•猜测的点、注意事项：

1、Linux Web 代理，例如 nginx，假如后端 web 有多个站点（用不同域名区分），此时 nginx 代理上没有配置 proxy_set_header Host $host; 这就会导致代理的 Host 头部为 IP，导致所有请求都只发给了默认站点，其他域名就无法访问了。
2、：Windows/Linux 机器（所有模块通用）有着 IPv4 与 IPv6 双栈 IP，IPv4 地址配置了网关，IPv6 地址没有配置网关，IPv4 和 IPv6 同时配置了 dns 服务器地址，Windows 优先会使用 IPv6 的 DNS 服务器，客户端与 DNS 服务器不在同一网段，此时一方没有配置 IPv6 的网关，导致 IPv6 的 DNS 服务器地址无法通信，但是 IPv4 地址是通的，导致无法解析域名
3、# MPLS：
配置 vrf NAT 时，例如环境：R1（vrf NAT） - R2 - R3 - Client
R1 上有全局默认路由，R2、R3 上也有全局默认路由，但是 R1 上没有 vrf 的出口默认路由，就会导致客户端 nat 无法出去，看似是 nat 的问题，其实是路由的问题
4、在 windows 中，默认情况下，一个目录中：Abc 和 abc 是被视为同一个 文件、文件夹，它默认是不区分大小写的，并且不能够同时存在两个名字一样但是大小写不一样的 文件、文件夹，例如不允许同时存在 Abc、abc 文件、文件夹
但是如果开启了：fsutil.exe file SetCaseSensitiveInfo C:\test enable 后，这个路径下的文件就会严格区分大小写，并且能够同时存在 Abc、abc 这样的 文件、文件夹，例如此时一些路由要访问的是 Abc，但是路径写的是 abc，那么就会导致出问题
5、目录权限必须要有 x 权限，如果目录没有 x 权限，例如是 644 时，就会导致这样的问题，例如：ftp 能够登陆成功，但是无法查看目录，ls 是报错的，这样你排除时就会被误导以为是 20 端口被阻断，而且看文件夹权限时，644 不注意还发现不了问题。所以这里文件夹权限需要是 755
6、（C 模块）排错可能在某个路由器、或者网关接口上不开启 M 和 O 选项，并且关闭了 SLAAC 导致客户都无法获取 IPv6 地址，并且 DNS 解析到的地址还是 IPv6

一、SSH

1、Linux SSH：

1）host key 丢失，导致 ssh、sshd 服务无法启动：

排查过程：
systemctl status sshd 发现服务没启动；
ls /etc/ssh 发现该目录下文件明显少于其他主机

Ticket No. 9

Message from the client	*Hello,* *I am responsible for operating the Proxy service.* *I attempted to connect from the CLIENT1 device to the DEBSRV1 server via SSH in order to update the Proxy service configuration, but the connection is currently failing. As a result, we are unable to proceed with the scheduled Proxy service configuration changes and server update tasks.* *Since the service update is being delayed, please take prompt action to ensure that CLIENT1 can connect to DEBSRV1 via SSH successfully.*
Description of the root cause of the problem	The SSH daemon on DEBSRV1 is inactive. The logs report a no hostkeys available error, and no SSH host keys exist in the /etc/ssh directory.
Recommended solution	Generate SSH host keys in /etc/ssh on DEBSRV1 using the ssh-keygen -A command. Restart the SSH daemon: systemctl restart ssh

2）sshd.service 中配置了 ConditionPathExists，导致服务无法启动：

Troubleshooting Ticket 10

Hey, I think there's an issue with svr2. When I try to access it via SSH using the tech02 account from svr1, it doesn't work. Did you configure any security settings on the server or apply firewall rules that might be blocking access?

Problems:

SSH cannot be started due to /etc/ssh/sshd_not_to_be_run file exists on svr2

Maximum session login for user in @tech group on the svr2 is set to 0 on /etc/security/limits.conf

On SVR2:

The sshd service can not be started, because the /etc/systemd/system/sshd.services is incorrectly set "ConditionPathExists=!/etc/ssh/sshd_not_to_be_run"

Maximum session login for user in @tech group on the svr2 is set to 0 on /etc/security/limits.conf

Solutions:

Remove /etc/ssh/sshd_not_to_be_run file on svr2

Disable maximum session login on /etc/security/limits.conf OR remove the configuration about the maximum session login

3）用户 shell 是 /usr/sbin/nologin：

Troubleshooting ticket 6

Problem

Dear Sir or madam,
I am having trouble connecting to lnx01 over SSH with my local user account, john with Skill39@Lyon as the password, from lnx03. I tried to login locally over Console too, I am not able to login. I'm sure the password is correct.

What are the causes of the problem?

- Wrong shell has been set for user john
- User john is only allowed to login locally and not remotely

On LNX01:
The john user shell is /usr/sbin/nologin instead of /bin/bash or /bin/sh.
The /etc/security/access.conf is defined john user can login locally, can not login remotely.

Recommended solutions to fix this:

- Fix shell of user john to /bin/bash or /bin/sh in /etc/passwd (other solutions resulting to this state are accepted as well) on lnx01
- Adjust access rule in /etc/security/access.conf on lnx01
  - Change line from +:john:LOCAL to +:john:ALL in /etc/security/access.conf on lnx01. In addition, remove line -:john:ALL
  - Alternative solution: Remove lines "+:john:LOCAL" and "-:john:ALL" in /etc/security/access.conf

2、Cisco SSH：

1）SSH 密钥长度小于 1024 bit 导致 SSHv2 是禁用状态：

Troubleshooting ticket 5

Problem

Our team is having trouble connecting to the HQRTR02 over SSH using IPv6 over its loopback interface from lnx01. We are currently attempting with the admin user. Can you please have a look into it?

What are the causes of the problem?

- Loopback0 is not advertised in OSPFv3
- SSH version 2 is disabled due to missing a capable SSH key with a minimum length of 1024 bit.

On HQRTR02:
The loopback0 is not advertise in OSPFv3 process.
The SSH version 2 is disable, because the SSH key length is less than 1024 bit.

Recommended solutions to fix this:

- Advertise Loopback0 to OSPFv3

```
interface Loopback0
 ipv6 ospf 1 area 0
```

- Generate new SSH key with min length of 1024 with crypto key generate rsa

二、mail:

1、dovecot 没有开启 SASL 的 unix 监听:

在客户端上查看、用 systemctl status postfix 发现发送报错
查看 main.cf 文件发现用了 sasl，在 dovecot 上排查时发现 unix 没有启动

Ticket No. 15 3 3 3

Message from the client	*Hello,* *I am a system administrator.* *I am using Thunderbird on the CLIENT1 device with the administrator account to check business notification emails ar forward the relevant information to the appropriate personne* *Incoming emails can be received and viewed normally. Howev when I try to forward an email to the responsible person or se a new email, the message fails to send. As a result, the follow- process after reviewing incident notifications is being delayed.* *Please identify the exact cause of the sending failure and take necessary actions so that email sending and forwarding can w properly.*
Description of the root cause of the problem	On DEBSRV2: the dovecot is not enable and listen the unix socket: /var/spool/postfix/private/auth, so the postfix sasl authentication fail and the client can not send email.

Recommended solution	On DEBSRV2:
	modify /etc/dovecot/conf.d/10-master.conf file:
	uncomment the following line:
	“
	unix_listener /var/spool/postfix/private/auth {
	mode = 0666
	}
	”
	and restart dovecot and postfix service

三、webmail：

1、连接协议是 tls，端口却是 993，导致 webmail 网页无法正确打开：

摘要：使用 tls://（STARTTLS）协议去连接隐式 993 端口

webmail 网页连接失败（白屏）

打开 /etc/roundcube/config.inc.php 文件发现 imap 协议使用的是 tls，但是端口却是 993

原因：
在 config.inc.php 中，连接 imap 的使用的协议是 STARTTLS 的 tls:// ，但是端口确是隐式的 993
On DEBSRV2:
The roundcube configuration file /etc/roundcube/config.inc.php is configured to connect imap 993 use STARTTLS.

解决方法：
modify /etc/roundcube/config.inc.php
change “$config[‘imap_host’] = [“tls://mx.wsc2026.sh:993”]” to “$config[‘imap_host’] = [“ssl://mx.wsc2026.sh:993”]”
或者（但是能用 ssl，最好还是用 ssl）：
change “$config[‘imap_host’] = [“tls://mx.wsc2026.sh:993”]” to “$config[‘imap_host’] = [“tls://mx.wsc2026.sh:143”]”

•补充知识点：

roundcube 连接地址前缀作用：
1）不带前缀：例如
$config['imap_host'] = 'mx.wsc2026.sh:143'; $config['smtp_host'] = 'mx.wsc2026.sh:587';
直接建立不加密的连接（143、25、587）
2）tls:// 前缀，例如：
$config['imap_host'] = 'tls://mx.wsc2026.sh:143'; $config['smtp_host'] = 'tls://mx.wsc2026.sh:587';
就是 STARTTLS，一开始是明文，然后可以升级为 TLS
3）ssl:// 前缀，例如：
$config['imap_host'] = 'ssl://mx.wsc2026.sh:993'; $config['smtp_host'] = 'ssl://mx.wsc2026.sh:465';
隐式 TLS（后面可以省略端口，smtp 默认 465，imap 默认 993）

Ticket No. 2

Message from the client	*Hello,* *I accessed "https://mail.wsc2026.sh" to use the webmail service and attempted to log in with the user account hu.rui011.* *However, after submitting the login credentials, the mailbox does not open normally and the page is redirected to an error page.* *In addition, please review the relevant logs to identify the exact cause of the issue and take the necessary actions so that the user can log in successfully.*
Description of the root cause of the problem	The Roundcube IMAP server is configured to use port 993 with STARTTLS, preventing normal access to the Dovecot service.
Recommended solution	In /etc/roundcube/config.inc.php on DEBSRV2, change the value of $config['imap_host'] to tls://mx.wsc2026.sh:143 or ssl://mx.wsc2026.sh:993.

