows远程桌面服务的远程代码执行漏洞CVE-2019-0708（https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-0708），此漏洞是预身份验证且无需用户交互（无证系统账户密码），这就意味着这个漏洞可以通过网络蠕虫的方式被利用。

影响范围：

该漏洞影响了某些旧版本的Windows系统，如下：

Windows 7

Windows Server 2008 R2

Windows Server 2008

Windows 2003

Windows XP

NSFOCUS

安全防护机制简述 – EFS文件加密

01

什么是EFS文件加密

Windows系统上特有的一个实用的功能，对于NTFS卷上的文件和数据，都可以直接被操作系统加密保存，在很大程度上提高了数据的安全性。

02

EFS文件加密的好处

1 EFS加密机制与操作系统紧密结合，不必要额外安装数据加密软件。

2 加密系统对用户是透明的，其他非授权用户试图访问加密过的数据时，会收到“访问拒绝”的错误提示。

1.2

安全配置分类说明

a. 账号与口令管理

b. 网络与服务

c. 日志安全要求

d. 认证与授权

安全配置分类说明 – 账号与口令管理

账号口令

1 密码长度、复杂度、高危帐户

- 要求：操作系统帐户口令长度至少为8位，且应为数字、字母和特殊符号中至少3类的组合；删除或禁用高危帐户（guest）
- 作用：杜绝弱口令

2 口令生存周期、密码历史

- 要求：设置口令的最长使用期限小于90天；不能重复使用最近 5 次（含 5 次）内已使用的口令
- 作用：强制用户更改密码，防止攻击者通过社工或者撞库的方式登陆操作系统

3 账号管理

- 要求：按照权限、责任创建、使用用户账号；按组进行用户管理；Administrator帐户重命名
- 作用：防止多个用户采用同一个账号进行操作

4 运维安全

- 要求：连续认证失败次数为5次，锁定该帐户30分钟；域环境下禁止计算机帐户更改密码”
- 作用：保证运维安全；降低暴力破解风险

安全配置分类说明 – 网络与服务

Windows防火墙、TCP/IP筛选

要求：开启Windows防火墙、启用TCP/IP筛选功能
作用：安全防护；访问控制

远程桌面(RDP)服务端口

要求：修改默认的远程桌面(RDP)服务端口为非标准端口
作用：降低暴力破解和漏洞扫描风险

SNMP服务

要求：关闭SNMP Service服务或删除public团体
作用：防止攻击者利用SNMP默认通行字对系统进行攻击

SYN、ICMP、TCP碎片、源路由攻击保护

要求：按要求设置并启用相应攻击保护
作用：防止DDOS等网络攻击

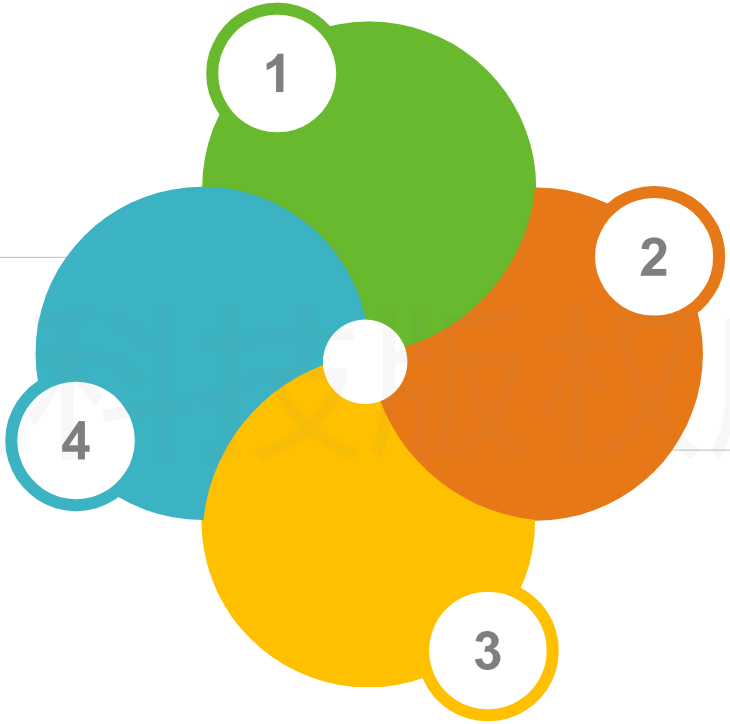
失效网关检测和路由发现功能

要求：禁用失效网关检测和路由发现
作用：防止攻击者探测网络信息

TCP“连接存活时间”和重传单独数据片段的次数

要求：配置TCP“连接存活时间”和重传单独数据片段的次数
作用：防止DDOS攻击

安全配置分类说明 – 日志安全要求



配置系统日志

配置审核(日志记录)策略

配置应用程序日志

正确配置安全日志

安全配置分类说明 – 认证与授权

禁止远程访问注册表

要求：删除可远程访问的注册表路径和子路径；删除可匿名访问的共享和命名管道

作用：防止攻击者远程攻击服务器

限制匿名登录

要求：限制匿名用户连接

作用：保证系统的安全性，降低被入侵风险

访问控制

要求：限制（可从远端）关闭系统的帐户和组；配置“允许本地登录”、“从网络访问此计算机”策略；

作用：合理分配用户权限，便于溯源

权限控制

要求：限制“取得文件或其它对象的所有权”的帐户和组

作用：最小特权原则，降低系统和数据风险

NSFOCUS

1.3

核心安全配置作用及参数

a. 账号口令
b. 关闭不必要的服务
c. 修改远程登陆端口
d. 开启日志审计

核心安全配置作用及参数– 账号口令（操作）

1

- 打开命令提示符，运行命令 “gpedit.msc”打开组策略编辑器

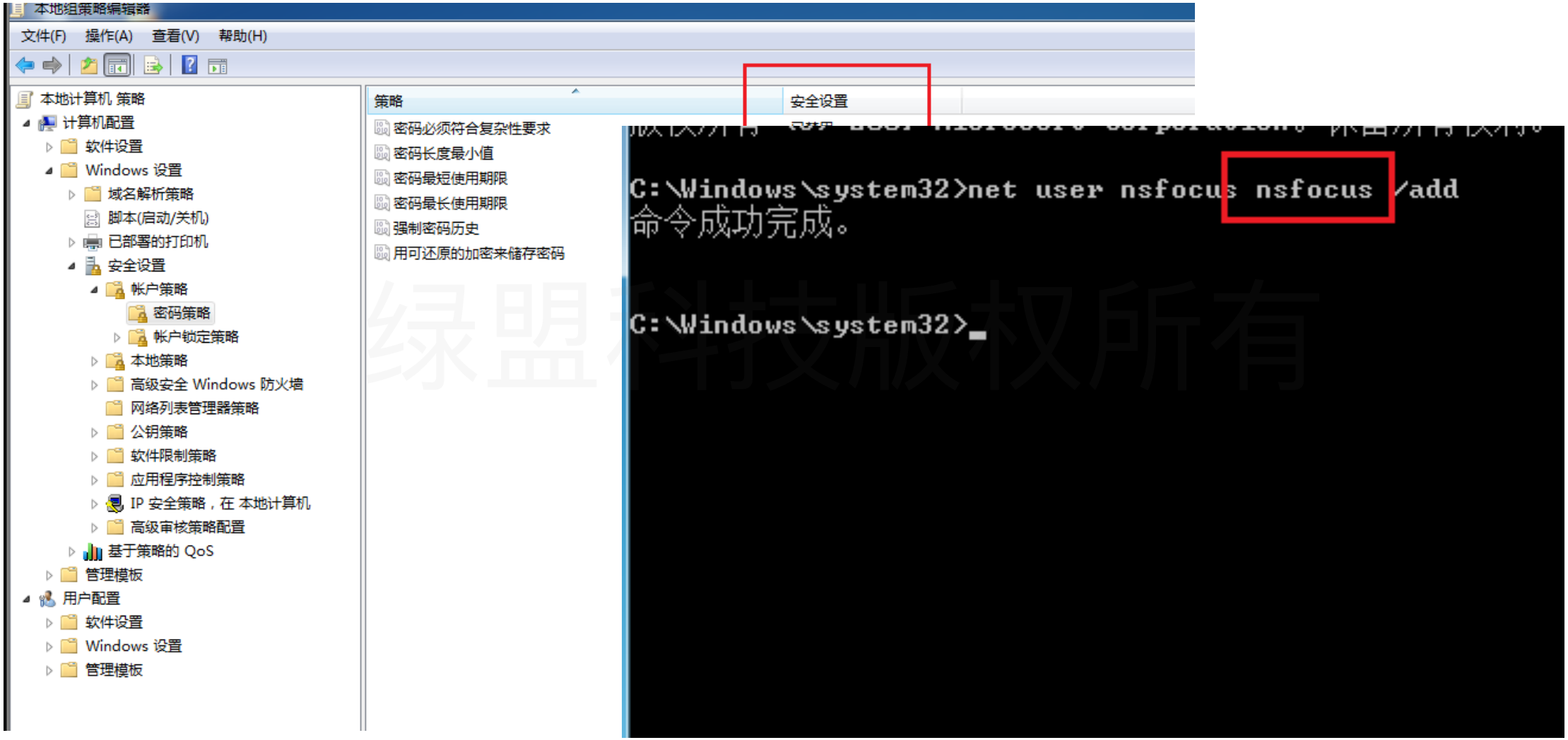
2

浏览到路径 “本地计算机策略\计算机配置\Windows设置\安全设置\帐户策略\密码策略”

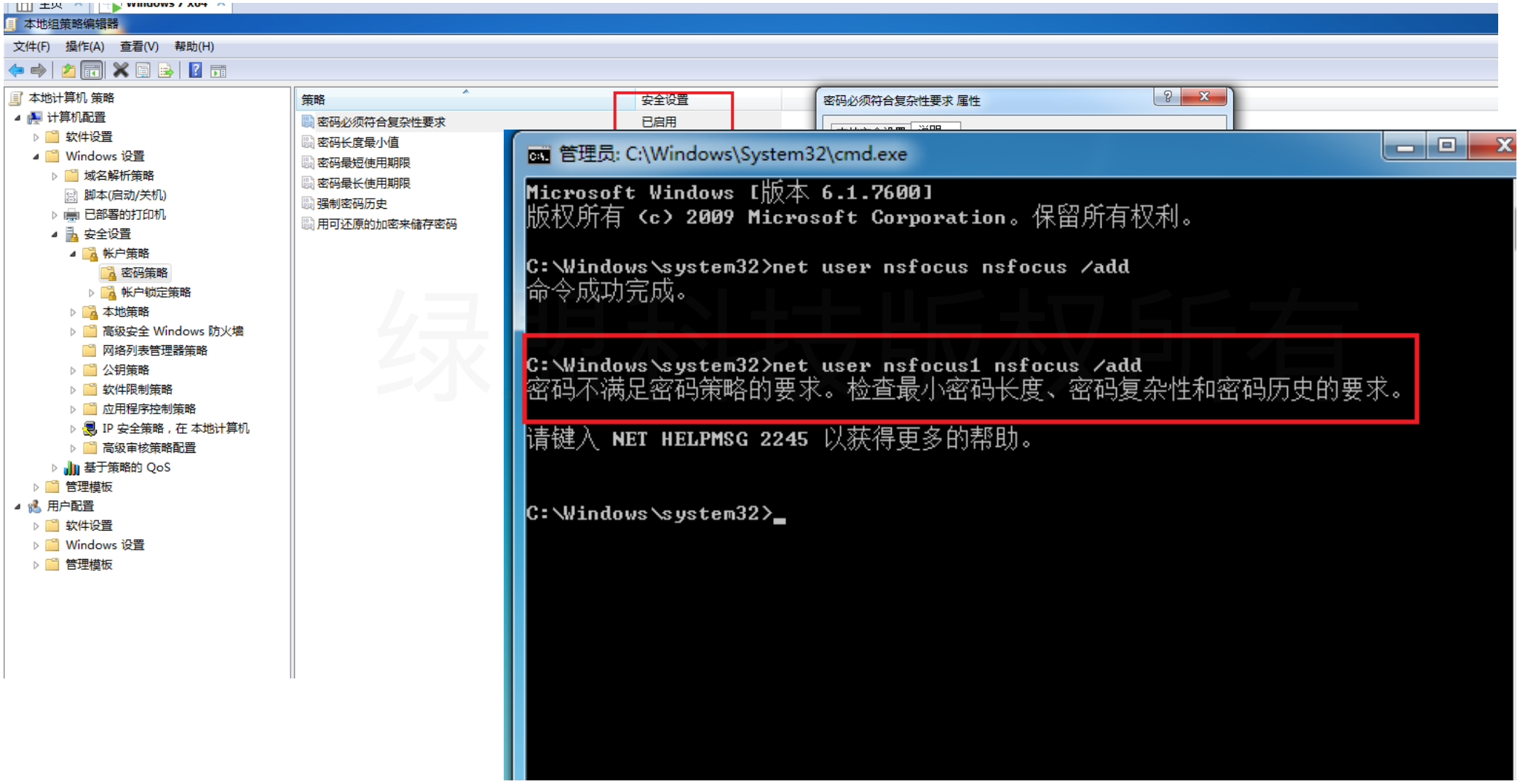
3

在右边窗格中找到 “密码必须符合复杂性要求” ，配置为 “已启用” 。密码长度最小值” ，配置为不小于标准值的值。 “密码最短/长存留期(使用期限)”，配置为非0值。

