telcoItaly FastDelivery's Documentation

Day to day activities

FB, GS

Version 1.8.6, 19/03/2025

telcoItaly FastDelivery Activities

Table 1. Revision history

Version	Date	Authors	Description
1.8	**13/05/2024**	**GS**	Merged Fastdelivery’s wiki
1.8.1	**23/05/2024**	**FB**	Restore All Services On Servers
1.8.1.1	**11/07/2024**	**GS**	Added software versions
1.8.1.2	**12/12/2024**	**GS**	Updated Disk Space table references
1.8.2	**16/12/2024**	**GS**	Added Decommissioning steps
			Moved CM under ASA
			Updated Project Owners table
1.8.3	**27/01/2025**	**GS**	Expanded decommission, added Assyst contact, refined osq282v cert
1.8.3.1	**30/01/2025**	**GS**	Finally found how report.apptitcare works
1.8.3.2	**03/02/2025**	**GS**	pfx extraction of pem and key file
1.8.4	**25/02/2025**	**FB**	certificate error fix
1.8.5	**25/02/2025**	**FB**	DNS decommision on telcoItaly.it
1.8.6	**19/03/2025**	**GS**	SunOS commands reference
1.8.7	**26/06/2025**	**GS**	Updated certificates link

1. Network Device Table

Table 2. Partial Device Table

Hostname	IP	Management IP	Description
MI-TSR90	10.933.379.131	10.429.379.44	Terminal Server
MI-VFX900 chassis	10.971.379.971		Firewall DC F&D - active
MI-VFX901 chassis	10.971.379.134		Firewall DC F&D - standbyF
MI-VFX900	10.971.379.141		ASA FirePower
MI-VFX901	10.971.379.142		
MI-VFX900 MGMT		10.429.379.36	ASA Firepower Contextes
MI-VFX901 MGMT		10.429.379.37	
MI-VFX900 DMZ		10.429.379.38	
MI-VFX901 DMZ		10.429.379.39	
MI-VFX900 BACKEND		10.429.379.40	
MI-VFX901 BACKEND		10.429.379.41	
MI-VFX900 FRONTEND		10.429.379.42	
MI-VFX901 FRONTEND		10.429.379.43	
MI-VMX900	10.971.379.135	10.429.379.49	Router DC F&D
MI-VMX901	10.971.379.136	10.429.379.50	
MI-VMX904	10.971.379.139	10.429.379.51	
MI-VMX905	10.971.379.140	10.429.379.52	
MI-VSX906		10.429.126.135	Hardware ISE
MI-VSX907		10.429.126.136	
MI-VSX909		10.429.719.7	ISE Application
MI-VSX910		10.429.719.8	
MIVLB513		10.429.126.165	F5 Pre bilanciatore standalone
MIVLB514		10.429.126.175	F5 Pro bilanciatore standby
MIVLB515		10.429.126.176	F5 Pro bilanciatore active
miobmplbs1		10.971.225.126	Virtualized F5 Pro bilanciatore active

Hostname	IP	Management IP	Description
miobmplbs2		10.971.225.379	Virtualized F5 Pro bilanciatore standby
osx100v		10.256.166.100	Proxy Active
osx222v		10.256.166.102	Proxy Standby
VIP for system admin		10.256.166.101:8080	Proxy VIP
mi5fdsx008		10.429.719.5	DNS master
osx101v		10.256.166.21	DNS public/external
osx102v		10.256.166.22	
osx103v		10.256.169.21	DNS private/internal
osx104v		10.256.169.22	
osx215v		10.256.164.114	Certificates dump
mi5fdsx001		10.429.719.78	Backup server

2. ASA Firepower Firewall

Table 3. Cisco ASA

DNS	IP	Model	ASA Version	FXOS Version	Description
MI-VFX900	10.971.379.971	Firepower 4110	9.18.4.29	2.12(1.172)	Active
MI-VFX901	10.971.379.134				Passive

Support

Cisco Case
Cisco compatibility matrix

2.1. Configuring ACL

- This can be done with the private IP or a network plus the subnet mask
- To get the Private IP from powershell do: `nslookup <PublicIPaddress>`
- Check from where that IP will arrive:
  - From the correct MI-VFX900-1 context run: `show route <IPaddress>`

Example:

```
MIVFX900-1/BACKEND/pri/act# show route 198.19.32.144
Routing Table: BACKEND
Routing entry for 198.19.32.0 255.255.254.0, supernet
Known via "static", distance 1, metric 0
Routing Descriptor Blocks:
-192.168.25.1, via ITDCC
Route metric is 0, traffic share count is 1
```

This specific example was done from BACKEND context because the VFR (Virtual routing and forwarding) routes through that context

2.1.1. To Add an IP

> Also called "an opening" or "un'apertura"

- Log into MI-VFX900-1
- Check the IP source to know which context will be
- Run the following:

```
change context <contextName>
configuration terminal
access-list GLOBAL_ACL extended permit <protocol> host <sourceIP> host <destinationIP>
eq <port>
```

```
access-list GLOBAL_ACL extended permit tcp host X.X.X.X host X.X.X.X eq https
write
```

Has to be repeated in needed contexts

2.1.2. To Add Using a Network

- When the mask is provided run:
  - `access-list GLOBAL_ACL extended permit tcp 10.106.116.0 255.255.252.0 host 10.256.171.43 eq 443`
  - `access-list GLOBAL_ACL extended permit <protocol> <sourceIP> <sourceMask> host <destinationIP> eq <port>`

2.1.3. To Delete an ACL

- Search for the ACL you need to erase using: `show access-list | include x.x.x.x`
- Put `no` in front of the line.
  - Example: `no access-list GLOBAL_ACL extended permit tcp 10.106.116.0 255.255.252.0 host 10.256.171.43 eq 443`

In Case of Errors check:

- the contexts routing table
- the Network Scheme
- if all the involving teams where contacted, such as Montesano

2.1.4. ACL using object-group

- There are some cases where you will add the source IP to an `object-group` that compress all the destination IPs.
  - Example: `access-list GLOBAL_ACL extended permit tcp host 10.132.181.117 `object-group objN-MgmT-Net eq 22`
  - In this case we have a server that wants to reach an IP inside MGMT context where there is an `object-group` containing all the IPs `object-group network objN-MgmT-Net`
- To search an `object-group` run `show object-group | include <keyWordOrIp>` from the needed context, then use the `<line number>` to find the object-group.

Remember to search in all contextes.

2.1.5. Access Control List Additional Info

You can find additional informations here

- An e-mail request will start the procedure

- If the `object-group` is not mentioned it has to be retrieved
  - From `10.429.719.78 2022/MI-VFX900` most recent backup run `grep <ipAddress/KeyWord> 2022/MI-VFX900/<mostRecent>`
  - From `10.429.719.78 2022/MI-VFX900` most recent backup open it with mobaXterm or download it and with `ctrl+f <ipAddress/KeyWord>`
- Configure the ACL inside the DMZ context like explained above with correct `object-group`, in the example is objN-VPN-Reply and the correspondent IP
  - Example: `access-list GLOBAL_ACL extended permit tcp ``object-group` **objN-VPN-Reply** host x.x.x.x eq https`

In case you need to find the Private IP or just want to corroborate info run from powershell while in VPN telcoItaly and logged-in ASA `nslookup <FQDN>` (Fully Qualified Domain Name)

The inverted flux is not permitted: `access-list GLOBAL_ACL line 5493 extended permit tcp host 10.256.170.39 ``object-group` objN-VPN-Reply eq https (hitcnt=0) 0x4b4e153c`

2.2. Block IP from Firewall

1. Connect to MIVFX900 firewall via `ssh 10.971.379.141`
2. Change context to DMZ: `MIVFX900-1/MGMT/sec/act# changeto context DMZ`
3. Create group with the objects that needs to be blocked:

```
MIVFX900-1/DMZ/sec/act# configuration terminal
MIVFX900-1/DMZ/sec/act(config)# object-group network CNG_DD_MM_YYYY
MIVFX900-1/DMZ/sec/act(config-network-object-group)# network-object host x.x.x.x
MIVFX900-1/DMZ/sec/act(config-network-object-group)# network-object host y.y.y.y
MIVFX900-1/DMZ/sec/act(config-network-object-group)# exit
```

4. Select macro-group IP_DENY_container: (config-network-object-group)
   - `object-group network IP_DENY_container`
5. Add the blocked IP group to the macro-group: (config-network-object-group)
   - `group-object CNG_DD_MM_YYYY`
6. Verify:
   - Check if IPs are added correctly to the object-group: `show object-group id CNG_05_04_2022`
   - Check if the object-group is in the IP_DENY_container:
     - `show object-group id IP_DENY_container | i CNG_DD_MM_YYYY`
7. Save the configuration: `write memory`

Example

```
MIVFX900-1/DMZ/sec/act(config)# object-group network CNG_04_03_2021
MIVFX900-1/DMZ/sec/act(config-network-object-group)# network-object host
193.877.192.219
network-object host 915.254.43.18
network-object host 480.92.205.81
network-object host 436.15.8.116
network-object host 195.272.154.116
MIVFX900-1/DMZ/sec/act(config-network-object-group)# exit
MIVFX900-1/DMZ/sec/act(config)# object-group network IP_DENY_container
MIVFX900-1/DMZ/sec/act(config-network-object-group)# group-object CNG_04_03_2021
MIVFX900-1/DMZ/sec/act(config-network-object-group)# exit
MIVFX900-1/DMZ/sec/act(config)# show object-group id IP_DENY_container | i
CNG_04_03_2021
object-group network IP_DENY_container
 group-object CNG_04_03_2021
```

2.3. Communication Matrix (CM)

Table 4. IP owning table

Context	IP class
DMZ	`10.429.0.0 255.255.0.0`
	`10.256.0.0 255.255.0.0`

Table 5. VRF table

Context	Virtual Routing Forwarding
ASA Firepower	DSL_DATA
Frontend	UNTRUSTED_U2S
	SERVICE_CTP
Backend	EITO_PROD
	IT_CSP_TRANSIT
	TRUSTED_S2S
	ITDCC

> Image example needed

1. what lines are mine? Are always the last ones highlighted? ==== Is it from the inside or the outside?
2. If the VRF is given: Check the VRF table
    a. If it's not given, start from Backend: `show route <destinationIP>`

```
MIVFX900-1/BACKEND/sec/act# sh route 104.242.226.240

Routing Table: BACKEND
Routing entry for 04.442.226.240 255.255.255.240
  Known via "static", distance 1, metric 0
  Routing Descriptor Blocks:
  * 192.168.28.1, via IT_CSP_TRANSIT
      Route metric is 0, traffic share count is 1
```

1. what questions do I need?
2. Log into ASR
   a. Look for the prefix set: `show rpl prefix-set <VRF_NAME>`
3. Log into Nexus 5k
   a. Look for the prefix set: `show vrf <VRF_NAME>`

2.4. Essentials Firewall Actions

Verify the Connection

- Type: `show connection all | i <target IP>`
- Verify Inbound connection flag

To Recover the VIP

- From powershell run `nslookup <FQDN>` Ex: `nslookup it.infobyip.com`
- Log into MI-VFX900-1 and from DMZ context run `show nat | i <publicIP>` to fetch the private IP used by F5

Access Chassis from CLI to check physical interfaces

- Connect through SSH to the IP `10.971.379.971/4` or using the Chassis session from MobaXterm access to the ASA Chassis
- Once inside run the following commands:
  - `connect fxos` && `sh int e1/5` (or any desired interface)

Test Connectivity of ACL implementated

- Inside ASA from the needed context launch the command `ping` and enter
- From the choices type `y`to proceed
- Insert the target IP
- Insert destination port
- The option will appear Specify source type `y`to proceed
- Insert the source IP then press enter 3 times to proceed with the test

```
MIVFX900-1/DMZ/pri/act# ping
```

```
TCP Ping [n]: y
Interface: DMZ-FRONT
Target IP address: 10.456.470.30
Destination port: [80] 22
Specify source? [n]: y
Source IP address: 10.432.318.24
Source port: [0]
Repeat count: [5]
Timeout in seconds: [2]
Type escape sequence to abort.
Warning! Specified source interface DMZ-FRONT is different
than expected source interface LEGACY-PRE!
Sending 5 TCP SYN requests to 10.256.170.30 port 22
from 10.132.18.24, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/1/1 ms
```

- For the `packet-tracer` command
  - Type input, insert the interface, the protocol, then the IP source, select the port number or protocol, Enter the destination address, and select the port number or protocol. as the example below:

```
MIVFX900-1/DMZ/pri/act# packet-tracer input DMZ-FRONT tcp 10.532.19.24 7194
10.756.470.30 22 detailed
Result:
input-interface: DMZ-FRONT
input-status: up
input-line-status: up
```

2.5. Firewall capture

Mind disk space, when using `capture`, with `max buffer`

1. Connect to the firewall `MIVFX900-1 10.971.379.141`
2. Switch to needed context Ex: `MIVFX900-1/MGMT/sec/act# changeto context DMZ`
3. Run: `capture <name> type raw-data {trace buffer | circular-buffer} interface <int> match <protocol> <sourceIP> <destinationIP> <port>`

Example output

```
capture ADE type raw-data interface APPLICATION-BACK circular-buffer [Capturing *
524259 bytes]
match tcp host 10.256.174.17 any4 eq 27017
```

For more info on Using Packet Capture to troubleshoot: MI-VFX900-1 Firewall

2.6. NAT in ASA FirePower

For any doubts consult NAT Configuration Guide

2.6.1. AUTO NAT

- Create an `object network` for a private IP inside a NAT
- Check from which interface comes the IP `show route X.X.X.X`
- From `Configuration terminal` run:
- Create the object network as shown in the example below:

Example: from `10.256.171.76` map a `91.80.46.115`

```
conf t
object network obj-10.256.171.76
host 10.256.171.76
```

- Then configure the nat inside the object network

```
nat (LEGACY-PRE,DSL_DATA) static 91.80.46.115 no-proxy-arp
```

Remember to check and update the IP table and CM if it's available

2.6.2. Type 2 NAT

Create an `object-network` for a private IP inside a NAT

```
configuration terminal
MIVFX900-1/DMZ/pri/act(config)# object network host-10.429.429.9
MIVFX900-1/DMZ/pri/act(config-network-object)# host 10.429.429.3
exit
```

Localize the VRF of origin and destination

```
MIVFX900-1/DMZ/pri/act(config)# nat (internal interface, external interface) source
static host-37.25.228.243 host-37.25.228.243 destination static host-83.224.74.49
host-10.429.429.9
```

Define a specific NAT rule for translating source and destination IP addresses

```
nat (internal interface, external interface) source static host-37.25.228.243 host-
37.25.228.243 destination static host-83.224.74.49 host-10.429.429.9
```

In summary, the command configures a NAT rule that keeps the source IP address unchanged

(37.25.228.243) for outbound traffic from the "internal interface."
For inbound traffic through the "external interface," it translates the destination IP address 83.224.74.49 to 10.429.429.9.

2.6.3. Delete an existing NAT

- Select the needed network object:
  - MIVFX900-1/DMZ/pri/act(config)# object network obj-10.256.171.153
- Inside `conf t` run one of this 3 examples:

```
MIVFX900-1/DMZ/pri/act(config)# no object network obj-<Private IP>
MIVFX900-1/DMZ/pri/act(config)# no nat static <Public IP>
MIVFX900-1/DMZ/pri/act(config)# no nat (LEGACY*PRE,DSL_DATA) static <Public IP> no-
proxy-arp(optional)
```

2.7. Failover

Right now primary is in standby

IPS Primary	IPS Secondary
MIVIX505	MIVIX503
IT4SECFPRFTD01	IT4SECSOU3D01
`MIVFX900-1/sec/act#`	`MIVFX900-1/pri/stby#`

1. Connect to the devices shown above
2. Change context to System: `change context system`
3. Verify: `show failover state`
4. From the standby run: `failover active`
5. Wait to reconnect and run `show failover state`

2.8. Adding Routes on the ASA

- To add a Route in the Firewall use the following command `route if_name dest_ip mask gateway_ip [ distance ]`
  - Example: `route ITDCC 198.19.148.192 255.255.255.224 192.168.25.1 1`
- Sometimes you will need to add the route from the Backend context up to DMZ. The following example shows the established routes coming from the ITDCC VRF in order:

```
From VRF to Backend
route ITDCC X.X.X.X (destination IP) Y.Y.Y.Y (subnet mask) 192.168.25.1 1
From Frontend to Backend -> This is established in the FE context
route FRONT-BACK X.X.X.X (destination IP) Y.Y.Y.Y (subnet mask) 192.168.65.3 1
```

```
From Frontend to DMZ -> This is configured in the DMZ context
route DMZ-FRONT X.X.X.X (destination IP) Y.Y.Y.Y (subnet mask)  192.168.64.3 1
```

The VRF can vary according to what is indicated in the mail/request or the routing in the ASR 9000

2.9. Change logging server

This has to be done in all contexts, beware of the specific interface for each context

- Search for the needed interface where the configuration is stablished
- Add the route using the command known
- Go inside the Configuration Terminal, and then direct yourself into the interface
- Once in there use the command: `logging host interfaceName Destination IP protocol/port`

Example:

```
MIVFX900-1/MGMT/sec/act# route FDmgmt-MGMT 10.971.213.22 255.255.255.255 10.429.379.33
1
MIVFX900-1/MGMT/sec/act# conf t
MIVFX900-1/MGMT/sec/act(config)# interface Port-channel1.2600
MIVFX900-1/MGMT/sec/act(config-if)#
logging host FDmgmt-MGMT 10.971.213.22 17/12514
wr
```

3. ASR 9001

Table 6. Cisco ASA

DNS	IP	Device	IOS XR	ROM
MI-VMX900	10.971.379.135	Cisco ASR 9001	6.4.2	3.04
MI-VMX901	10.971.379.136			

Support

Cisco Case

3.1. Add route to existing prefix

Verify the configuration of the VRF: `show run vrf UNTRUSTED_U2S`

To configure the VRF

```
configuration terminal
vrf context UNTRUSTED_U2S
ip route X.X.X.X/X Vlan<id> IP next-hop address in format i.i.i.i
```

You don't need to go into 'conf t' to add or remove the routes

prefix	cmd
see	`show rpl prefix-set`
add	`edit prefix-set pfx_ITDCC_fromPE inline add "198.19.145.32/27 le 32"`
remove	`edit prefix-set pfx_ITDCC_fromPE inline remove "198.19.145.32/27 le 32"`

> When PE is source: From PE //
> When PE is destination: To PE

3.2. Verifying the subnet of the network to add in the prefix

- Insert the IP in the following Tool
- The result will indicate both the network and the subnet.
- If subnet on CCP tool is marked with:

```
GDC Dedicated VF-Italy is equal to ITDCC
GDC Internal Shared - VOD is equal to EITOPROD
```

3.3. Verifying Reachability

Table 7. Use the following commands to verify routing exchange and reachability informations in Border Gateway Protocol (BGP)

Input Command	Command Description
show route	Shows information about the routing table
sh bgp all unicast	Displays information about the BGP routing table entry
show bgp ipv4 unicast 10.971.227.6	Displays information about the BGP routing table entry for the specific IP address
show bgp vrf ITDCC neighbors	Displays information about BGP neighbors within a specific VRF
show bgp vrf ITDCC neighbors 10.177.37.1 received routes	Displays configuration information and statistics for BGP4 neighbors of the device for a virtual routing and forwarding (VRF) instance
sh bgp route + rpl_CE-PE_vrf-XXXX-IN/OUT	Displays information about the current BGP routing state and the paths available for routing traffic through the network

Additional Info regarding BGP VRF

3.4. Useful Commands

Input Command	Command Description
`show tech-support bcdl`	Displays technical support information for the BCDL module.
`show bdcl consumers`	Shows information about BDCL (Block Distributed Control Loop) consumers.
`show process blocked location all`	Shows all blocked processes and their locations.
`show bdf session`	Displays information about the BDF (Binary Data Format) sessions.
`show bdf session detail`	Shows detailed information about the BDF (Binary Data Format) sessions.
`show bgp nei 3.3.3.2`	Displays BGP (Border Gateway Protocol) neighbors for the specified IP.
`show bgp vrf <name> nei 3.12.1.2`	Displays BGP neighbors for the specified VRF (Virtual Routing and Forwarding).
`show route bgp`	Shows BGP (Border Gateway Protocol) routes.
`bgp auto-policy-soft-reset disable`	Disables automatic soft reset for BGP.
`no bgp auto-policy-soft-reset disable`	Enables automatic soft reset for BGP.

Input Command	Command Description
`bgp graceful-restart`	Enables graceful restart for BGP.
`no bgp graceful-restart`	Disables graceful restart for BGP.
`show bgp neighbor 10.0.101.1 config`	Displays the configuration of the BGP neighbor with the specified IP.
`show bgp process`	Shows information about the BGP process.
`clear bgp ipv4 multicast dampening 172.20.0.0/16`	Clears BGP multicast dampening for the specified IPv4 address range.
`clear bgp external`	Clears external BGP (Border Gateway Protocol) sessions.
`clear bgp vrf vrf_A nexthop performance stats`	Clears the performance statistics for the specified VRF nexthop.
`show bgp vpnv4 unicast vrf`	Displays BGP VPNv4 (Virtual Private Network version 4) unicast for the VRF.

4. ISE

Table 8. Cisco UCS-ISE

DNS	IP	Description
MI-VSX906	10.429.126.135	Cisco Integrated Management Controller
MI-VSX907	10.429.126.136	
MI-VSX909	10.429.719.7	Active node
MI-VSX910	10.429.719.8	Secondary node

Support

Cisco Case

4.1. Password Change and Reset in Cisco ISE

4.1.1. Admin Password

In Cisco ISE the WebGUI and CLI admin username and passwords are separate.

In order to change the passwords you can use the following methods:

When doing the CLI password keep a shell of both nodes `MI-VSX909/10` in order to avoid login issues.

- Run `password`. The CLI password is unique to each ISE node but we usually put the same
- WebGUI password can be changed from CLI with `application reset-passwd ise <username-here>`.

Example:

```
MIVSX909/admin# password
Enter old password:
Enter new password:
% Password must contain at least one digit.
Enter new password:
Confirm new password:
MIVSX909/admin# application rese
reset-config  reset-passwd
MIVSX909/admin# application reset-passwd ise admin
Enter new password:
Confirm new password:


Password reset successfully.

MIVSX909/admin#
```

Reset the password from another account .Example:

```
MIVSX909/zzsaronnig# conf t
MIVSX909/zzsaronnig(config)# username admin password plain IlEhe;1CiQqIEUqP role admin
```

The WebGUI password must be reset on the Primary PAN, this password is then synchronised to all ISE nodes.

WebGUI:

- Navigate to `Administration` → `System` → `Admin Access` → `Administrators` → `Admin Users`

Has to be done in **both** Cisco devices

4.1.2. ISE GUI Password Recovery Mechanism

1. Use the CLI admin account to log in on the console.

Remember that the console admin account is different than the web GUI admin account. They have the same username but can have different passwords.