2、Nginx 使用了错误的 php unix，mariadb-server 没有启动：

因为 webmail 用的是 php，所以首先怀疑 php
查看配置文件发现 php socket 路径写错了
然后发现 php socket 文件的属主和属组不是 www-data
然后发现问题还是没有修复，开始排查后端数据问题，发现数据库没有启动

Troubleshooting Ticket 5 KR-2 CN-2

Hi mate this is Richard, I wanna check my email through the company webmail mail.itnsa.net. But when I try to access this webmail, it says “Bad Gateway”. Could you fix this? I need to check my email right now.

After the webmail already working, could you please check it again if we can use our login credentials to use the mail server, because I don’t want to create a new account anymore to use this mail service.

Problems:

On SVR1.itnsa.local:

1. The nginx config file /etc/nginx/snippets/fastcgi-php.conf have incorrect unix path.

```
fastcgi_pass unix:/run/php/php8-fpm.sock;
```

2. The www-data user and group not have read permission about the /run/php/php8.4-fpm.sock file.

On SVR2.itnsa.local:

1. The mariadb service not start, and service startup is disable.

Solutions:

On SVR1.itnsa.local:

1. Modify file /etc/nginx/snippets/fastcgi-php.conf

```
fastcgi_pass unix:/run/php/php8.4-fpm.sock;
```

Systemctl restart nginx

2. Execute the follow commnad to give www-data user and group read permission about the /run/php/php8.4-fpm.sock file:

Chown www-data:www-data /run/php/php8.4-fpm.sock

Systemctl restart nginx

On SVR2.itnsa.local:

Execute the follow command:

Systemctl start mariadb

Systemctl enable mariadb

Troubleshooting Ticket 5

Hi mate this is Richard, I wanna check my email through the company webmail mail.itnsa.net. But when I try to access this webmail, it says "Bad Gateway". Could you fix this? I need to check my email right now.

After the webmail already working, could you please check it again if we can use our login credentials to use the mail server, because I don't want to create a new account anymore to use this mail service.

Problems:

MariaDB service for Roundcube on svr2 is disabled

Incorrect PHP-FPM socket is configured in /etc/nginx/snippets/fastcgi-php.conf on svr1

Search base in /etc/nslcd.conf on srv1 is incorrect

Solutions:

Enable the Mariadb database on svr2 (systemctl enable mariadb)

Fix PHP-FPM socket to unix:/run/php/php8.4-fpm.sock

Fix search base on /etc/nslcd.conf from dc=itnsa,dc=net to dc=itnsa,dc=local

**If a competitor not mention enabling the MariaDB server at boot, full marks should not be given*

四、FHRP（GLBP、HSRP、VRRP）

设置密码时要加说明，要求两边设置一样的密码

1、没有配置预共享密钥导致两边路由器都是主 Master，导致流量一会走左边，一会走右边：

发现 ping 包有时候会丢一两个，就开始排查网关，发现有一边网关没有配置 ip nat inside 然后看到网关地址是 standby 的，看两边 standby 的状态，发现两边都是 active，然后进行排查发现没有配置预共享密钥

Ticket No. 3

Message from the client	*Dear Network Engieenr,* *We are currently performing a network stability validation regarding an issue where Internet connectivity for HQ infrastructure users is intermittently interrupted.* *The symptoms identified so far are as follows.* *When running the "ping 1.1.1.1 repeat 1000" command from HQSW1 toward the external Internet segment, intermittent packet loss was observed. However, when running the "ping 10.20.10.10 repeat 1000" command toward an internal Datacenter host address, no packet loss or network reachability issues were identified.* *Please investigate the exact point at which the packet loss occurs and identify the root cause. In addition, please take the necessary configuration improvements and corrective actions to prevent the same issue from recurring.*
Description of the root cause of the problem	On HQR2: in g0/4.99 interface are miss HSRP authentication configuration. in g0/4.99 interface area miss “ip nat inside" configuration. so the HQSW1 toward the external Internet intermittent packet loss.
Recommended solution	On HQR2: execute the following command: int g0/4.99 standby 99 authentication md5 key-string Skill39** ip nat inside do wr

答案原文：

Ticket No. 3

Message from the client	*Dear Network Engieenr,* *We are currently performing a network stability validation regarding an issue where Internet connectivity for HQ infrastructure users is intermittently interrupted.* *The symptoms identified so far are as follows.* *When running the "ping 1.1.1.1 repeat 1000" command from HQSW1 toward the external Internet segment, intermittent packet loss was observed. However, when running the "ping 10.20.10.10 repeat 1000" command toward an internal Datacenter host address, no packet loss or network reachability issues were identified.* *Please investigate the exact point at which the packet loss occurs and identify the root cause. In addition, please take the necessary configuration improvements and corrective actions to prevent the same issue from recurring.*
Description of the root cause of the problem	When HQSW1 communicates with 1.1.1.1 through the VLAN 99 SVI, traffic is sent to the gateway address 10.10.99.1. However, both HQR1 and HQR2 are currently operating in the HSRP active state. As a result, the gateway MAC address is continuously relearned, causing both HQR1 and HQR2 to forward traffic. Because the NAT configuration on HQR2 is incorrect, traffic is dropped whenever it is forwarded through HQR2.
Recommended solution	Configure HQR2 as follows: interface GigabitEthernet 0/4.99 standby 99 authentication md5 key-string Skill39** ip nat inside

第 47 届世赛：

Troubleshooting ticket 3

Problem

Hi mate, I did a software upgrade on HQRTR01 and assumed that HQRTR02 would take over. However, all workstations experienced an outage and couldn't connect to the domain controller. Management wants to know the root cause by the end of the day. Can you find out why HQRTR02 didn't take over the traffic?

What are the causes of the problem?

- Inconsistent virtual IPv4 address for HSRP between HQRTR01 and HQRTR02 or the virtual IPv4 address on both HQRTR01 and HQRTR02 for HSRP group 100 is different.
- HSRP group 101 was not in sync due to inconsistent HSRP password between HQRTR01 and HQRTR02

On HQRTR01 and HQRTR02：

The virtual ip address is different on HSRP group 100, so the HSRP group 100 can not establish active/standby mode.

The password is different on HSRP group 101, so the HSRP group 101 can not establish active/standby mode.

Recommended solutions to fix this:

- Set HSRP group 100 virtual IPv4 address to 10.1.0.1 on HQRTR02
- Set HSRP group 101 password to Skill39@Lyon for IPv6 on HQRTR02

On HQRTR01 and HQRTR02:

Set HSRP group 101 password to Skills39 or Skill39@Lyon, keep password consistent.

HQRTR01

```
interface GigabitEthernet0/0.100
 encapsulation dot1Q 100
 ip address 10.1.0.2 255.255.254.0
 ip helper-address 10.1.64.10
 standby version 2
 standby 100 ip 10.1.0.1
 standby 100 priority 110
 standby 100 preempt delay minimum 180
 standby 100 authentication md5 key-string Skills39
 standby 101 ipv6 autoconfig
 standby 101 priority 110
 standby 101 preempt delay minimum 180
 standby 101 authentication md5 key-string Skills39
 ipv6 address 2001:DB8:CAFE:100::2/64
 ipv6 enable
 ipv6 ospf 1 area 0
!
interface GigabitEthernet0/0.150
 encapsulation dot1Q 150
 ip address 10.1.128.2 255.255.255.128
 standby version 2
 standby 150 ip 10.1.128.1
 standby 150 priority 110
 standby 150 preempt delay minimum 180
 standby 150 authentication md5 key-string Skills39
 standby 151 ipv6 autoconfig
 standby 151 priority 110
 standby 151 preempt delay minimum 180
 standby 151 authentication md5 key-string Skills39
 ipv6 address 2001:DB8:CAFE:150::2/64
 ipv6 enable
 ipv6 ospf 1 area 0
!
```