核心安全配置作用及参数– 账号口令（操作）



核心安全配置作用及参数– 账号口令（操作）



核心安全配置作用及参数– 关闭不必要服务（操作）

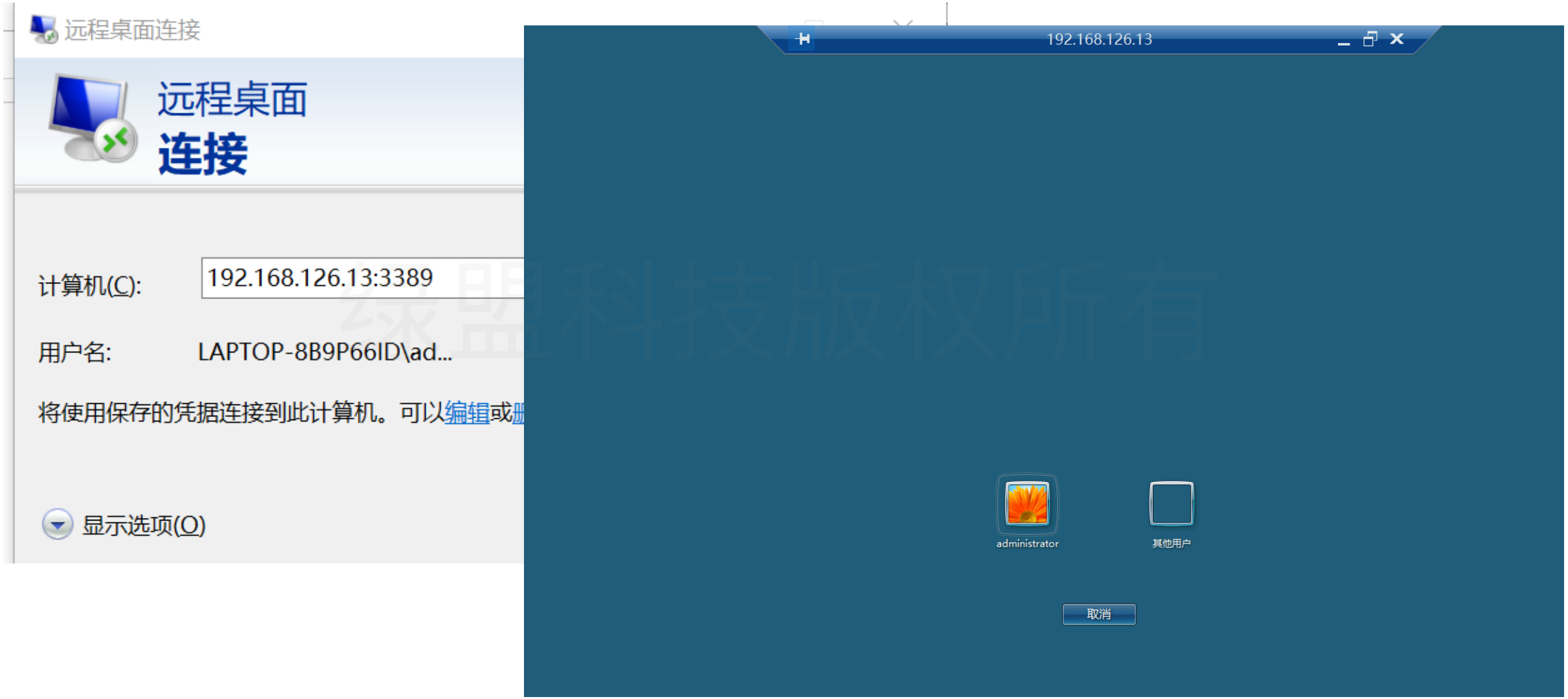
开命令提示符，运行命令 “services.msc”打开服务管理器

01

02

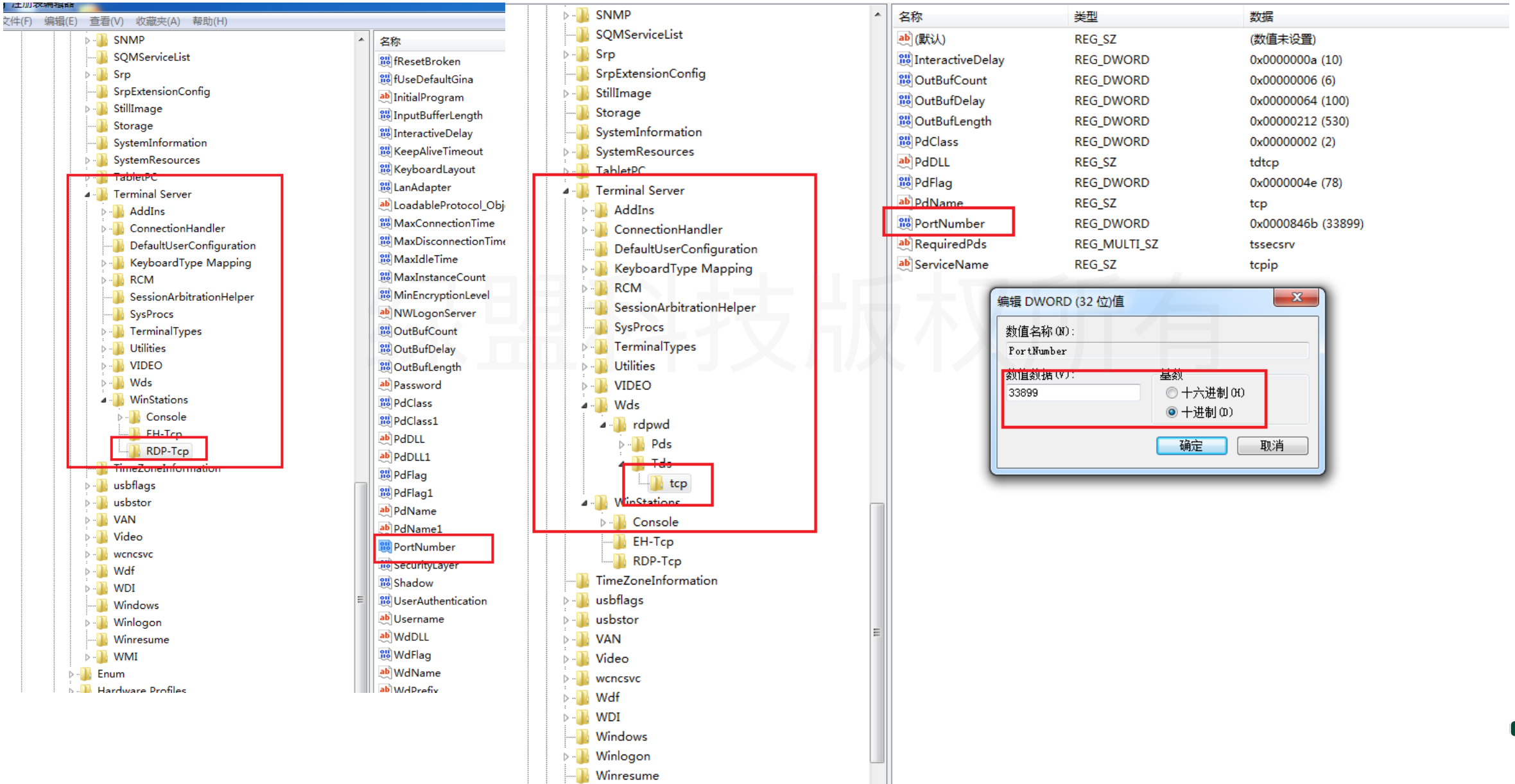
停止显示名称为DHCP Client”、 “Message Queuing”、 “Simple Mail Transport Protocol (SMTP)”、 “Windows Internet Name Service (WINS)”、 “DHCP Server”、 “Remote Access Connection Manager” “Simple TCP/IP Services” 的服务。