2. From the command prompt, use the `application reset-passwd ise admin` command to set a new web GUI admin password.
3. Prompt to reset password appears as shown in this image:

```
ISE-2-0/admin# application reset-passwd ise admin
Enter new password:
Confirm new password:

Password reset successfully.
ISE-2-0/admin#
```

4. Enter the new password as required.
5. To confirm that the new password works, use the new password to log in to GUI.

4.1.3. Personal Account Password zz<youruser>

- Go to ISE `10.429.719.7` log in with the admin credentials in the GUI
- Open `Administration`
- Go to `Identities`
- Search the needed username
- Click it → edit → create the new password

4.1.4. Resetting a forgotten ISE Password

If you have forgotten the ISE CLI password you can only reset this by booting from the ISE DVD/ISO

Figure 1. Select option 3 or 4

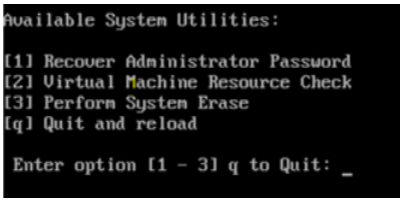


Figure 2. Select option [1] Recover Administrator Password

- Select Admin account and enter the new password
- Save changes and exit to reboot the ISE node

4.2. Configure Repository mi5fdsx001 on ISE

- Cause: 90gg password expire
- For more information. Refer to Cisco Documentation

ISE Alarm: Info: Scheduled report export failed. Unable to copy the exported file to repository.

- Fix: Change mi5fdsx001 password
  - Update inventory
  - Update **both** ISE devices.

```
Connect to repository MI5FDSX001
MIVSX909/admin# configure terminal
MIVSX909/admin(config)# repository MI5FDSX001
  url sftp://10.429.719.78/app/usrbck/iseusrbck
  user fpusrbck password plain <putThePlainPswHere>
```

Host key of the server must be added using 'crypto host_key add' exec command before sftp repository can be used.

```
MIVSX909/admin(config-Repository)#exit
MIVSX909/admin# crypto host_key add host MI5FDSX001
host key fingerprint added
Operating in CiscoSSL FIPS mode
```

```
# Host MI5FDSX001 found: line 1
MI5FDSX001 RSA SHA256:UMzbvD0MI4GRFaQNvq5X2ZK4H5qjbpt5+rC56aTCXWY
```

- If the alarm keeps arriving check ISE GUI. Go to Administration → System → Maintenance → Repository.
- Select the repository `MI5FDSX001` and click edit. Update the psw.

> *Don't ask me why they do not use ssh key exchange*

4.3. Make a Bundle in Cisco ISE

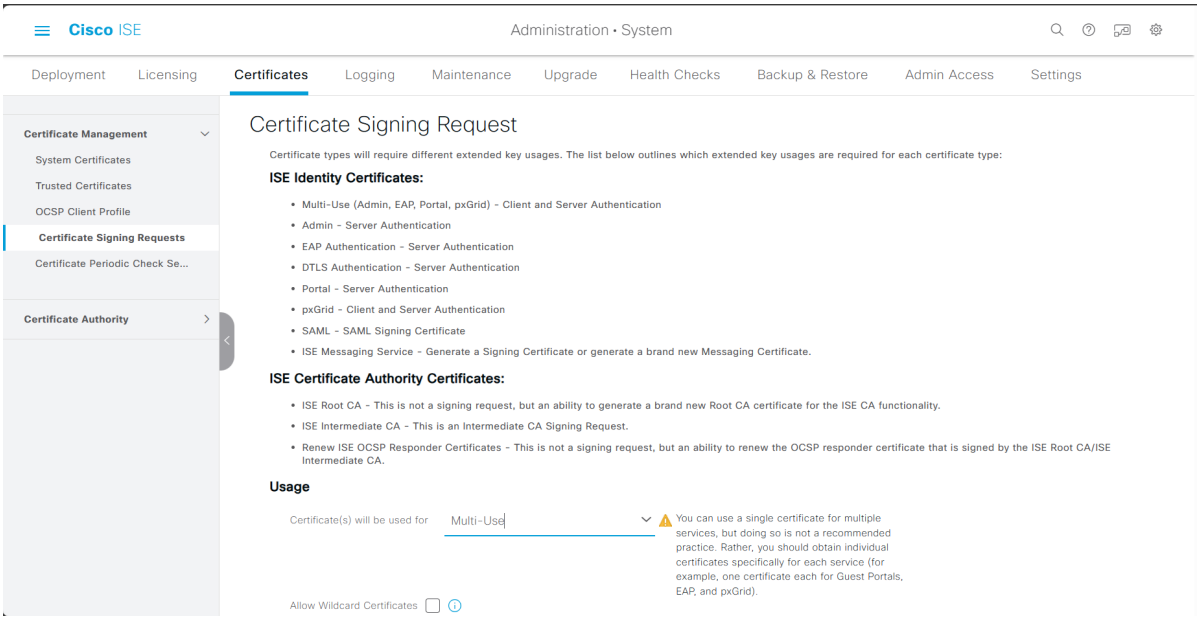
- Go to the `10.429.719.7` address log in with the admin credentials:
  - Has to be done in **both** nodes
  - Choose an encryption key bundle719
  - Choose key's longevity
- The saved logs are:
  - Debug logs
  - Local logs
  - Monitoring and reporting logs
  - System logs

4.4. OCSP Certificate Renewal

- This certificate is autogenerated inside the Cisco ISE `MI-VSX909`, to access the CSR generator follow the steps below:

You must request one certificate for each node

- To generate new self-signed certificates, navigate to Administration > System > Certificates > System Certificates. Click the Generate Self Signed Certificate.



- Under the Usage section, select the role to be used from the drop-down menu. To Renew OCSP Certificate select the corresponding option.
- ISE itself will autogenerate and update the certificates for both nodes. Last step will be to control everything is up to date.

5. Cisco Nexus 5000

Table 9. Cisco Nexus 5612

DNS	IP	Device	BIOS	System
MI-VMX904	10.971.379.139	Cisco Nexus 5612	3.7.0	7.3(3)N1(1)
MI-VMX905	10.971.379.140			

Support

Cisco Case

5.1. Check the routing

- Log into the MIVMX904 or MIVMX905. Run `sh ip prefix-list ?` to show existing prefixs. Example:

```
MIVMX904# sh ip prefix-list ?
  <CR>
  >                    Redirect it to a file
  >>                   Redirect it to a file in append mode
  WORD                 Name of prefix-list (Max Size 63)
  static-DSL_DATA      Known prefix-list name
  static-EITO_PROD     Known prefix-list name
  static-ITDCC         Known prefix-list name
  static-IT_CSP_TRANSIT  Known prefix-list name
  static-MGMT          Known prefix-list name
  static-SERVICE_CTP   Known prefix-list name
  static-TRUSTED_S2S   Known prefix-list name
  static-UNTRUSTED_U2S   Known prefix-list name
  |                    Pipe command output to filter

MIVMX904#sh ip prefix-list static-IT_CSP_TRANSIT
ip prefix-list static-IT_CSP_TRANSIT: 2 entries
   seq 5 permit 10.256.160.0/20
   seq 10 permit 10.429.429.0/22
```

- Has to be picked depending on the VRF
- If the IP is already inside the prefix there's no need to configure the routing, add the ACL to each context

5.2. Network insertion on prefix-list

- To insert a new IP in the prefix-list follow the steps below:
- Go to `configure terminal`
- Type the command `ip prefix-list name description string` → Optional: Adds an information

string about the prefix list or `ip prefix-list name [ seq number ] [{ permit | deny } prefix {[ eq prefix-length ] | [ ge prefix-length ] [ le prefix-length ]}]`

Example:

```
ip prefix-list static-UNTRUSTED_U2S seq 45 permit 10.429.429.0 le 24
show ip prefix-list _name_ -> to review the list
copy running-config startup-config
```

5.3. Configuring the Route in an existing Interface

- To configure a new route inside the interface follow the steps below: .Example:

```
sh run vrf UNTRUSTED_U2S
conf t
vrf context UNTRUSTED_U2S
ip route X.X.X.X/X Vlan<id> IP next-hop address in format i.i.i.i
copy running-config startup-config
```

6. F5

Table 10. BIG-IP Devices

DNS	IP	Description	Version
MIVLB515	10.429.126.176 GUI	Production Active	15.1.10.2 Build 0.44.2
MIVLB514	10.429.126.175 GUI	Production Passive	
MIVLB513	10.429.126.165 GUI	PreProduction	
miobmplbs1	10.971.225.126 GUI	Virtualized on GMIVCFE01 F5 Pro active	

Support

- Lantech Support
- e-mail:

6.1. Nodes description

Status Indicator	Description
Green circle	The object is available. This icon indicates that the BIG-IP system services traffic destined for this object. For BIG-IP APM sessions, this icon indicates that the session is established.
Blue square	The availability of the object is unknown. For example, this status can occur when the object is not configured for service checking, the IP address of the object is misconfigured, or the object is disconnected from the network. For BIG-IP APM sessions, this icon indicates that the session is pending and not yet established. **Note:** Pool members and nodes with a status of unknown are eligible to receive client requests.
Yellow triangle	The object is not currently available but might become available later with no user intervention. For example, an object that has reached its configured connection limit might show a yellow status and then switch to a green status when the number of connections falls below the configured limit.
Red diamond	The object is unavailable. This icon indicates that the BIG-IP system cannot service traffic destined for this object. For example, this status can occur when a node fails service checking because it has become unavailable. This status requires user intervention to restore the object status to green.
Black circle	A user has actively disabled an available object.
Black diamond	A user has actively disabled an unavailable object.
Gray icons	A parent object has disabled the object, or the object is enabled but unavailable because of another disabled object.
Black Square	The availability of the object is unknown, and the object is disabled.

source
source

To deepen the information about the F5 go here

6.2. Remediation of the header using the iRule Pro

`iRule:/F5_FE-DMZ-ext/RemoveX-Header-Response_Irule`

- With the IP search in the virtual server list from ALL contextes

- Open the correspondent service
- Go to resources from the needed context, otherwise it will be in Read Only
- Pick the correct iRule then press finished

From CLI

1. `tmsh`
2. `cd /FE-`<needed context>
3. `list ltm virtual` if you need to find the name
4. `modify ltm virtual [virtual_server_name] rules RemoveX-Header-Response_Irule`

Some useful commands

- If a replacement is needed you can: `modify ltm virtual my_vs rules { my_irule }`
- If you need to find the iRule you can: `list ltm rule`

6.3. Find the devices in the F5 Production enviroment

GUI

- Log into the GUI → local traffic → network map
- Select the partition ALL → introduce in filter the IP or VM

CLI

- Log into the F5 CLI and run `tmsh`
- List items → `cd / to root → list /ltm node recursive <nodeName>`
- Or this can run from bash: `tmsh -c "cd /; list /ltm node recursive" | grep -b2 <nodeName>`
- To list all the nodes from all contextes run: `cd /`
  - `list /ltm node recursive`
- Once found the correct one run: `cd <context>`
  - `list /ltm node <nodeName>`

From bash `tmsh -h` helps you with what to do, `tmsh --help` gives you detailed info

6.4. Verifying the TSL

GUI

- Log into needed F5 and look for the server:
  - Inside the server you should search for the advanced conf and see the available conf

CLI

- Log into needed F5 and:
  - Type `openssl s_client -connect VIP:port number`

    - Example: `openssl s_client -connect 10.10.10.10:443 tslversion`
- This command will verify all the certificates configured in the f5:

```
show /ltm profile client-ssl | grep -E "TLS|Ltm::ClientSSL" | grep -v 1.2 | grep -v
DTLS | grep -v ' 0'
Output Example:
Ltm::ClientSSL Profile: pre-discovery.telcoItaly.it_cert
TLSv1.3 0-RTT
  TLS Protocol Version 1.0                                        1.6K
  TLS Protocol Version 1.1                                          91
  TLS Protocol Version 1.2                                        65.5K
  TLS Protocol Version 1.3                                            0
  DTLS Protocol Version 1                                             0
  DTLS Tx Pushbacks                                                   0
```

6.5. Patching Activity

- This activity runs from MIVLB515.private.it
- A notification mail must be sent to monitoring group to signal the beginning
- Turn off nodes as instructed from dedicated file depending on number: T71, T72 or T73
    - Log in MIVLB515.private.it and run: `bash t7_all-main_v01.3.sh`
- Contact the needed collegue and comunicate that nodes are offline and activity can begin **

Do not contact him through: company mail. He does not read it

- Terraneo will contact you back to ask you to turn on the nodes
- Once the nodes are back online notify Reply to verify.
    - Rep Reply 349 213 9442
    - Alberto Steri 347 781 8763
    - They will verify once the shift starts according to CEST time zone
- A notification mail must be sent to monitoring group to signal the end

> Insert sample and link to patching procedure. Or include it here The other T7 patching doc must be shipped together with this one or implemented here

If problems occurs you can find documentation in consulences Onedrive inside Cyclic Patching folder

6.6. Modify the banner in F5 CLI

Do not take `vi` or `vim` lightly! Take sometime to read how to use it. Read me!

From F5's CLI

```
vi /config/ssh/ssh_banner
#Insert Banner
----------------------------------------
             telcoItaly Italy

      This network is protected by
         a data security system

          Unauthorized access
          will be prosecuted.
----------------------------------------

Equipment: MIVLB513

Customer : telcoItaly

Descr.   : F5 BIG-IP LTM-I4600
----------------------------------------

tmsh modify /sys sshd include "Banner /config/ssh/ssh_banner"

tmsh save /sys config   #safe the config file
```

6.7. Rule configuration on LTM to accept incoming requests from specific IP

*Example: 178.239.182.26 * CRM di Facile.it to a specific URL (https://scoprioffer.telcoItaly.it/api)*

- If the public IP of the service is not available, use `nslookup` or press nslookup site
- Once the IP is obtained, find the corresponding private IP by querying the MIVFX900 firewall (10.971.379.141):

```
- MIVFX900-1 / DMZ / sec / act # show run nat
object network obj-10.256.166.36
 nat (LEGACY-DMZ, DSL_DATA) static 91.80.46.37 no-proxy-arp
```

6.7.1. From F5

GUI

- Select "F5_FE_DMZ_ext" from the "Partion" drop-down menu

- From Main → Local Traffic → Virtual Server
- Put private IP 10.256.166.36, followed by wildcard *
- Click on the entry of the server with Service Port 443 (HTTPS)
- "Resources" from the horizontal menu above
- Select the text contained in the "Name" field under "iRules" and copy (Ctrl + C or right mouse button)
- Click on iRules from the menu on the left
- Paste in the search field the text previously copied followed by wildcard *

- Insert the new instruction in the iRule code. Example:

```
when HTTP_REQUEST {
  #CHG 84220
  switch [HTTP :: host] {

"discoveroffer.telcoItaly.it" -
"discoveroffer.voda.it" {
switch -glob [HTTP :: uri] {
"/ api *" {
if {([class match [IP :: client_addr] equals
ministi02_Tool_https://eag.telcoItaly.com/vpn/index.html[EAG]LE_Reply_net]) or
([class match [IP :: client_addr] equals ministi02_Tool_VDL_net]) or
!!!!!!! new instruction inserted ---------> ([class match [IP :: client_addr] equals
ministi02_CRM_Facile_it_net]) or <--------
 ([class match [IP :: client_addr] equals ministi02_Vola_net]) or
```

- Click on Update to save the changes
- Click on Pending Sync at the top left next to the F5 logo, to synchronize the changes made with the backup F5
- Select the line corresponding to the device with "Sync Status" in yellow from the Device box and click on the "Sync" button

6.8. Update User List for alsmobile

- Connect to the active F5 BIG-IP LTM GUI `10.429.126.176` then import the file containing the user lists:

It has to be done from `Common` Partition

1. Main → System → File Management → Data Group File List
   - ~~Check latest "App-Android_msisdn_users_v2" number, as of 20230705 is 19~~
2. Main → System → File Management → Data Group File List → Import (button on the right)
3. "Choose file" button
4. Pick "Overwrite existing"
5. In "Name" pick: "App-Android_msisdn_users_v2"
6. In "File Contents" select the "String" item
7. In "Data Group Name" enter the name of the group: "App-Android_msisdn_users_v2"
8. Import

The following text is no longer necessary, but can be useful

`Update the reference to the Data Group File List in the iRule:`

1. Main → Local Traffic → iRules
2. Partition F5_FE-DMZ-Ext
3. Select the first iRule `APP-android_v2-http_iRule`

Beware that there is another one is `s`, APP-android_v2-http**s**_iRule

4. Modify line 6 `set static :: user_for_MSISDN "App-Android_msisdn_users_v19` with the updated value
5. Click bottom left on Update

`If F5 reports an error in compiling the file, proceed as follows:`

1. Copy only line 1 of the file and paste it in the F5 box
2. Click on Import
3. Go to the .txt file, select all the lines except line 1 already copied
4. Paste the selected lines in the F5 box
5. Import

It rarely happens but: If there is Pending Sync at the top left next to the F5 logo, click it to synchronize the changes made with the backup F5

6.9. Implement ACL in F5

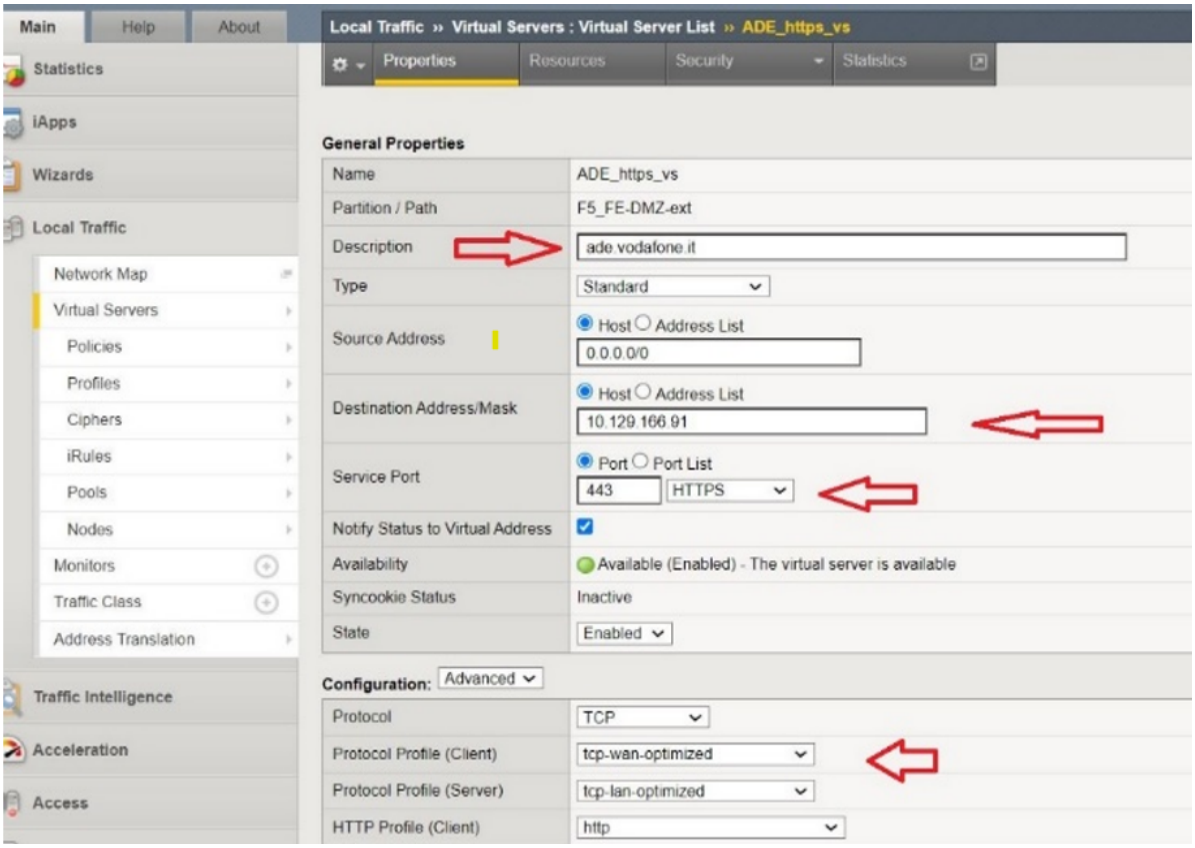
- Find out service name:
  1. from `cmd` run: `nslookup <URL/FQDN> without https and without trailing /`
  2. pick up the public IP and log into the firewall `10.971.379.142 MI-VFX901`
  3. from DMZ context look for the local IP: show nat | i `<publicIP>`
- Look up the ACL group:
  1. login into F5, PRE or PRO depending on the request
  2. Click the Virtual Servers on the left menu
  3. From top right select All[Read only] partition
  4. Put the private IP in the search bar surrounded by wildcards *
  5. From Resources Tab the iRules, always choose the `https` secure one
  6. Look in each iRule the name, it's usually after "equal" inside the TCL script
  7. From the left menu Local Traffic → iRules → Data Group List
  8. Change partition to needed one
  9. Put iRules name in the search bar surrounded by wildcards *

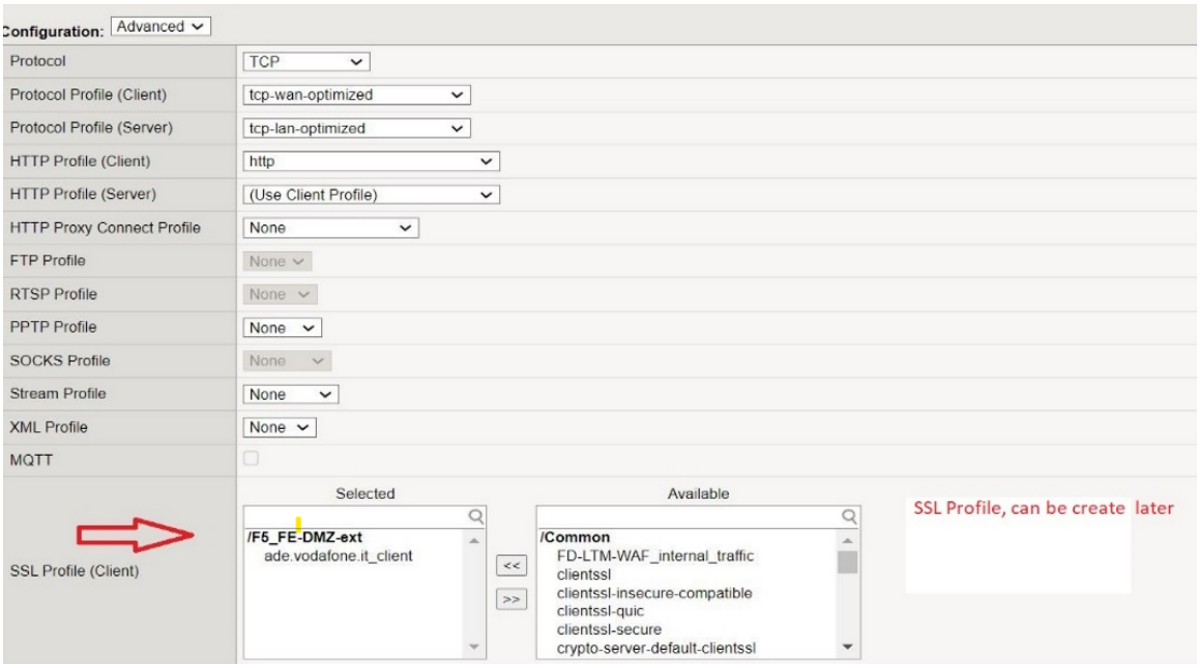
10. From the CMatrix get the IP and put it in Address
11. From the CM get the Note cell and put it in Value
12. Press Add and Update
13. Repeat the last steps until all the IPs are added