HQRTR02

```
interface GigabitEthernet0/0.100
 encapsulation dot1Q 100
 ip address 10.1.0.3 255.255.254.0
 ip helper-address 10.1.64.10
 standby version 2
 standby 100 ip 10.1.0.5
 standby 100 authentication md5 key-string Skills39
 standby 101 ipv6 autoconfig
 standby 101 authentication md5 key-string Skillss39
 ipv6 address 2001:DB8:CAFE:100::3/64
 ipv6 enable
 ipv6 ospf 1 area 0
!
interface GigabitEthernet0/0.150
 encapsulation dot1Q 150
 ip address 10.1.128.3 255.255.255.128
 standby version 2
 standby 150 ip 10.1.128.1
 standby 150 authentication md5 key-string Skills39
 standby 151 ipv6 autoconfig
 standby 151 authentication md5 key-string Skills39
 ipv6 address 2001:DB8:CAFE:150::3/64
 ipv6 enable
 ipv6 ospf 1 area 0
!
```

五、防火墙、NAT：

1、Linux 防火墙：

1）拒绝默认流量，没有允许 TCP 22，导致 ssh 无法连接：

发现路由 ICMP 能 ping 通，但是 TCP 不通，所以开始排查服务、security.conf、nftables 的问题

Ticket No. 4

Message from the client	*Hello,* *When attempting to connect to DEBSRV3 via SSH, the connection was successful from CLIENT2, but it failed from CLIENT1.* *Could you please investigate the exact cause of the issue and take the necessary actions so that CLIENT1 can connect to DEBSRV3 via SSH successfully?*
Description of the root cause of the problem	On DEVSRV3: The nftables rule input chain is not configured to allow the tcp 22 port connect , so the CLIENT1 can't connect to DEBSRV3 via SSH.
Recommended solution	On DEVSRV3: add the following in nftables input chain: ip saddr { 10.20.30.0/24, 10.10.30.0/24 } tcp dport 22 accept and reload the nftables service

2、Cisco NAT：

1）没有在子接口配置 ip nat inside，而是在主接口配置 ip nat inside：

ticket 跟 四-1 是共用的

2）没有配置 公网端口映射：

Ticket No. 10

Message from the client	*Hello,* *We are currently receiving multiple reports of access issues related to the external web service at "https://www.wsc2026.sh"* *At the initial stage of the issue, users accessing the URL were unexpectedly redirected or connected to a different system. At this time, the service appears to be completely inaccessible from the external network.* *As a result, external users are unable to use the web service, so we request an urgent investigation.* *Please take immediate action to restore the service so that external network users can access "https://www.wsc2026.sh" and use the service normally.*
Description of the root cause of the problem	DCR does not have a TCP port 443 NAT rule for the Proxy server, so the Proxy service cannot be accessed from the external network. In addition, the Proxy service backend is incorrectly configured, causing web traffic to be forwarded to the web service on DEBSRV2.
Recommended solution	Configure static NAT on DCR: ip nat inside source static tcp 10.20.10.10 443 203.0.113.9 443 vrf CORP extendable In the HAProxy configuration, correct the option that selects the backend based on the Host header: use_backend be_www if host_www Restart the HAProxy daemon: systemctl restart haproxy

3）使用 Loopback /24 网段作为 NAT 地址池，但是 OSPF 默认将 Loopback 通告为 /32 网段，导致 NAT 转换失败：

Ticket No. 12

Message from the client	*Hello,* *Users in the internal networks 192.168.10.0/24 and 192.168.20.0/24, which are connected to HQR3, are currently unable to communicate with external networks.* *Previously, external communication from these networks was working normally. However, the issue appears to have started after the recent network optimization work. As a result, users in these network segments are unable to access the Internet and external services.* *Please identify the exact cause of the issue and take the necessary actions so that users in the 192.168.10.0/24 and 192.168.20.0/24 networks can communicate with external networks normally.*
Description of the root cause of the problem	Internal devices connected to HQR3 are translated to 10.30.10.10 and 10.30.20.10, respectively. However, the 10.30.10.0/24 and 10.30.20.0/24 networks are currently advertised to HQR1 and HQR2 as /32 routes, even though HQR1 and HQR2 perform NAT toward the external network. As a result, HQR1 and HQR2 do not have valid route reachability to the translated addresses.
Recommended solution	Configure HQR3 to advertise 10.30.10.0/24 and 10.30.20.0/24 to HQR1 and HQR2 as valid network prefixes. This may be done by applying ip ospf network point-to-point to Loopback10 and Loopback20, configuring Null redistribution, or using another equivalent method: interface Loopback10 ip ospf network point-to-point interface Loopback20 ip ospf network point-to-point

六、AAA：

1、AAA 没有应用在 vty 中

摘要：没有在 vty 中应用 AAA

原因：

vty line 中没有应用这个叫 SSH 的 AAA 授权

On HQSW1:

the AAA authorization named “SSH” is not applied in the vty line.

解决方案：

On HQSW1:

execute the following command:
line vty 0 4
 authorization exec SSH
do wr

Ticket No. 1

Message from the client	*Good morning!* *I attempted to access HQSW1 from DEBSRV3 via SSH using the admin account in order to modify the configuration of HQSW1.* *Although the SSH session itself is established successfully, it appears that the current account does not have the required administrative privileges.* *Please investigate and resolve the permission issue so that the necessary configuration changes can be performed on HQSW1.*
Description of the root cause of the problem	On HQSW1: The AAA authorization named "SSH" is not apply to vty line, so the admin account login does not have the administrative privileges.
Recommended solution	On HQSW1: execute the following command: line vty 0 4 authorization exec SSH do wr

2、AAA fallback 认证方式为 none，并且指定了错误的源接口：

•补充知识点：

如果 AAA 身份认证方式是 none，那么任何用户都能使用任何凭据来登录

Troubleshooting Ticket 3

Hello, Anthony here. I noticed that I cannot remotely access the Office Router via SSH from workstation, I try to reconfigure the device's authentication method to meet the company's security requirements but I'm not sure why it doesn't work. Also please validate that only tech account can access the Office Router.

Problems:

There is misconfigured access-list called SSH_MGMT that block SSH connection

In the AAA authentication and authorization list (ITNSA-RADIUS), the fallback method is set to **none**, which creates a security vulnerability, if RADIUS fails, any user can gain access using any credentials

Source interface used by OFFICE-ROUTER to communicate with RADIUS is incorrect

Acl named "SSH_MGMT" have configured "10 deny any any," it block any traffic.

The AAA authentication and authorization named ITNSA-RADIUS only configure one RADIUS authentication method, the fallback authentication method is none, if RADIUS fail, any user can login without correct credential.

The NPS Server only allow OFFICE-ROUTER Loopback0 10.10.10.1 address to connect,but there is misconfigured Source interface "e0/0" on OFFICE-ROUTER.

Solutions:

Fix SSH_MGMT access-list by removing rule: 10 deny any

Remove fallback method none OR change none method it to local on AAA authentication & authorization (ITNSA-RADIUS), configuration should be like this:

aaa authentication login ITNSA-RADIUS group radius

aaa authorization exec ITNSA-RADIUS group radius

OR

aaa authorization exec ITNSA-RADIUS group radius local

aaa authentication login ITNSA-RADIUS group radius local

Fix RADIUS source interface to Loopback0 on OFFICE-ROUTER

On OFFICE-ROUTER:

Execute the follow command:

No ip radius source-interface e0/0

ip radius source-interface Loopback0

do wr

七、IPv6：

1、Cisco：

1）接口禁止了发送 ra，导致客户端无法获取到 IPv6 默认路由，导致无法访问其他网段：

Ticket No. 5

Message from the client	*Hi!* *It appears that there is an IPv6 connectivity issue on the CLIENT1 device.* *At the moment, there does not seem to be any immediate service impact. However, to prevent any potential issues, please investigate and resolve the IPv6 connectivity problem on CLIENT1.*
Description of the root cause of the problem	On DCSW: the client1 can not recive the ipv6 default route,because the DCSW device vlan 130 have wrongly configuration “ipv6 nd ra lifetime 0”. so there is IPv6 connectivity issue on the CLIENT1.
Recommended solution	On DCSW: execute the following command: int vlan 130 no ipv6 nd ra lifetime 0 do wr

八、Web、proxy：

1、Linux Web：

•补充知识点：

.htaccess 也需要排查，它能够对单独一个目录进行自定义权限控制

1）Apache2 没有允许访问根目录的配置；监听错端口

Ticket No. 6

Message from the client	*Hello,* *We attempted to access the web service at "https://web.wsc2026.sh" from a client device, but the web page does not open properly.* *Please check the status of the related services and review the relevant logs to identify the exact cause of the issue. Also, please take the necessary actions so that the client can access the web service normally.*
Description of the root cause of the problem	On DEBSRV3: the apache2 https listen port is wrongly configure to 4433 in the apache2 configuration file /etc/apache2/apache2.conf, it not granted with permission of the /var/www/html directory. so the https://web.wsc2026.sh web page doest not open properly.
Recommended solution	On DEBSRV3: modify the /etc/apache2/ports.conf fle: change the 4433 to 443 add the following line into /etc/apache2/apache2.conf file: <Directory /var/www/html> Options FollowSymLinks AllowOverride None Require all granted </Directory> and restart apache2 service

2）squid 拒绝了所有流量、DNS 解析指错：

Troubleshooting ticket 8

Problem

Hi support, it's William from the finance department. My colleague advised me to enter www.wsc2024.org into the browser from ws01 to access our public webpage running on lnx01. My colleague told me I should be able to see a "Welcome to WSC2024.org" message. However, I am unable to access the site at all! Your internet sucks!