核心安全配置作用及参数– 修改默认3389端口

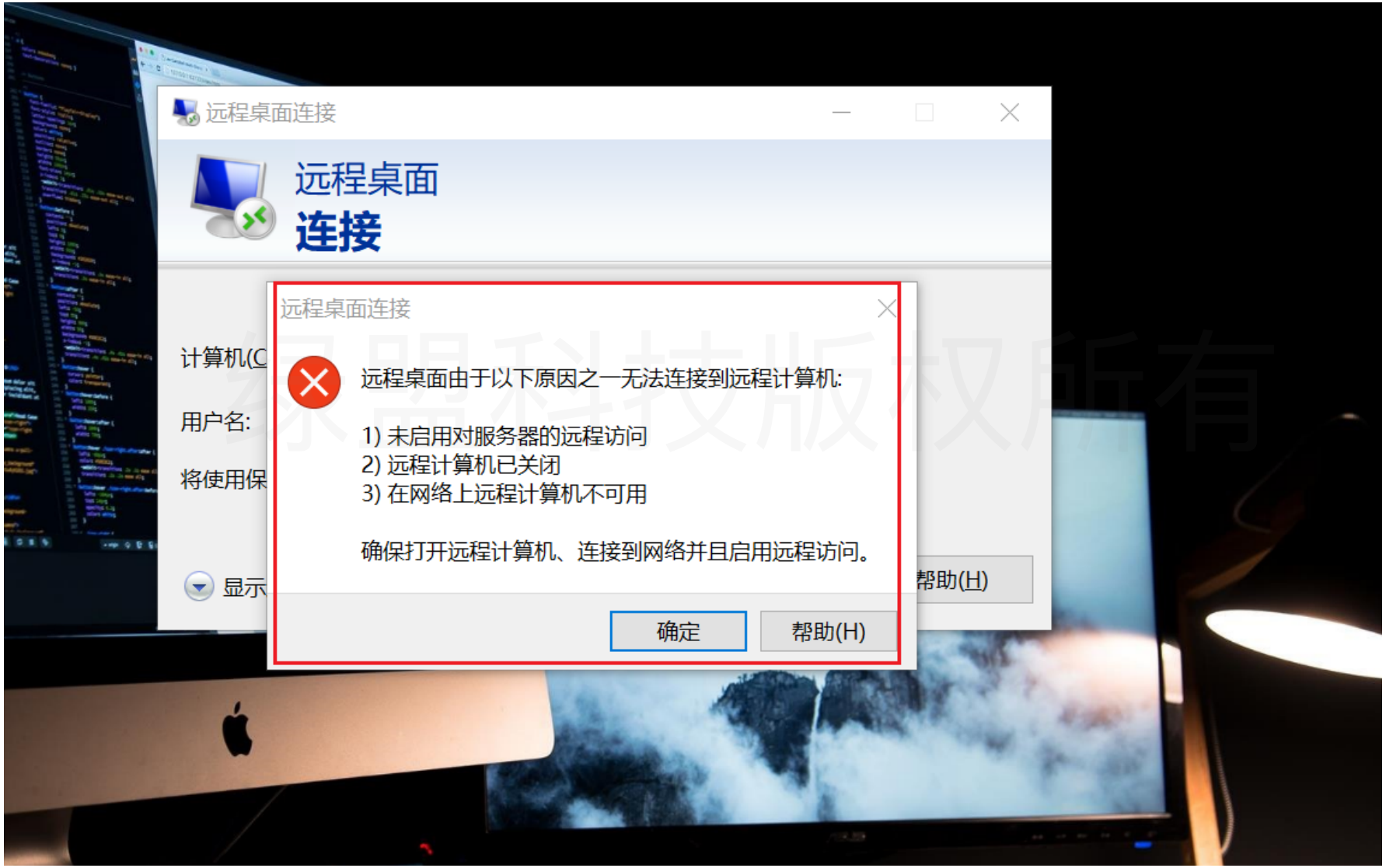


NSFOCUS

核心安全配置作用及参数– 修改默认3389端口

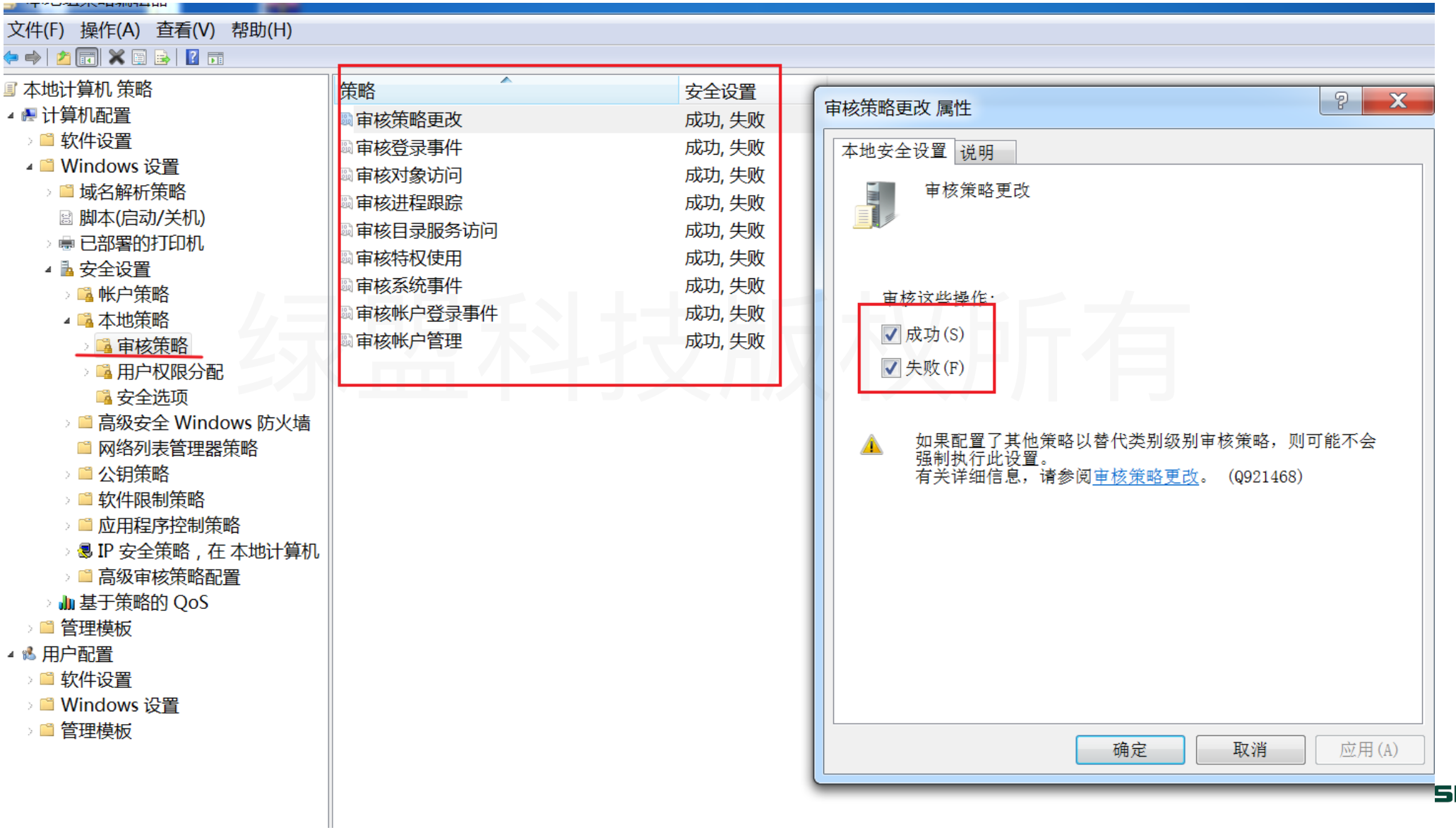


核心安全配置作用及参数– 修改默认3389端口

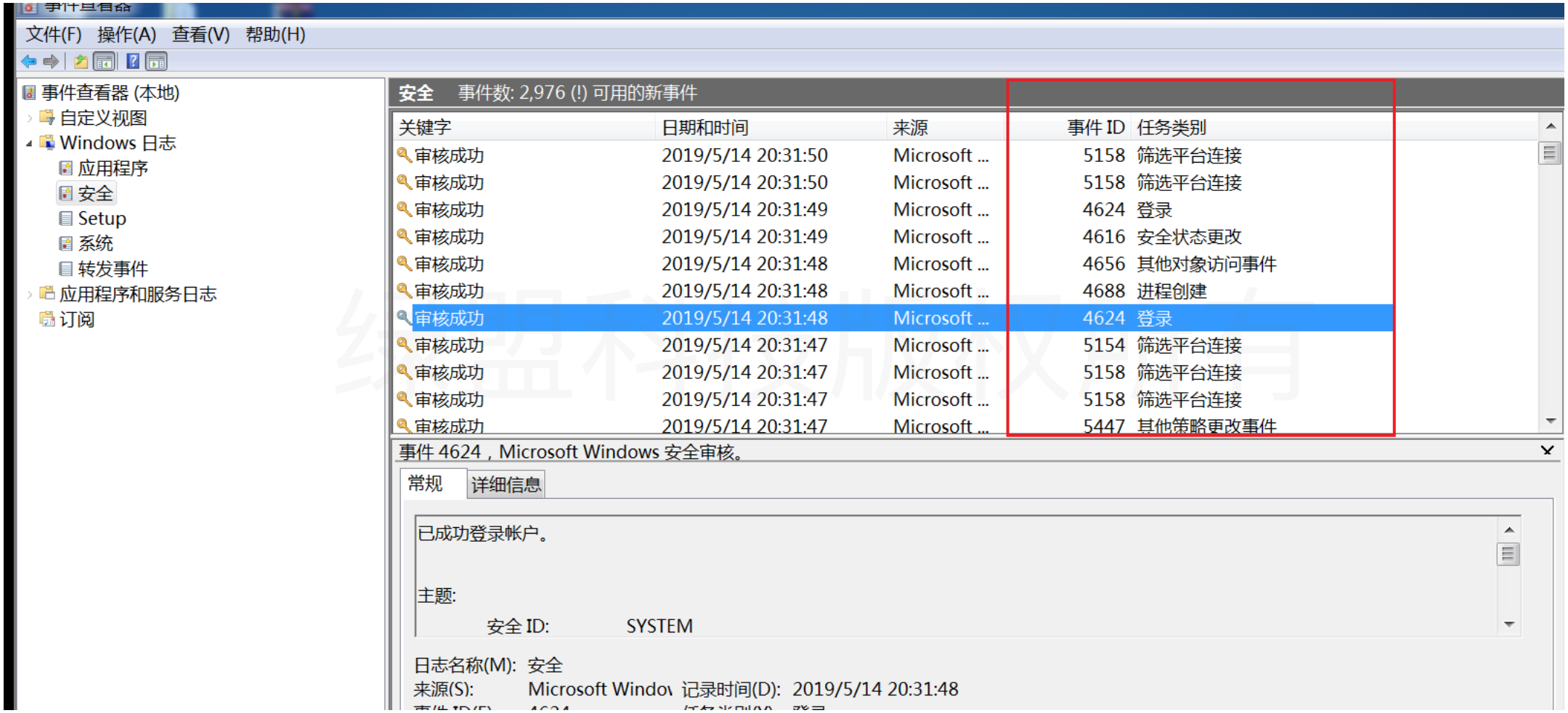


NSFOCUS

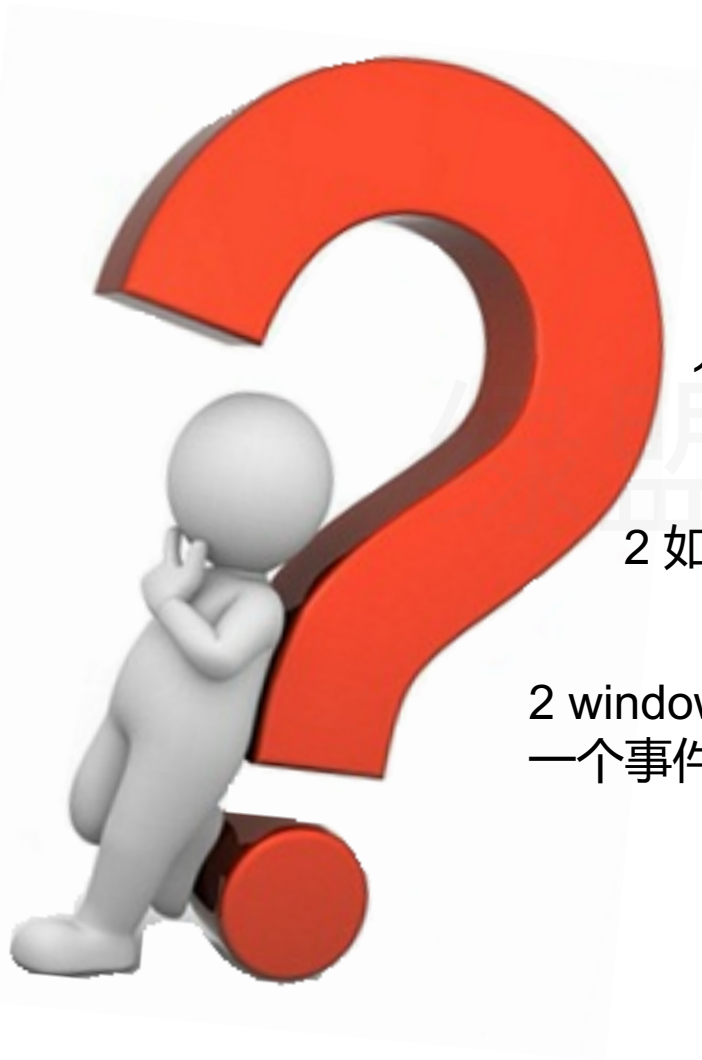
核心安全配置作用及参数– 开启日志审计



核心安全配置作用及参数– 开启日志审计



FAQ



1 如何通过设置防火墙策略，阻止攻击者采用MS17-010从445端口进行攻击

2 如何通过IPSec设置访问白名单，只允许特定的IP从3389端口登陆本机？

2 windows的安全日志是入侵排查的关键日志文件，其中记录的每一条事件都有一个事件ID，其中的每个ID代表什么意思？

01

RedHat 安全配置解析

1. 安全防护机制简述
2. 安全配置分类说明
3. 核心安全配置作用及参数

NSFOCUS

2.1

安全防护机制简述

a. 认证授权

b. 文件系统权限管理

c. 日志文件

安全防护机制简述 – 认证授权

任何程序需要使用认证功能时，都可以使用PAM机制的API实现认证功能！

安全防护机制简述 – 认证授权

配置文件

PAM的配置文件位置位于/etc/pam.conf, 也可以在/etc/pam.d/文件夹下配置单独的文件，要实现认证机制可以往配置文件里面写入特定形式的内容。

配置格式

配置文件主要分为五个字段， service、type、control、module-path、module-argments，不同字段设置不同的值可实现不同的认证功能

安全防护机制简述 – 文件系统权限管理

文件权限

What

Linux上存在着许多文件，这些文件包含公用的文件和私密的个人文件，Linux为这些文件配置了不同的访问限制条件

Who

文件所属者

文件所属组

其他用户

How

r 可读w可写x可执行

SUID

SGUI

Sticky

安全防护机制简述 – 文件系统权限管理

```
[root@bogon pam.d]# cd /home
[root@bogon home]# ls -al
总用量 8
drwxr-xr-x.  4 root    root       32 8月   15 2018 .
dr-xr-xr-x. 17 root    root      224 8月   19 2018 ..
drwx------. 16 fang    fang     4096 9月    8 2017 fang
drwx------. 19 oracle oinstall 4096 8月   18 2018 oracle
[root@bogon home]#
```

每个用户的家目录只有自己可访问

```
[root@bogon home]# cd /etc/
[root@bogon etc]# ls -al /etc/passwd
-rw-r--r--. 1 root root 3318 8月   15 2018 /etc/passwd
[root@bogon etc]#
```

passwd文件必须要所有人都可读

安全防护机制简述 – 文件系统权限管理

```
passwd: /usr/bin/passwd /etc/passwd /usr/share/man/man1/passwd.1.gz /usr/share/man/man5/passwd.5.gz
[root@bogon etc]# ls -ak /usr/bin/passwd
/usr/bin/passwd
[root@bogon etc]# ls -al /usr/bin/passwd
-rwsr-xr-x. 1 root root 27832 6月  10 2014 /usr/bin/passwd
[root@bogon etc]#
```

修改密码时是通过修改shadow文件进行的，因此需要passwd程序有SUID权限

```
drwxr-xr-x.  2 root root       6 7月  25 2018 音乐
drwxr-xr-x.  2 root root       6 7月  26 2018 桌面
[root@localhost log]# ls -al /root |grep history
-rw-------.  1 root root    5979 3月  13 10:47 .bash_history
-rw-------.  1 root root     778 8月   2 2018 .gdb_history
[root@localhost log]# su fang
[fang@localhost log]$ cat /root/.bash_history
cat: /root/.bash_history: 权限不够
[fang@localhost log]$
```

只有root才能读写的文件

其他用户读取时，显示权限不够

安全防护机制简述 – 日志文件

01.Who

Syslog，Linux系统默认的日志守护进程，将各个程序的日志写入到系统文件中

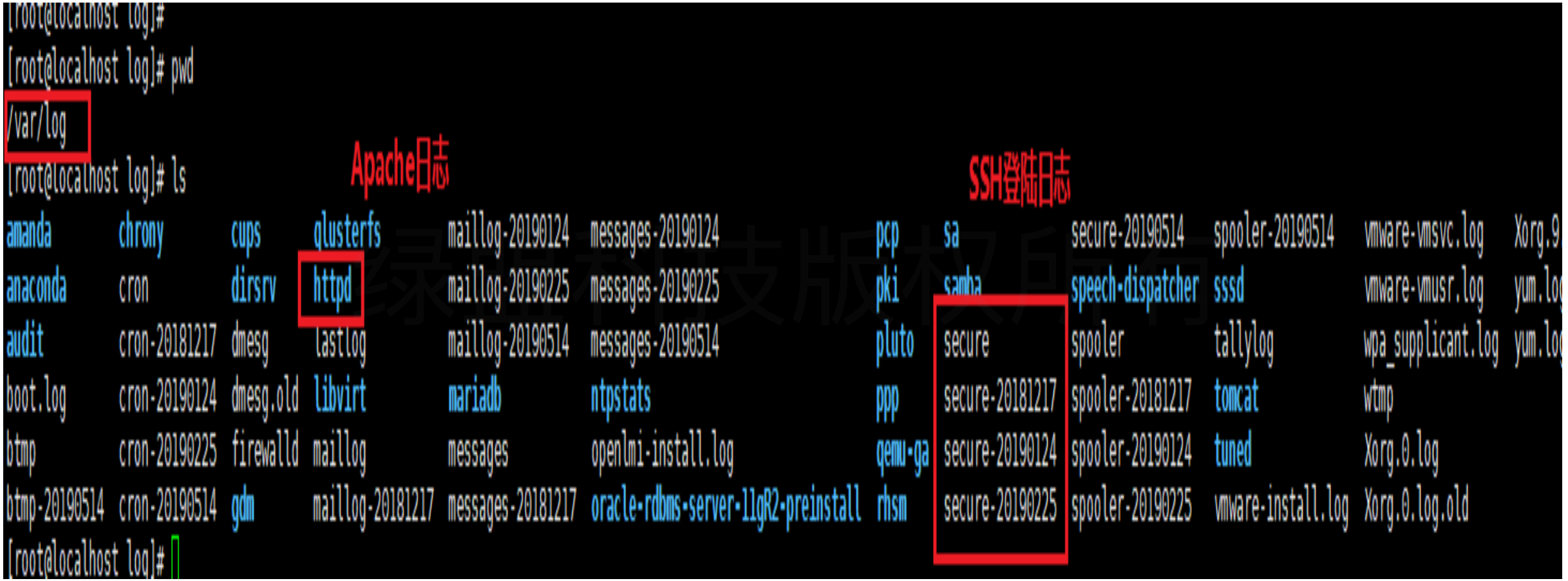
02.Why

Linux系统内核和许多程序会产生各种错误信息，告警信息和其他提示信息，这些信息对管理员了解系统运行状态是非常有用的。

03.Where

Syslog将许多程序的日志记录到/var/log目录下，同时也可修改/etc/syslog.conf配置文件进行日志记录的配置

安全防护机制简述 – 日志文件



安全防护机制简述 – 日志文件

常用日志类型

类型	说明
auth	用户认证时产生的日志，如login命令、su命令。
console	针对系统控制台的消息。
cron	系统定期执行计划任务时产生的日志。
daemon	某些守护进程产生的日志。
kern	系统内核消息
mail	邮件日志
news	网络新闻传输协议(nntp)产生的消息。
ntp	网络时间协议(ntp)产生的消息。
user	用户进程。

安全防护机制简述 – 日志文件

常用日志优先级

类型	说明
emerg	紧急情况，系统不可用（例如系统崩溃），一般会通知所有用户。
alert	需要立即修复，例如系统数据库损坏。
crit	危险情况，例如硬盘错误，可能会阻碍程序的部分功能。
err	一般错误消息。
warning	警告。
notice	不是错误，但是可能需要处理。
info	通用性消息，一般用来提供有用信息。
debug	调试程序产生的信息。
none	没有优先级，不记录任何日志消息。

安全防护机制简述 – 日志文件

常用的日志

- 1. /var/log/messages: 包括整体系统普通信息，其中也包含系统启动期间的日志。
- 2. /var/log/syslog:它上messages日志不同，它只记录警告信息，通常是系统出问题的信息。
- 3. /var/log/user.log: 记录所有等级用户信息的日志.
- 4. /var/log/auth.log: 包含系统授权信息，用户登陆和使用权限机制
- 5. /var/log/daemon.log: 包含各种系统后台守护进程日志信息
- 6. /var/log/kern.log: 包含内核产生的日志，有助于在定制内核时解决问题.