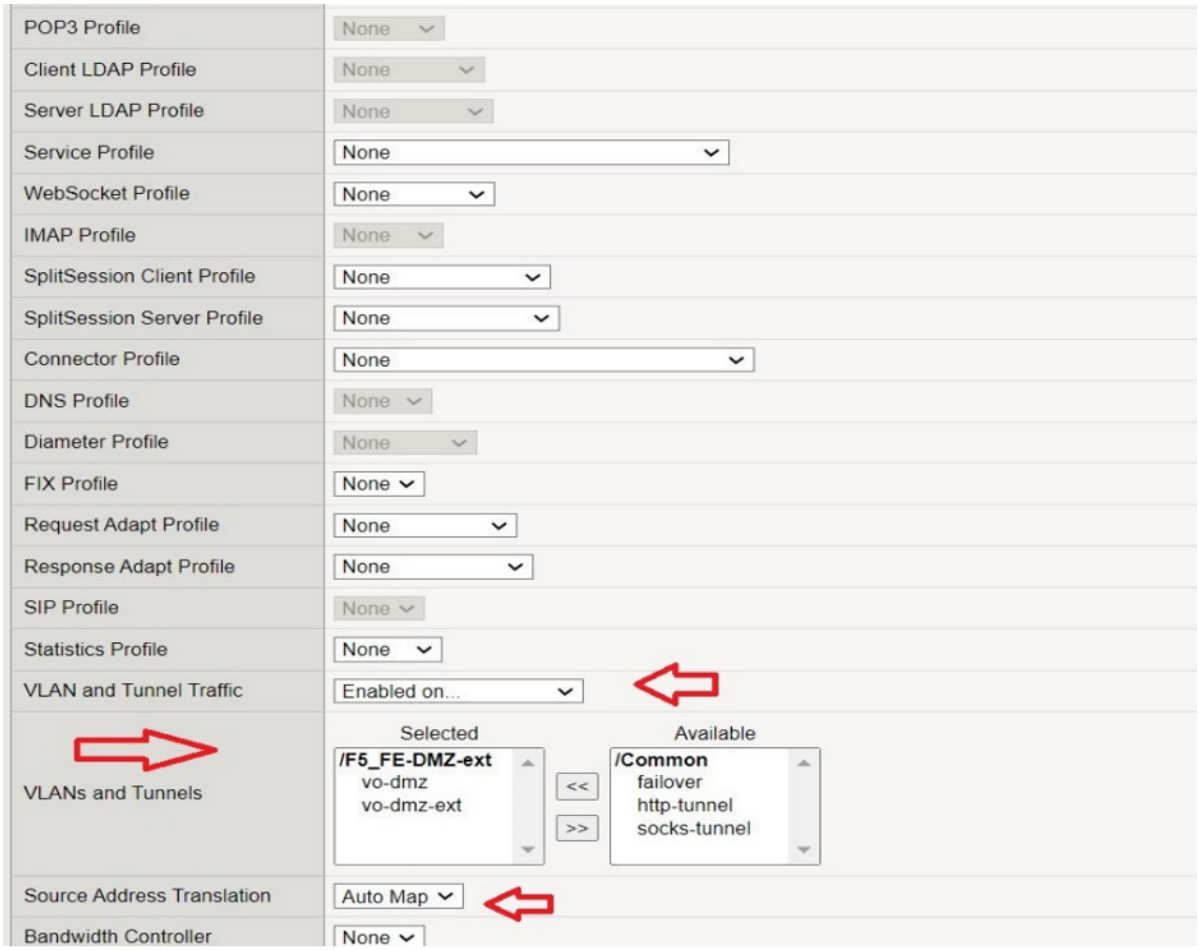
- Answer the e-mail

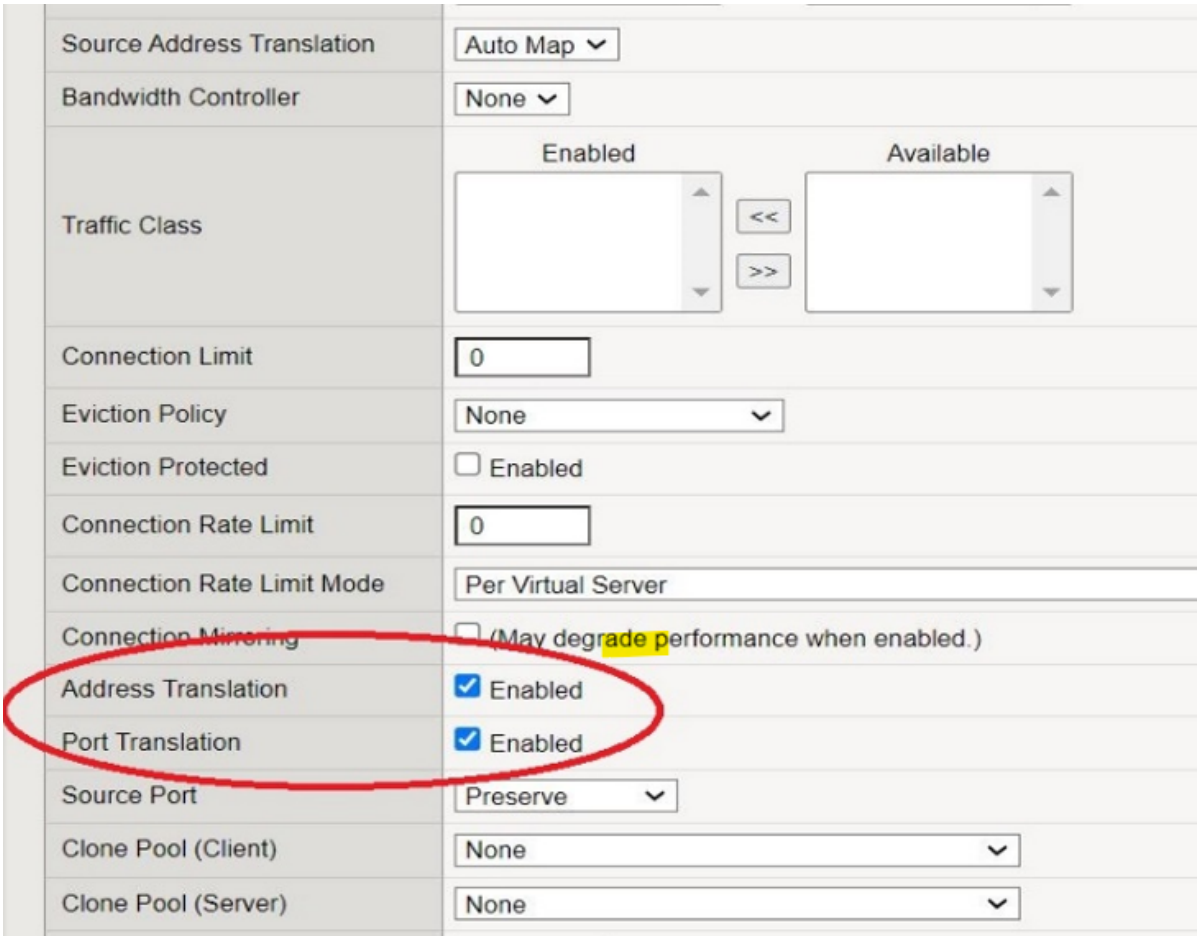
6.10. Create a Virtual Server (GUI)

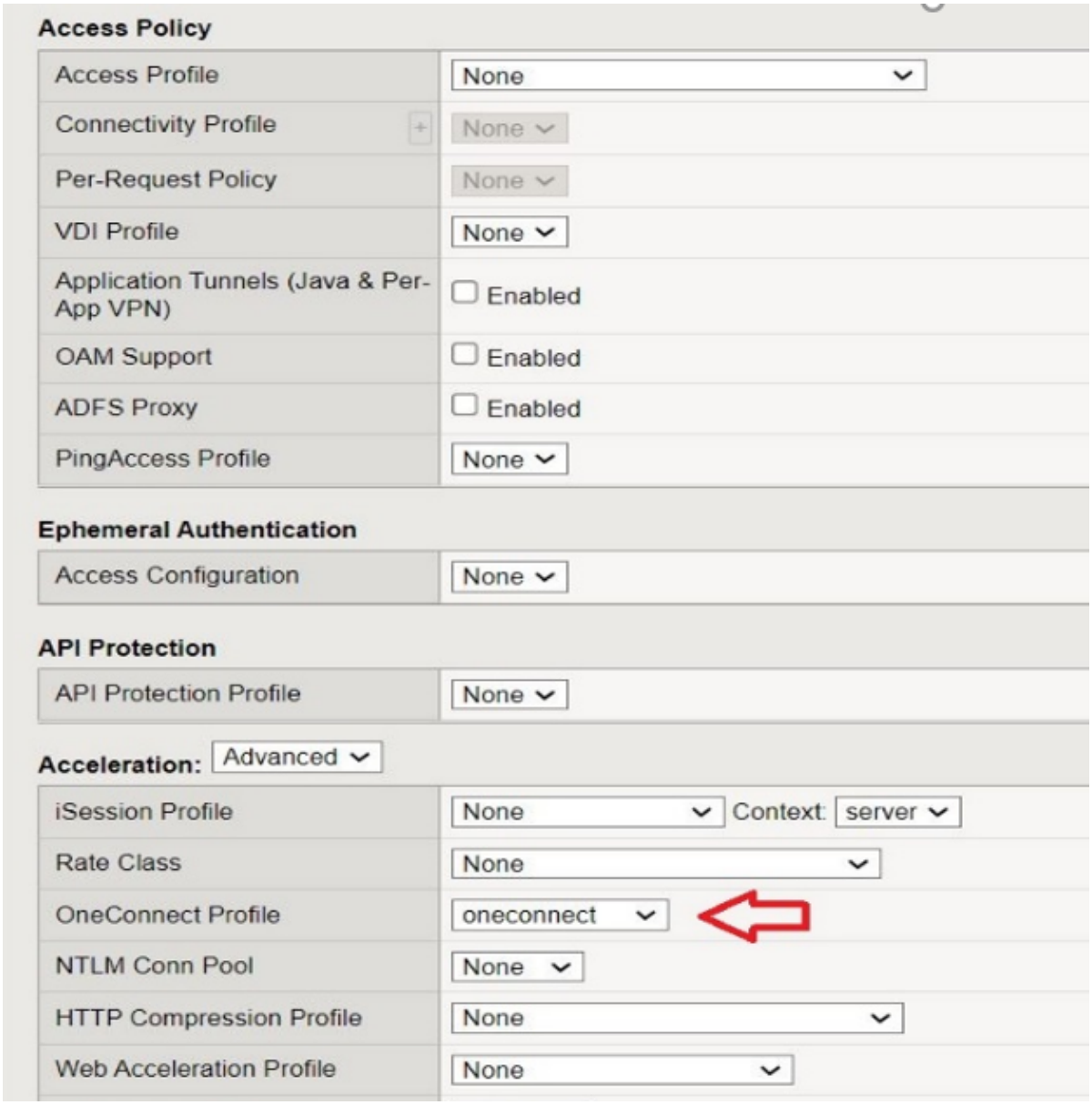
- Go to F5 GUI, inside Virtual Server → Create.
- Follow the images below to continue the configuration




Configuration: Advanced
Protocol
TCP
Protocol Profile (Client)
tcp-wan-optimized
Protocol Profile (Server)
tcp-lan-optimized
HTTP Profile (Client)
http
HTTP Profile (Server)
(Use Client Profile)
HTTP Proxy Connect Profile
None
FTP Profile
None
RTSP Profile
None
PPTP Profile
None
SOCKS Profile
None
Stream Profile
None
XML Profile
None
MQTT
SSL Profile (Client)
Selected
/F5_FE-DMZ-ext
ade.vodafone.it_client
Available
/Common
FD-LTM-WAF_internal_traffic
clientssl
clientssl-insecure-compatible
clientssl-quic
clientssl-secure
crypto-server-default-clientssl
SSL Profile, can be create later


POP3 Profile
None
Client LDAP Profile
None
Server LDAP Profile
None
Service Profile
None
WebSocket Profile
None
IMAP Profile
None
SplitSession Client Profile
None
SplitSession Server Profile
None
Connector Profile
None
DNS Profile
None
Diameter Profile
None
FIX Profile
None
Request Adapt Profile
None
Response Adapt Profile
None
SIP Profile
None
Statistics Profile
None
VLAN and Tunnel Traffic
Enabled on...
VLANs and Tunnels
Selected
/F5_FE-DMZ-ext
vo-dmz
vo-dmz-ext
Available
/Common
failover
http-tunnel
socks-tunnel
Source Address Translation
Auto Map
Bandwidth Controller
None


Source Address Translation
Auto Map
Bandwidth Controller
None
Traffic Class
Enabled
Available
<<
>>
Connection Limit
0
Eviction Policy
None
Eviction Protected
Enabled
Connection Rate Limit
0
Connection Rate Limit Mode
Per Virtual Server
Connection Mirroring
(May degrade performance when enabled.)
Address Translation
Enabled
Port Translation
Enabled
Source Port
Preserve
Clone Pool (Client)
None
Clone Pool (Server)
None


Access Policy
Access Profile
None
Connectivity Profile
None
Per-Request Policy
None
VDI Profile
None
Application Tunnels (Java & Per-App VPN)
Enabled
OAM Support
Enabled
ADFS Proxy
Enabled
PingAccess Profile
None
Ephemeral Authentication
Access Configuration
None
API Protection
API Protection Profile
None
Acceleration:
Advanced
iSession Profile
None
Context:
server
Rate Class
None
OneConnect Profile
oneconnect
NTLM Conn Pool
None
HTTP Compression Profile
None
Web Acceleration Profile
None