Best regards,
William Hull

What are the causes of the problem?

- AAAA & A record of lnx01 DNS server of www.wsc2024.org points to an unreachable address
- Squid proxy on lnx03 blocks requests from any clients

On Lnx01:
The www.wsc2024.org AAAA/A record is point to 1.1.1.1 address instead of 2.2.2.2.
On Lnx03:
The Squid is wrongly configure "deny any", so the any client can not use this proxy.

Recommended solutions to fix this:

- Fix AAAA record to 2001:db8:cafe:200::10 on lnx01 & A record to 10.1.64.10 on lnx01, and clear the cache on DC01's DNS server.
- Change http_access statement from deny to allow in squid config (/etc/squid/conf.d/wsc2024.conf)

3）在 nsswithch.conf 中，dns 解析优先于 hosts 文件；web 配置了错误的重定向

Troubleshooting ticket 10

Problem

Hi guys, I am testing a new application. For that purpose, I have overwritten the domain resolution by adding a new entry in the hosts file on lnx03. If I attempt to curl the domain app.wsc2024.org on lnx03 using the command "curl -L app.wsc2024.org", it is expected to land on lnx03 and not on lnx01. I should receive a text similar to “Welcome to the NEW webpage of WSC2024.org”. But my domain resolution overwrite is not working at all. What am I doing wrong?

What are the causes of the problem?

- lnx03 uses first DNS resolution and then its own local hosts database because the order of values in the "hosts" parameter in file /etc/nsswitch.conf is wrong. As DNS returns a valid response, lnx02 uses that address to connect to the web server.
- If a user’s request arrives at Apache2 running on lnx03, it redirects the user to maintenance.wsc2024.org because a redirect has been configured in Apache2

On lnx03:
in /etc/nsswithch.conf the “dns” is prior to “files” at line that start with hosts
The apache2 is configure a HTTP redirect to maintenance.wsc2024.org, so the client access to a different web page.

Recommended solutions to fix this:

- parameter “files” must be before parameter “dns” for hosts option in /etc/nsswitch.conf on lnx03

  hosts: files dns
- Remove Redirect directive in the Apache vhost configuration in /etc/apache2/sites-available/000-default.conf on lnx03

4) 配置了 nftables redirect，把正确的端口重定向了：

Troubleshooting ticket 11

Problem

Greetings, I am attempting to access my new secret webpage http://app.wsc2024.local:8080 from ws01. The website should return a website containing "Welcome to Secret app at WSC2024.org". However, I am receiving the webpage running on port 80 with the content "Welcome to WSC2024.org.", which I don't expect from port 8080. As the web application is still under development, I don't want anybody to access the site using default port 80. Please help me to resolve the issue.

What are the causes of the problem?

- Apache Webserver on lnx01 is not listening on port 8080
- Unnecessary DNAT rule is redirecting users from port 8080 to 80 on lnx01

On lnx01:
The apache2 is not listen TCP 8080 port.
There is a incorrect DNAT rule that redirect the tcp 8080 to tcp 80 in nftables.

Recommended solutions to fix this:

- Delete nftable DNAT rule in /etc/firewall/rules/common.conf on lnx01, which is redirecting users from port 8080 to 80, and reload nftables using systemctl reload nftables

Add Listen Directive for port 8080 in /etc/apache2/httpd.conf file on lnx01 and restart apache2

2、Windows IIS：

1）网页认证用户没有权限读取 web 根目录：

•补充知识点：

·如果有 Windows 身份认证，那么客户端用什么用户认证，IIS 就会用什么用户访问 IIS Web 根目录
·如果是匿名身份认证，那么 IIS 就会用 IUSR 用户去访 IIS Web 根目录（所以如果网页是匿名身份认证，还可以排查是否给了 IUSR 拒绝的权限）
这里的问题是因为这个登陆的用户没有 IIS 根目录的读取权限

Ticket No. 8

Message from the client	*Hello,* *We are currently experiencing an issue where the internal user web service at "https://auth.wsc2026.sh" cannot be accessed properly.* *After accessing the service, I attempted to log in with my user account, li.xiang004, but authentication did not complete successfully. As a result, I am currently unable to use the service.* *Since this site should be available to all WSC2026 China employees, please verify whether the same issue is affecting not only my account but also other internal users.*
Description of the root cause of the problem	Authentication fails and users are redirected to a 401 error page because domain users do not have sufficient permissions to access the web content.
Recommended solution	In the permissions for C:\inetpub\wwwroot on WINSRV3, change the GG_CN_ALL domain group's permission from Traverse folder / execute file to Read & execute.

九、路由：

1、BGP 出站策略限制，导致路由缺失：

CloudDCR1 和 CloudDCR2 是 iBGP 邻居，它们连接 ISP 的接口有出站策略，只允许了本机的网络，没有允许 peer 的网络。

Ticket No. 7

Message from the client	*Dear IT support team,* *I am the SRE Manager for the Cloud Datacenter.* *We are currently validating a network failover scenario assuming an Internet uplink failure.* *During the validation process, we identified an issue where, if the Internet uplink connected to either CloudDCR1 or CloudDCR2 goes down, the routing path does not fail over properly, causing network reachability issues for Cloud Datacenter services.* *For now, all related network environments and links have been restored to their original state to ensure normal service operation.* *Please review the relevant routing and failover configurations to ensure that, in the event of an Internet uplink failure, the existing route is withdrawn properly and traffic is switched to the alternate path as expected.*
Description of the root cause of the problem	Outbound BGP advertisement filtering is configured on CloudDCR1 and CloudDCR2, but the prefix lists do not permit the routes learned from the peer. Consequently, those routes are filtered and are not advertised.
Recommended solution	Add the following entries to the existing prefix list on CloudDCR1: ip prefix-list CLOUD1-PUBLIC-OUT seq 130 permit 18.126.247.0/24 ip prefix-list CLOUD1-PUBLIC-OUT seq 140 permit 27.215.52.0/24 ip prefix-list CLOUD1-PUBLIC-OUT seq 150 permit 39.83.194.0/24 ip prefix-list CLOUD1-PUBLIC-OUT seq 160 permit 52.167.11.0/24 ip prefix-list CLOUD1-PUBLIC-OUT seq 170 permit 68.25.136.0/24 ip prefix-list CLOUD1-PUBLIC-OUT seq 180 permit 81.232.79.0/24 ip prefix-list CLOUD1-PUBLIC-OUT seq 190 permit 94.108.225.0/24 ip prefix-list CLOUD1-PUBLIC-OUT seq 200 permit 109.143.34.0/24 ip prefix-list CLOUD1-PUBLIC-OUT seq 210 permit 123.197.166.0/24 ip prefix-list CLOUD1-PUBLIC-OUT seq 220 permit 137.54.203.0/24 ip prefix-list CLOUD1-PUBLIC-OUT seq 230 permit 152.176.96.0/24 ip prefix-list CLOUD1-PUBLIC-OUT seq 240 permit 166.219.17.0/24 Add the following entries to the existing prefix list on CloudDCR2: ip prefix-list CLOUD2-PUBLIC-OUT seq 130 permit 23.47.181.0/24 ip prefix-list CLOUD2-PUBLIC-OUT seq 140 permit 31.208.74.0/24

2、OSPF 网络类型错误导致邻居能够建立，但是接收不到路由：

Troubleshooting Ticket 4

Recently, we asked the Junior NetAdmin to configure a hot standby protocol on the core switches for datacenter traffic failover. We use DCS3-2 as the primary link. When we tested it by disabling the VLAN255 interface of DCS3-2, the failover did not work as expected, and the servers could not communicate with the Internet. Can you find out why this can be happened?

Problems:

Datacenter subnet (172.31.255.0/24) is not advertised in the OSPF process on DCS3-1

OSPF network type at uplink interface (E0/0) of DCS3-1 is broadcast, although the adjacency successfully established, the route exchange is not performed between DCS3-1 and EDGE-RTR

Solutions:

Advertise datacenter subnet in the OSPF process using network 172.31.255.0 0.0.0.255 area 255

Set OSPF network type on uplink interface of DCS3-1 (E0/0) to point-to-point

3、BGP 一端缺少 password authentication：

Troubleshooting Ticket 8

I was checking IPv6 connectivity on server1 and server2. When I tried to verify it by pinging a public server, it did not work. As far as I remember, our ISP informed us that they increased BGP security by enabling additional security mechanisms during the peering process

Problems:

Password is not set for IPv6 BGP peering authentication on EDGE-RTR

The OSPFv3 process ID used for route redistribution from OSPF to BGP on EDGE-RTR is incorrect

On Server1：

The bgp is not set IPv6 password authentication with Server2 peer.

On EDGE-RTR:

The bgp redistribute ospfv3, but the ospfv3 process ID is incorrect.