安全防护机制简述 – 日志文件

```
May 14 13:29:40 bogon sshd[34504]: pam_unix(sshd:session): session opened for user root by (uid=0)
May 14 13:31:38 bogon sshd[34963]: reverse mapping checking getaddrinfo for bogon [192.168.126.1] failed - POSSIBLE BREAK-IN ATTEMPT!
May 14 13:31:42 bogon unix_chkpwd[34980]: password check failed for user (root)
May 14 13:31:42 bogon sshd[34963]: pam_unix(sshd:auth): authentication failure; logname= uid=0 euid=0 tty=ssh ruser= rhost=192.168.126.1  user=root
May 14 13:31:42 bogon sshd[34963]: pam_succeed_if(sshd:auth): requirement "uid >= 1000" not met by user "root"
May 14 13:31:44 bogon sshd[34963]: Failed password for root from 192.168.126.1 port 42416 ssh2
May 14 13:31:48 bogon unix_chkpwd[34996]: password check failed for user (root)
May 14 13:31:48 bogon sshd[34963]: pam_succeed_if(sshd:auth): requirement "uid >= 1000" not met by user "root"
May 14 13:31:50 bogon sshd[34963]: Failed password for root from 192.168.126.1 port 42416 ssh2
May 14 13:31:51 bogon unix_chkpwd[35012]: password check failed for user (root)
May 14 13:31:51 bogon sshd[34963]: pam_succeed_if(sshd:auth): requirement "uid >= 1000" not met by user "root"
May 14 13:31:54 bogon sshd[34963]: Failed password for root from 192.168.126.1 port 42416 ssh2
May 14 13:31:55 bogon unix_chkpwd[35028]: password check failed for user (root)
May 14 13:31:55 bogon sshd[34963]: pam_succeed_if(sshd:auth): requirement "uid >= 1000" not met by user "root"
May 14 13:31:57 bogon sshd[34963]: Failed password for root from 192.168.126.1 port 42416 ssh2
May 14 13:31:58 bogon sshd[34963]: error: Received disconnect from 192.168.126.1: 0:  [preauth]
May 14 13:31:58 bogon sshd[34963]: PAM 3 more authentication failures; logname= uid=0 euid=0 tty=ssh ruser= rhost=192.168.126.1  user=root
May 14 13:31:58 bogon sshd[34963]: PAM service(sshd) ignoring max retries; 4 > 3
[root@localhost log]#
```

SSH登陆日志，常用于排查登陆爆破

- 11. /var/log/wtmp:此日志文件永久记录每个用户登录，注销及系统的启动，停机的事件，用last查看
- 12. /var/log/utmp:记录有关当前登录的每个用户的信息。如who,w,users,finger等需要访问此文件

安全防

```
May 14 13:29:40 bogon sshd[34504]: pam_
May 14 13:31:38 bogon sshd[34963]: reve
May 14 13:31:42 bogon unix_chkpwd[34980
May 14 13:31:42 bogon sshd[34963]: pam_
May 14 13:31:42 bogon sshd[34963]: pam_
May 14 13:31:44 bogon sshd[34963]: Fail
May 14 13:31:48 bogon unix_chkpwd[34996
May 14 13:31:48 bogon sshd[34963]: pam_
May 14 13:31:50 bogon sshd[34963]: Fail
May 14 13:31:51 bogon unix_chkpwd[35012
May 14 13:31:51 bogon sshd[34963]: pam_
May 14 13:31:54 bogon sshd[34963]: Fail
May 14 13:31:55 bogon unix_chkpwd[35028
May 14 13:31:55 bogon sshd[34963]: pam_
May 14 13:31:57 bogon sshd[34963]: Fail
May 14 13:31:58 bogon sshd[34963]: erro
May 14 13:31:58 bogon sshd[34963]: PAM
May 14 13:31:58 bogon sshd[34963]: PAM
[root@localhost log]#
```

```
[root@localhost log]# lastlog
用户名           端口     来自             最后登陆时间
root             pts/2    192.168.126.1    二 5月 14 13:29:40 +0800 2019
bin                                        **从未登录过**
daemon                                     **从未登录过**
adm                                        **从未登录过**
lp                                         **从未登录过**
sync                                       **从未登录过**
shutdown                                   **从未登录过**
halt                                       **从未登录过**
mail                                       **从未登录过**
operator                                   **从未登录过**
games                                      **从未登录过**
ftp                                        **从未登录过**
nobody                                     **从未登录过**
pegasus                                    **从未登录过**
ods                                        **从未登录过**
systemd-bus-proxy                          **从未登录过**
systemd-network                            **从未登录过**
dbus                                       **从未登录过**
polkitd                                    **从未登录过**
apache                                     **从未登录过**
tss                                        **从未登录过**
colord                                     **从未登录过**
abrt                                       **从未登录过**
unbound                                    **从未登录过**
usbmuxd                                    **从未登录过**
libstoragemgmt                             **从未登录过**
saslauth                                   **从未登录过**
dirsrv                                     **从未登录过**
rpc                                        **从未登录过**
amandabackup                               **从未登录过**
pcp                                        **从未登录过**
geoclue                                    **从未登录过**
setroubleshoot                             **从未登录过**
memcached                                  **从未登录过**
postfix                                    **从未登录过**
rtkit                                      **从未登录过**
qemu                                       **从未登录过**
mysql                                      **从未登录过**
radvd                                      **从未登录过**
```

lastlog登陆日志，用户最后一次登录

6.1 user=root

常用于排查登陆爆破

=root

NSFOCUS

2.1

安全配置分类说明

a. 账号与口令管理

b. 日志安全要求

c. 认证授权

d. 协议安全

安全配置分类说明 – 账号与口令管理

账号口令

1 密码长度、复杂度、

- 要求：操作系统帐户口令长度至少为8位，且应为数字、字母和特殊符号中至少3类的组合
- 作用：杜绝弱口令

2 口令生存周期、密码历史

- 要求：设置口令的最长使用期限小于90天；不能重复使用最近 5 次（含 5 次）内已使用的口令；口令过期前警告天数
- 作用：强制用户更改密码，防止攻击者通过社工或者撞库的方式登陆操作系统

3 账号管理

- 要求：更改管理员帐户名称；按照权限、责任创建、使用用户账号；按组进行用户管理；空口令账号
- 作用：防止多个用户采用同一个账号进行操作

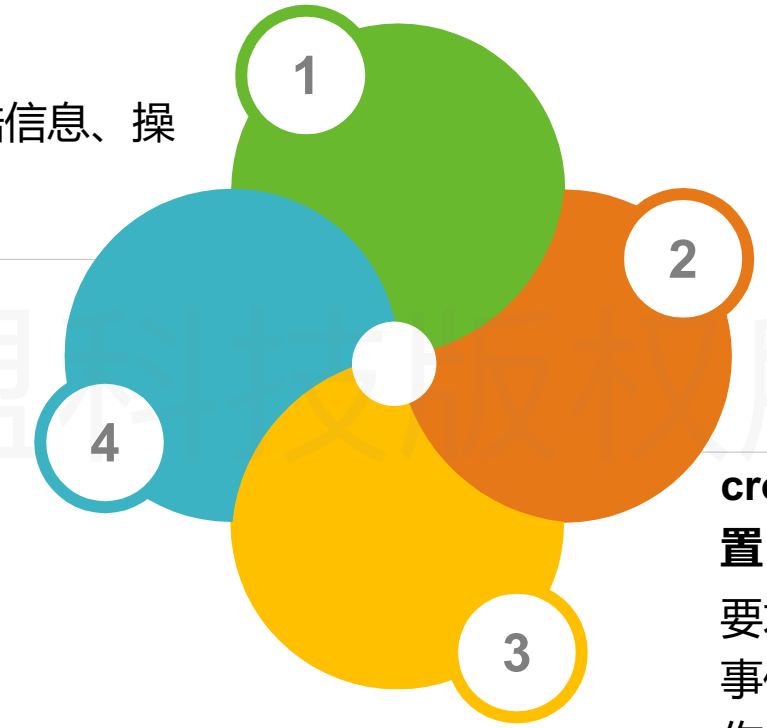
4 运维安全

- 要求：设置除root之外UID为0的用户
- 作用：保证运维安全；降低暴力破解风险

安全配置分类说明 – 日志安全要求

配置日志功能，记录用户登陆信息、操作行为、记录su命令使用情况

要求：配置设备开启日志审计，记录用户登陆信息、操作行为、记录su命令使用情况
作用：审查用户的敏感操作，便于溯源



配置远程日志功能

要求：设备应配置远程日志服务器
作用：将设备日志存储到远程服务器上，方便管理与查看

日志文件是否非全局可写

要求：日志文件权限设置为775
作用：记录用户行为等

cron行为日志、安全事件日志配置

要求： 开启cron行为日志、安全事件日志配置
作用：记录定时任务信息、安全事件信息

安全配置分类说明 – 认证授权

用户目录缺省访问权限设置

要求：设置用户目录默认权限（/etc/login.defs），设置umask 027

作用：设置默认的访问权限

重要目录或文件权限设置

要求：正确设置/etc/shadow、/etc/security等重要文件、目录权限

作用：最小特权原则，降低系统风险

用户umask设置

要求：配置/etc/csh.cshrc、/etc/profile等文件的umask值为077

作用：合理分配用户权限

重要文件属性设置

要求：对shadow等重要文件执行chattr +i 操作

作用：设定文件不能被删除、改名、设定链接关系，同时不能写入或新增内容。

设置ssh登录前警告Banner

要求：修改ssh默认banner

作用：规避信息探测和漏洞扫描

安全配置分类说明 – 协议安全

使用IP协议远程维护的设备配置SSH协议，禁用telnet协议

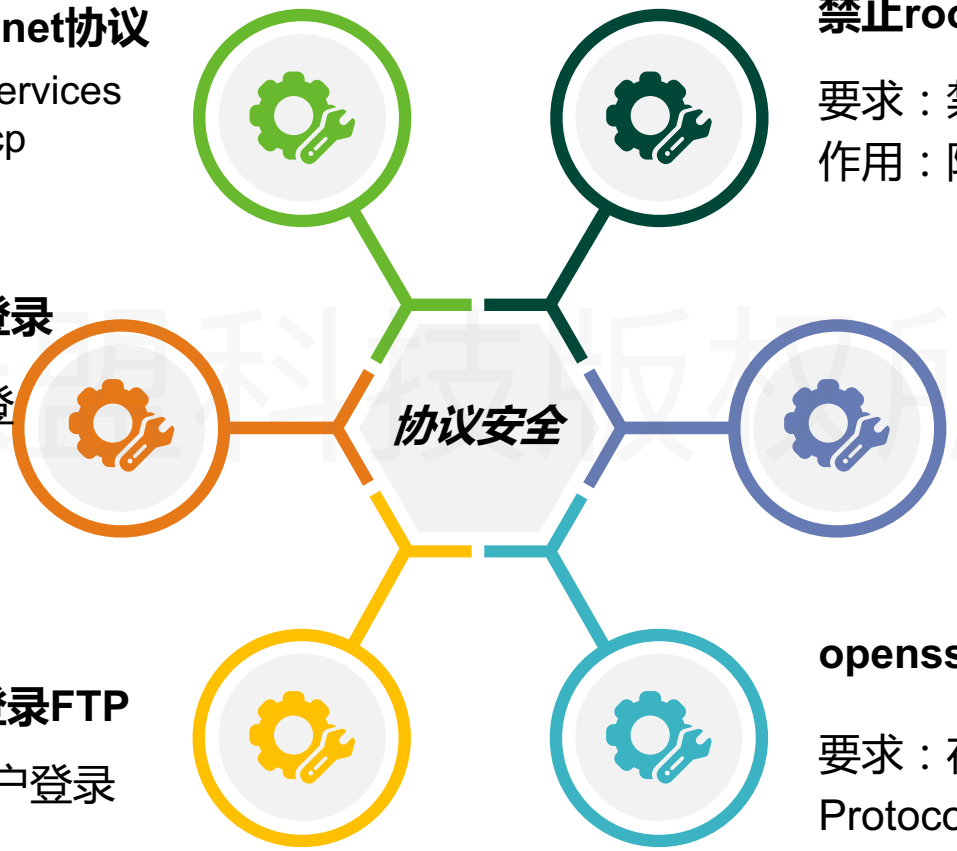
要求：安装ssh，并在/etc/services文件中，注释掉 telnet 23/tcp
作用：增加传输安全性

禁止root用户远程登录

要求：禁止root用户远程telnet、ssh登录
作用：防止暴力破解，降低安全风险

禁止匿名用户登录FTP

要求：禁止匿名WU-FTP、VSFTP用户登录
作用：防止黑客匿名访问FTP服务



禁止root用户登录FTP

要求：禁止root登录WU-FTP、VSFTP
作用：降低暴力破解等安全风险

修改snmp默认团体字

要求：修改community OR/RW 通行字不为private和public
作用：防止攻击者利用SNMP默认通行字对系统进行攻击

openssh安全配置

要求：在sshd_config或sshd2_config中配置：Protocol 2 、PermitRootLogin no
作用：仅使用SSH2；不允许root用户使用SSH登陆。降低安全风险。

1.3

核心安全配置作用及参数

a. 账号口令

b. 关闭不必要服务

c. Ssh安全加固

核心安全配置作用及参数 – 账号口令

- 设置口令策略
  - #vi /etc/login.defs
  - 修改配置文件
    - PASS_MAX_DAYS 180　　密码使用最长期限为180天
    - PASS_MIN_DAYS 1　　密码1天之内不能更改
    - PASS_WARN_AGE 28　　密码过期之前28天提示修改
    - PASS_MIN_LEN 8　　密码长度最小8位字符

- chage设置Linux帐号策略

  chage -m 0 -M 30 -E 2019-10-11 -I 3 -W 7 <用户名>

  chage -d 0 <用户名>（强制密码过期）

核心安全配置作用及参数 – 账号口令

```
MAIL_DIR        /var/spool/mail
#MAIL_FILE      .mail

# Password aging controls:
#
#       PASS_MAX_DAYS   Maximum number of days a password may be used.
#       PASS_MIN_DAYS   Minimum number of days allowed between password ch
#       PASS_MIN_LEN    Minimum acceptable password length.
#       PASS_WARN_AGE   Number of days warning given before a password exp
#
PASS_MAX_DAYS   99999
PASS_MIN_DAYS   0
PASS_MIN_LEN    5
PASS_WARN_AGE   7

#
# Min/max values for automatic uid selection in useradd
#
UID_MIN                  1000
UID_MAX                 60000
# System accounts
SYS_UID_MIN               201
SYS_UID_MAX               999

#
# Min/max values for automatic gid selection in groupadd
#
GID_MIN                  1000
GID_MAX                 60000
# System accounts
SYS_GID_MIN               201
SYS_GID_MAX               999

#
```

```
[root@localhost ~]# useradd test -p 123456
[root@localhost ~]#
```


NSFOCUS

核心安全配置作用及参数 – 账号口令

```
MAIL_DIR        /var/spool/mail
#MAIL_FILE      .mail

# Password aging controls:
#
#       PASS_MAX_DAYS   Maximum number of days a password
#       PASS_MIN_DAYS   Minimum number of days allowed betw
#       PASS_MIN_LEN    Minimum acceptable password length
#       PASS_WARN_AGE   Number of days warning given before
#
PASS_MAX_DAYS   99999
PASS_MIN_DAYS   0
PASS_MIN_LEN    8
PASS_WARN_AGE   7

#
# Min/max values for automatic uid selection in useradd
#
UID_MIN                  1000
"/etc/login.defs" 72L, 2028C
```

```
[root@localhost pam.d]# vim /etc/login.defs
[root@localhost pam.d]# passwd test
更改用户 test 的密码 。
新的 密码:
无效的密码: 密码少于 8 个字符
重新输入新的 密码:
```