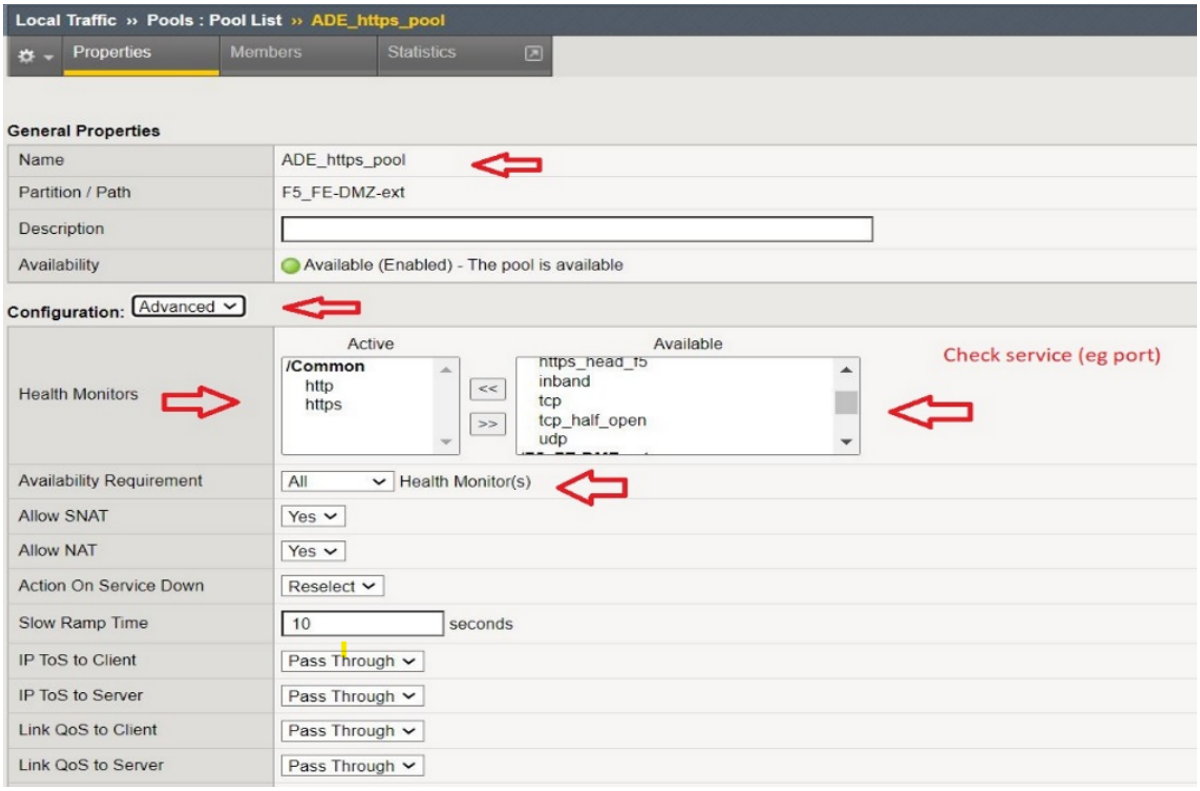


Figure 3. Pool Creation

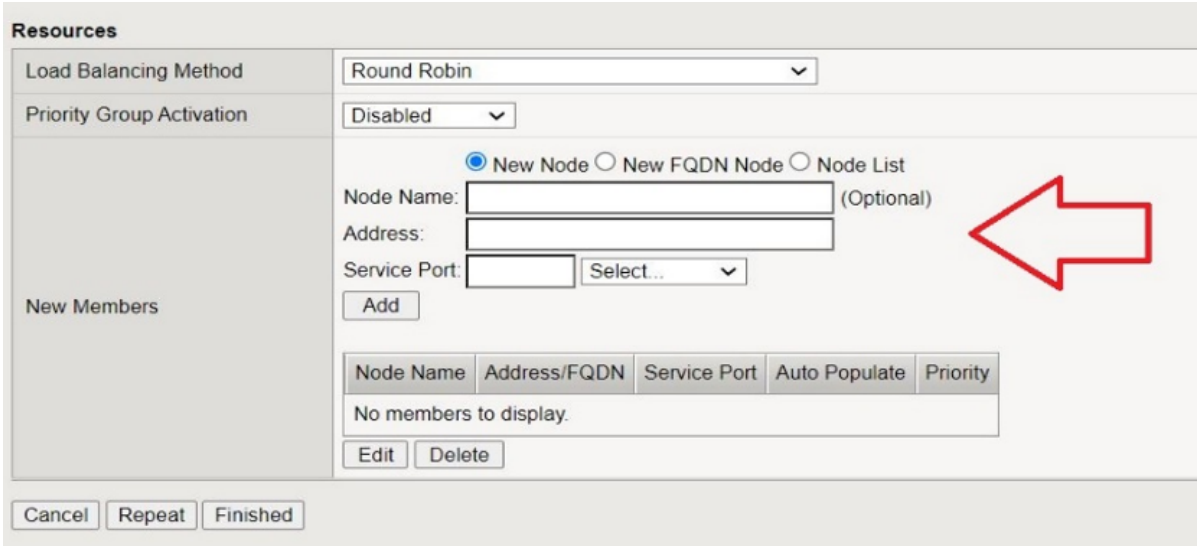


Figure 4. If it is a new Pool

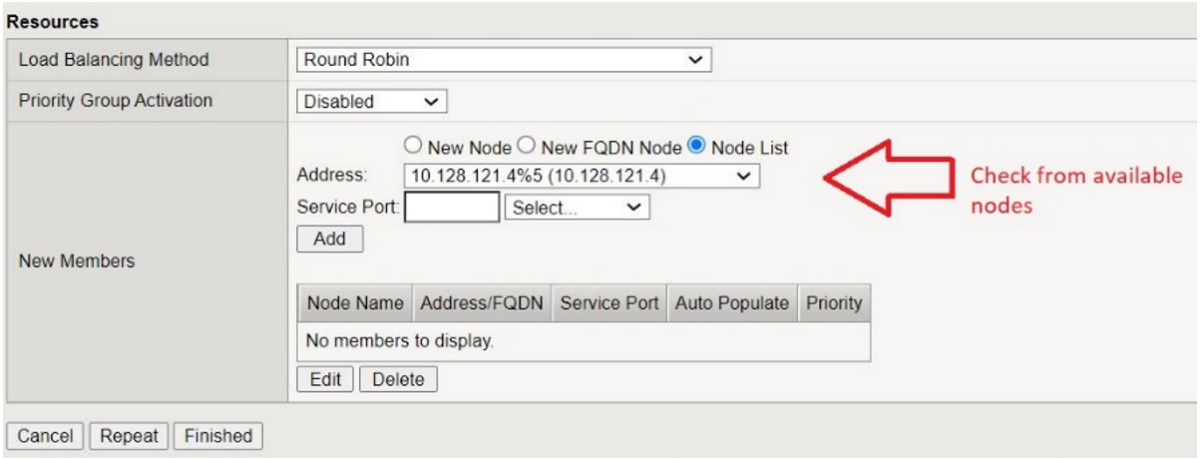


Figure 5. If are available, please check from Node List

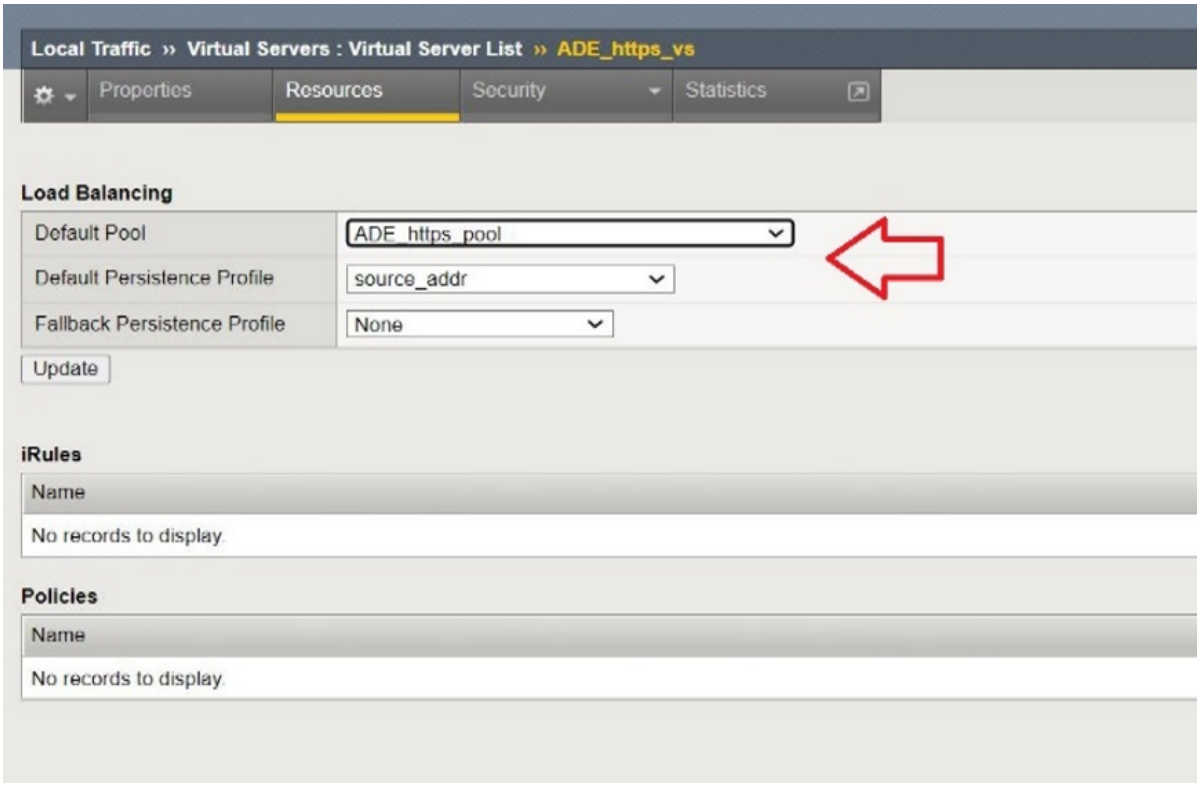


Figure 6. Then, associate Pool and Default Persistence profile to Virtual Server

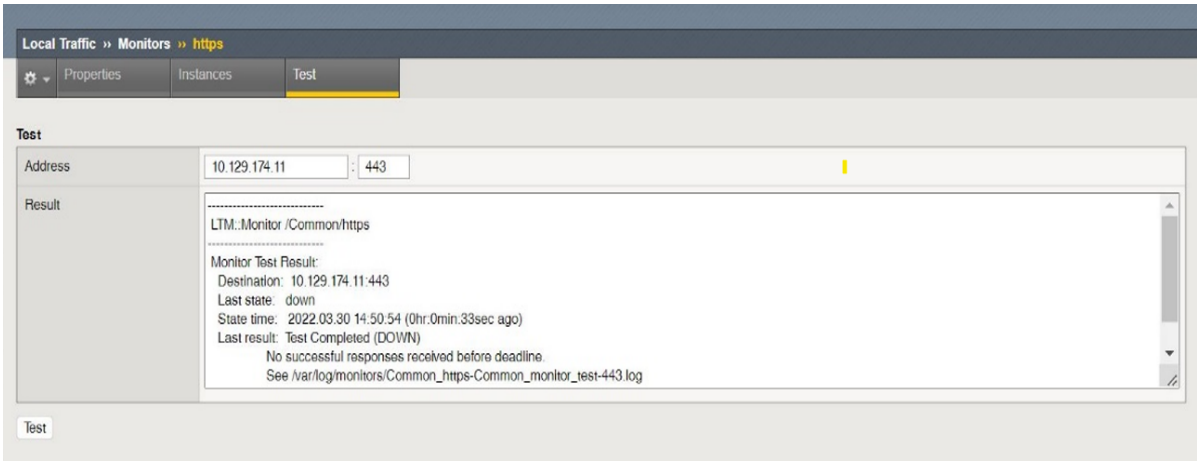


Figure 7. Health Monitor Check

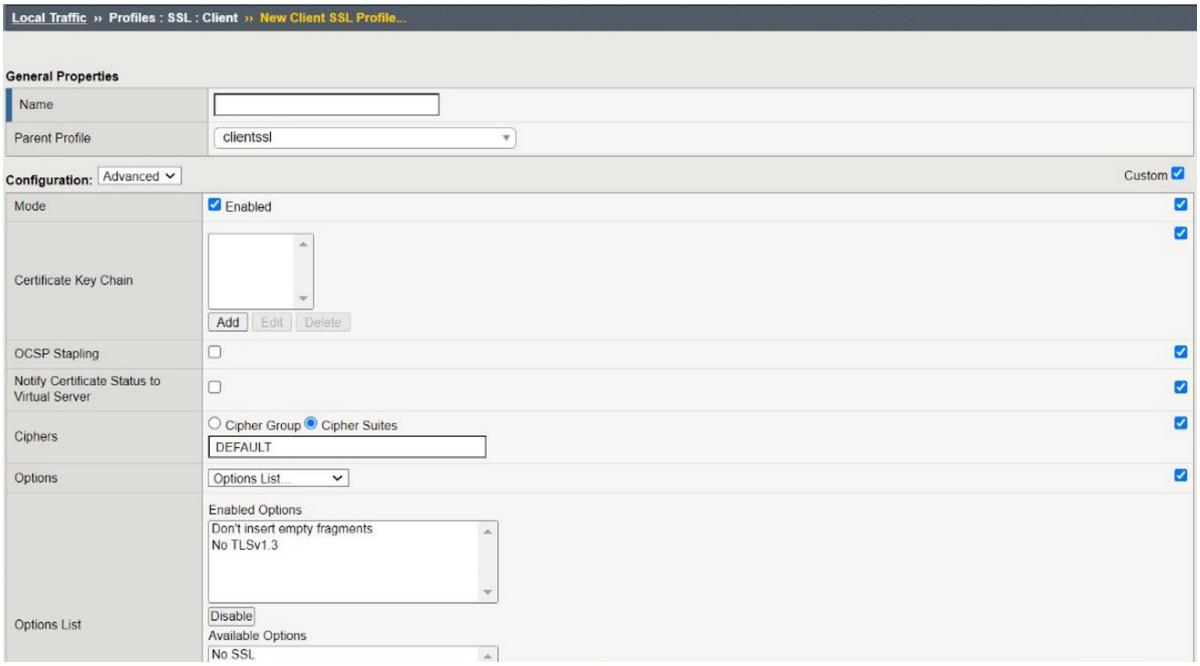
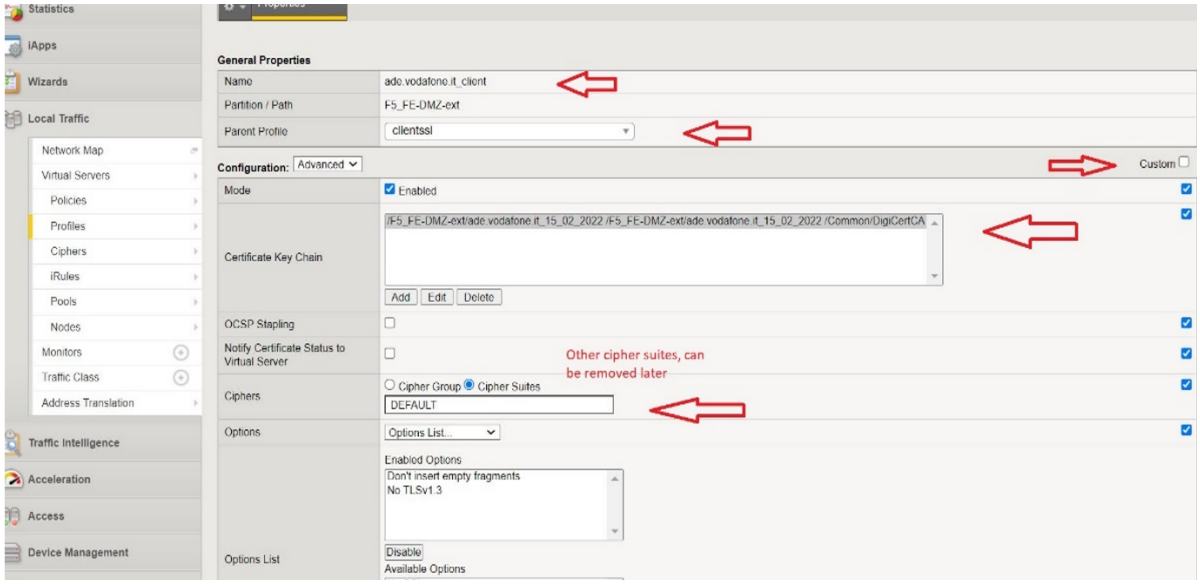


Figure 8. New Client SSL profile creation



6.11. Update or Upgrade BIG-IP

- For more information go to the F5 guide or follow the manual
- A case to Lantech must be opened in order to retrieve the updates.
- If it's an HA (High Availability) Active Stand-by configuration:
  - Start from Standby device
  - In case of configuration changes: `cpcfg --source=<volumeA> <volumeB>`
  - Disable automatic Sync in order to prevent sync errors from the different installed versions
    - Check actual status: `tmsh list /cm device-group` or `tmsh list /cm device-group Device-group-1`
    - Disable auto-sync: `tmsh modify /cm device-group Device-group-1 auto-sync disabled` and save `tmsh save /sys config`

Once Automatic Sync is disabled, the configuration changes must be manually synchronized.

Update Steps CLI

- Push the needed isos to the path `/shared/images`
- Go as root to the path `/shared/images`
- Check volume software: `tmsh show sys software` to view software informations or list the images: `tmsh list sys software image`
- Create the new volume for the new iso: `tmsh install sys software image <BIG-IP image ISO name> volume <volume_name> create-volume`
  - If you need to install an Hotfix: : `tmsh install sys software hotfix <BIG-IP hotfix-name.hotfix> volume <volume_name> create-volume`

If you get space error you have to remove an old volume: `tmsh delete sys software volume <volume_name>`

- Check install status: `tmsh show sys software status` or `watch -n 30 "tmsh show sys software status"`
- Reboot into the new volume: `tmsh reboot volume <volume_name>`

After you enter this command, the system immediately begins restarting. The system drops all existing connections and does not pass traffic until the restart completes and the BIG-IP configuration loads.

In case of configuration changes in the volume

- Use the following syntax to copy the configuration from the current active configuration to the new boot location, prior to restarting and booting into the new volume: `cpcfg --source=<volumeA> <volumeB>`

6.12. F5 Failover

To initiate a Manual Failover from the currently Active HA Peer BIG-IP in the Traffic Group, the following steps can be performed:

GUI Failover:

1. Log in to the active BIG-IP as the administrator
2. Click the Active link in the upper left hand corner next to the F5 Ball and Online. This is a shortcut link that takes you directly to Device Management > Traffic Group and into the Traffic Group for which the BIG-IP is currently the Active HA Peer BIG-IP.
3. Near the bottom of the Traffic Group's config page, click the Force to Standby button to initiate the Manual Failover. And watch the HA Role of that BIG-IP move into the Standby HA Role in the upper left hand corner next to the F5 Ball and Online.

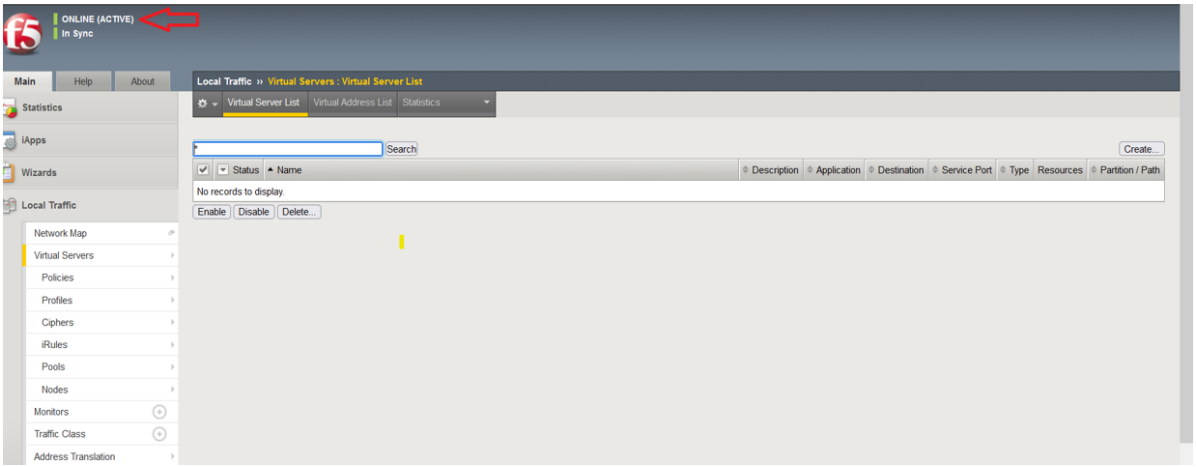


Figure 9. Reach the active `MIVLB515.private.it` as shown below:

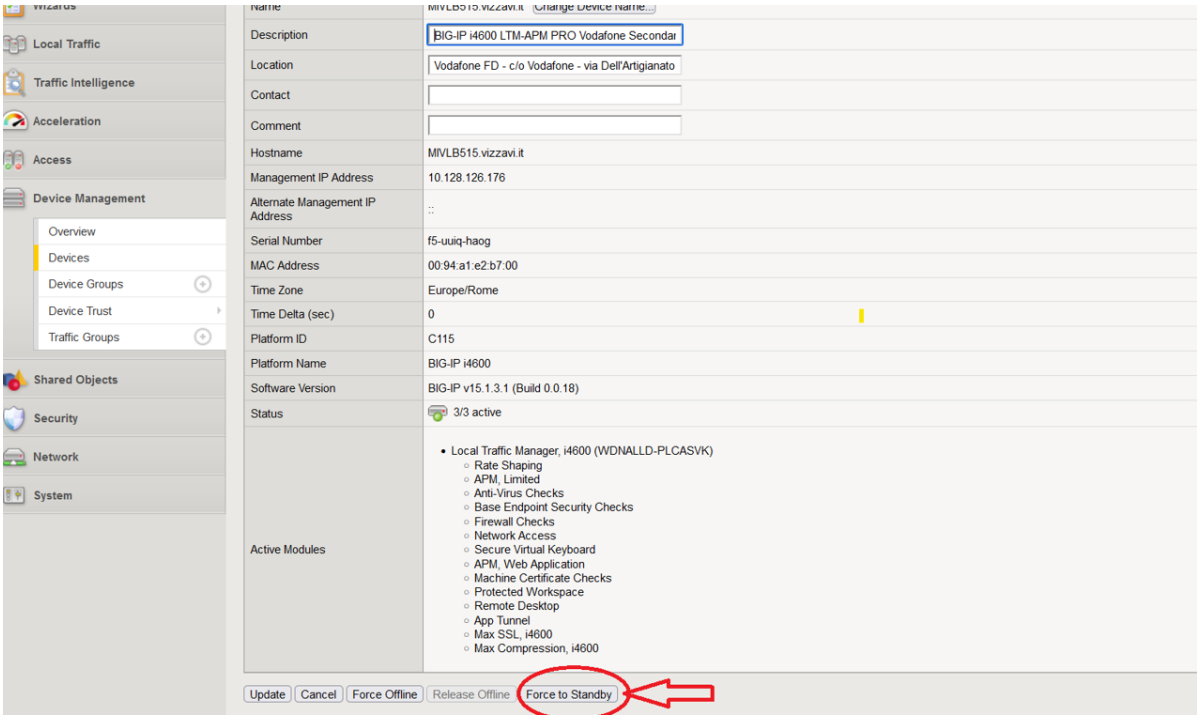


Figure 10. Inside Devices → Change the Description and Press force `Stand by`

CLI Failover:

1. Log in to the active BIG-IP CLI as the administrator.
2. Navigate to the LTM module by typing `tmsh`.
3. Check the current state of the devices by running the command `show sys failover`.
4. Trigger the failover with `run sys failover standby`.

6.13. About Data-Group

6.13.1. Search data-group in F5 CLI

- Go to the needed enviroment PRE or PROD
- From `tmsh` run :`cd /`
- To search the context where the data-group is stored type `list ltm data-group recursive | grep data-groupName`
  - Example: `list ltm data-group recursive | grep TiTCare-PRE_net`
- Then to get the info needed from the data-group `list ltm data-group internal data-groupName`
  - Example: `list ltm data-group internal TiTCare-PRE_net`

6.13.2. Add IPs to a data-group in F5 from GUI

Inside the excel take the URL do `nslookup xyz.telcoItaly.it`

Example:

```
  PS C:\> nslookup backoffice.telcoItaly.it
Server:  ns-office-it2.telcoItaly.com
Address:  10.21.100.239 --> Priv IP

Name:    backoffice.voda.it
Address:  91.80.46.172
Aliases:  backoffice.telcoItaly.it
```

With the Public IP go to the DMZ context in ASA, and run a `sh nat | i <publicIP>`. DMZ context is used because ther is NAT

Example:

```
MIVFX900-1/DMZ/pri/act#  sh nat | i 91.80.46.172
36 (LEGACY-DMZ) to (DSL_DATA) source static obj-10.256.166.149 91.80.46.172  no-proxy-
arp
```

- With the IP given from the ASA go to F5 Network map with partition: All. Be aware of the port you need, 80 or 443
- Take the Virtual Server name
- Search in the VS List the name you got from the prior step → Resources → click on the iRule, it leads you to the Properties of the iRule, read what it says and select the Datagroup
- Then go inside iRules → Datagroup List → Paste the datagroup.
  - Example: `Backoffice_BE190_net`
- Go inside the datagroup and Add the needed IPs

- Remember: to comment the added IPs using the Value option
- Press Add and Update to save the changes

In some cases you wil have more `data-groups` inside the `iRule`, verify the name from the CM, in some cases the IP has to be add into a `object-group`, in others a new `data-group` must be created

6.13.3. Add/Remove IPs to a data-group in F5 from CLI

To add

- A single entry
  - `tmsh create /ltm data-group internal <datagroup_name> records add { <entry_value> }`
- Multiple entries at once
  - `tmsh create /ltm data-group internal <datagroup_name> records add { <entry1_value> <entry2_value> ⋯ }`

To remove

- A single entry
  - `tmsh delete /ltm data-group internal <datagroup_name> records delete { <entry_value> }`
- Multiple entries at once
  - `tmsh delete /ltm data-group internal <datagroup_name> records delete { <entry1_value> <entry2_value> ⋯ }`
- Example:

```
[zzyourUser@MIVLB515:Active:In Sync] ~ # tmsh
cdzzyourUser@(MIVLB515)(cfg-sync In Sync)(Active)(/Common)(tmos)# cd /
zzyourUser@(MIVLB515)(cfg-sync In Sync)(Active)(/)(tmos)# cd F5_FE-DMZ/
zzyourUser@(MIVLB515)(cfg-sync In Sync)(Active)(/F5_FE-DMZ)(tmos)# modify /ltm data-
group internal TiTCare-pro_net records
Options:
  add               delete            modify            none              replace-
all-with
zzyourUser@(MIVLB515)(cfg-sync In Sync)(Active)(/F5_FE-DMZ)(tmos)# modify /ltm data-
group internal TiTCare-pro_net records add/delete {n.n.n.n}
```

6.13.4. Add a new data-group to the F5

Example: CM 8.18

```
PS C:\Windows\system32> nslookup scopriofferta.telcoItaly.it
DNS request timed out.
    timeout was 2 seconds.
Server:  UnKnown
Address:  10.21.100.239
```

```
Name:    scopriofferta.voda.it
Address:  91.80.46.37
Aliases:  scopriofferta.telcoItaly.it

Private IP
10.256.166.36

VS name
minisiti02pro-discovery_HTTPS_vs

iRule
/F5_FE-DMZ-ext/minisiti02pro-discovery_HTTPS_iRule
```

In this case once we get to the iRule we noticed there is no datagroup that corresponds to the service needed in the Cm so we proceed to create it

- Log in the F5 GUI → go to iRules → select Data-group → create the name → select a type in this case was `address` → add the IP address needed and the value, a comment → press Update

6.13.5. Add the datagroup inside the needed iRules:

1. Data-group name = `minisiti02_CRM_Smart_Contact_net`
2. IP address = `51.77.222.142`
3. Line added to the iRule referring to the datagroup = `([class match [IP::client_addr] equals minisiti02_CRM_Smart_Contact_net]) or`

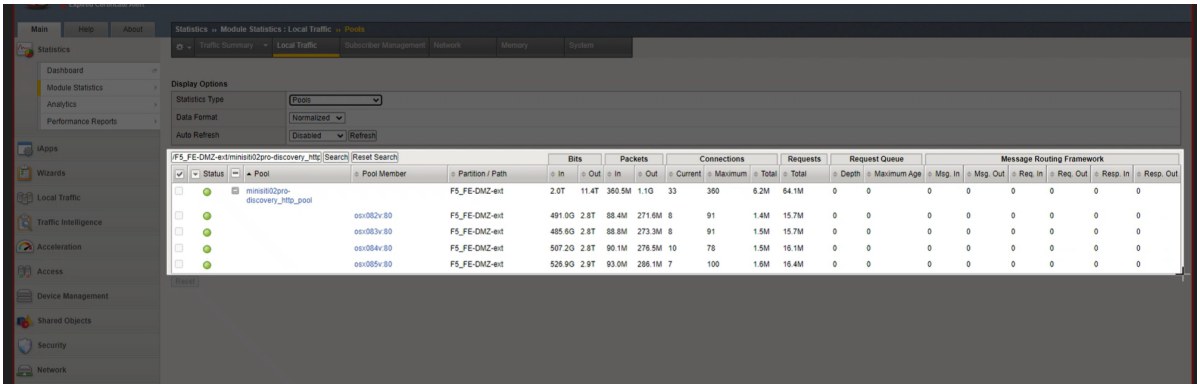
6.14. Removing a host from node/pool list

To do this task you must have the node and pool name, to fetch those go to the Network Map

- Go inside the pool list, search the needed pool and direct to the right context finally remove the node from the pool
- After that direct to the node list, search the node and delete it

6.15. Check if nodes has traffic

- Inside the F5 GUI, go to statistics → Module Statistics from there search the needed pool and go to local traffic. As shown in the below example:



Remember to be in All contexts

7. DNS BIND9

Table 11. DNS devices

DNS	IP	Role
mi5fdsx008	10.429.719.5	DNS master
osx101v	10.256.166.21	DNS Public / External
osx102v	10.256.166.22	
osx103v	10.256.169.21	DNS Private / Internal
osx104v	10.256.169.22	

DNS System Official Documentation BIND 9

7.1. Insert or Delete a Record inside the server BIND 9 DNS Master (Internal sync)

7.1.1. CLI

- Log into `mi5fdsx008`
- Path is: `cd /var/named/addr`
- Check db: `grep -R <regex> *`

Description	Commands
Serial number update	Test: `sed -E -n "s/[0-9]{8}/$(date +%Y%m%d)/p" ternal/db.voda.it`
	`sed -E -i "s/[0-9]{8}/$(date +%Y%m%d)/" ternal/db.voda.it`
Comment	Test: `sed -n '/bookinglearn/s/^/;/p' ternal/db.voda.it`
	`sed -i '/bookinglearn/s/^/;/' ternal/db.voda.it`
Uncomment	Test: `sed -n '/^;bookinglearn/s/^;//p' ternal/db.voda.it`
	`sed -i '/^;bookinglearn/s/^;//' ternal/db.voda.it`
Add a line after a specific regex pattern	Test: `sed -n '/regex/a\new_line' ternal/db.voda.it`
	`sed -i '/regex/a\new_line' ternal/db.voda.it`
Add a line after a specific line number	Test: `sed -n '4a\bookinglearn' ternal/db.voda.it`
	`sed -i '4a\bookinglearn' ternal/db.voda.it`
Append a line	Test: `sed -n '$a\bookinglearn' ternal/db.voda.it`
	`sed -i '$a\bookinglearn' ternal/db.voda.it`

Commit changes: `rndc reload`

Update serial number date on Master every time it gets modified. Otherwise it

> does not update the slaves.