Solutions:

Configure a password for IPv6 BGP peering authentication on EDGE-RTR

Set the OSPFv3 process ID to 10 for route redistribution from OSPF to BGP on EDGE-RTR

4、BGP 重分发了错误的 OSPF 进程：

Troubleshooting Ticket 8

I was checking IPv6 connectivity on server1 and server2. When I tried to verify it by pinging a public server, it did not work. As far as I remember, our ISP informed us that they increased BGP security by enabling additional security mechanisms during the peering process

Problems:

Password is not set for IPv6 BGP peering authentication on EDGE-RTR

The OSPFv3 process ID used for route redistribution from OSPF to BGP on EDGE-RTR is incorrect

On Server1：

The bgp is not set IPv6 password authentication with Server2 peer.

On EDGE-RTR:

The bgp redistribute ospfv3, but the ospfv3 process ID is incorrect.

Solutions:

Configure a password for IPv6 BGP peering authentication on EDGE-RTR

Set the OSPFv3 process ID to 10 for route redistribution from OSPF to BGP on EDGE-RTR

5、二层交换机没有配置 ip default-gateway:

Troubleshooting Ticket 11

Our network administrator has configured centralized logging on all data center switches to send logs to svr2, where they should be stored in the /var/log/netdev/ directory. However, upon checking, logs are only being received from DCS3-1 and DCS3-2. Logs from DCS2-L are not appearing.

Problems:

Default gateway is not set on DCS2-L

Logging host and logging facility configuration on DCS2-L are incorrect

There is a incorrectly configured Loggins host to 172.31.1.1 on DCS2-L.

There is not configured default gateway On DCS2-L.

Solutions:

Set the default gateway on DCS2-L to 192.168.99.6 using: ip default-gateway 192.168.99.6

Set the logging host to the IP address of svr2 (172.31.255.200) and the facility to local7, matching the facility configured on svr2.

**If the competitor proposes creating a default route and enabling IP routing on DCS2-L, full marks should not be given*

6、distribute-list 没有允许路由：

Troubleshooting Ticket 12

Last week, the network engineering team allocated dedicated subnets for future LAB deployment: 192.168.100.0/24 and 192.168.200.0/24. Another network engineer mentioned that the LAB gateway, which uses the last host IP address, is already active. However, when I try to ping the LAB gateway from the office router, it does not respond. Could you help trace the problem and resolve it?

Problems:

Loopback100 and Loopback200 interfaces on DCS3-2 are down, preventing EIGRP routes from being redistributed into OSPF

The LAB networks are being filtered in the OSPF process on both EDGE-RTR and OFFICE-ROUTER by a distribute-list INTERNAL_NETWORK access list

On DCS3-2:

The Loopback100 and Loopback200 interface is down, so the EIGRP route can not get into OSPF.

The ACL named "INTERNAL_NETWORK" is not configured to permit "192.168.100.0/24","192.168.200.0/24" subnet.

Solutions:

Enable Loopback100 and Loopback200 interfaces on DCS3-2 to allow EIGRP routes to be redistributed into OSPF

Update the INTERNAL_NETWORK access list on both EDGE-RTR and OFFICE-ROUTER to include 192.168.100.0/24 192.168.200.0/24

7、NAT 转换成私网地址、ACL 拒绝了流量：

Troubleshooting ticket 13

Problem

Hi pal, lnx03 is having trouble pinging 8.8.8.8 since yesterday. I am really busy. Can you please take over this issue for me and have a look?

What are the causes of the problem?

- NAT Exception for lnx03 is unnecessarily configured on BORDERRTR01. So, lnx03 goes with an unroutable private IP address to the Internet. ISP cannot route the traffic back to lnx03 due to the unroutable private IPv4 address
- ICMP traffic towards 8.8.8.8 is filtered by an access control list called FILTER-BOGUS-OUT on CORE-RTR

On the BORDERRTR01:
the nat is translation to a private address go to ISP, so the ISP traffic can not back.
On CORE-RTR:
The ACL named "FILTER-BOGUS-OUT" block the destination 8.8.8.8 ICMP traffic.

Recommended solutions to fix this:

- Remove ACL entry with the IPv4 address of lnx03 in the standard ACL with the number 10 on BORDERRTR01
- Remove entry 8.8.8.8 from ACL FILTER-BOGUS-OUT on CORE-RTR

8、接口没有 link local 地址，没有配置 ipv6 enable；没有通告 ospfv3 进程：

Troubleshooting ticket 14

Problem

Hi there, I am evaluating a new router model in our lab. I have connected the new lab router named LABRTR01 to our core router, CORERTR01, and configured the most important things on both of them to get IPv6-only connectivity. But I am unable to ping 2001:DB8:CAFE:254::14. I have spent many hours trying to troubleshoot this issue, and I am still not sure where to look.

What are the causes of the problem?

- There is no link local address configured on gi1/1 interface on CORERTR01 as IPv6 has not enabled on that interface
- OSPF Area 0 is discontiguous as the link between LABRTR01 & CORERTR01 is in area 1. CORERTR01 Gi1/1 also not configured with OSPFv3.

On CORERTR01:
The g1/1 interface is not have link local address, because it is not configure “ipv6 enable”.
The ospfv3 area 0 process is not enable in g1/1 interface, so the ospfv3 process is not recive the g1/1 interface ipv6 route.

Recommended solutions to fix this:

- Enable IPv6 on gi1/1 on CORERTR01
- Link between LABORRTR01 & CORERTE01 must be changed to area 0 OR the loopback interface 0 on LABORRTR01 must be changed to area 1

十、日志：

1、Cisco rsyslog：

路由器/交换机 无法访问日志服务器进行记录日志

Ticket No. 11 2 3 3

Message from the client	*Hello,* *We have been notified by the monitoring team that there is an issue with Syslog collection from the network devices.* *Currently, DEBSRV3 is expected to collect logs from each network device separately under the /var/log/cisco directory and use those logs for log review and visualization. However, logs sent from all devices are not being recorded under that path at all, making it impossible to monitor device status and events.* *Please identify the exact cause and restore the service promptly so that per-device log collection and log visualization can function properly.*
Description of the root cause of the problem	On DEBSRV3: the rsyslog service only listen tcp 514 port,but network device send log use udp 514 port. so the log is unable to send to the DEBSRV3 /var/log/cisco directory. the nftables input chain is only allow the udp 514 port , not allow tcp 514 port.
Recommended solution	Can chose one: 1. On DEBSRV3: add the following line into /etc/nftables.conf file: ip saddr @v4_allowed_net tcp dport 514 accept ip saddr @v6_allowed_net tcp dport 514 accept and reload nftables service On all network device: execute the following command: no logging host 10.10.20.10 logging host 10.10.20.10 transport tcp port 514 do wr or: 2. On DEBSRV3: modify /etc/rsyslog.conf file change “module(load=”imtcp”)” to “module(load=”imudp”)” and restart rsyslog service

2、主机没有设置 facility，日志服务器只匹配 facility 进行保存:

Troubleshooting Ticket 11

Our network administrator has configured centralized logging on all data center switches to send logs to svr2, where they should be stored in the /var/log/netdev/ directory. However, upon checking, logs are only being received from DCS3-1 and DCS3-2. Logs from DCS2-L are not appearing.

Problems:

Default gateway is not set on DCS2-L

Logging host and logging facility configuration on DCS2-L are incorrect

There is a incorrectly configured Loggins host to 172.31.1.1 on DCS2-L.

There is not configured default gateway On DCS2-L.

Solutions:

Set the default gateway on DCS2-L to 192.168.99.6 using: ip default-gateway 192.168.99.6

Set the logging host to the IP address of svr2 (172.31.255.200) and the facility to local7, matching the facility configured on svr2.

**If the competitor proposes creating a default route and enabling IP routing on DCS2-L, full marks should not be given*

十一、FTP：

1、Proftpd：

1）没有加载模块：

Troubleshooting Ticket 13

Hey, this is Michael Jones. You mentioned that our FTP service (ftp.itnsa.net) is secured using a certificate from the DC, but I tried testing it from workstation1 yesterday using FileZilla, and it's not working. I'm unable to establish a connection, and it seems the secure configuration isn't functioning as expected.

Problems:

Proftpd TLS module is not enabled on /etc/proftpd/modules.conf

Certificate (/etc/proftpd/ftp.itnsa.net.crt) and private key (/etc/proftpd/ftp.itnsa.net.key) is not match, mismatch can be verified by comparing the modulus of the certificate and private key

On svr2.itnsa.local:

The proftpd service is not enable mod_tls.c module.

The proftpd SSL certificate(/etc/proftpd/ftp.itnsa.net.crt) and private key(/etc/proftpd/ftp.itnsa.net.eky) is not match, so the client can not establish connection.

Solutions:

Enable Proftpd TLS module on /etc/proftpd/modules.conf

Within /etc/proftpd/ directory, there is ftp.itnsa.net.pfx file that bundles certificate & private key, extract .crt and .key from that .pfx file then replace the existing certificate and private key used by proftpd with the extracted files

2、tftp-hpa：

Troubleshooting Ticket 14

I noticed an issue with our router backups. The EDGE-RTR was previously configured to perform automatic backups using TFTP to svr2, but recently it doesn't seem to be working anymore. I can't find any recent backup files on the server.

Could you please check what's causing this issue and fix it? We need to ensure the automatic backup process is running properly again.

Problems:

The tftpd-hpa configuration on svr2 is missing the --create option

The TFTP root directory /srv/tftp is owned by root:root, preventing file creation

On svr2.itnsa.local:

The tftp-hpa configuration is missing "--create" option, so the tftp client can not upload and create new file and directory.