NSFOCUS

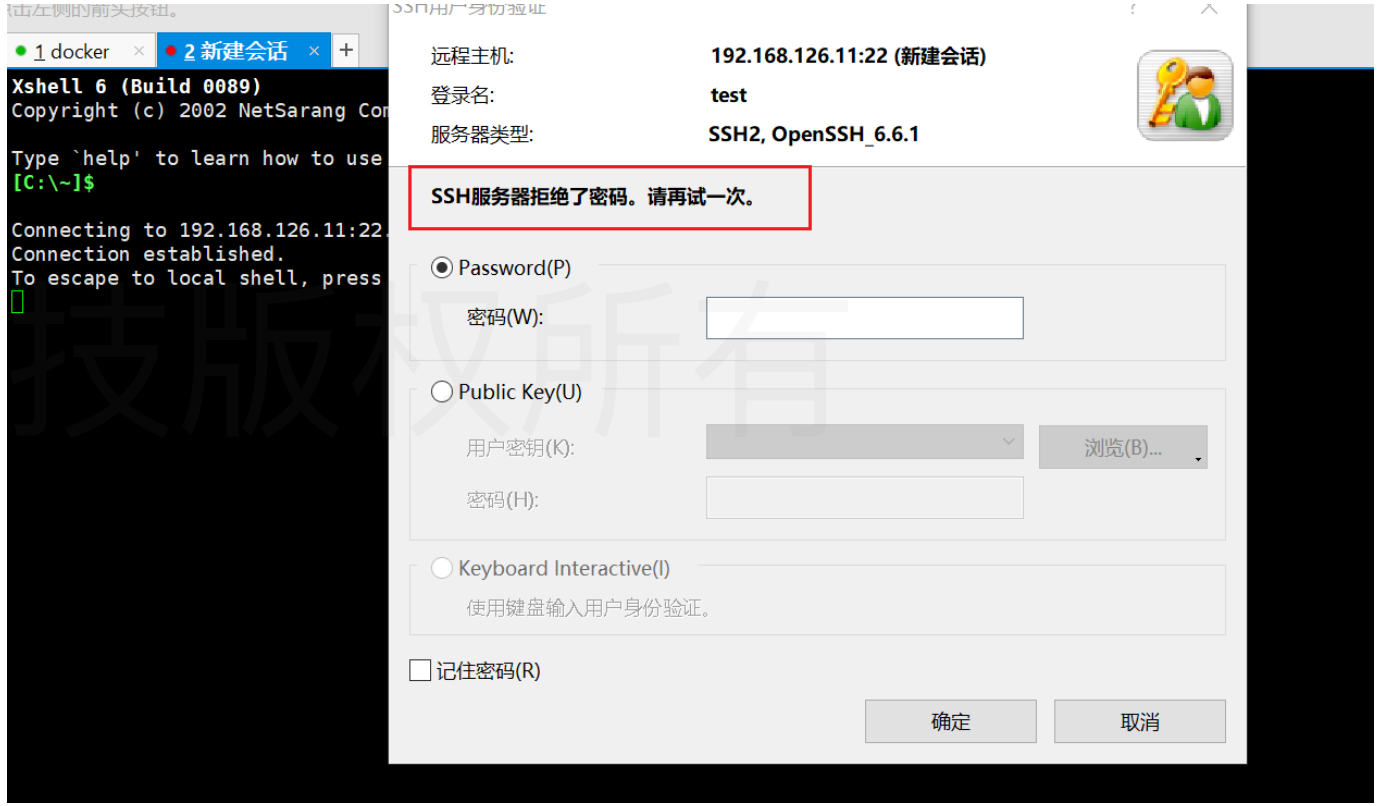
核心安全配置作用及参数 – 关闭不必要服务

- 关闭xinetd控制服务
  - 修改/etc/xinetd.d/目录下各服务的配置文件：
  - 把 disable = no 改为 yes
  - #service xinetd restart 重启xinetd
  - 其他需要关闭的服务有：
    telnet klogin kshell ntalk tftp

- 回退方法
  - 把xinetd.conf文件里关闭的服务，disable 改为 yes

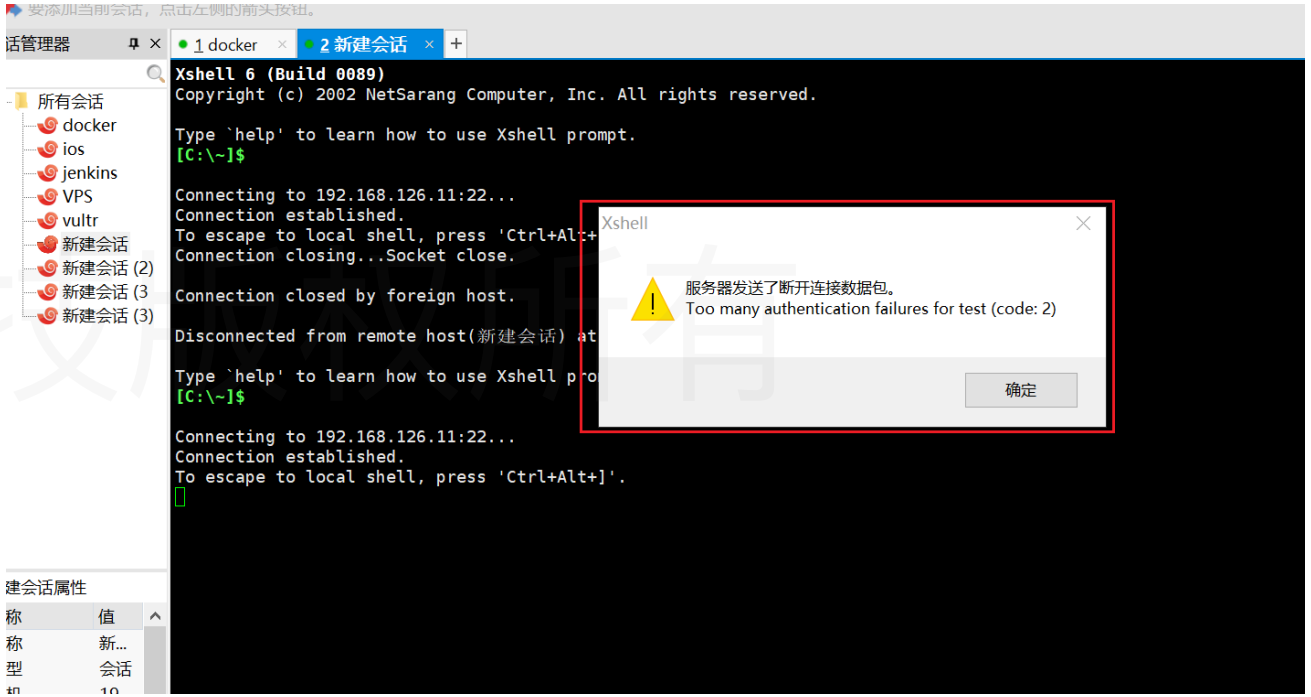
核心安全配置作用及参数 – 配置ssh服务

```
#RekeyLimit default none

# Logging
# obsoletes QuietMode and FascistLogging
#SyslogFacility AUTH
SyslogFacility AUTHPRIV
#LogLevel INFO

# Authentication:

#LoginGraceTime 2m
#PermitRootLogin yes
#StrictModes yes
#MaxAuthTries 6
#MaxSessions 10

#RSAAuthentication yes
#PubkeyAuthentication yes

# The default is to check both .ssh/authorized_
# but this is overridden so installations will
AuthorizedKeysFile      .ssh/authorized_keys

#AuthorizedPrincipalsFile none

#AuthorizedKeysCommand none
#AuthorizedKeysCommandUser nobody

# For this to work you will also need host keys
#RhostsRSAAuthentication no
```



核心安全配置作用及参数 – 配置ssh服务

```
#ServerKeyBits 1024

# Ciphers and keying
#RekeyLimit default none

# Logging
# obsoletes QuietMode and FascistLogging
#SyslogFacility AUTH
SyslogFacility AUTHPRIV
#LogLevel INFO

# Authentication:

#LoginGraceTime 2m
#PermitRootLogin yes
#StrictModes yes
MaxAuthTries 6
#MaxSessions 10

#RSAAuthentication yes
#PubkeyAuthentication yes

# The default is to check both .ssh/authorized_keys and .ssh/authorize
# but this is overridden so installations will only check .ssh/authori
AuthorizedKeysFile      .ssh/authorized_keys

#AuthorizedPrincipalsFile none

#AuthorizedKeysCommand none
#AuthorizedKeysCommandUser nobody

# For this to work you will also need host keys in /etc/ssh/ssh_known_
#RhostsRSAAuthentication no
```



FAQ

1 ssh登录日志位于哪个地方，日志中的每一项分别代表什么意思？如果存在攻击者暴力破解登录，ssh日志会有什么特征？

2 umask是什么？要配置umask的值需要修改什么文件？umask的值应该设置为多少？

3 PAM是linux的认证模块，如何通过PAM机制配置Linux系统的密码复杂度策略？

01

Oracle 安全配置解析

1. 安全防护机制简述
2. 安全配置分类说明
3. 核心安全配置作用及参数

NSFOCUS

2.1

安全防护机制简述

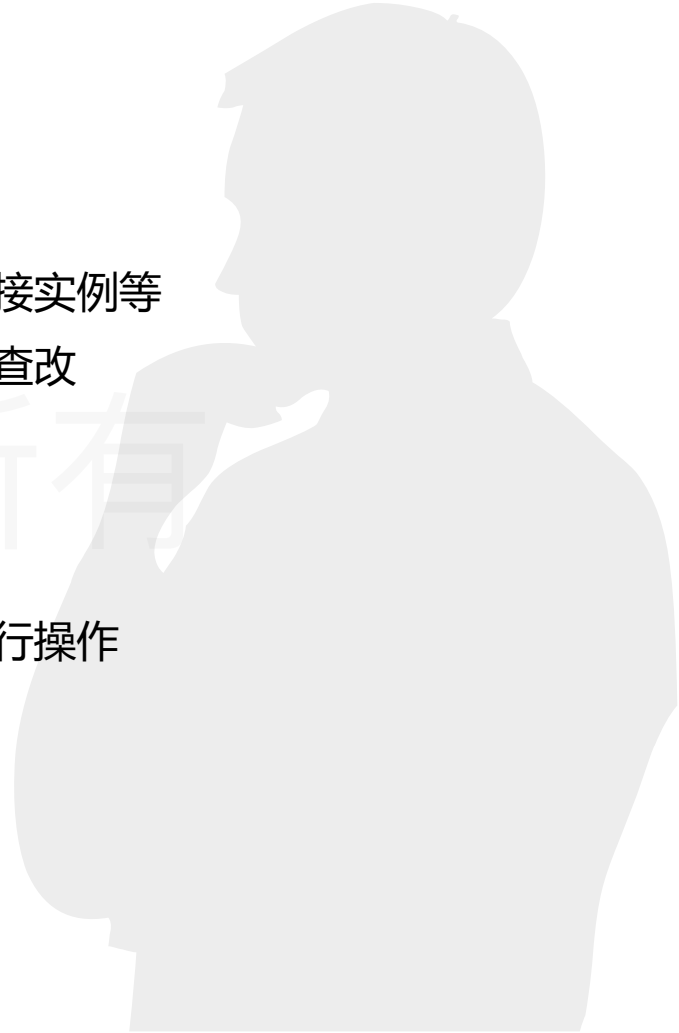
a. 用户角色、权限

b. 日志文件

c. 安全组件介绍

d. 补丁机制

安全防护机制简述 – 用户角色、权限



01.权限

- 系统权限：允许用户执行特定的数据库动作，如创建表，创建索引，连接实例等
- 对象权限：允许用户操作一些特定的对象，如读取视图，数据库的增删查改

02.角色

- 一组权限的集合，每个角色对数据库的操作权限不同
- 可以给用户赋予不同的角色，让用户具有对应角色的权限，对数据库进行操作

安全防护机制简述 – 用户角色、权限

01.DBA Role

数据库管理员角色，拥有所有的系统权限

无限制的空间限额，给其他用户授予各种权限

03.CONNECT Role

连接角色，给临时用户使用，特别是

那些不需要建表的用户

02.Resource Role

资源角色，更可靠更正式的数据库

用户可以授予该角色

安全防护机制简述 – 用户角色、权限

角色

权限

各角色各司其职

根据需要赋予用户不同的角色，一般按照用户的最低需求赋予用户对应的角色，保证低权限用户无法越权获取多余数据库信息，将对数据库的恶意伤害降低到最低

定操作

限控制，可以将不合特定用户，也可特定权限。权限划里用户提供便利

```
1  select * from user_role_privs;
```

dba用户具有的角色

信息 | Result 1

USERNAME	GRANTED_ROLE	ADMIN_OPTION	DEFAULT_ROLE	OS_GRANTED
SYS	ADM_PARALLEL_EXECUTE_TASK	YES	YES	NO
SYS	APEX_ADMINISTRATOR_ROLE	YES	YES	NO
SYS	AQ_ADMINISTRATOR_ROLE	YES	YES	NO
SYS	AQ_USER_ROLE	YES	YES	NO
SYS	AUTHENTICATEDUSER	YES	YES	NO
SYS	CONNECT	YES	YES	NO
SYS	CSW_USR_ROLE	YES	NO	NO