> 20230705 This does sync all the slaves!!!!!!!!!

7.1.2. Monkey CLI

```
@                       86400   IN      SOA     dns1.private.it.
postmaster.private.it.
                                                2023032001      ; serial number
                                                3600            ; refresh [1h]
                                                600             ; retry [10m]
                                                1209600         ; expire[14d]
                                                3600            ; min TTL [1h]

@                       86400   IN      SOA     dns1.private.it.
postmaster.private.it.
                                                2023032001      ; serial number
                                                3600            ; refresh [1h]
                                                600             ; retry [10m]
                                                1209600         ; expire[14d]
                                                3600            ; min TTL [1h]
```

This process allows to replicate the files "DB" in the DNS to the two external and the two internal slaves osx101-2-3-4v

1. Log into server Master `MI5FDSX008` as root
2. Use `grep -R <regex> <filename/*>` to check if the info has to be added in another db
3. Edit the relative file to the zone that has to be modified.
    - Example:
    - `vi /var/named/addr/internal/<dbFileName>`
    - `vi /var/named/addr/external/<dbFileName>`

> Do not take `vi` or `vim` lightly! Take sometime to read how to use it. Read me!

4. Update the Serial Number in all the db's you are working, internal, external.
5. Run `rndc reload` to restart the service and apply latest changes

> Do not execute the following process. It leads to unsynchronized slaves and loss of changes. Because if changes aren't saved in the master, once restarted it imposes its own version.

The following is informative

Ultra monkey, *single files on each slave*

1. Log in the needed DNS slave osx101-2-3-4v

2. Go to `cd /var/named/slaves/external/`
3. Open the file with `vi <db.name>`
4. Commit changes: `service named restart`, in order to verify: `service named status`

Alternative route to DNS

- Log into nexus 5k MIVMX904 or MIVMX905
- Connect to DNS internal or External using `ssh zzbicchieri@10.256.166.21 vrf <vrfName>`
- Gain admin privileges `sudo su - `
- Look for needed info: `grep <regex> /var/named/slaves/internal/*`

7.1.3. DNS decommission on telcoItaly.it

1. To decommission a domain inside telcoItaly.it the client must make the request in V-DNA Home

8. MTA Sendmail (Now Proofpoint)

Table 12. DNS devices

DNS	IP	Description
mta_vs	10.256.166.19	vIP external
osx101v	10.256.166.21	MTA external
osx102v	10.256.166.22	
mta-int_vs	10.256.166.20	vIP internal
osx103v	10.256.169.21	MTA internal
osx104v	10.256.169.22	

MTA = Mail Transfer Agent, it runs on port 25 and yes, same devices as DNS

> RHEL 6 configuration of Sendmail Official Proofpoint website

8.1. Add new Recipient

1. Login to the two servers, osx101v and osx102v
2. `cd /etc/mail`
3. Add the new recipient: `echo "@net.telcoItaly.it MailtelcoItaly:[10.256.166.20]" >> /etc/mail/smarttable`
4. Rebuild the hash database file `makemap hash /etc/mail/smarttable.db < /etc/mail/smarttable`
5. Restart the Sendmail service for the changes to take effect: `service sendmail restart`

8.2. Edit Mail Files

- Files can be `/etc/mail/`:
  - access
  - smarttable
- Make a backup of the current `/etc/mail/<file>` as showed `cp /etc/mail/<file> /etc/mail/<file>.bak`
- Edit the `/etc/mail/<file>`
  - VIM
  - If you need to append a line to the file you can `echo "@net.telcoItaly.it MailtelcoItaly:[10.256.166.20]" >> /etc/mail/smarttable`
- Rebuild the hash database file: `makemap hash /etc/mail/<file> < /etc/mail/<file>`
- Restart the Sendmail service for the changes to take effect: `service sendmail restart`

8.3. Migrate MTA destination (Untested)

1. Install the necessary TLS libraries: `$ sudo yum install openssl openssl-devel`
2. Edit the MTA configuration file to enable TLS 1.2:
    - If you are using Postfix, you can edit the `/etc/postfix/main.cf` configuration file and add the following lines:

```
smtpd_tls_security_level = may
smtpd_tls_protocols = !SSLv2,!SSLv3,!TLSv1,!TLSv1.1, TLSv1.2
smtpd_tls_mandatory_protocols = TLSv1.2
smtp_tls_protocols = !SSLv2,!SSLv3,!TLSv1,!TLSv1.1, TLSv1.2
smtp_tls_mandatory_protocols = TLSv1.2
```

- These lines set the minimum allowed TLS protocol version to 1.2 for both incoming and outgoing connections.
    1. Restart the MTA service: `$ sudo systemctl restart postfix`
    2. Test the TLS configuration:
- TLS scanning tool like SSL Labs or Qualys SSL Labs can be used to test the TLS configuration of your MTA and check if it has valid certificates. You can also use a network sniffer like `tcpdump` to capture and analyze the network traffic between the server and the clients to verify that the traffic is encrypted with TLS.
- A TLS certificate is needed in order to use TLS encryption with your MTA. The certificate will be used to authenticate the server to clients and establish a secure connection.

8.4. Verify The log MTA

1. Connect to the machines: `osx101v.private.it` `10.256.166.21` and `osx102v.private.it` `10.256.166.22`

These machines can be reached from Ansible itmi3pans001 `10.971.59.24`

2. Log in as root and check the logs in `/var/log/mailog-`
3. Look for needed info: `zgrep <regex> /var/log/*`
    - If needed to unzip gz files run: `gunzip maillog.1.gz`
4. The activity of each individual mail delivery is identified by a code:

```
Mar  9 09:22:19 osx101v sendmail[100119]: STARTTLS=client,
relay=smtp.telcoItaly.arubamail.it., version=TLSv1/SSLv3, verify=FAIL, cipher=DHE-RSA-
AES256-SHA, bits=256/256

Mar  9 09:22:19 osx101v sendmail[100119]: 2568MECF100117: to=<vo-
monitorcb@vola.it>,<redcarpet.1821@mail.telcoItaly.it>, delay=00:00:00,
xdelay=00:00:00, mailer=telcoItaly, pri=171351, relay=smtp.telcoItaly.arubamail.it.
```

```
[62.149.178.100], dsn=5.0.0, stat=Service unavailable

Mar  9 09:22:19 osx101v sendmail[100119]: 2568MECF100117: 2568MJCF100119: DSN: Service
unavailable
```

or

```
Mar  9 09:37:32 osx101v sendmail[101076]: 2568bRqr101076: ruleset=check_rcpt,
arg1=<test_qualysscan@smtpcheckqualys.smtp>, relay=sn001.s01.sea01.qualys.com
[64.39.106.101] (may beforged), reject=550 5.7.1
<test_qualysscan@smtpcheckqualys.smtp>... Relaying denied. IP name possibly forged
[64.39.106.101]

Mar  9 09:37:32 osx101v sendmail[101076]: 2568bRqr101076:
from=<qualysscan_test@smtpcheckqualys.smtp>, size=0, class=0, nrcpts=0, proto=SMTP,
daemon=MTA1-private, relay=sn001.s01.sea01.qualys.com [64.39.106.101] (may be forged)

Mar  9 09:37:32 osx101v sendmail[101076]: 2568bRqs101076: ruleset=check_rcpt,
arg1=<qgmrtest%qualysguard.com@[91.80.46.120]>, relay=sn001.s01.sea01.qualys.com
[64.39.106.101] (maybe forged), reject=550 5.7.1
<qgmrtest%qualysguard.com@[91.80.46.120]>... Relaying denied. IP name possibly forged
[64.39.106.101]

Mar  9 09:37:32 osx101v sendmail[101076]: 2568bRqs101076: lost input channel from
sn001.s01.sea01.qualys.com [64.39.106.101] (may be forged) to MTA1-private after rcpt

Mar  9 09:37:32 osx101v sendmail[101076]: 2568bRqs101076:
from=<qgmrfrom@[91.80.46.120]>, size=0, class=0, nrcpts=0, proto=SMTP, daemon=MTA1-
private, relay=sn001.s01.sea01.qualys.com [64.39.106.101] (may be forged)
```

9. Squid Proxy

Table 13. Proxy devices

DNS	IP	Role	Version
osx100v	10.256.166.100	Proxy Active	4.15
osx222v	10.256.166.102	Proxy Standby	
Proxy VIP	10.256.166.101:8080	Balanced on F5	

9.1. Proxy Squid Configuration

- Connect to Ansible through EAG
- Check on ASA Firewall inside DMZ context
- If there are ACLs towards the service port add: `access-list GLOBAL_ACL extended permit tcp host 10.256.166.102 any4 eq 8226`
- From itmi3pans001 log into 10.256.166.100 aka osx100v
- With root access create file in `/etc/squid/`
- Insert domains in the file: `allowed-ACL_NAME.squid`
- Edit the file:

Do not take `vi` or `vim` lightly! Take sometime to read how to use it. Read me!

```
[root@osx100v squid]# vi allowed-win_act.squid
# YYYYMMDD
# If edited after creation keep track of it with: YYYYMMDD_v0.1
.microsoft.com
.windowsupdate.com
.windows.com
```

- Edit `/etc/squid/squid.conf` file and add the following:
  - For one or more IPs search the needed rule and add it `x.x.x.x/32`
  - In the case of adding a rule follow the example below to configure it

```
############################################################
# Win Activation YYYYMMDD
acl Win_Act src 10.429.124.15/32 10.429.124.16/32
acl Win_Sites dstdomain "/etc/squid/allowed-win_act.squid"
http_access allow Win_Act Win_Sites
############################################################
```

- Check at the beginning of the file if the destination port it's inside the ACL

- Example: acl SSL_ports port 8226
- You can find the line with: `grep {portNumber} {fileName}`

- Restart the service: `service squid restart`

Mirror the configurations on `osx222v 10.256.166.102`

Test it

```
[root@osx222v squid]# tail -fn 100 /var/log/squid/access.log | grep api.think4u.cloud
07/Jun/2021:16:49:35 +0200     23 10.256.166.112 TCP_MISS/503 0 CONNECT
api.think4u.cloud:8226 DIRECT/151.8.211.971
07/Jun/2021:16:50:20 +0200      0 10.256.166.112 TCP_MISS/503 0 CONNECT
api.think4u.cloud:8226 DIRECT/151.8.211.971

[root@osx222v squid]# grep api.think4u.cloud /var/log/squid/access.log
```

In case the implementation doesn't work check if the source IP's added to the proxy are configured inside ASA

9.1.1. Useful Squid Commands

To restart and control the status of the proxy `systemctl restart squid && systemctl status squid`

9.1.2. How to read needed files

- Unzip all the folder: `unzip -d . squid_osx100v_20221028.zip`
- Open it: `less etc/squid/squid.conf`
- Look at files inside zip: `unzip -l squid_osx100v_20221028.zip`
- Unzip only squid.conf: `unzip -j squid_osx100v_20221028.zip etc/squid/squid.conf -d .`
- Open it: `less etc/squid/squid.con`

10. Certificates Renewal

Please notice this important step before asking to renew a certificate

- The FQDN should be resolved from a DNS, public and/or private. You can use this public tool to verify if the service is resolved in Public DNS: Domain and IP bulk lookup tool
- You can use “nslookup” from telcoItaly internal network to verify if it is resolved in Internal DNS.
- The certificate can be renewed if the service is resolved at least in one of the 2 DNS (public or internal).
- Check inventory if date is set to 01/01/1970 that means dismissed

In case it results dismissed please update the inventory.

10.1. Update notification mail of certificates about to expire (FastDelivery - Certificates - Expiring Date)

- Log into gminnms116, inventory’s device as root
- edit file `/home/oracle/scripts/certificates/check_certificate.sh` at line 63

Any changes to be made to that mail can be done from that script

10.2. Folder on pans

1. Connecto to EAG
2. SSH to `10.971.59.24 itmi3pans001` with preferred application
3. Gain root privileges. (`su`)
4. `/home/ansysad/certsFD`
5. `ls -lrth`
6. The last file, right above the terminal is the needed certificate
7. `sudo cp <cert> /home/zzYOURUSER` or `sudo zip /home/zzYOURUSER/certs.zip *keyWord` make a zip with all the needed certificates
8. SFTP the cert out of the home directory in itmi3pans001. I strongly suggest to use MobaXterm with the shared configuration

10.3. Extract pem and key from pfx

- Get the pem file: `openssl pkcs12 -in vola_account_prod.pfx -out vola_account_prod.pem -nodes`
- Extract the key: `openssl rsa -in vola_account_prod.pem -out vola_account_prod.key`

10.4. Create private key and CSR (common to all SHA2 type certificates)

1. Create CSR in PEM format and KEY.
   a. `cd` into configuration files' folder
   b. Edit `vi openssl-XXX.conf` depending on certificate type using CN or DSN if there's SAN.
      - `openssl-SHA2.conf`
      - `openssl-SHA2-SAN.conf`
      - `openssl-SHA1-PRV.conf`
2. SHA2 commands: `openssl req -new -newkey rsa:2048 -nodes -sha256 -out common_name.csr -keyout common_name.key -config <openssl-SHA2-??.conf>`
3. SHA1 commands: `openssl req -new -newkey rsa:2048 -nodes -sha1 -out abthq-pre.telcoItaly.it.csr -keyout common_name.key -config openssl-SHA1-PRV.conf`
4. Insert Common_Name when prompted, do not put password
5. Check if `.csr` and `.key` are inside the certificate's folder

10.5. Check CSR content

1. Run `sslshopper` or similar and check it with decipher
2. Copy file content `.csr` and check if the received fields are correct.
3. CA Private telcoItaly Signature
4. CA Private FastDel Signature

10.6. Archiving

1. Inside FD's shared folder `\\ovlfs01\07-Sicurezza\RINNOVO CERTIFICATI\ARCHIVIO\`
2. Create a new folder with the naming convention `<num.ticket>-<common name>` (eg `R17100-tdmauth.telcoItaly.it`)
3. Put inside `.csr` e `.key` files
4. Delete what has been created locally at first step.

10.7. CA Public telcoItaly Signature

1. Reach website
2. Click on "standard SSL" if the certificate has one DNS only → "Order now"
3. Click on "Multi-domain SSL" if there are more than one DNS → "Order now"
4. Compile like below (Answers are inside "certificate request" ticket):

[image]

[image]

[image]

[image]

10.7.1. Additional e-mails

theBoss@telcoItaly.com

"Specify the environment". Specify Prod if the certificate is production, Pre-prod if it is PreProduction
[image]

5. Click on submit and send email to theBoss@telcoItaly.com asking for approval.

10.8. CA Private telcoItaly Signature

Connect with domain user

[image]

1. If the device is PRO, leave "Web Server Certificate - Production" selected in the first field.
2. Copy what was created above into the second field.
3. In the SAN field specify DNS/SAN list.
    - If there is one CN only put it inside the field anyway.
4. In "Request/Service Description" specify a generic value: "web service"
5. Local Market/Country: "IT"
6. Operational/Delivery/Service Owner’s and Business Owner’s Email address specify: DL-certificates@internal.telcoItaly.com
7. Required Contacts: dl-another-whynot@telcoItaly.com; theBoss@telcoItaly.com; DL-theDL@telcoItaly.com
8. Keep track of request’s number putting it inside the previously created share
9. You’ll receive certificate by the e-mail.

As shown below:

[image]

10.9. CA Private FastDel Signature

Once generated the CSR, common procedure to all certificates, and checked the correctness, to sign the CSR on CA FastDel:

root privileges needed.

1. `cd /app/causer`.
2. Move `.key` e `.csr` into `/app/causer`: `cp *.csr *.key /app/causer/`
3. The command depends on the certificate:
   - Server type:
     - SERVER SHA2: `openssl ca -config openssl-FD.conf -in <file_richiesta.csr> -out certs/<cn_specified_in_the_request>.crt -policy policy_loose -extensions server_cert`
     - SERVER SHA1: `openssl ca -config openssl-FD.conf -md sha1 -in <file_richiesta.csr> -out certs/<cn_specified_in_the_request>.crt -policy policy_loose -extensions server_cert`
   - Client type:
     - CLIENT SHA2: `openssl ca -config openssl-FD.conf -in <file_richiesta.csr> -out certs/<cn_specified_in_the_request>.crt -policy policy_loose -extensions usr_cert`
     - CLIENT SHA1: `openssl ca -config openssl-FD.conf -md sha1 -in <file_richiesta.csr> -out certs/<cn_specified_in_the_request>.crt -policy policy_loose -extensions usr_cert`
   - LDAP type:
     - LDAP SERVER SHA2: `openssl ca -config openssl-FD.conf -in <file_richiesta.csr> -out certs/<cn_specified_in_the_request>.crt -policy policy_loose_LDAP -extensions server_cert`
     - LDAP SERVER SHA1: `openssl ca -config openssl-FD.conf -md sha1 -in <file_richiesta.csr> -out certs/<cn_specified_in_the_request>.crt -policy policy_loose_LDAP -extensions server_cert`
     - LDAP CLIENT SHA2: `openssl ca -config openssl-FD.conf -in <file_richiesta.csr> -out certs/<cn_specified_in_the_request>.crt -policy policy_loose_LDAP -extensions usr_cert`
     - LDAP CLIENT SHA1: `openssl ca -config openssl-FD.conf -md sha1 -in <file_richiesta.csr> -out certs/<cn_specified_in_the_request>.crt -policy policy_loose_LDAP -extensions usr_cert`
4. Once executed CA Fast-Del's passphrase is prompted, after that answer `Y` to the following requests.
   a. The certificate will be archived into `/app/causer/certs`
   b. Copy it inside the path where we created `.key` and `.csr`
   c. Create `.pfx`

d. Archive everything in the share.

If there are problems with the certificate signature (crt) it's necessary to revoke the certificate before to try again: `cd /app/causer/ \ openssl ca -revoke <certificate_name>.crt -config openssl-FD.conf`

10.10. Signed certificate reception, comunication and archiving

The certificate has to be checked and has to be aligned with the request. If it isn't it has to be requested or signaled via e-mail

1. Create file `.pfx` (PKCS12): `openssl pkcs12 -export -in common_name.crt -inkey common_name.key -out common_name.pfx`

Sometimes the certificate has dots "." replaced by underscore "_". + Leave password field empty

10.10.1. In case the file PFX creation fails

1. Create a `.PEM` file in order to create the `.PFX`
2. It happens often that CA Private telcoItaly sends a new signed certificate in binary format (DER) instead of PEM.
3. To check if it's in binary look at the file with `less`

It it's shown in this way it has to be converted in PEM format

[image]

If there isn't any DER it will be:

```
-----BEGIN CERTIFICATE-----
MIIGUjCCBTqgAwIBwoTxI0xurZiqhkiG9w0BAQsFADBN
MQswCQYDVQMBGlnaUNlcnQgSW5jMQYDVQQDEx5E
aWdpQ2VydCBTSEEyIFwHsAxMjE1MDAwMDAwWhcN
MwCQYDVQQGEwJHQjEQMA4dsBxMHTmV3YnVyeTEo
-----END CERTIFICATE-----
```

4. Convert the file to binary: `openssl x509 -inform der -in <certificate-name-DER> -out common_name.pem`
5. Generate pfx file with `.PEM` file: `openssl pkcs12 -export -in <common_name.pem> -inkey common_name.key -out common_name.pfx`
6. Open SFTP client in order to upload the valid certificate and the `.pfx` inside FastDelivery share
7. Compress the following files with pass password (`.7z` or `.zip`):
   - Key
   - CSR
   - CRT (certificate)
   - CA certificate (If it's DigiCert0 two are needed, root and middle)
   - PFX
   - Eventual PEM
8. zip: `zip -p <password> <my_file>.zip <whatIwanToZip>`
9. 7z: `7z a -r <my_file>.7z <whatIwanTo7zip> -p<"password">`

Example:

[image]

Table 14. Attach the 3 CA based on which CA they come from:

Public CA telcoItaly - DigiCert	**Private CA telcoItaly**	**CA FastDel**
DigiCertCA.crt [image]	*telcoItaly_Internal_Root_CA.crt* [image] *telcoItaly_Internal_CA.crt* [image]	*CA-FastDel.crt* [image]

9. Send an e-mail to whom requested the certificate to inform it's ready. Specify expire date and wait installation instructions.

Do not send PRO's certificates unless directly expressed by the Project Manager

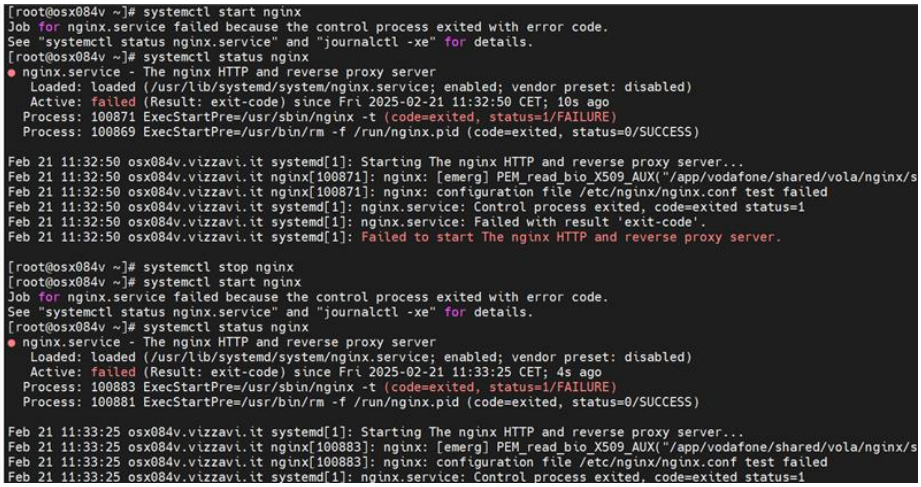
10. Update expiring dates on the 2 excel files

10.11. Certificate install on systems

After receiving confirm to install the certificates on the systems, we can have three different installation typologies

10.11.1. In case CRT file is not working on NGINX (VOLA)

1. When the error after the `systemctl restart nginx` shows this:



2. You need to autogenerate a new crt file `openssl x509 -inform DER -in certificate.crt -text -noout`
3. To check the file use the following command `openssl x509 -in certificate.crt -text -noout`
4. Change the name of the crt file using `mv certificate.crt so-vim-ws-internal.telcoItaly.it.crt` and then restart the service `systemctl restart nginx`
5. Chech the application using this URL

To check the status using `systemctl status nginx`. Remember to inform the client

10.11.2. F5 BIG-IP

1. Connecto to F5 with `Common` partition
2. Reach "System → File Management → SSL Certificate List" path
[image]
3. Look for expiring certificate like in the screenshot below (**certificate_name**) check if it's actually close to the expiring date, than Click on import
[image]
4. Put the key and an id name for the new certificate (ex: vastv.cc.telcoItaly.it_03_12_20)
[image]
5. At the end click Import:
6. Click again on the newly created certificate
7. Upload `.crt` file, the new expire date should be shown
8. Click "Local Traffic → Profiles → SSL Client"
9. Look for the certificate that needs update

Watch out for the partition, it's different for every certificate

[image]

9. Change the highlighted fields in the screenshot with the new certificate. Delete the old one. Click on Update lower left: [image]
10. Once finished, remember to sync the F5
    [image]

Certification update (private key+certificate+chain) has to be done simultaneously on F5 and Imperva, when the certificate is Public CA.