The tftp user and group not have the write permission about /srv/tftp directory, because the /srv/tftp directory owner is root:root.so the tftp-hpa can not write into this directory.

Solutions:

Add the --create option to the tftpd-hpa configuration on svr2

Change the ownership of /srv/tftp to tftp:tftp

**If the competitor changes the default permissions of /srv/tftp directory like 777 instead of fixing ownership, full marks should not be given*

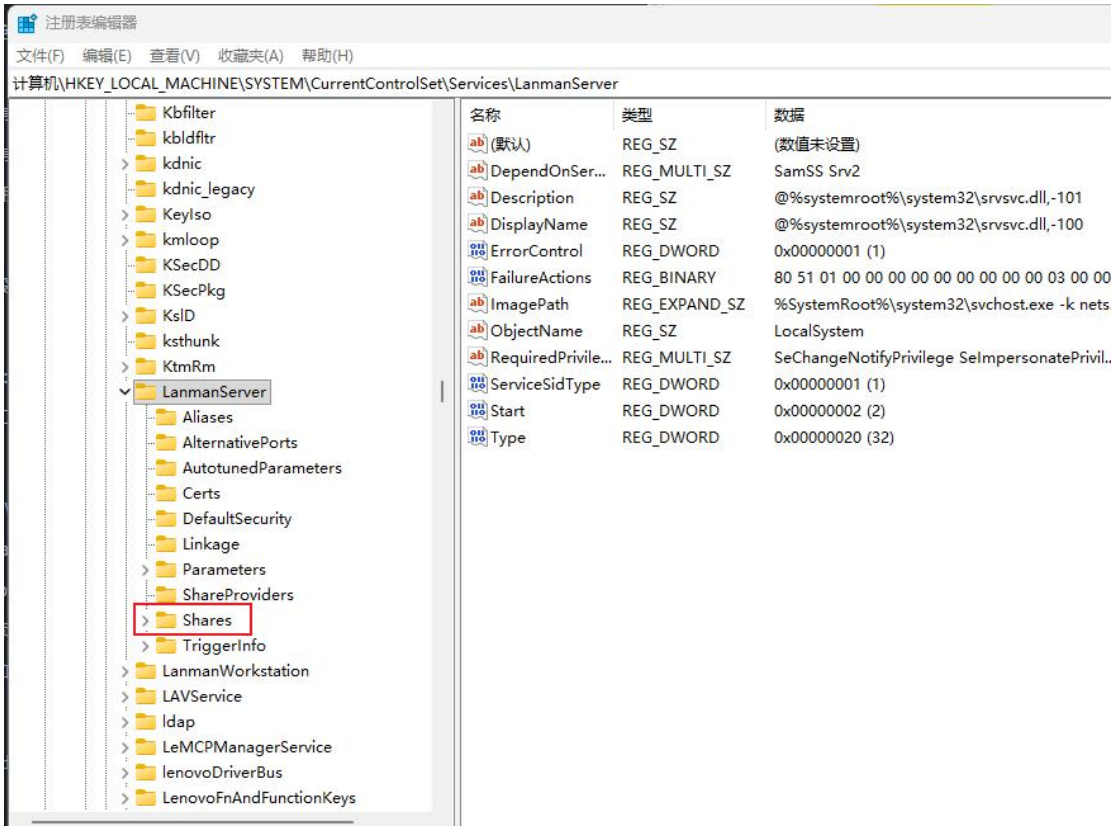
十二、共享、DFS：

1、共享文件夹 根文件夹名称被修改：

这里当时排查的不仔细，提早下定论了，需要先去 HKLM\SYSTEM\CurrentControlSet\Services\LanmanServer 这个注册表路径下查看这个共享的真实名称

Ticket No. 14 1 0 1

Message from the client	*Hello,* *I attempted to access the HR shared folder on WINSRV3 using the user account cai.jie027 in order to back up department work materials, but I am currently unable to connect to the shared resource properly.* *This is not an urgent service-impacting issue. However, due to this problem, I am unable to proceed with department data backup and file management tasks.* *Could you please check the issue and provide assistance so that the work can be carried out smoothly?*
Description of the root cause of the problem	On WINSRV3: the c:\Share\HQ file is not share. On WINSRV3: the HR shared folder root directory is changed from C:\Shares\HR to C:\share\HR. so the cai.jie027 user can not access the HR shared folder.
Recommended solution	On WINSRV3: execute the folloing cmd command: net share HR=c:\Share\HR /grant:GG_CN_HR,full Using the value recorded under LanmanServer\Shares in the registry or the log information, change the directory path from C:\share to C:\shares. Restart the file sharing service: Restart-Service LanmanServer -Force



2、DFS、共享文件夹没有开启枚举（access-based enumeration）：

Troubleshooting Ticket 15

We received a complaint from Robert Brown with ID worker04 that he is unable to access his home drive from workstation1. Instead, he can see the home drives of other users, although he does not have access to open them. This behavior is not expected, as users should only be able to view and access their own home directories.

Could you please investigate and fix this issue? Also, make sure that proper configuration on are applied on Home drive so that users can only see and access their own home drives

Problems:

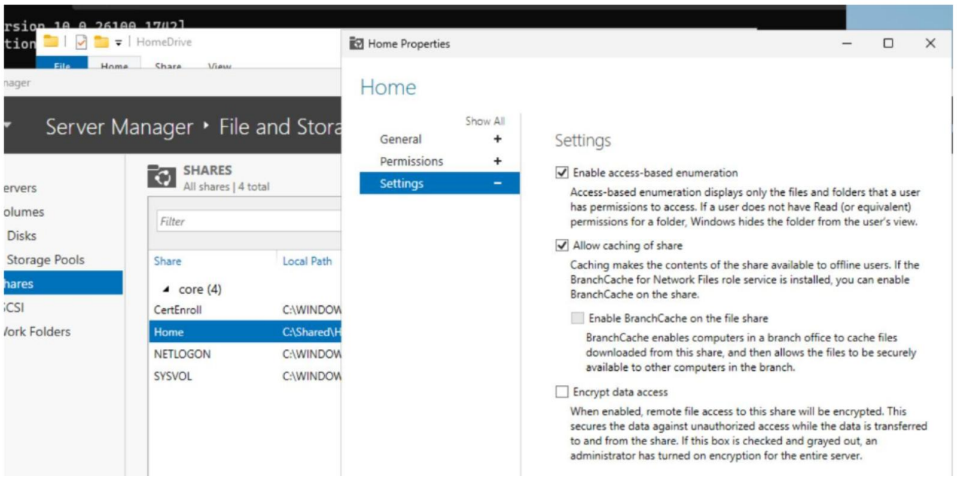
Home folder path of worker04 (Robert Brown) is incorrect, it is set to \\core\Home

Folder Enumeration Mode on Home shared folder is not configured

Solutions:

Fix home folder path of worker04 (Robert Brown) to \\core\Home\worker04

Set Folder Enumeration Mode on Home shared folder to AccessBased



3、用户 Home Driver 共享路径指错：

Troubleshooting Ticket 15

We received a complaint from Robert Brown with ID worker04 that he is unable to access his home drive from workstation1. Instead, he can see the home drives of other users, although he does not have access to open them. This behavior is not expected, as users should only be able to view and access their own home directories.

Could you please investigate and fix this issue? Also, make sure that proper configuration on are applied on Home drive so that users can only see and access their own home drives

Problems:

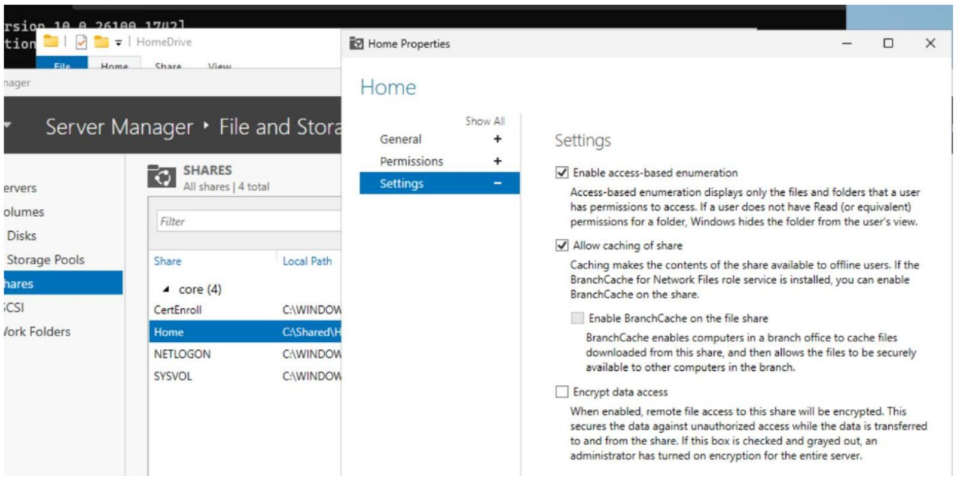
Home folder path of worker04 (Robert Brown) is incorrect, it is set to \\core\Home

Folder Enumeration Mode on Home shared folder is not configured

Solutions:

Fix home folder path of worker04 (Robert Brown) to \\core\Home\worker04

Set Folder Enumeration Mode on Home shared folder to AccessBased



4、访问用户不属于 NTFS 权限所允许的组中：

排除权限时，记得用 net group/net user 查看 用户/组 是否位于文件允许的组中

Troubleshooting ticket 7

Problem

Dear support team, my name is Kyle Carter. I am currently employed in the finance department and working on my computer ws01. I am experiencing difficulty in accessing and editing any files on the departmental file share located on dc01. The network share is mapped as letter Z on my computer ws01. I already asked your colleague and he told me that he will check but never let me know when he can resolve the issue. Please help me resolve this issue by end of today! I have a super important deadline!