保存 | 查询创建工具 | 美化 SQL | 文本 | 导出结果

oracle_11g | 运行

```
1  select * from user_sys_privs
```

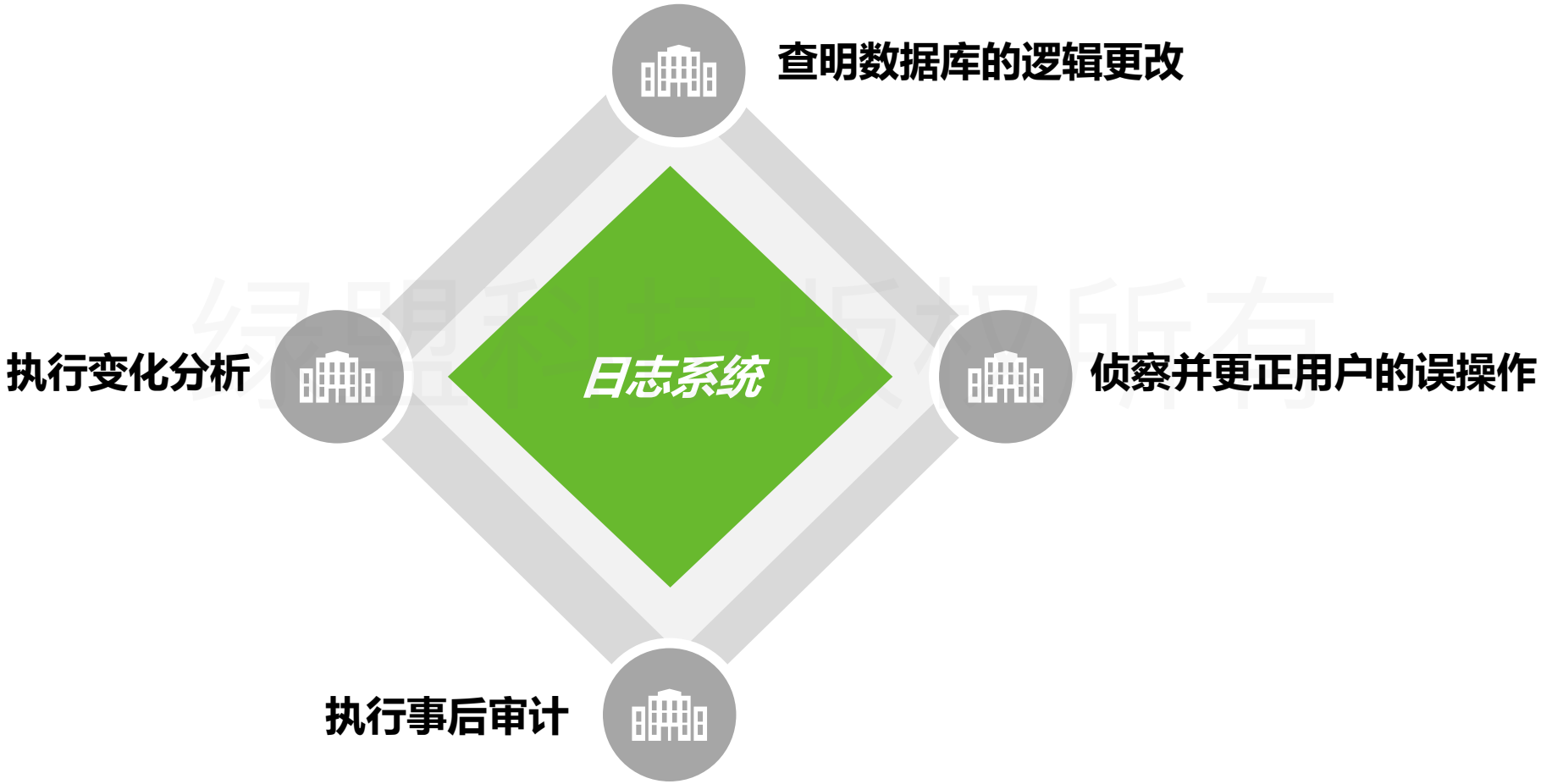
dba用户具有的权限

信息 | Result 1

USERNAME	PRIVILEGE	ADMIN_OPTION
SYS	AUDIT SYSTEM	NO
SYS	ALTER SESSION	NO
SYS	ALTER ROLLBACK SEGMEN	NO
SYS	ALTER ANY CLUSTER	NO
SYS	CREATE ANY INDEX	NO
SYS	CREATE DATABASE LINK	NO
SYS	DROP PUBLIC DATABASE I	NO
SYS	GRANT ANY ROLE	NO
SYS	ALTER ANY ROLE	NO
SYS	EXECUTE ANY PROCEDUR	NO
SYS	CREATE ANY MATERIALIZ	NO
SYS	ALTER ANY INDEXTYPE	NO

NSFOCUS

安全防护机制简述 – 日志文件



安全防护机制简述 – 日志文件

01.告警日志（Alert log files）

- 所有内部错误（ORA-600）、块损坏错误(ora-578)、死锁(ORA-60)信息等
- 管理操作，如CREATE，DROP语句，以及数据库启动，关闭等信息
- 物化视图的自动刷新过程中出现的错误
- ……

02.跟踪日志 (Trace files)

- 记录数据库在启动、关闭、运行期间后台进程的活动情况
- 连接到Oracle的用户进程生成的用户跟踪文件
- ……

03.重做日志 (Redo log)

- 记录每一个对数据库的更改
- 提供一种恢复机制
- …….

安全防护机制简述 – 日志文件

告警日志

管理员可根据告警日志了解数据库的变化与异常，及时响应并介入处理

跟踪日志

对于了解数据库应用的内部工作有着非凡意义

重做日志

通过记录数据的所有改变情况对系统或者介质故障提供恢复机制

安全防护机制简述 – 安全组件介绍

Oracle 组件

由Oracle公司提供的工具程序，在oracle的安装过程中可根据需要安装相应的组件，后续利用这些组件对数据库进行管理

一	二	三	四	五
• 为管理、调试数据库提供便利	• 提升数据库的安全性	• 给数据库提供容错机制	• 提升数据库性能	• ……

安全防护机制简述 – 安全组件介绍

VPD（虚拟专用数据库）

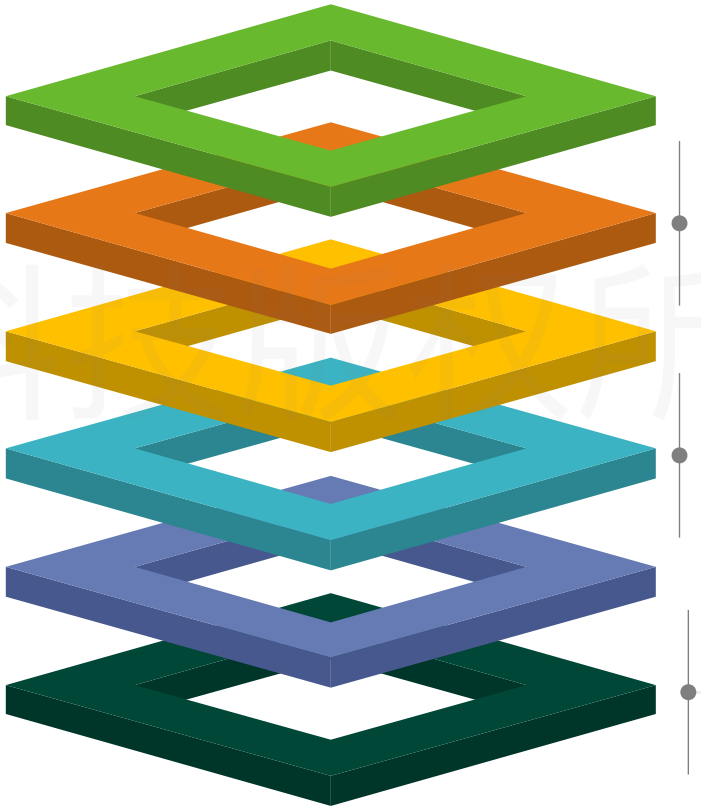
提供角色和视图无法提供的行级访问控制，确保每个用户只能看到同一张表中属于自己的行，无法查看其他用户的数据.

Oracle Audit Vault

自动将审计数据合并到一个安全的数据仓库，使得能够更加有效的进行监控和报告

TDE（透明数据加密）

当用户插入数据库自动将数据加密存储，读取数据时自动将数据进行解密，防止存储介质丢失后数据被攻击者读取.



Oracle Database Vault

1 保护敏感数据
2 防止未授权的数据库更改
3 利用多种可信因素来授权访问
4 ……

Oracle Label Security

通过创建一个或者多个安全策略，每个策略包含一组标签指定用户可访问哪种类型的数据。

……

安全防护机制简述 – 补丁机制

What?

Oracle针对其产品在使用的过程中暴露的缺陷，发布特定的小程序对缺陷进行修复，这些小程序俗称补丁

How ?

Oracle具有健全的补丁体系，存在多个种类的补丁，每种补丁的作用不同。

Who ?

Windows系统，Linux系统，集群环境，单机环境……

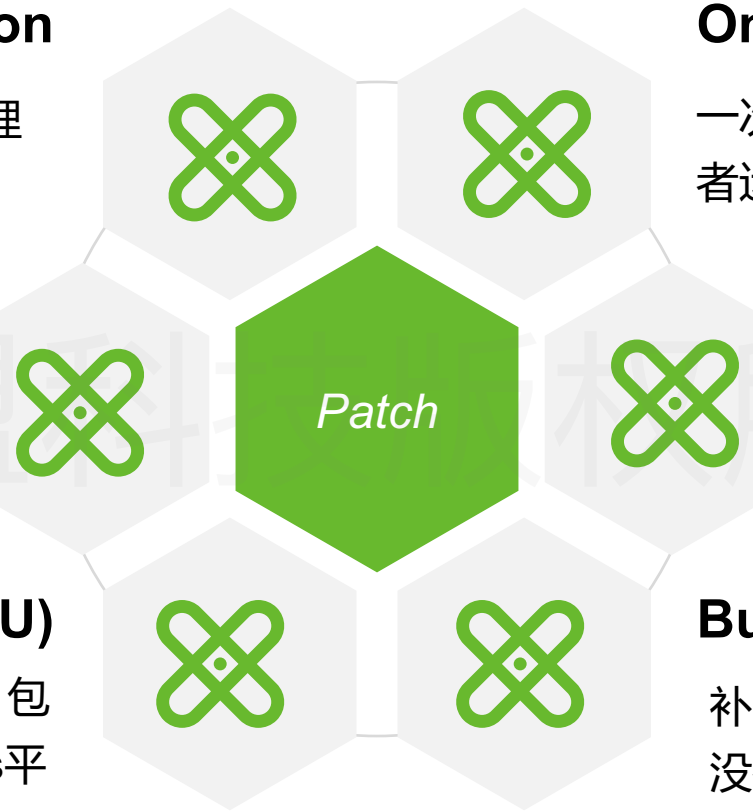
安全防护机制简述 – 补丁机制

Release Version

针对前一个维护版本的所有补丁进行整理

One-off patches

一次性补丁，针对特定的数据库版本或者运行平台通常较小，使用最为频繁



Merged patch

合并的补丁，当几个小补丁有冲突时，需要提供这种Merged Patch

Critical Patch Update(CPU)

每季度提供一次的高优先级修复程序，往往针对安全问题。积累型补丁，只需要安装最近最后一个即可

Patch set update(PSU)

每季度发布一次，修复比较严重的问题，包含每季度的CPU，也为累积型，windows平台上没有cpu和psu

Bundle patch

补丁集，修复多个Bug,在windows平台上没有小补丁，只有这种补丁集，至少每季度发布一次，也为累积型

2.1

安全配置分类说明

a. 账号与口令管理

b. 认证授权管理

c. 日志安全要求

d. 其他（保密要求等）

安全配置分类说明 – 账号与口令管理

账号口令

1 密码复杂度

- 要求：口令长度至少为8位，并包括数字，小写字符，大写字符和特殊符号4类中至少两类
- 作用：防止用户采用弱口令，防止攻击者通过口令猜测的方式入侵数据库

2 默认账号口令

- 要求：应修改默认的账户密码
- 作用：防止攻击者通过默认的账号密码，类似于system/system这样方式入侵数据库

3 用户属性控制

- 要求：为数据库用户创建prifile策略文件
- 作用：profile策略文件中设置了用户账号密码相关安全项，保证账号安全性

4 账号口令生存期

- 要求：账号口令的生存期不大于90天
- 作用：强制用户更改密码，防止攻击者通过社工或者撞库的方式登陆数据库

安全配置分类说明 – 账号与口令管理

5 删除不必要账号

要求：应删除或者锁定与数据库运行、维护等工作无关的账号

作用：去除无用账号，防止他人利用这些账号进行数据库操作，危害数据库安全

6 重复口令使用策略

要求：用户不能重复使用最近5次（含5次）内已使用的口令

作用：禁止用户采用重复口令，防止用户密码泄露以及撞库带来的数据库风险

7 密码更改策略

要求：所有开启用户的口令到达终止时间后的宽限天数不大于7天

作用：强制用户更改到期口令

安全配置分类说明 – 认证授权管理

认证授权

要求

应设置oracle数据库所有开启用户的连续失败登陆次数限制不大于10次

作用

防止攻击者通过暴力破解的方式将用户的密码猜解出来

安全配置分类说明 – 日志安全要求

日志审计

要求

应开启数据库日志审计功能

作用

通过日志审计功能，可审查可疑的活动，监察和收集关于指定数据库活动的数据

安全配置分类说明 – 其他

超级管理员远程登陆限制

要求：禁止具有超级管理员权限的用户远程登陆

作用：防止攻击者从某种方式获取超级管理员账号密码后远程登陆，危害数据库安全

Oracle监听器

要求：应设置oracle监听器保护

作用：oracle监听器在初始状态下是没有口令的，通过设置监听器的口令能够防止监听器被免密登陆

Oracle数据字典访问权限

要求：应启用数据字典保护，限制是有SYSDBA用户才能访问数据字典基础表

作用：防止其他低权限用户获取数据字典里面的数据

Oracle数据字典访问限制

要求：应配置限制IP登陆的开关限制，应设置只有信任的IP地址才能哦通过监听器访问数据库

作用：防止攻击者通过不信任IP对数据字典进行访问

Oracel断开超时的空闲远程连接

要求：设置Oracel数据库连接超时时，将自动断开超过规定时间的空闲远程连接

作用：释放数据库连接资源，提高数据库性能

1.3

核心安全配置作用及参数

a. 账号与口令配置

b. 认证授权配置

c. 日志审计配置

NSFOCUS

账号与口令配置– 密码复杂度策略

密码复杂度策略文件

- Oracle设置密码复杂度的策略文件位于&ORACLE_HOME/rdbms/admin/文件夹中的utlpwdmg.sql文件中

密码复杂度函数

策略文件中的verify_function_11G为密码复杂度验证函数，该函数中设置了一系列的密码复杂度检测步骤，修改该文件内容即可定制复杂度策略

执行修改命令

以dba权限的用户登陆进sqlplus后执行命令：@?/rdbms/admin/utlpwdmg.sql即可配置密码复杂度策略

账号与口令配置– 密码复杂度策略

```
-- 密码至少含有一个字符一个数字
-- Check if the password contains at least one letter, one digit
-- 1. Check for the digit
isdigit:=FALSE;
m := length(password);
FOR i IN 1..10 LOOP
   FOR j IN 1..m LOOP
      IF substr(password,j,1) = substr(digitarray,i,1) THEN
         isdigit:=TRUE;
          GOTO findchar;
      END IF;
   END LOOP;
END LOOP;
```

```
--创建密码最小长度，length(password)<8 表示密码最小长度为 8
-- Check for the minimum length of the password
IF length(password) < 8 THEN
   raise application error(-20001, 'Password length less than 8');
END IF;
```

账号与口令配置– 密码复杂度策略

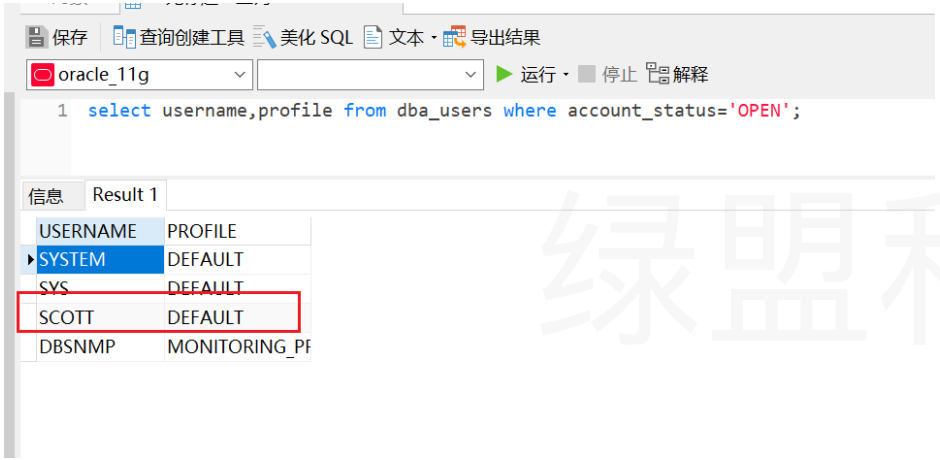
```
SQL> create user testq21 identified by "123";
create user testq21 identified by "123"
*
ERROR at line 1:
ORA-28003: password verification for the specified password failed
ORA-20001: Password length less than 8


SQL>
```

```
SQL> create user testq21 identified by "111111111";
create user testq21 identified by "111111111"
*
ERROR at line 1:
ORA-28003: password verification for the specified password failed
ORA-20009: Password must contain at least one \
digit, and one character


SQL>
```