?? For some certificates we will need to add a double bundle in f5, the procedure is below

10.11.3. Linux Server

1. Load the certificate on the server.
2. Find previous certificates path `find / -name <certName>*` or `find / -name .crt`
3. Make `<today_date>_rch` folder and put the old certificates
4. Move the new certificates
5. If it's docker
   - The file owner must be `jsyssrv` run: `chown jsyssrv:jsyssrv fdcgw.telcoItaly.it.key`
   - Restart the container `[jsyssrv@mi5fdsx006 ~]$ docker service update --force fdcgw_kong`
   - The command **must** be launched on one machine only, docker will restart the other one.
     - > 20230518 I don't know which one. I tested it today from 6 and 4 and they restarted itself only
6. Otherwise
   - owners must be `root:root` run: `chown root:root <filename>`
   - Restart `nginx` service with: `/etc/init.d/nginx restart` or look in history for the right command: `grep restart ~/.bash_history`

10.11.4. Windows Server

1. Connect to the host, or the bridge machine to connect to the host, through Remote Desktop Connection from EAG.
2. Right click the IP left column
3. Select "Properties" → "Local Resources" → "Redirect options"
4. Flag "Drives"
5. Click OK
6. Connect to the host, Right click the IP from the left column
7. Click on "Reconnect server"
8. Load the certificate on the server
9. Run IIS "Internet Information Service"
10. Select hostname from left window "Server Certificates"
11. Import `.pfx` certificate
12. Locally save with "Export" button
13. Move the old certificate into the folder `C:\Certificati\certificate_old`
14. Click on "Sites" from the left list
15. Select the site correspoding to the certificate
16. Inside actions, on the right click "Edit Site" → "Binding" → "Edit"
17. Inside "SSL Certificate" click the new certificate
18. Click OK
19. Click top left "Host"
20. Click top right "Manager Server"
21. Click "restart".

> for the new machines CA root and Intermediate CA may be needed

10.11.5. MMC install

1. Open console
2. From windows serach
3. "mmc"
4. [image]
5. [image]
6. [image]
7. Import certificates
   [image]

8. Restart IIS
   [image]

10.11.6. Custom step for report.apptitc.telcoItaly.it certificate on OSQ282v

This procedure is needed only in OSQ282v yearly certificate renewal process.

1. Install the new certificate on BIG-IP and WAF
2. Connect to `osq282v` through Remote Desktop Connection from EAG.
3. Click the `.pfx` file, select "Local Machine", next a few times
4. Select "Automatically select the certificate store based on the type of certificate

   Certificate is located in Certificates (Local Computer) Personal > Certificates

5. Open the Report Server Configuration Manager
6. Choose "Microsoft Report BI Report Server"
7. Click connect
8. Click "Web Service URL" from left menu
9. Select the dropdown menu "HTTPS Certificate" than select the report.apptitc.telcoItaly.it
10. Now Apply is clicable. Click Apply

Sample result

[image]

Verify at URL

Expected output

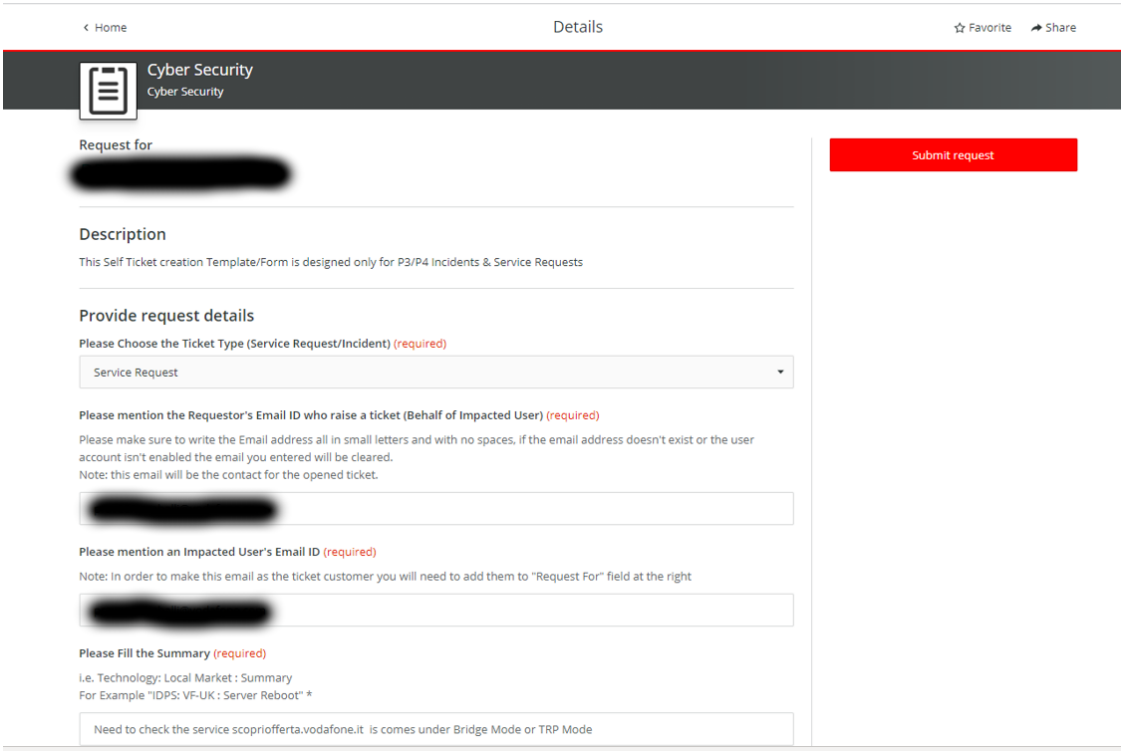
[image]

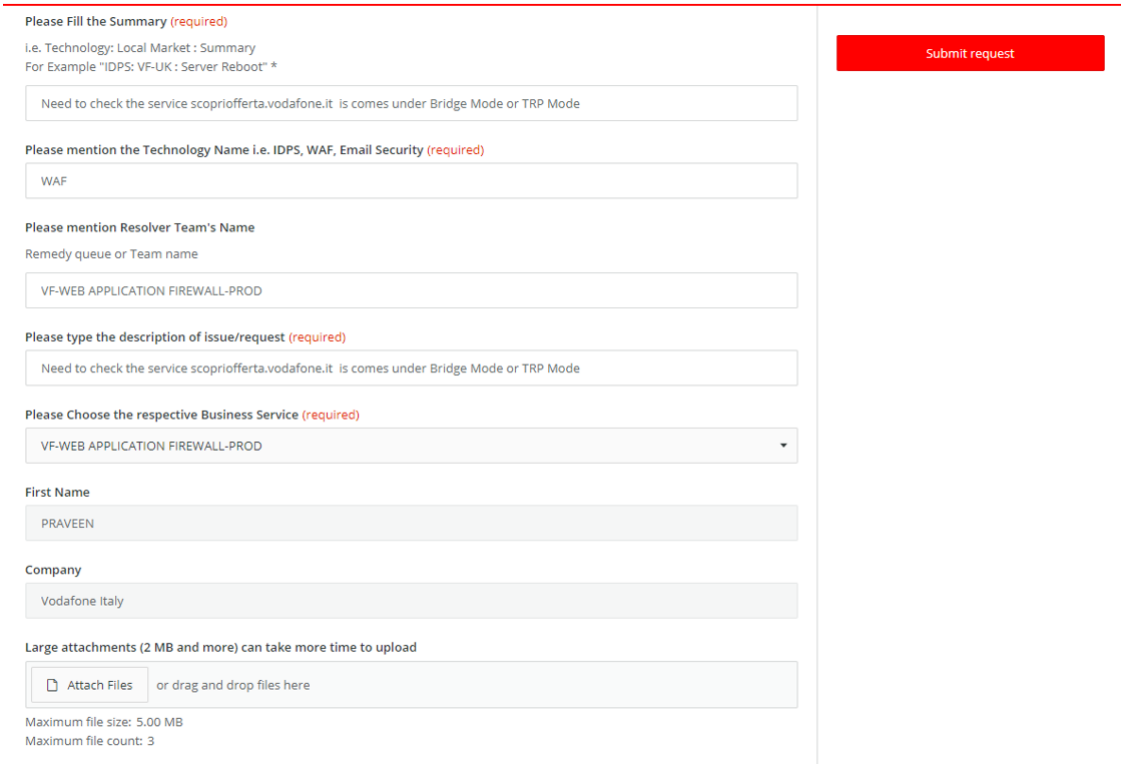
10.12. Service Request with WAF Team

This procedure is necessary when updating a certificate together with the WAF team

```
> To check whether the service comes under Bridge or TRP Mode
```

- Click on the link and it will autologin using telcoItaly credentials
- From the Menu `Browse Categories` → `Technology_VOIS` → `Cyber Security` and follow the steps as per screenshots:






```
> To update the certificate in WAF
```

- Follow the same procedure as mentioned above screenshot but change the description in tab

[image]

11. VMWare

Table 15. VMWare from EAG

Description	IP
vRealize Log Insight	https://10.429.719.31/
Network Insight	https://10.429.719.55/
NSX vSphere	https://10.429.719.9/

11.1. Create the IPSET in vSPhere

Ip Sets work like the object-groups created in the ASA FW

This is configured for services that are available on the internet such as MINISITI - VOLA - AWS

- From the Menu `Network and Security` → `Groups and tags` → `IP Sets`
- Create a new `IP Set`. Using the name given or previously chosen. Example: AWSvola
- Add the IPs needed in the set and press `save`

11.2. Add the IPSET in the rules to have data flux

- Go inside `Network and Security` → `Firewall` → Search the machine or Rule (in this case osx263v)
- If there is none under that name with the needed IPs then Create one in `Add Rule`
- Be aware of creating the Rule in the corresponding Section
- Give the new Rule a name
- Select the `Object Type` → in this case the `Virtual Machine` → osx263v as source
- Add the destination machine in this case AWSvola, after this specify the Service in case there is no Service set as the one you need → add a new one, specifying:
  1. Name (XXXX)
  2. Layer (in this case Layer3)
  3. Protocol (TCP or UDP)
  4. Port number (443)
- Press Publish

12. Zabbix

Table 16. Zabbix devices

DNS	IP	Description
MI5FDSX011	10.429.719.93	Zabbix DB server 1
MI5FDSX012	10.429.719.94	Zabbix DB server 2
MI5FDSX013	10.429.719.95	Zabbix DB Backup
MI5FDSX014	10.429.719.97	Zabbix Engine / FrontEnd 1
MI5FDSX015	10.429.719.98	Zabbix Engine / FrontEnd 2

12.1. To dismiss Certificates in Zabbix

- When you receive a request from telcoItaly, for info in one or more Certificates
- Go inside the inventory: `Registries` → `Certificates` → type the name an search for it → you get the info needed
- Go to F5 (PRO or PRE) → `Local Traffic` → `Network Map` inside search for the correspondent service:
- With the name of the certificate do an nslookup to have the IP determine if it is private or public. Example: `nslookup vas.cc.telcoItaly.it`
- If it is public from the firewall run `show nat | i <publicIP>`
- With the IP go to F5 and search for it in the Virtual Server List or in Network Map type
- If you have to dismiss one or more Certificates: `Registries` → `Certificates` → type the name an search for it
- Once that done change the Expire Date, X date in a thousand years and the SAN, servizio dismesso

12.2. Proactive Monitoring FastDelivery Network

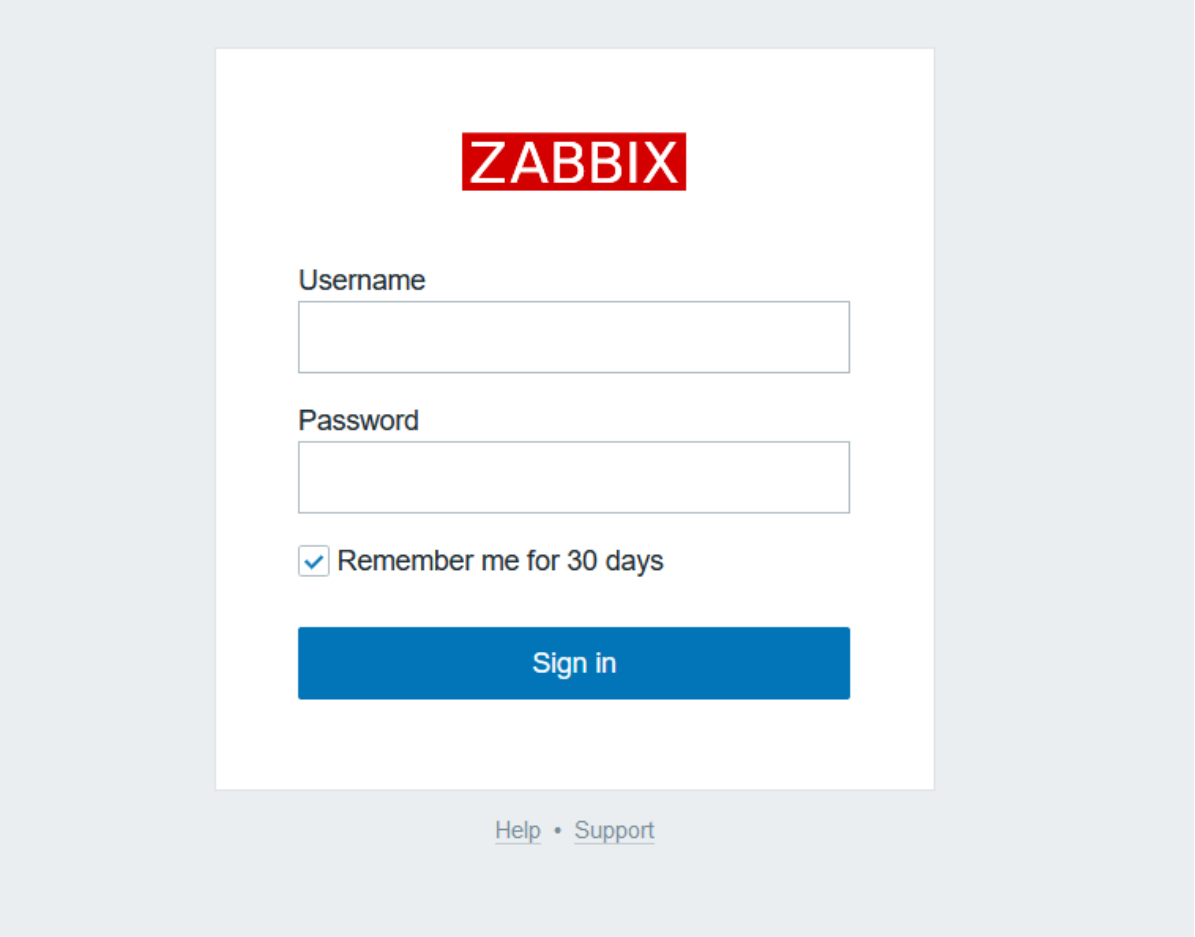


Figure 11. Open Zabbix

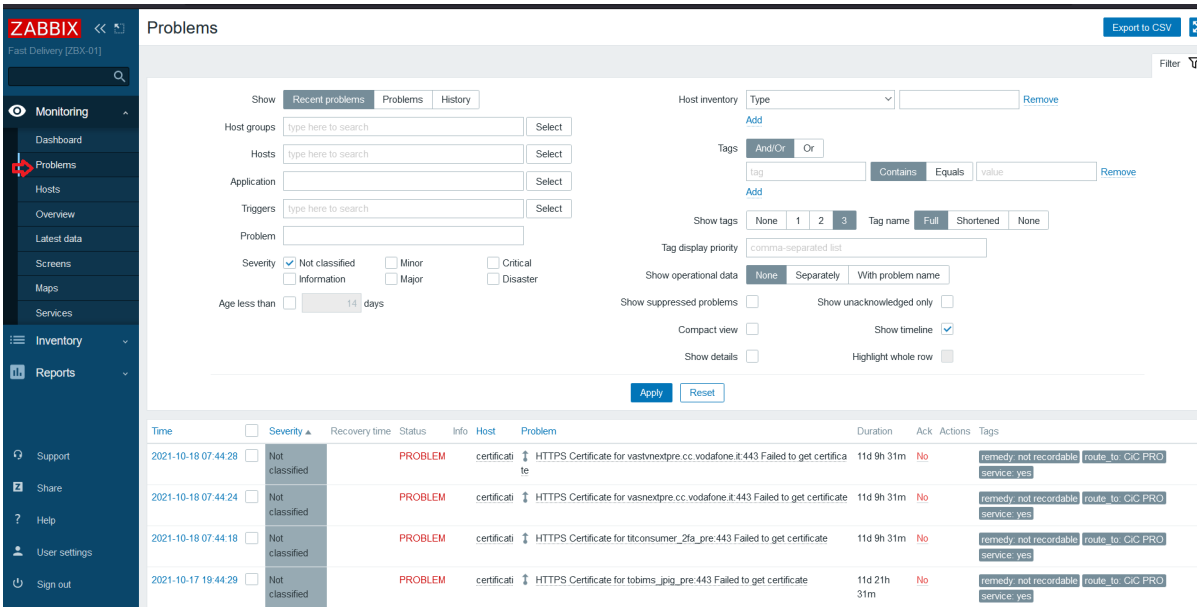


Figure 12. Go to Tab Problems, where will be showed All Devices, in Fast Delivery:

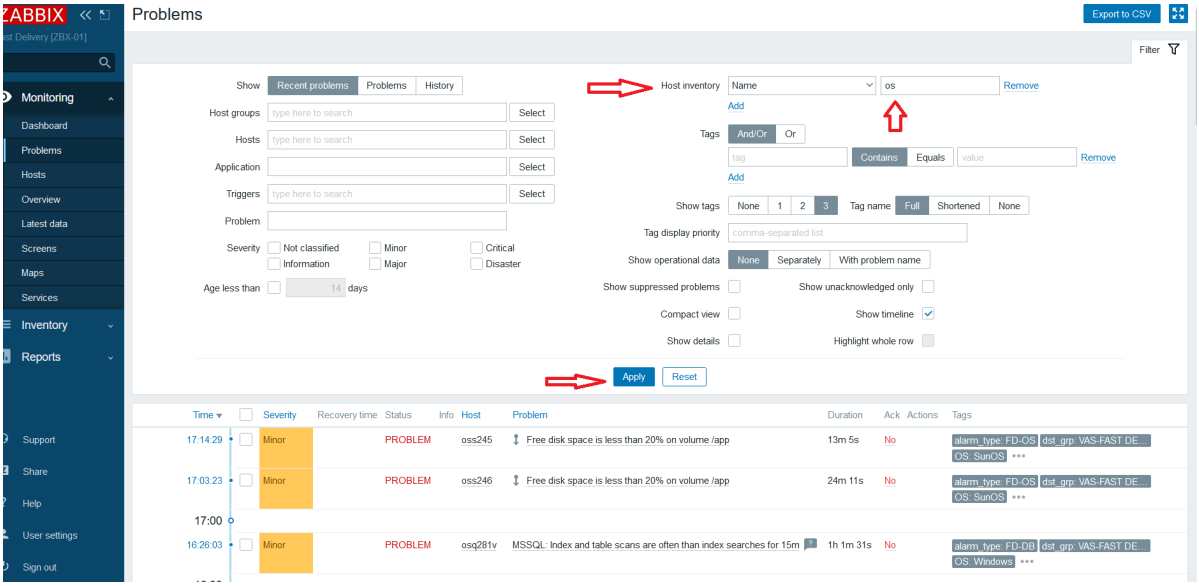


Figure 13. Then apply the filter in the Tab on the right:

Now you can see alarms for all the server in charge in VF FastDelivery.

- Refer to only these alarms:
  - Free disk space.
  - High Memory Utilization.
  - Disk space is very low
  - Any information related to server: Big-IP Production MIVLB515.private.it MIVLB514.private.it
- After performing any checks on Big-IP o other Network device, please use this template to advise our colleagues from Application side.