What are the causes of the problem?

- Nobody can access the share as the group "Everyone" has no permissions at all in the share permissions
- No modify/write NTFS permission for users in the finance department

On dc01:
the everyone does not have share permission in the Finance Shared Folder.
The GL-Finance group is not member in DL-FS_Finance-RW Group.

Recommended solutions to fix this:

- Possible Solution 1
  - Give Everyone group full access in "Sharing" permission, or
  - Remove Everyone from the "Sharing" permission and add GL-Finance group with full access.
- Possible Solution 2
  - Add AD group "GL-Finance" in "DL-FS_Finance-RW" AD group, or
  - Add "carter" account in "DL-FS_Finance-RW" AD group.

5、FSRM 组织了 .csv 文件扩展名 存储：

Troubleshooting ticket 12

Problem

Dear Sir or madam, my name is Nigel and I'm from Marketing department. Since yesterday, I cannot copy my file on ws01 called C:\data\popular_influencers.csv to the marketing file share when I sign in using my account. The marketing group share is mapped as network drive Z: on my computer ws01.There is another problem as well. I have just discovered that other members from the marketing department can see the confidential project folder "PROJECT_ALPHA" located in the marketing share. However, they cannot access it, which is fine. It is confidential, so please make sure this folder is not listed in the Windows Explorer for them.

Best regards,
Nigel Weiss

What are the causes of the problem?

- File Server Resource Manager prohibits csv file extension on Marketing file share
- Windows Server is not hiding folders where the user does not have access to them, as access-based enumeration is not enabled on the marketing share.

On lnx02：
The FSRM service is not allow all .csv file extension to save on Marketing file share.
The Marketing file share is not enable access-based enumeration, so the user can see other folders that the user not have permission to access.

Recommended solutions to fix this:

- Remove csv file extension from FSRM File screen group WSC2024_Blacklist
- Enable Access-based enumeration on the marketing share

十三、DHCP、DNS：

1、未配置中继，作用域未激活：

Troubleshooting Ticket 1

Dear Admin,

Why I can't access any resources from workstation1. Please fix it now! I need to do my work using this station!

Problems:

DHCP relay is not configured on OFFICE-ROUTER interface Ethernet0/0.10

DHCP scope for workstation1 on core server is deactivated

On OFFICE-ROUTER：
OFFICE-ROUTER not configured dhcp relay for vlan10 on Ethernet0/0.10.

On core.itnsa.local：

The DHCP Scope about 192.168.10.0/24 Subnet named "OFFICE-10" is inactive.

Solutions:

Configure DHCP relay on OFFICE-ROUTER interface Ethernet0/0.10 (ip helper-address 172.31.255.1)

Activate DHCP scope for workstation1 on core server

On OFFICE-ROUTER:

Execute the follow command:

Int e0/0.10

ip helper-address 172.31.255.1

Do wr

On core.itnsa.local:

Open dhcpmgmt.msc, manual active the OFFICE-10 dhcp scope

On workstation1.itnsa.local:

Renew the dhcp address:

Ipconfig /renew

2、NS 记录写错，导致无法解析：

Troubleshooting Ticket 9

We got a message from clients outside the company. They said, our company domain www.itnsa.net cannot be resolved. Can you verify what happen to our public DNS? It will be great if you can also fix it as soon as possible.

Problems:

Destination address in the port forwarding rules for DNS traffic on EDGE-RTR is incorrect

Domain zone on svr1 is not loaded because there is misconfigured DNS record

On EDGE-RTR:

The port port-map(DNAT) destination private address about udp 53 port is incorrectly set to 172.31.255.200 instead of 172.31.255.100.

On svr1:

The ns record is incorectly set to nss.itnsa.net in /etc/named.conf/db.itnsa.net on itnsa.net zone

Solutions:

Update the port forwarding rule on EDGE-RTR to forward DNS traffic to svr1 (172.31.255.100) instead of 172.31.255.200

Fix the NS record of itnsa.net from nss.itnsa.net to ns.itnsa.net on svr1 server

十四、端口安全：

1、绑定了错误的 MAC 地址导致接口进入 err-disable 状态：

Troubleshooting Ticket 6

Hello, I am Mark Anderson. I tried to use workstation2, but when I accessed it, the display appeared in black and white. Please fix the issue and make sure that I can use the workstation2 to access our portal.itnsa.net website

Problems:

Systemd default target is set to emergency.target

Port E1/2 on INTS2, connected to workstation2, has been shut down (err-disabled) due to a port-security violation

On workstation2:

The systemd default target is set to emergency.target

On INTS2:

Port E1/2 is enabled port-security, but the incorrect mac-address is binding at interface, so E1/2 interface is in error disable state.

Solutions:

Set default systemd target to graphical.target OR multi-users.target

Recover manually port E1/2 on INTS2 from err-disabled state caused by a port-security violation

47 届世赛：

Troubleshooting ticket 1

Problem

Dear support,

Today is a special day for me because I brought my dog for the first time to the office. My coworkers in the marketing department were excited to see him. Before I did the round tour with my dog in the office, I turned on my workstation, ws02. After returning from the round tour, I would like to start work and launch my internet browser, but I couldn't open any web pages like http://app.wsc2024.local. Could you please help me?

What are the causes of the problem?

- Port-Security was configured on Gi0/1 with a wrong MAC address. As a result, the switch has shutdown the port connected to ws02 on HQSW01.
- The switchport Gi0/1 is configured with a Trunk Port with 802.1q encapsulation instead of access mode on HQSW01 with the following commands and cause the network not working:
    - switchport trunk allowed vlan 100
    - switchport trunk encapsulation dot1q

Recommended solutions to fix this:

- Set correct mac address of the ws02
    - In addition, shutdown and no shutdown of the gi0/1 port is required
- Change the switchport Gi0/1 to Access mode with vlan 100, i.e.:
    - switchport access vlan 100
    - no switchport trunk encapsulation dot1q
    - no switchport trunk allowed vlan 100

十五、Systemd default target：

1、设置了错误的 systemd default target，导致机器无法正常启动：

Troubleshooting Ticket 6

Hello, I am Mark Anderson. I tried to use workstation2, but when I accessed it, the display appeared in black and white. Please fix the issue and make sure that I can use the workstation2 to access our portal.itnsa.net website

Problems:

Systemd default target is set to emergency.target

Port E1/2 on INTS2, connected to workstation2, has been shut down (err-disabled) due to a port-security violation

On workstation2:

The systemd default target is set to emergency.target

On INTS2:

Port E1/2 is enabled port-security, but the incorrect mac-address is binding at interface, so E1/2 interface is in error disable state.

Solutions:

Set default systemd target to graphical.target OR multi-users.target

Recover manually port E1/2 on INTS2 from err-disabled state caused by a port-security violation

十六、systemd、timer

1、systemd timer 定时运行时间设置错误：

Troubleshooting ticket 2

Problem

SUPER IMPORTANT, an extremely critical synchronization job, called “partner-sync” on **lnx01** server is not running every 15 minutes anymore and is unable to retrieve any data after a change by a junior system engineer!!!! This job downloads mission-critical data from our partner via FTP.

This needs to be fixed As Soon As Possible! The error message from the job says “failed: Connection timed out”

What are the causes of the problem?

- systemctl timer partner-sync.timer is set to hourly instead of every 15 mins
- nftable rule on lnx01 is blocking outgoing FTP connection

On inx01：

The systemctl timer named “partner-sync.timer” is set every one hour running instead of 15 mins.

nftables output rule is block tcp dport 21 port, so the device can not access the ftp service.

Recommended solutions to fix this:

- Set systemctl timer of that job (/etc/systemd/system/partner-sync.timer or systemctl edit partner-sync.timer) to every 15 mins and execute systemd daemon reload (systemctl daemon-reload)
  - Example: OnCalendar=*:0/15 or OnCalendar=*:0,15,30,45
  - NOTE: Exact time pattern not required for full mark
- remove **“drop”** from the nftable rule “tcp dport 21 ~~drop~~” or remove this rule completely, which is blocking FTP connection, in /etc/nftables.conf and reload nftables with “systemctl restart nftables”. Removing nfttable rule temporary using nftable command is not enough!

```
#!/usr/sbin/nft -f

flush ruleset

include "/etc/firewall/rules/*"

table inet filter {
        chain input {
                type filter hook input priority filter;
        }
        chain forward {
                type filter hook forward priority filter;
        }
        chain output {
                type filter hook output priority filter;
                tcp dport 21 drop
        }
}
```

十七、组策略：

1、在 Delegation tab 中，拒绝了用户的访问、应用权限：

Troubleshooting Ticket 7

User: Robert Garcia

Category: Severe

Dear support,

I received information from colleagues that the Finance shared folder is currently accessible by everyone, and users are able to modify files within it. However, when I tried to access it from workstation1, I could not find the Finance shared folder at all.