认证授权配置-连续登陆失败锁定

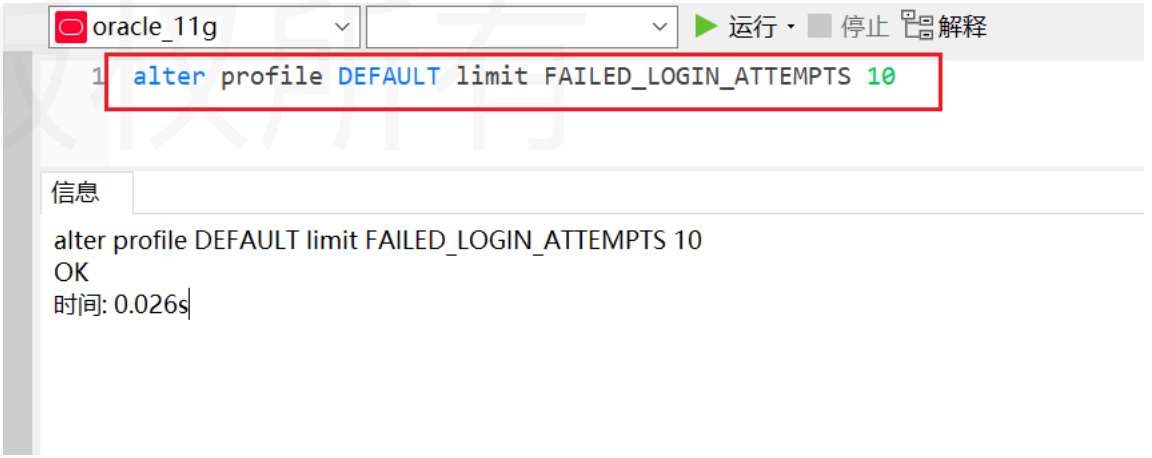
检查要配置该连续失败登陆锁定策略的用户的策略文件

01



02

修改策略文件中的对应项的值，将其修改为10



认证授权配置-连续登陆失败锁定

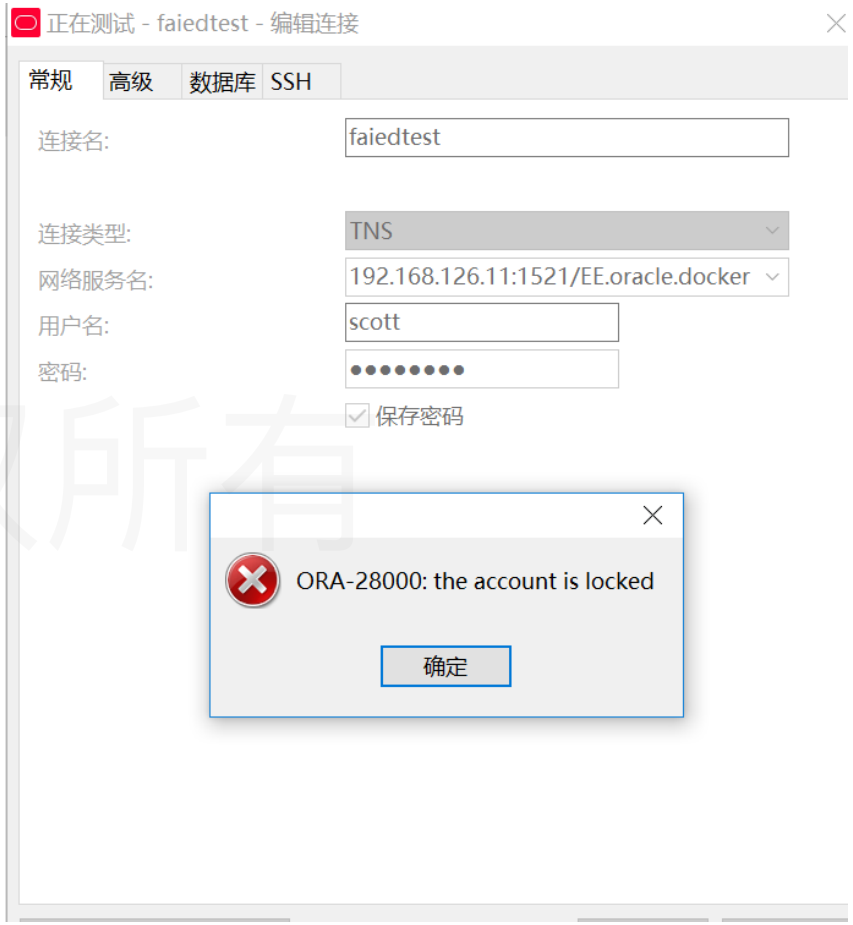
保存 查询创建工具 美化 SQL 文本 导出结果

oracle_11g 运行 停止 解释

```
1  select resource_name,limit from dba_profiles where profile='DEFAULT' and resource_type=
   'PASSWORD'
```

信息 Result 1

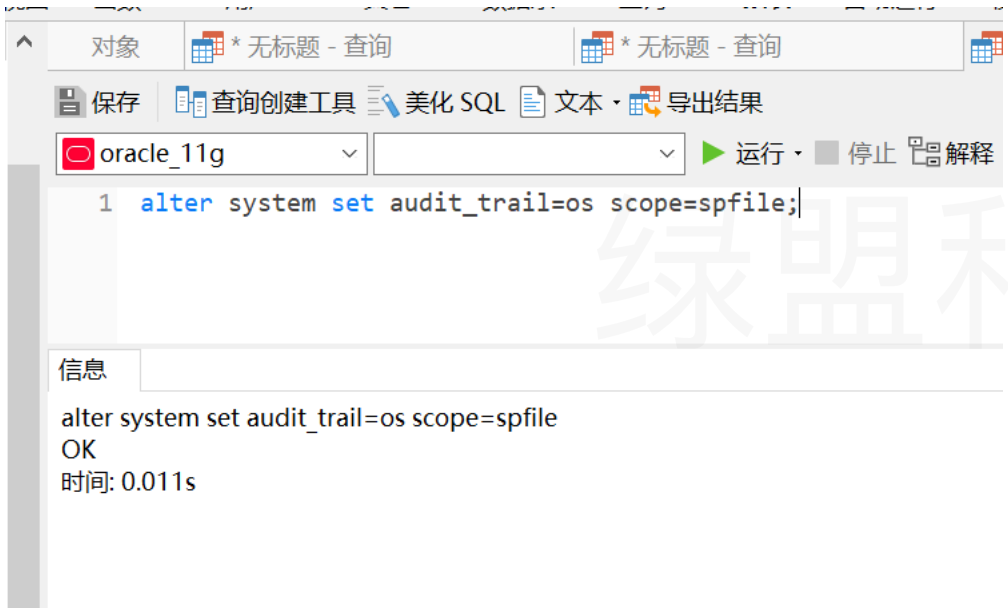
RESOURCE_NAME	LIMIT
FAILED_LOGIN_ATTEMPTS	10



日志审计配置-开启数据库日志审计

配置数据库开启数据库日志审计

01

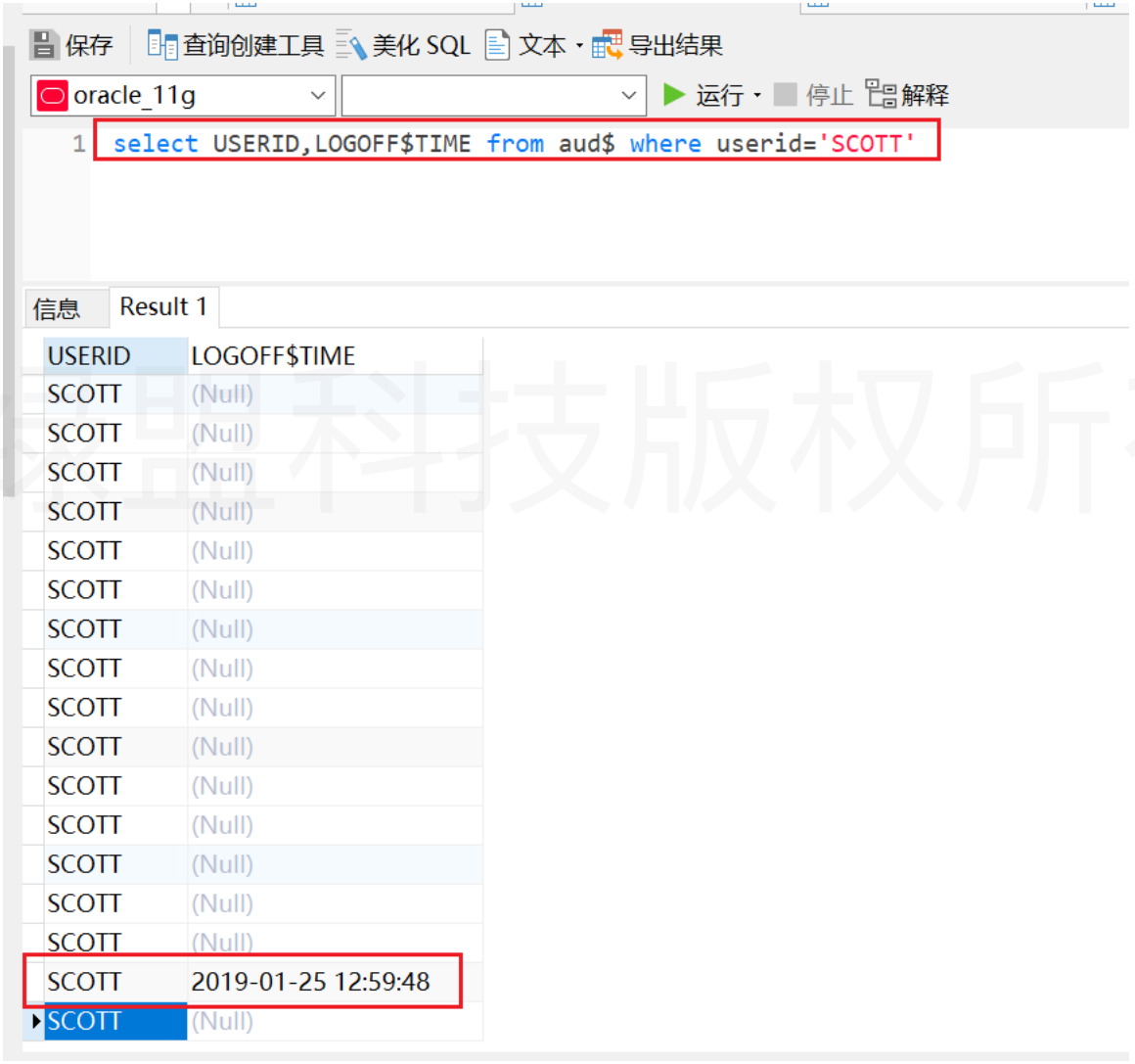


02

关闭并重启数据库，检查audit_trail是否非none

```
SQL> show parameter audit_trail;

NAME                                 TYPE        VALUE
------------------------------------ ----------- ------------------------------
audit_trail                          string      OS
SQL>
```

日志审计配置-开启数据库日志审计功能



FAQ

1 oracle有哪些默认账号口令？其默认账号口令分别是什么?