13. Decommissioning

13.1. Flag them as decommissioned on inventory

1. inventory
2. click "Edit"
3. Top right at the window there's a pen and a recycle bin. Click the Pen
4. 2nd column, 6th option "Virtual Device Status", select Dismissed
5. Bottom right of this small window press "Save"

13.2. Fetch the info

1. Identify project and devices from inventory
2. Log into F5 PRE/PRO into Local Traffic → Network Map
3. Type the device names and fetch:
    - DNS namings
    - Virtual IP address
    - Virtual Servers names
4. Log into Firewall:
    - `change context DMZ`
        - `show nat | include <Virtual IP address>`
        - Fetch the public IP and remove it
        - `show access-list | i <10.256.x.x>`
        - Identify and remove all of them
        - If they can't be removed check by ACL's line and get the object-group: `show access-list | i line <number>` (You can use the IP block section to remove a single IP from the object-group)
    - `change context FRONTEND`
        - `show access-list | i <10.256.x.x>`
        - Identify and remove all of them
        - If they can't be removed check by ACL's line and get the object-group: `show access-list | i line <number>` (You can use the IP block section to remove a single IP from the object-group)
    - `change context BACKEND`
        - `show access-list | i <10.256.x.x>`
        - Identify and remove all of them
        - If they can't be removed check by ACL's line and get the object-group: `show access-list |`

`i line <number>` (You can use the IP block section to remove a single IP from the object-group)

13.3. Execute the changes

1. On BIG-IP F5:
   - Set Virtual Server status as offline, black icon.
   - Set Nodes status as offline, black icon.

Everything on the device must be black in order for Zabbix to stop monitoring it

2. On excel: Striketrough the IPs and devices names in the IP table
   - Track the new freely available Public IPs, 91.80.46.x in the Tab and comment what they were used for, if there were any
3. Log on vCenter MIVSX920 10.429.719.9, from chrome EAG
4. Find the devices and shut them down. Keep them offline one week and than delete them
5. Send an e-mail to roberta.geranio@telcoItaly.com, elizabeth.spezzano2@consultant.telcoItalyomnitel.it, davide.desalve@telcoItaly.com, stefania.sallusti@telcoItaly.com, with roberto.di-martino@consultant.telcoItalyomnitel.it, fabianamaria.basso@telcoItaly.com and gabriele.saronni@telcoItaly.com in Cc asking to remove them from backup and patching schedule
6. If we don't own the DNS, please point them to the telcoItaly.it DNS team

13.4. Monitoring

1. send an e-mail to davide.dasaro@telcoItaly.com, dl-another-whynot@telcoItaly.com with roberto.di-martino@consultant.telcoItalyomnitel.it, fabianamaria.basso@telcoItaly.com and gabriele.saronni@telcoItaly.com in Cc asking to remove them from monitoring

14. Anexes

14.1. Procedure Examples

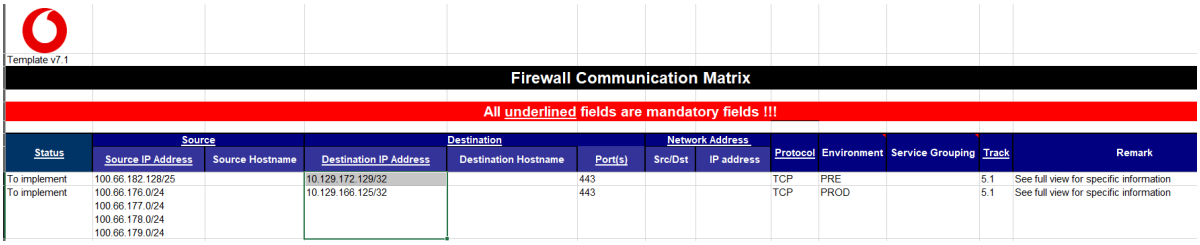
14.1.1. CM for ACL

Mail in inbox: → Re: 503024 Implementation of AWSLayer to IPLAN (Ironcloud Italy)

```
Ciao  Monica
In allegato una communication matrix che mi hanno spedito per il Progetto Ironcloud da
implementare su IT_CSP_TRANSIT (RT 34419:13119 both IM & EX),

Ho aperto a IP Design il per il 503025 controllo del routing.
Non necessita di NAT
```

If NAT is needed go to the ASA section regarding the actions



Template v7.1

Firewall Communication Matrix

All underlined fields are mandatory fields !!!

Status	Source		Destination			Network Address		Protocol	Environment	Service Grouping	Track	Remark
	Source IP Address	Source Hostname	Destination IP Address	Destination Hostname	Port(s)	Src/Dst	IP address					
To implement	100.66.182.128/25		10.129.172.129/32		443			TCP	PRE		5.1	See full view for specific information
To implement	100.66.176.0/24 100.66.177.0/24 100.66.178.0/24 100.66.179.0/24		10.129.166.125/32		443			TCP	PROD		5.1	See full view for specific information

Figure 14. CM example

Once checked where the VRF arrives inside the Network Scheme, go to check the first routers `ASR 9K` *and the* `Nexus 5K`

```
RP/0/RSP0/CPU0:MIVMX900#sh rpl prefix-set | i IT_CSP_TRANSIT
Wed Oct  5 15:04:46.511 CEST
prefix-set pfx_IT_CSP_TRANSIT_toPE
prefix-set pfx_IT_CSP_TRANSIT_fromPE

Cisco Nexus 5000
MIVMX904# sh ip prefix-list ?
  <CR>
  >                   Redirect it to a file
  >>                  Redirect it to a file in append mode
  WORD                Name of prefix-list (Max Size 63)
  static-DSL_DATA     Known prefix-list name
  static-EITO_PROD    Known prefix-list name
  static-ITDCC        Known prefix-list name
  static-IT_CSP_TRANSIT  Known prefix-list name
  static-MGMT         Known prefix-list name
  static-SERVICE_CTP  Known prefix-list name
  static-TRUSTED_S2S  Known prefix-list name
  static-UNTRUSTED_U2S   Known prefix-list name
```

```
  |                     Pipe command output to filter

MIVMX904#sh ip prefix-list static-IT_CSP_TRANSIT
ip prefix-list static-IT_CSP_TRANSIT: 2 entries
   seq 5 permit 10.256.160.0/20
   seq 10 permit 10.429.429.0/22
```

- As seen before, the prefix are configured. Follow the procedure for each of them in the corresponding section in the ASR 9000 and Nexus 5000
- Go to the MIVFX900-1 (firewall) and add in each context the new route → this might depend on the route you are pointing. This hop goes from IT_CSP_TRANSIT up to DMZ

In case you need to add routes inside ASA contexts

```
MIVFX900-1/MGMT/pri/act# ch co B
MIVFX900-1/BACKEND/pri/act# sh route | i 100.66.182.429
S        100.66.182.429 255.255.255.429 [1/0] via 192.168.28.1, IT_CSP_TRANSIT
```

The service comes from 192.168.28.1 (IT_CSP_TRANSIT). That route is added to the context

```
MIVFX900-1/BACKEND/pri/act# conf t
MIVFX900-1/BACKEND/pri/act(config)# route IT_CSP_TRANSIT NEEDED IP + SUBNET MASK +
ROUTE
MIVFX900-1/BACKEND/pri/act(config)# wr
```

The same procedure is added in each context, addig the corresponding route in the prior command

```
MIVFX900-1/BACKEND/pri/act# sh route
MIVFX900-1/BACKEND/pri/act# sh route | i FRONT
S-       0.0.0.0 0.0.0.0 [1/0] via 192.168.65.1, FRONT-BACK
MIVFX900-1/BACKEND/pri/act(config)# ch c F
MIVFX900-1/FRONTEND/pri/act(config)#
MIVFX900-1/FRONTEND/pri/act# sh run | i route
route DMZ-FRONT 0.0.0.0 0.0.0.0 192.168.64.1 1
route FRONT-BACK 10.0.0.0 255.0.0.0 192.168.65.3 1
MIVFX900-1/FRONTEND/pri/act# conf t
MIVFX900-1/FRONTEND/pri/act(config)# route FRONT-BACK 139.47.176.48 255.255.255.240
192.168.65.3
MIVFX900-1/DMZ/pri/act(config)# route DMZ-FRONT 139.47.176.48 255.255.255.240
192.168.64.
```

15. SysAdmin Info: System administrator notes and configurations

16. Commands

16.1. Linux Commands

Bash Manual Official Book

Manual	Syntax
find	find [-H] [-L] [-P] [-D debugopts] [-Olevel] [path…] [expression]
	`find / -name *.crt`
debugfs	debugfs [-Vwci] [-b blocksize] [-s superblock] [-f cmd_file] [-R request] [-d data_source_device] [device]
	`debugfs /dev/hda13`
df	df [OPTION]… [FILE]…
	`df -h`
mv	mv [OPTION]… SOURCE… DIRECTORY
cp	cp [OPTION]… [-T] SOURCE DEST
scp	scp [[user@]host1:]file1 … [[user@]host2:]file2
	`scp oss231:alpha.txt /home/ansysad`
ssh	ssh [user@]host1
	`ssh oss231v`
grep	grep [OPTIONS] PATTERN [FILE…]
userdel	userdel [options] [LOGIN]
unzip	unzip [-Z] [-cflptTuvz[abjnoqsCDKLMUVWX$/:^]] file[.zip] [file(s) …] [-x xfile(s) …] [-d exdir]
	`unzip file.zip`
passwd	passwd [-k] [-l] [-u [-f]] [-d] [-e] [-n mindays] [-x maxdays] [-w warndays] [-i inactivedays] [-S] [--stdin] [username]
	passwd [options] [LOGIN]
gunzip	gzip [-acdfhlLnNrtvV19] [-S suffix] [name …]

Get needed info on commands using `--help`, `-h` or `man` cmd

16.1.1. SunOS Commands

SunOS Manual

Diagnostic Commands

Command	Description	Impact
`zfs list`	Lists ZFS filesystems, volumes, and snapshots	Show only - displays filesystem information
`zfs list -o name,used,avail,refer,mountpoint,quota`	List ZFS datasets with specific properties	Show only - displays detailed filesystem information
`zfs list -t snapshot`	List all ZFS snapshots	Show only - displays snapshot information
`zfs list -o name,used -s used`	List ZFS datasets sorted by space usage	Show only - helps identify large space consumers
`zfs list -r -o name,used,refer,compressratio`	List ZFS datasets with compression details	Show only - shows space efficiency
`beadm list`	List boot environments	Show only - displays bootable system snapshots
`zpool list`	Display zpool statistics	Show only - shows pool size and utilization
`zpool status rpool`	Display detailed zpool status	Show only - shows health and configuration
`du -hs /*`	Display disk usage by top-level directories	Show only - helps identify large directories
`df -h`	Display filesystem space usage	Show only - shows mounted filesystem space

Modification Commands - Use With Caution

Command	Description	Impact
`zfs destroy dataset_name`	Remove a ZFS dataset	**Potentially destructive** - permanently deletes the specified dataset
`zfs destroy -r dataset_name`	Recursively remove a ZFS dataset	**Potentially destructive** - removes dataset and all descendants
`zfs set quota=size dataset_name`	Set a space limit on a dataset	Low risk - limits future growth but doesn't delete data
`zfs destroy snapshot_name`	Remove a snapshot	Low risk if snapshot isn't in use - frees snapshot space
`zoneadm -z zonename reboot`	Reboot a zone	**Causes downtime** - interrupts all services in the zone
`beadm create new_be`	Create a new boot environment	Low risk - creates a bootable system snapshot
`beadm activate be_name`	Set the default BE for next boot	**May affect next boot** - changes which system is loaded at startup
`beadm destroy be_name`	Delete a boot environment	**Potentially destructive** - removes a bootable system snapshot
`zpool upgrade pool_name`	Upgrade ZFS pool version	**May affect compatibility** - pool can't be imported on older systems after upgrade

Safe Space Recovery Commands for This System

Command	Description	Impact
`zfs set quota=300G rpool/zone/oss213v`	Set quota on oss213v zone	Safe - prevents zone from consuming more space
`zfs destroy -r rpool/zone/oss213v/oss213v/rpool/ROOT/zbe-0`	Remove unmounted ZBE	Safe if not mounted - removes old boot environment
`zfs destroy -r rpool/zone/oss213v/oss213v/rpool/ROOT/zbe-1`	Remove unmounted ZBE	Safe if not mounted - removes old boot environment
`zfs destroy -r rpool/zone/oss213v/oss213v/rpool/ROOT/zbe-2`	Remove unmounted ZBE	Safe if not mounted - removes old boot environment
`zfs destroy -r rpool/zone/oss213v/oss213v/rpool/ROOT/zbe-3`	Remove unmounted ZBE	Safe if not mounted - removes old boot environment
`zfs destroy -r rpool/zone/oss213v/oss213v/rpool/ROOT/zbe-4`	Remove unmounted ZBE	Safe if not mounted - removes old boot environment
`zfs destroy -r rpool/zone/oss213v/oss213v/rpool/ROOT/zbe-5`	Remove unmounted ZBE	Safe if not mounted - removes old boot environment
`zfs destroy -r rpool/zone/oss213v/oss213v/rpool/ROOT/zbe-6`	Remove unmounted ZBE	Safe if not mounted - removes old boot environment
`zfs destroy -r rpool/zone/oss213v/oss213v/rpool/ROOT/zbe-7`	Remove unmounted ZBE	Safe if not mounted - removes old boot environment
`zfs destroy -r rpool/zone/oss213v/oss213v/rpool/ROOT/zbe-8`	Remove unmounted ZBE	Safe if not mounted - removes old boot environment
`zfs destroy -r rpool/zone/oss213v/oss213v/rpool/ROOT/zbe-9`	Remove unmounted ZBE	Safe if not mounted - removes old boot environment

DANGER - High-Risk Commands

Command	Description	Impact
`zfs destroy rpool/zone/oss213v/oss213v/rpool/ROOT/zbe-10`	Remove the active ZBE	**EXTREMELY DESTRUCTIVE** - will crash the zone and cause data loss
`zfs destroy -r rpool/zone/oss213v`	Remove entire zone filesystem	**EXTREMELY DESTRUCTIVE** - deletes entire zone and all data

16.2. Windows Comands

Powershell Manual

Manual	Syntax
route	route [/f] [/p] [<command> [<destination>] [mask <netmask>] [<gateway>] [metric <metric>]] [if <interface>]]
	`route add 192.168.10.0 mask 255.255.255.0 192.168.1.1`
Net User	net user [<UserName> {<Password> \ *} [<Options>]] [/domain]
	`net user username password /add`
Get-ChildItem	Get-ChildItem [[-Path] <string[]>] [[-Filter] <string>] [-Include <string[]>] [-Exclude <string[]>] [-Recurse] [-Depth <uint>] [-Force] [-Name] [<CommonParameters>]
	`Get-ChildItem -Path "C:\YourFolderPath"`
Copy-Item	Copy-Item [-Path] <string[]> [-Destination] <string> [-Container] [-Force] [-Recurse] [-PassThru] [-Filter <string>] [-Include <string[]>] [-Exclude <string[]>] [-Credential <pscredential>] [-WhatIf] [-Confirm] [<CommonParameters>]
	`Copy-Item -Path "C:\Source\File.txt" -Destination "D:\Destination"`
Get-Process	Get-Process [[-Name] <string[]>] [-Id <int[]>] [-FileVersionInfo] [-Module] [-InputObject <Process[]>] [<CommonParameters>]
	`Get-Process winword, explorer | Format-List *`
Get-Service	Get-Service [[-Name] <string[]>] [-RequiredServices] [-DependentServices] [-ComputerName <string[]>] [-Exclude <string[]>] [-Include <string[]>] [<CommonParameters>]
	`Get-Service -Name "win*" -Exclude "WinRM"`
Start-Service	Start-Service [-Name] <string[]> [-DisplayName <string[]>] [-InputObject <System.ServiceProcess.ServiceController[]>] [-PassThru] [-Verbose] [-WhatIf] [-Confirm] [<CommonParameters>]
	`Start-Service -Name Quartz`
Stop-Service	Stop-Service [-Name] <string[]> [-DisplayName <string[]>] [-InputObject <System.ServiceProcess.ServiceController[]>] [-PassThru] [-Verbose] [-WhatIf] [-Confirm] [<CommonParameters>]
	`Stop-Service -Name Quartz`

You can look at all aliases with `alias` or with a specific command like:
Get needed info on commands using `Get-Help <cmd>`

```
alias ls

CommandType     Name                                               Version    Source
-----------     ----                                               -------    ------
Alias           ls -> Get-ChildItem
```

16.2.1. vCenter Snippets

```
Connect-VIServer -Server 10.113.124.11 -User root -Password YouWish -Force
New-VMHostAccount -Id "VCentConnect" -Password "GuessIT!" -Description
"SomeDescription"
New-VIPermission -Entity (Get-Folder ha-folder-root) -Principal "VCentConnect" -Role
Admin
Get-VIPermission

Get-VIAccount
Get-VIRole
Get-VIPermission

Role                      Principal       Propagate IsGroup
----                      ---------       --------- -------
Admin                     vpxuser         True      False
Admin                     dcui            True      False
Admin                     root            True      False

New-VMHostAccount -Id "VCentConnect" -Password "GuessIT!" -Description
"SomeDescription"
New-VIPermission -Entity (Get-Folder ha-folder-root) -Principal "VCentConnect" -Role
Admin
#Set-VIPermission -Entity (Get-Folder ha-folder-root) -Principal "VCentConnect" -Role
Admin

Disconnect-VIServer -Server 10.113.124.11 -Confirm:$false
```

17. Remote Shell Login

itmi3pans001

- Become ansysad: `sudo su - ansysad`
- `ssh <DNS or IPaddress>`

As of 20230523 all machines should be connected to Ansible

gminnms117

- `ssh -T -o StrictHostKeyChecking=no <IPaddress> 'cmd <neededCommand>'`
- `ssh -T -o StrictHostKeyChecking=no <IPaddress> 'powershell <neededCommand>'`
- `sftp <IPaddress>`

18. RDP login

> If you're lucky you can access it locally from telcoItaly laptop, from run dialog (win+r) and type `mstsc`

- Log into EAG and open Remote Desktop Connection Manager or MobaXterm
  - Create a new connection if necessary
- RDP to the device with needed domain credentials

Request for MobaXterm access to make the workflow faster

19. Allow a Device to be Reached by Remote Shell

Execute RDP login

1. Open Server Manager
2. Go to `Tools`
3. `Computer Management`
4. Go to `Local Users and Groups`
5. Search the user sys_kpi
6. Inside the `Properties` in members
7. `Add`
8. Select the location the server
9. Add the Administrators group
10. Check inside `ProgramData`

inside `C:` remember to flag show hidden folders

11. Inside the ssh folder right click `administrators_authorized_keys` and select `Properties`
12. Choose `Security` tab
13. `Advanced`
14. Click `Change option`
15. Select the machines as location
16. Add the group Administrators
17. Check the connection

If it doesn't work, check inside `Services`, if the ssh application is running you will have to request open the port

20. Gather Rilascio Files

20.1. RDP version

From file explorer powershell can be invoked with `shit + right click`

1. Log into EAG
2. Open Remote Desktop Connection Manager or MobaXterm
   a. Remote Desktop Connection
      i. If there's no connection: Create settings `File` > `New`
      ii. Create connection to `10.256.175.32` aka `osq001v`
      iii. Go to `Properties` > `Local Resources`
      iv. Unflag `Inherit from parent`
      v. Flag `Drives` (Make sure all drives are flagged)
3. Inside `Properties`
   a. `Remote Desktop Settings`: Lets you decide screensize
   b. `Logon Credentials`: add your credentials zz + vpnpassword

Inside the machine

- The "rilascio" files are inside `D:\FTPRoot\WAPPORTAL\ftptest`
- Your PC should be reachable from `Y:` or `V:` network shared drive. `:\Users\zz<youruser>\`
- From powershell run: `Copy-Item -Path D:\FTPRoot\WAPPORTAL\ftptest\<nameOfTheFolder> -Destination Y:\Users\zz<yourUser>\Downloads -Recurse`

Most of the times your personal files aren't reachable unless clicked from File Explorer

20.2. Terminal version

From gminnms117

- From pans log in `gminnms117`
- Log as `ansysad` then `sudo su - sys_kpi`
- With this user `sftp` into `10.256.175.32` aka osq001v usually
  - Example:
    - `sftp://ftptest@10.256.175.32/RILASCI_PRO_DONATION/DIST-Argo-2022-12-15-S17390-Argo_Update`
    - `sftp> get /D/FTPRoot/WAPPORTAL/ftptest/RILASCI_PRO_DONATION/DIST-Argo-2022-12-15-S17390-Argo_Update/*zip`
- Return `ansysad`

- move the retrieved file to ansysad home folder: `sudo mv /home/sys_kpi/*zip /home/ansysad`
- Go back to itmi3pans001
- Get the file to pans folder: `scp gminnms117:Filename.zip .`

21. User Management

21.1. Windows

Create

- Create user `ssh -T -o StrictHostKeyChecking=no X.X.X.X 'cmd /c net user /create <userName>'`
- net user <username> <password> /add

Delete

- Check if user exists `ssh -T -o StrictHostKeyChecking=no X.X.X.X 'cmd /c net user <userName>'`
- Delete user `ssh -T -o StrictHostKeyChecking=no X.X.X.X 'cmd /c net user /delete <userName>'`

Check RDP Users: `net localgroup "Remote Desktop Users"` Add RDP Users: `net localgroup "Remote Desktop Users" /add <username>`

21.2. Linux

21.2.1. Create and delete

Create as root

```
useradd -m -c "Added by Sysadmin" -g users $user
passwd $user
chage --mindays 1 $user
chage --warndays 5 $user
chage --maxdays 90 $user
```

Delete as root

- Check if user exists `grep -c userName /etc/passwd`
- Delete user `userdel userName`

21.2.2. Reset and unblock

As root

- Check if user exists: `grep -i userName /etc/passwd`
- Check user status: `passwd -s userName`
  - Is it blocked?: `passwd -u userName`
- Reset password: `passwd userName`
  - `-s`: This command displays information about the user account
  - `-u`: It re-enables the account if it has been previously locked due to excessive login failures or other reasons.

21.2.3. Expiracy Date

As root for Suse and Unix Systems

- To change the date to never expire: `chage -M -1 userName` or `chage -I -1 -m 0 -M 99999 -E -1 userName`
  - To check the status inside SunOS: `chage -l userName` or `grep -ni userName /etc/passwd`
  - To check the status inside Suse: `id userName`

As Root for SunOS

- To change the date to never expire: `passwd -x -1 userName`

To check the RSA key `cat /home/sys_kpi/.ssh/authorized_keys`

21.2.4. Application Users

As root for RHEL

```
chage -E -1 -m 0 -M 99999 -I -1 -W -1 userName
```

- `-E -1:` Sets the account expiration date to "never."
- `-m 0`: Sets the minimum number of days between password changes to 0.
- `-M 99999`: Sets the maximum number of days between password changes to a very large number, effectively making it never expire.
- `-I -1`: Sets the inactive (locked) period to "never."
- `-W -1`: Sets the warning period to "never."

As root for SunOS

```
passwd -x -1 -N userName
```

- `-x -1`: This part of the command sets the maximum number of days a password is valid to -1, effectively disabling password expiration.
- `-N`: This option is used to clear the password aging information for the specified user, which further ensures that there are no password expiration settings in place.

21.2.5. Restablish RSA keys for a user

Unblock the user as root

- Generate RSA Keys
  - Log in as the required user.
  - Check if the `.ssh` folder exists. If not, create it using `mkdir .ssh`.
  - Navigate into the `.ssh` folder.
  - Generate the RSA key pair by running: ` ssh-keygen -t rsa -b 4096 -C "username@yourDomain.com" `
  - When prompted, choose the default location to save the key pair by pressing Enter.

    - For the passphrase, leave it blank and press Enter.
- Add Public Key to Authorized Keys
    - After generating the key pair, two files are created: `id_rsa` (private key) and `id_rsa.pub` (public key).
    - Append the public key to the `authorized_keys` file using: `` ` cat id_rsa.pub >> authorized_keys ` ``
- Adjust Permissions
    - Ensure correct permissions for security: `` ` chmod 700 ~/.ssh chmod 600 authorized_keys ` ``

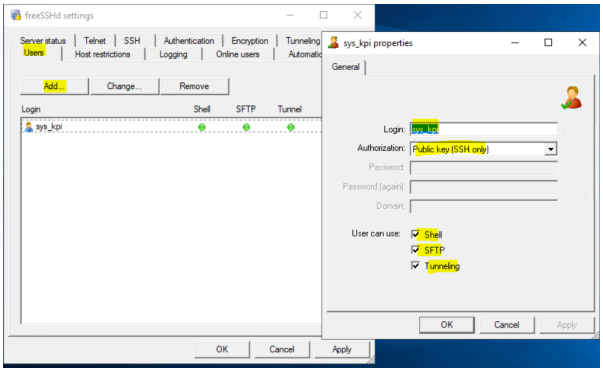
Please reply to the request and send the private key in a separate email to the requester.