Please fix this issue. Ensure that the Finance shared folder is accessible only to Finance members, and not to all users. Also, make sure the shared folder is accessible from Windows Explorer on workstation1

Problems:

Permission of /srv/smb/Department/Finance directory on svr2 is set to 777

There is Drive Maps Item-level Targeting rule on Department GPO that deny users in group Finance to mount \svr2\Department

On SR2：

The /srv/smb/Department/Finance directory permission is set to 777.

The GPO named “Drive Maps” is deny Finance group user to apply in Delegation tab.

Solutions:

Set directory permissions to 770 (More restrictive is better)

Fix the Drive Maps Item-level Targeting rule in the Department GPO by removing the invalid rule that deny Finance group users to mount \svr2\Department

2、Security Filtering 中定义了错误的组、组策略未启用：

Troubleshooting ticket 4

Problem

Hello, my newly created GPO called “WSC2024_DO_NOT_ALLOW_REGEDIT” is not applied to users at the finance department. I noticed that ws01 doesn't apply the new GPO. Please have a look, why this GPO is not applied.

What are the causes of the problem?

- Possible cause #1
  - GPO is linked to the wsc2024.local but not enabled, or
  - GPO is not linked to Finance OU and it is not enabled.
- Possible cause #2
  - The GPO’s Security Filtering is set to GL-Marketing group instead of Authenticated Users (Default) or
  - Finance users and the computer object ws01 have no read permission to that GPO as it has been assigned to the wrong AD group GL-Marketing

On DC1:
The GPO named “WSC2024_DO_NOT_ALLOW_REGEDIT” is not enable.
The GPO named “WSC2024_DO_NOT_ALLOW_REGEDIT” Security Filtering is set GL-Marketing instead of Authenticated Users with read permission.

Recommended solutions to fix this:

- In Security Filtering, change to AD group “Authenticated Users” in the GPO policy “WSC2024_DO_NOT_ALLOW_REGEDIT”
- Change GPO link state of GPO WSC2024_DO_NOT_ALLOW_REGEDIT to “enabled”

十八：PAM、limits.conf、access.conf：

1、Maximum session 为 0，导致无法登陆：

Troubleshooting Ticket 10

Hey, I think there's an issue with svr2. When I try to access it via SSH using the tech02 account from svr1, it doesn't work. Did you configure any security settings on the server or apply firewall rules that might be blocking access?

Problems:

SSH cannot be started due to /etc/ssh/sshd_not_to_be_run file exists on svr2

Maximum session login for user in @tech group on the svr2 is set to 0 on /etc/security/limits.conf

On SVR2:

The sshd service can not be started, because the /etc/systemd/system/sshd.services is incorrectly set "ConditionPathExists=!/etc/ssh/sshd_not_to_be_run"

Maximum session login for user in @tech group on the svr2 is set to 0 on /etc/security/limits.conf

Solutions:

Remove /etc/ssh/sshd_not_to_be_run file on svr2

Disable maximum session login on /etc/security/limits.conf OR remove the configuration about the maximum session login

2、access.conf 只允许本地登陆，导致无法远程登陆：

Troubleshooting ticket 6

Problem

Dear Sir or madam,
I am having trouble connecting to lnx01 over SSH with my local user account, john with Skill39@Lyon as the password, from lnx03. I tried to login locally over Console too, I am not able to login. I'm sure the password is correct.

What are the causes of the problem?

- Wrong shell has been set for user john
- User john is only allowed to login locally and not remotely

On LNX01:
The john user shell is /usr/sbin/nologin instead of /bin/bash or /bin/sh.
The /etc/security/access.conf is defined john user can login locally, can not login remotely.

Recommended solutions to fix this:

- Fix shell of user john to /bin/bash or /bin/sh in /etc/passwd (other solutions resulting to this state are accepted as well) on lnx01
- Adjust access rule in /etc/security/access.conf on lnx01
    - Change line from +:john:LOCAL to +:john:ALL in /etc/security/access.conf on lnx01. In addition, remove line -:john:ALL
    - Alternative solution: Remove lines "+:john:LOCAL" and "-:john:ALL" in /etc/security/access.conf

3、PAM 文件 中有拼写错误：

Troubleshooting ticket 9

Problem

Hi guys, I followed a tutorial from the internet and completely messed up lnx02 after following it! I am no longer able to log in to our server lnx02 with any user. The root account isn't working as well! I don't get any password prompts. Moreover, the lnx02 is not accessible through IPv6 at all.
Please HELP!!

TIP) It is recommended to utilize both access options in CML, namely VNC and Serial. Grub will exclusively display its output through VNC, and Linux kernel will alter the output to serial during boot.

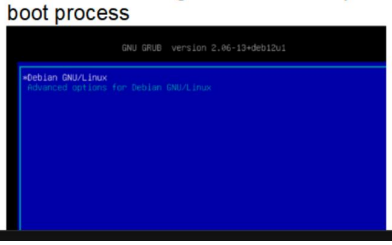
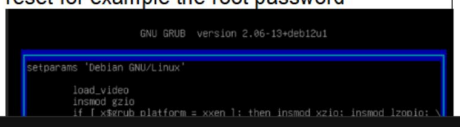
What are the causes of the problem?

- A typo in /etc/pam.d/common-auth always matches pam_deny.so, which denies all login requests.
- IPv6 has been completely disabled on ens3 interface.

On lnx02:
There is typo: "a0th" in /etc/pam.d/common-auth.
The ens3 interface ipv6 is disabled in /etc/sysctl.conf.

Recommended solutions to fix this:

- Reboot machine in single user mode and fix the typo from "a0th" to "auth" in /etc/pam.d/common-auth
- Remove line net.ipv6.conf.ens3.disable_ipv6 = 1 from sysctl.conf

Press ESC during boot to interrupt the boot process	Press "e" to edit the grub. Edit the line starting with "linux". Replace there "ro" with "rw", add single after rw and add at the end of the line "init=/bin/bash". This is a standard procedure boot any linux machine in single user mode to reset for example the root password
	

十九、SSL：

1、证书和私钥不匹配：

```
# 使用命令查看：
openssl x509 -noout -modulus -in server.crt | openssl sha256
openssl rsa -noout -modulus -in server.key | openssl sha256
```

Troubleshooting Ticket 13

Hey, this is Michael Jones. You mentioned that our FTP service (ftp.itnsa.net) is secured using a certificate from the DC, but I tried testing it from workstation1 yesterday using FileZilla, and it's not working. I'm unable to establish a connection, and it seems the secure configuration isn't functioning as expected.

Problems:

Proftpd TLS module is not enabled on /etc/proftpd/modules.conf

Certificate (/etc/proftpd/ftp.itnsa.net.crt) and private key (/etc/proftpd/ftp.itnsa.net.key) is not match, mismatch can be verified by comparing the modulus of the certificate and private key

On svr2.itnsa.local:

The proftpd service is not enable mod_tls.c module.

The proftpd SSL certificate(/etc/proftpd/ftp.itnsa.net.crt) and private key(/etc/proftpd/ftp.itnsa.net.eky) is not match, so the client can not establish connection.

Solutions:

Enable Proftpd TLS module on /etc/proftpd/modules.conf

Within /etc/proftpd/ directory, there is ftp.itnsa.net.pfx file that bundles certificate & private key, extract .crt and .key from that .pfx file then replace the existing certificate and private key used by proftpd with the extracted files

二十、DNS：

1、bind9 可能配置 allow-query 来仅限制某个网段的客户端能够解析域名，这样就会导致其他没有定义的网段无法解析这个域名。

二十一：用户：

1、用户登陆时间设置为白天导致晚上无法登陆；脚本没有放到

PATH system environment variable:

Troubleshooting ticket 15

Problem

Hello, I am a PowerShell developer and last week I have heard that there is a new version of Powershell. I think the newest version is called Powershell 7. Yesterday, I was playing around on my machine ws01 using the sysop local account and now I can no longer start pwsh.exe anywhere from cmd anymore, instead, I need to start the pwsh.exe from C:\Program Files\Powershell\7 folder instead. Can you resolve this problem?
By the way, I met in the morning my colleague Reese Terry from the night shift and she complained that she was unable to work last night on ws01 as she was unable to login. Due to this reason, she instead dealt with the paperwork throughout the entire night. Could check this issue as well before she starts her night shift again?

What are the causes of the problem?

- pwsh.exe cannot be found in any folder defined in the PATH system environment variable.
- Logon hours set for account terry during the day instead of night

On lnx02:
The pwsh.exe script have not define into PATH system environment variable.
The terry account is set login hour during the day instead of night.

Recommended solutions to fix this:

- Fix typo in PATH system environment variable to C:\Program Files\Powershell\7\
- Logon hours for account terry needs to be adjusted during night