2 是否一定要关闭远程登陆功能？关闭远程登陆功能的利与弊？

04

Apache 安全配置解析

1. 安全防护机制简述
2. 安全配置分类说明
3. 核心安全配置作用及参数

NSFOCUS

4.1

安全防护机制简述

a. 认证和授权

b. 通信安全

c. 日志文件

安全防护机制简述 – 认证和授权

01.认证

- 访问者是否具有权限进入Apache服务所提供的资源池中。

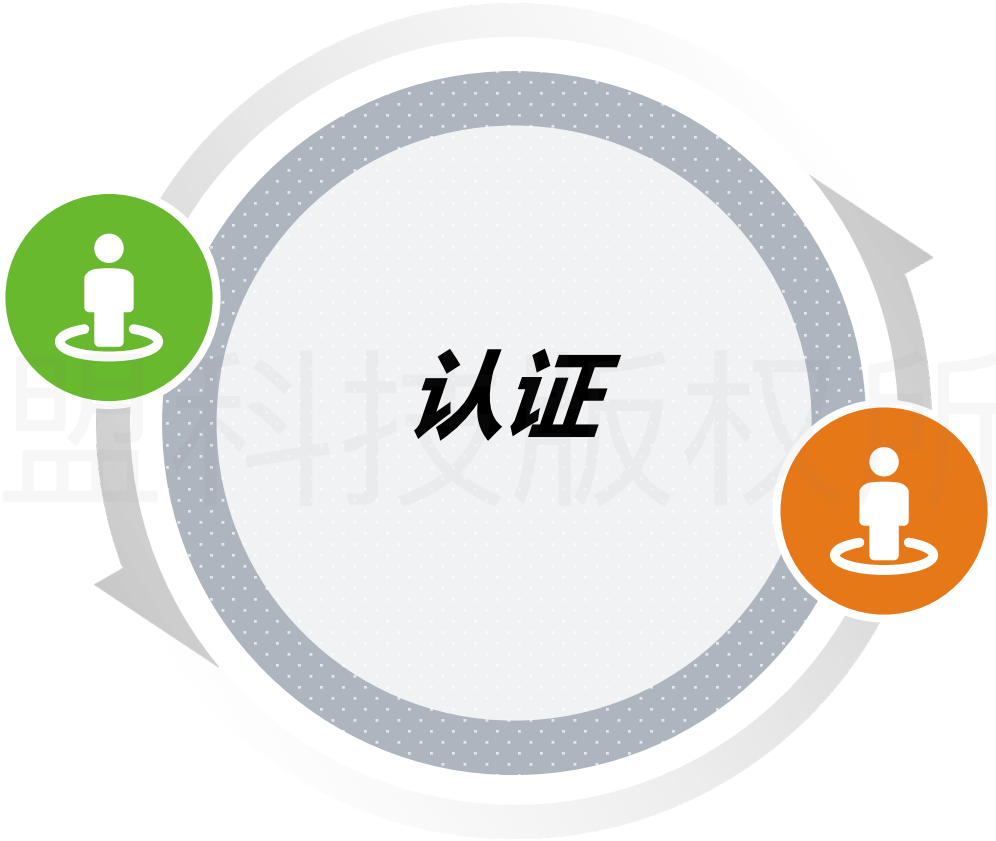
02.授权

- 访问者是否具有权限访问Apache服务资源池中的特定资源。

安全防护机制简述 – 认证和授权

明文认证

以明文的方式建给用户名与密码发送至服务器，服务器接受到用户名与密码后在认证文件或者数据库中进行比对，以此判断成功



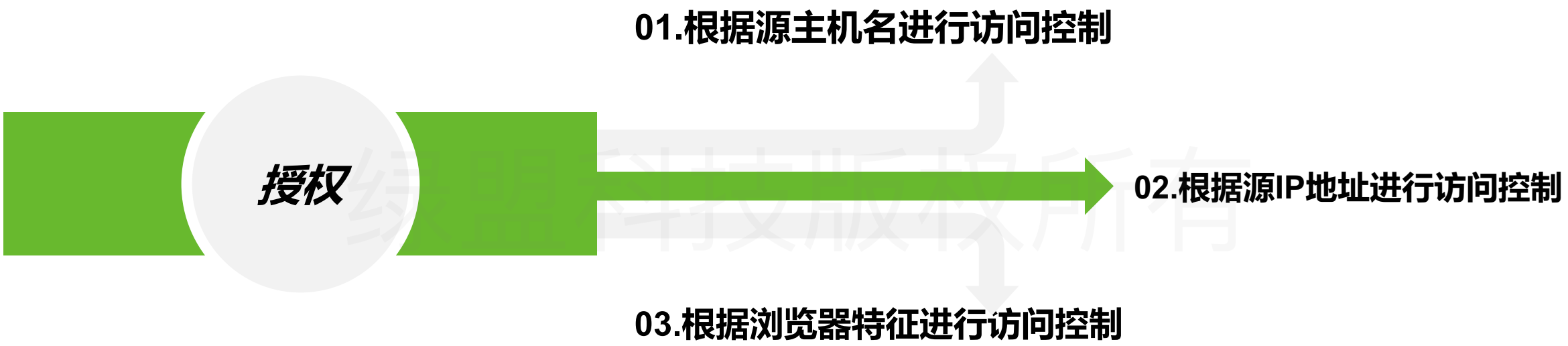
摘要认证

将用户输入的密码进行散列算法后发送给服务器，一定程度上提高了用户密码的安全性

安全防护机制简述 – 认证和授权

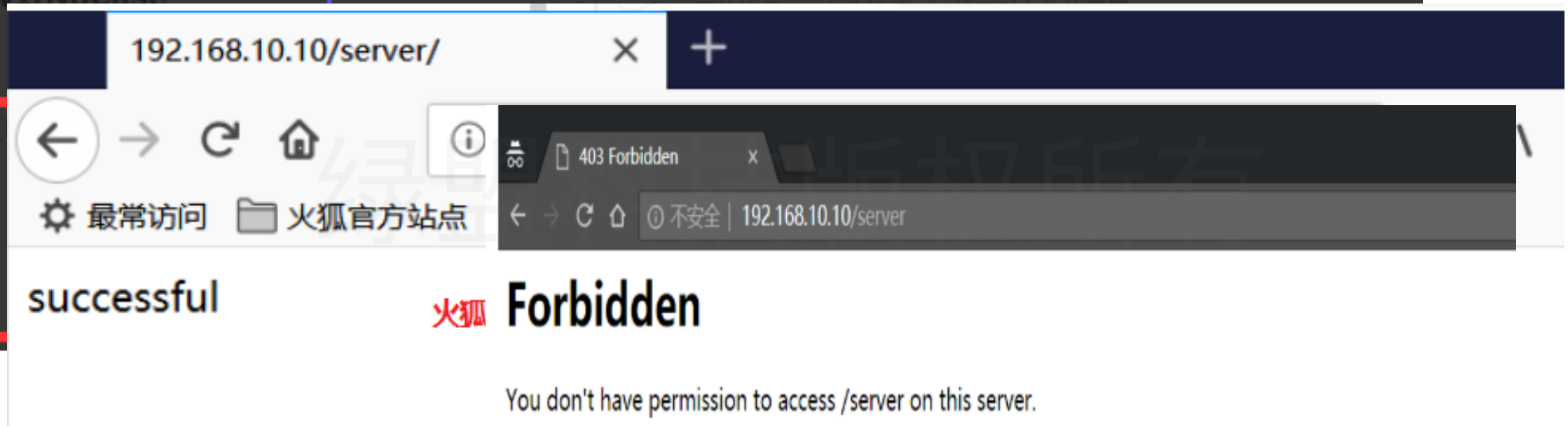
```
#则需要重新编译apr-util，是它生成一个名为apr_dbd_mysql.so的动态链接库。
Listen 80
ServerName localhost
```

安全防护机制简述 – 认证和授权



安全防护机制简述 – 认证和授权

```
124 <Directory "/var/www">
125     AllowOverride None
126     # Allow open access:
127
128
129
130
131
132
133
```



安全防护机制简述 – 通信安全

How

采用SSL，也就是HTTPS协议传输数据

why

Apache服务器与客户端的通信是明文方式，因此通过HTTP协议传送数据将会受到黑客的威胁

what

服务端与客户端交换信息的方式

安全防护机制简述 – 日志文件

访问日志	记录所有对Web服务器的访问活动
错误日志	记录了服务器运行期间遇到的各种错误

安全防护机制简述 – 访问日志

01.远程IP地址

表明访问网站的是谁

02.E-mail

记录了访问者的邮箱，一般不记录，用-代替

03.登陆名

用于记录浏览者进行身份验证时提供的名字

04.请求时间

用方括号保卫，记录请求者请求的时间

05.方法+资源+协议

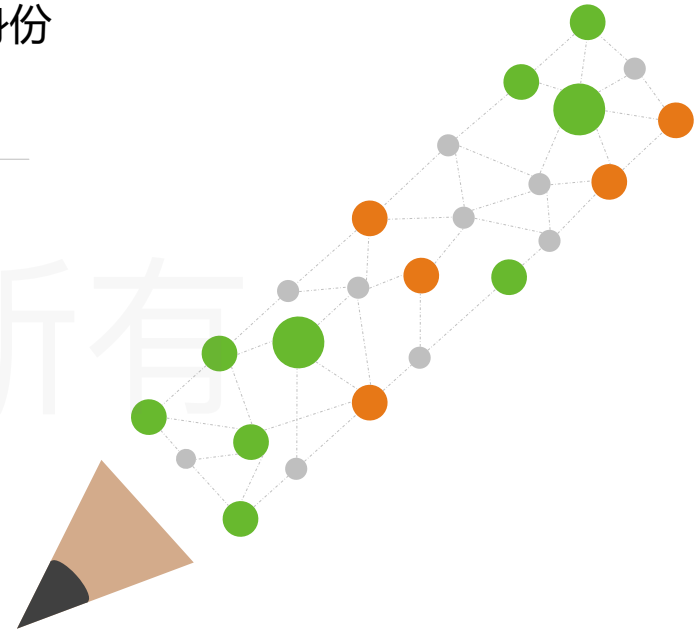
服务器收到的是一个什么样的请求

06.状态代码

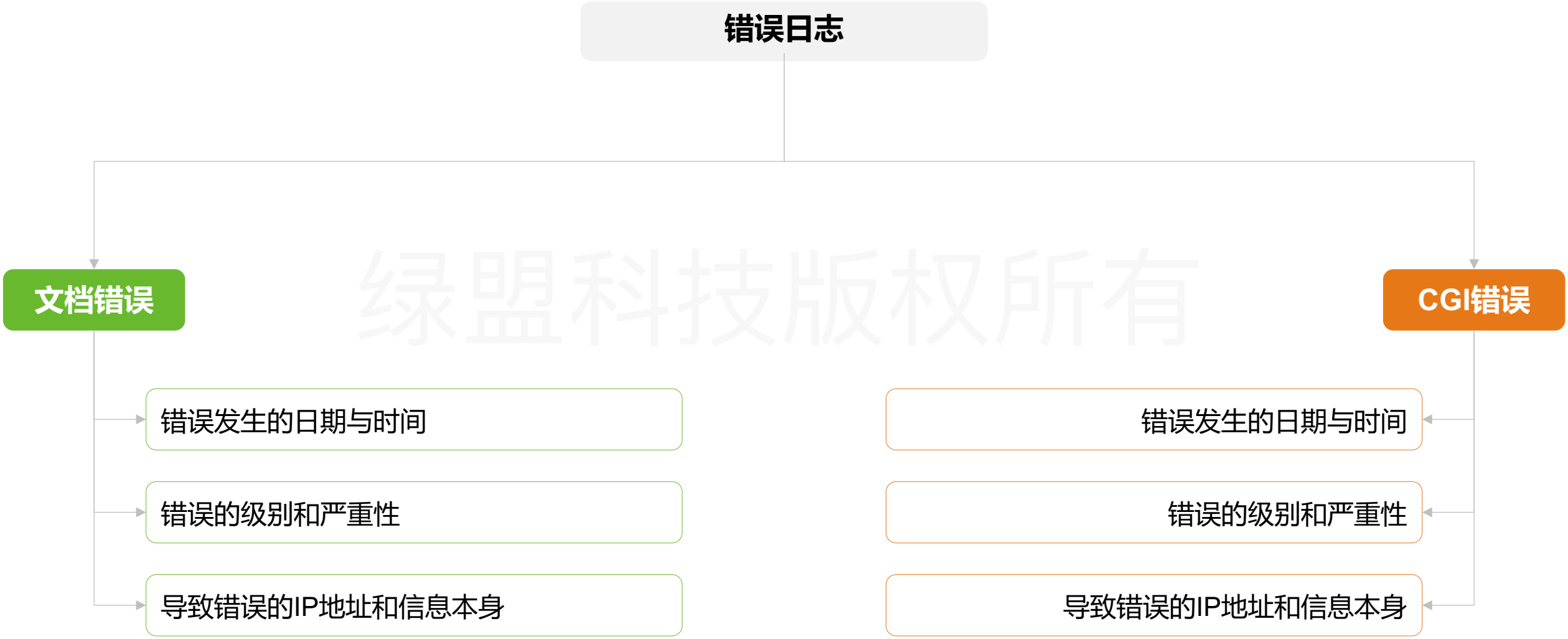
请求是否成功，或者是遇到了什么样的错误

07.发送字节数

发送给客户端的字节数



安全防护机制简述 – 错误日志



4.2

安全配置分类说明

a. 认证授权
b. 日志审计
c. 协议安全
d. 其他安全

安全配置分类说明 – 认证授权

1

为Apache创建单独的账号和组

要求：以专门的用户账号和组运行Apache

作用：为系统上的文件读取等作出限制，确保文件安全等。

2

配置/日志文件的访问权限

要求：限制非owner用户对配置/日志文件的访问权限

作用：确保非Apache的用户修改配置和日志文件，影响Apahce运行

3

Apache服务器保护

要求：禁止非root用户修改apache服务器根目录

作用：确保非Apache对服务器目录进行修改，影响Apache运行

安全配置分类说明 – 日志审计

1

配置错误日志

要求：配置Apache开启错误日志

作用：记录Apache在运行过程中出现的错误。

2

配置/日志文件的访问权限

要求：配置Apache开启访问日志

作用：记录何时何人何地访问什么资源等信息，可用于入侵排查

3

Apache服务器保护

要求：配置日志格式

作用：配置日志记录内容的格式，可记录较为详细的内容

安全配置分类说明 – 协议安全

协议安全

要求

配置Apache使用HTTPS协议进行数据传输

作用

防止服务端与客户端的数据别恶意攻击者获取。

安全配置分类说明 – 其他安全

01.禁止Apache显示目录结构

杜绝目录浏览漏洞.

02.禁止访问Web目录外的文件

保护非Web目录下的文件不被恶意攻击者所访问

03.删除默认安装的无用文件

删除无用文件

04.禁止PUT、DELETE、TRACE等危险方法

防止攻击者通过这些为危险方法进行攻击

05.隐藏Apache版本号

防止多余的敏感信息泄露，恶意攻击者可通过获取版本号觉得下一步攻击

06.禁用CGI

防止攻击者通过CGI目录执行系统命令

07.设置错误页面重定向

防止错误页面输出敏感的错误信息

4.3

核心安全配置作用及参数

a. 禁止目录遍历

b. 禁止访问Web目录以外的文件

c. 禁用PUT、DELETE、TRACE

核心安全配置作用及参数 – 禁止目录遍历

- 作用：禁止Apache显示目录中的文件
- 参数：在httpd.conf配置文件中，将所有Options关键字后的Indexes去掉，如

```
<Directory "/Web">
Options FollowSymlinks
</Directory>
```

目录遍历

```
# Further relax access to the default document root:
<Directory "/var/www/html">
    #
    # Possible values for t
    # or any combination of
    #   Indexes Includes Fo
    #
    # Note that "MultiViews
    # doesn't give it to yo
    #
    # The Options directive
    # http://httpd.apache.o
    # for more information.
    #
    Options Indexes Follow

    #
    # AllowOverride control
    # It can be "All", "Non
    #   Options FileInfo Au
    #
    AllowOverride None

    #
    # Controls who can get
    #
    Require all granted
</Directory>

#
```

不安全 | 192.168.126.11/dvwa/

Index of /dvwa

Name	Last modified	Size	Description
Parent Directory		-	
css/	2019-05-14 14:45	-	
images/	2019-05-14 14:45	-	
includes/	2019-05-14 14:45	-	
js/	2019-05-14 14:45	-	

禁止目录遍历

```
# Further relax access to the default document root:
<Directory "/var/www/html">
    #
    # Possible values for the Options directive are "None", "All",
    # or any combination of:
    #   Indexes Includes FollowSymLinks SymLinksifOwnerMatch ExecCGI MultiViews
    #
    # Note that "MultiViews" must be named *explicitly* --- "Options All"
    # doesn't give it to yo
    #
    # The Options directive
    # http://httpd.apache.o
    # for more information.
    #
    Options FollowSymLinks

    #
    # AllowOverride control
    # It can be "All", "Non
    #   Options FileInfo Au
    #
    AllowOverride None

    #
    # Controls who can get
    #
    Require all granted
</Directory>

#
# DirectoryIndex: sets the
```

禁止访问Web目录以外的文件

- 作用：防止目录遍历到根目录从而造成任意文件下载
- 参数：在配置文件httpd.conf中添加如下语句，禁止对根目录的访问：

```
<Directory />
Order deny,allow
Deny from all
</Directory>
```

禁用PUT、DELETE、TRACE

- 作用：PUT上传文件；DELETE删除文件；TRACE回显服务器收到的请求
- 参数：在httpd.conf中，添加如下内容：

```
<LimitExcept GET POST>
Deny from all
</LimitExcept>
TraceEnable Off
```

FAQ

1 Apache的日志存放在哪？日志中记录的每一项内容代表什么？当出现扫描器对网站进行扫描时，日志会有什么特征？

2 如果应用存在后台，如何配置后台目录，使得后台只允许特定IP进行访问？

谢谢！

NSFOCUS