22. Add sys_kpi to gminnms117

- If it does not exist, create `sys_kpi` user and add it to `Administrator and remote desktop users` group
- Install `freeSSHd.exe` package with Admin user.
- Create the txt file name it `sys_kpi` and copy & paste the following key inside it:

```
ssh-rsa
AAAAB3NzaC1yc2EAAAABIwAAAIEA1Ee4hKw6NxsGOegq1Oflu2me1SCPe/gl5Lpjx8v142dXhX1MNOjgRqSNij
JtfFK1fo2DcwF7EfaafZVPCgCa2ptDUzH7+BYYc6gkuCUV7F9CuHgSNOdxjVe44TSL7Gd3VDzL7IK6UCTEtwIr
PhQyGQ5DqUOHT0R/c63WNVxrKDs= sys_kpi@gminnms117
```

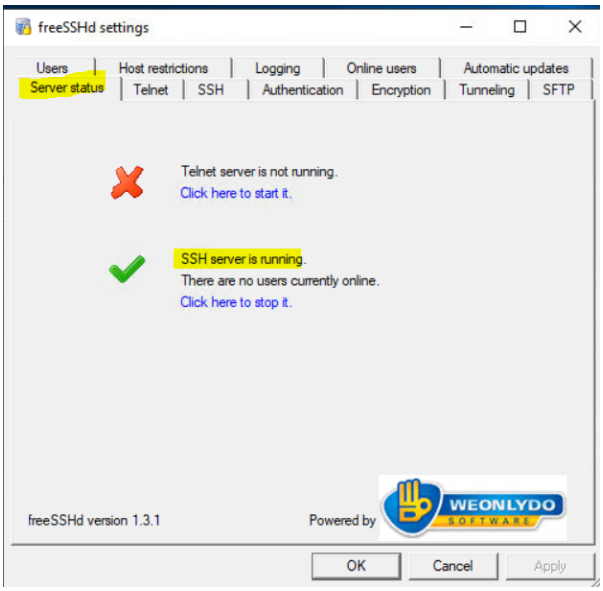
- Copy the text file to the following location: `C:\Program Files (x86)\freeSSHd`
- Run freesshd management console from desktop icon
    - Create `sys_kpi` user as shown in the figure:



- Click on `apply` and test the connection from gminnms117.
- Run `ssh -T -o StrictHostKeyChecking = no IPserverwindows 'cmd / c net user'`
- If the key exchange does not work, restart `freesshd` service

Workaround

- If the ssh command returns // without the machine name:
  - Stop the freesshd service and set it manually
  - Start the management console from the link on the desktop
  - Start ssh from the server status tab



23. Disk Space Activity

23.1. Windows GUI

1. Get WizTree portable
2. Copy the zip into the needed device
3. Attach screenshots to the mail

23.2. Commands Reference

Table 17. Unix means works on both RHEL and SunOS

OS	Command
RHEL	`du -h`
RHEL	`du -h -d1 / | sort -hr | head -n 10`
SunOS	`zfs list`
SunOS	`zpool list`
SunOS	`du -hs *``
SunOS	`du -hs * | grep G`
SunOS	`du -d 1 -k / | sort -rn | head -n 10`
SunOS	`du -d 1 -ks / | sort -rn | head -n 10`
SunOS	`du -h | sort -r | head -n 10`
SunOS	`du -d 1 -k / | awk '{size=$1/1000000; printf "%.2f MB\t%s\n", size, $2}' | sort -rn | head -n 10`
SunOS	`du -d 1 -ks / | awk '{size=$1/1000000; printf "%.2f MB\t%s\n", size, $2}' | sort -rn | head -n 10`
Unix	`find / -type d -size +10G`
Unix	`du -d1 --block-size=1G / | awk '$1 > 10'`
Unix	`du -h -d1 / | sort -hr | head -n 10`
Windows	`Get-ChildItem -Path C:\ -Directory -Recurse | Where-Object { $_.Length -gt 10GB }`
Windows	`Get-ChildItem -Recurse | sort -Descending length | select -First 7`
Windows	`Get-ChildItem -Path C:\ -Directory -Recurse | Where-Object { $_.Length -gt 10GB }`

In case of a huge file you can look for the specific line from which they are needed: + `grep -in '2022/01' filename` or similar combinations.
Usually around one year worth of logs, and use the following range: `sed -i '1,14091155d' filename` where 1 is the first line and 14091155 is the first match of the above `grep` command.

`Sed` will buffer the file. Be sure to have enough space before running it!

23.2.1. Crontab issues

First thing to do is to verify what's inside crontab:

1. Check first root's crontab: `crontab -l`
2. Since it's usually empty you can check the specific user on the system: `crontab -l applicationUser`
    - It can be erif, jboss, jsyssrv. The latter is the most frequent. If none ask which user has to be checked
3. If you see on top of the output: "Warning - 'applicationUser' password has expired and needs to be changed"
    a. You can look up User Management
    b. Once finished send an e-mail and ask if it's an application user that uses only rsa-keys to log and nobody uses User and Password login
    c. Once received affirmative answer you can proceed with Application Users otherwise you'll have to do this again in 90 days.
4. Fetch the path, which statistically is `/app/applicationUser/logpath/logcleaner`
5. Check if it has execution permissions: `ls -l /path/to/the/file`
    - if not you can add them with `chmod +x /path/to/the/file`

23.2.2. ZFS pool fix

1. Identify the global zone for the needed device. Inventory can help sometimes
2. Check allocated storage, "quota": `zfs get quota,reservation rpool/zone/oss0xx`
3. Check available space: `zpool list rpool` or whatever naming convention is chosen
4. If there's space raise the quota: `zfs set quota=60G rpool/zone/oss0xx`
5. Check actual status: `zfs get quota rpool/zone/oss0xx`
6. Once the cleaning has been done please shrink it back: `zfs set quota=55G rpool/zone/oss0xx`

Example:

```
oss164:{root}:/# df -h | grep 100
rpool/zone/oss059       55G    31G     0K   100%    /zone/oss059

oss164:{root}:/# zfs get quota,reservation rpool/zone/oss059
NAME                PROPERTY     VALUE   SOURCE
rpool/zone/oss059  quota        55G     local
rpool/zone/oss059  reservation  none    local

oss164:{root}:/# zpool list rpool
NAME   SIZE  ALLOC   FREE  CAP  HEALTH  ALTROOT
rpool  136G   120G  16.1G  88%  ONLINE  -

oss164:{root}:/# zfs set quota=60G rpool/zone/oss059
```

```
oss164:{root}:/# zfs get quota rpool/zone/oss059
NAME               PROPERTY  VALUE  SOURCE
rpool/zone/oss059  quota     60G    local

oss164:{root}:/# zfs list rpool/zone/oss059
NAME                USED  AVAIL  REFER  MOUNTPOINT
rpool/zone/oss059  55.0G  5.00G  30.6G  /zone/oss059

zfs set quota=55G rpool/zone/oss059
```

23.2.3. Infrastructure and Minicluster Machines

Client	Example Machines
Minicluster	mi5fds701mgt1
	mi5fds702mgt1
	mi5fds701mgt2
	mi5fds702mgt2
Infrastruttura	mi5fdsx005
	osx254v

- All devices are accessible from the almighty `itmi3pans001`
- Minicluster needs: `oracle@mi5fds70*` the password can be found in inventory

I've already updated all the macros and with mobaXterm or RoyalTS you'll be able to login automatically. Please notify me

23.2.4. Legacy

- Usually the folders are:

```
/u01/app/grid/diag/tnslsnr/mi5fds702db1/listener/alert
rm log_*

/u01/app/grid/diag/tnslsnr/mi5fds702db1/listener/trace
/u01/app/grid/diag/tnslsnr/mi5fds702db1/listener_scan_mgmt_scan1_net2/alert
rm log_*

/u01/app/grid/diag/tnslsnr/mi5fds702db1/listener_scan_mgmt_scan1_net2/trace
rm listener_scan_mgmt_scan1_net2_*

listener_scan_mgmt_scan3_net2/alert
rm log_*

/u01/app/grid/diag/tnslsnr/mi5fds702db1/listener_scan_mgmt_scan3_net2/trace
```

```
rm listener_scan_mgmt_scan3_net2_*

/app/oracle/diag/tnslsnr/mi5fdsx005/listener/trace
rm listener_*
```

- Look for `diag` directory and clear the `listener` logs
- In this case `cd /app/oracle/diag/tnslsnr/mi5fdsx005/listener/trace`
- Keep the original listener.log and deleted the older `listener_*`

After retreiving the device situation you can send an email to the group owner matching the group name against the below table

24. Database

24.1. Inventory

- Inventory device is gminnms116, 10.132.181.116
- Log into with SQLDeveloper

Sample query

```
SELECT * FROM SESYS_USERS WHERE USERNAME = 'zzcks'

DELETE FROM SESYS_USERS WHERE USERNAME = 'zzponnusamyr'
```

commit = F11

25. ICMF Application Restart

In increasing order the used servers are osx356v, 57v, 58v, 59v, 60v, and 61v, will be restarted.

In case the process refuses to stop you can `ps aux | grep <name>` and `kill -9`

25.1. osx356v

Become icmf: `su icmf`

Table 18. Processes

Process	Path	Command
Registry	/app/icmf/icmf_common/bin-local	./registry.sh status
ICMFRR		./component.sh ICMFRR status
NPSMB01	/app/icmf/icmf_nps/bin-local	./component.sh NPSMb01 status
Mb01	/app/icmf/icmf/bin-local/	./component.sh Mb01 status

The keyword "status" from the above table can be replaced with "stop" and "start"

Kill all snippet

```
su icmf
cd /app/icmf/icmf_common/bin-local/
./registry.sh stop
./component.sh ICMFRR stop
cd /app/icmf/icmf_nps/bin-local/
./component.sh NPSMb01 stop
cd /app/icmf/icmf/bin-local/
./component.sh Mb01 stop
```

Killing help `ps aux | grep -e "Mb01" -e "NPSMb01"`

Status snippet

```
su icmf
cd /app/icmf/icmf_common/bin-local/
./registry.sh status
./component.sh ICMFRR status
cd /app/icmf/icmf_nps/bin-local/
./component.sh NPSMb01 status
cd /app/icmf/icmf/bin-local/
./component.sh Mb01 status
```

Start snippet

```
su icmf
cd /app/icmf/icmf_common/bin-local/
./registry.sh start
./component.sh ICMFRR start
cd /app/icmf/icmf_nps/bin-local/
./component.sh NPSMb01 start
cd /app/icmf/icmf/bin-local/
./component.sh Mb01 start
```

25.2. osx357v

Become icmf: `su icmf`

Table 19. Processes

Process	Path	Command
ICMFRR	`/app/icmf/icmf_common/bin-local`	`./component.sh ICMFRR status`
NPSMb02	`/app/icmf/icmf_nps/bin-local`	`./component.sh NPSMb02 status`
Mb02	`/app/icmf/icmf/bin-local`	`./component.sh Mb02 status`

Stop snippet

```
su icmf
cd /app/icmf/icmf_common/bin-local/
./component.sh ICMFRR stop
cd /app/icmf/icmf_nps/bin-local/
./component.sh NPSMb02 stop
cd /app/icmf/icmf/bin-local/
./component.sh Mb02 stop
```

Killin help `ps aux | grep -e "Mb02" -e "NPSMb02"`

Status snippet

```
su icmf
cd /app/icmf/icmf_common/bin-local/
./component.sh ICMFRR status
cd /app/icmf/icmf_nps/bin-local/
./component.sh NPSMb02 status
cd /app/icmf/icmf/bin-local/
./component.sh Mb02 status
```

Start snippet

```
su icmf
```

```
cd /app/icmf/icmf_common/bin-local/
./component.sh ICMFRR start
cd /app/icmf/icmf_nps/bin-local/
./component.sh NPSMb02 start
cd /app/icmf/icmf/bin-local/
./component.sh Mb02 start
```

25.3. osx358v

Become icmf: `su icmf`

Table 20. Processes

Process	Path	Command
ICMFRR	`/app/icmf/icmf_common/bin-local`	`./component.sh ICMFRR status`
NPSCn01	`/app/icmf/icmf_nps/bin-local`	`./component.sh NPSCn01 status`
PullCn01	`/app/icmf/icmf/bin-local`	`./component.sh PullCn01 status`

Stop snippet

```
su icmf
cd /app/icmf/icmf_common/bin-local/
./component.sh ICMFRR stop
cd /app/icmf/icmf_nps/bin-local/
./component.sh NPSCn01 stop
cd /app/icmf/icmf/bin-local/
./component.sh PullCn01 stop
```

Status snippet

```
su icmf
cd /app/icmf/icmf_common/bin-local/
./component.sh ICMFRR status
cd /app/icmf/icmf_nps/bin-local/
./component.sh NPSCn01 status
cd /app/icmf/icmf/bin-local/
./component.sh PullCn01 status
```

Start snippet

```
su icmf
cd /app/icmf/icmf_common/bin-local/
./component.sh ICMFRR start
cd /app/icmf/icmf_nps/bin-local/
./component.sh NPSCn01 start
cd /app/icmf/icmf/bin-local/
```

```
./component.sh PullCn01 start
```

25.4. osx359v

Become icmf: `su icmf`

Table 21. Processes

Process	Path	Command
ICMFRR	/app/icmf/icmf_common/bin-local	./component.sh ICMFRR status
NPSCn02	/app/icmf/icmf_nps/bin-local	./component.sh NPSCn02 status
PushCn03	/app/icmf/icmf/bin-local	./component.sh PushCn03 status

Stop snippet

```
su icmf
cd /app/icmf/icmf_common/bin-local/
./component.sh ICMFRR stop
cd /app/icmf/icmf_nps/bin-local/
./component.sh NPSCn02 stop
cd /app/icmf/icmf/bin-local/
./component.sh PushCn03 stop
```

Status snippet

```
cd /app/icmf/icmf_common/bin-local/
./component.sh ICMFRR status
cd /app/icmf/icmf_nps/bin-local/
./component.sh NPSCn02 status
cd /app/icmf/icmf/bin-local/
./component.sh PushCn03 status
```

Start snippet

```
cd /app/icmf/icmf_common/bin-local/
./component.sh ICMFRR start
cd /app/icmf/icmf_nps/bin-local/
./component.sh NPSCn02 start
cd /app/icmf/icmf/bin-local/
./component.sh PushCn03 start
```

25.5. osx360v

Become icmf: `su icmf`

Table 22. Processes

Process	Path	Command
ICMFRR	/app/icmf/icmf_common/bin-local	./component.sh ICMFRR status
NPSMemDB1a	/app/icmf/icmf_nps/bin-local	./component.sh NPSMemDB1a status
NPSPr01		./component.sh NPSPr01 status
PushMemDB1a	/app/icmf/icmf/bin-local	./component.sh PushMemDB1a status
PushPr01		./component.sh PushPr01 status
PushMemDB2b		./component.sh PushMemDB2b status
PullMemDB1a		./component.sh PullMemDB1a status
PullPr01		./component.sh PullPr01 status

Stop snippet

```
su icmf
cd /app/icmf/icmf_common/bin-local/
./component.sh ICMFRR stop
cd /app/icmf/icmf_nps/bin-local/
./component.sh NPSMemDB1a stop
./component.sh NPSPr01 stop
cd /app/icmf/icmf/bin-local/
./component.sh PushMemDB1a stop
./component.sh PushPr01 stop
./component.sh PushMemDB2b stop
./component.sh PullMemDB1a stop
./component.sh PullPr01 stop
```

Status snippet

```
su icmf
cd /app/icmf/icmf_common/bin-local/
./component.sh ICMFRR status
cd /app/icmf/icmf_nps/bin-local/
./component.sh NPSMemDB1a status
./component.sh NPSPr01 status
cd /app/icmf/icmf/bin-local/
./component.sh PushMemDB1a status
./component.sh PushPr01 status
./component.sh PushMemDB2b status
./component.sh PullMemDB1a status
./component.sh PullPr01 status
```

Start snippet

```
su icmf
cd /app/icmf/icmf_common/bin-local/
```

```
./component.sh ICMFRR start
cd /app/icmf/icmf_nps/bin-local/
./component.sh NPSMemDB1a start
./component.sh NPSPr01 start
cd /app/icmf/icmf/bin-local/
./component.sh PushMemDB1a start
./component.sh PushPr01 start
./component.sh PushMemDB2b start
./component.sh PullMemDB1a start
./component.sh PullPr01 start
```

25.6. osx361v

Become icmf: `su icmf`

Table 23. Processes

Process	Path	Command
ICMFRR	/app/icmf/icmf_common/bin-local	./component.sh ICMFRR status
NPSMemDB1b	/app/icmf/icmf_nps/bin-local	./component.sh NPSMemDB1b status
NPSPr02		./component.sh NPSPr02 status
PushMemDB1b	/app/icmf/icmf/bin-local	./component.sh PushMemDB1b status
PullMemDB1b		./component.sh PullMemDB1b status
PushMemDB2a		./component.sh PushMemDB2a status
PushPr02		./component.sh PushPr02 status
PullPr02		./component.sh PullPr02 status

Stop snippet

```
su icmf
cd /app/icmf/icmf_common/bin-local/
./component.sh ICMFRR stop
cd /app/icmf/icmf_nps/bin-local/
./component.sh NPSMemDB1b stop
./component.sh NPSPr02 stop
cd /app/icmf/icmf/bin-local/
./component.sh PushMemDB1b stop
./component.sh PullMemDB1b stop
./component.sh PushMemDB2a stop
./component.sh PushPr02 stop
./component.sh PullPr02 stop
```

Killin help `ps aux | grep -e "Mb02" -e "NPSMb02"`

Status snippet

```
su icmf
cd /app/icmf/icmf_common/bin-local/
./component.sh ICMFRR status
cd /app/icmf/icmf_nps/bin-local/
./component.sh NPSMemDB1b status
./component.sh NPSPr02 status
cd /app/icmf/icmf/bin-local/
./component.sh PushMemDB2a status
./component.sh PushMemDB1b status
./component.sh PushPr02 status
./component.sh PullMemDB1b status
./component.sh PullPr02 status
```

Start snippet

```
su icmf
cd /app/icmf/icmf_common/bin-local/
./component.sh ICMFRR start
cd /app/icmf/icmf_nps/bin-local/
./component.sh NPSMemDB1b start
./component.sh NPSPr02 start
cd /app/icmf/icmf/bin-local/
./component.sh PushMemDB2a start
./component.sh PushMemDB1b start
./component.sh PushPr02 start
./component.sh PullMemDB1b start
./component.sh PullPr02 start
```

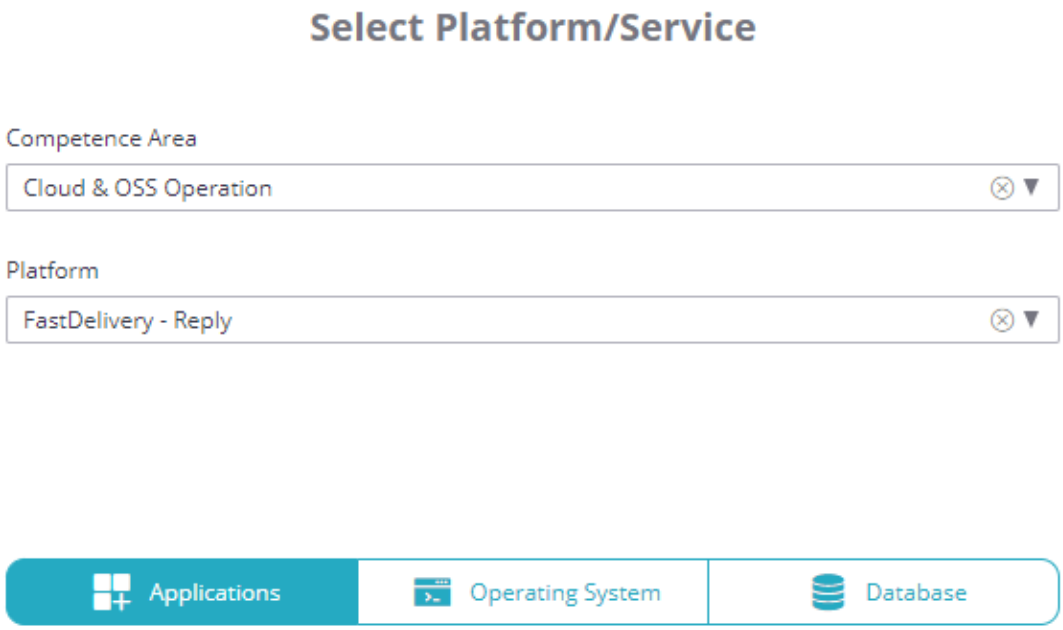
> 20230705 I can make custom macro for the checks

26. DWH Activity

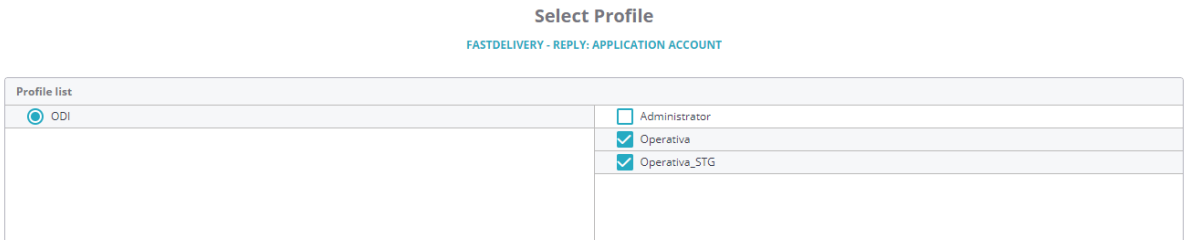
Reply	Machines
PRE	osq203v
PROD	• MI5FDSQ021 • MI5FDSQ022

26.1. For the User Creation:

- Enter IUAM
- Go to New Account Request and select for Competence Area `Cloud & OSS Operation` and platform `FastDelivery - Reply` as shown below:



- Then select the profile, in profile list press `ODI` and for the user pick `Operativa and Operativa_STG` as shown in the image:



- The last step will be to select your Personal Account and give a motivation that will be `Fastdelivery Operations`

26.2. Setting up the ODI Connection

This is a one time set up

26.2.1. ODI Studio

- Once inside the server open File Explorer and go to this path `C:\Oracle\Middleware\Oracle_home` press continue as administrator.
- Open ODI studio, Press `Connect to Repository`, it will prompt a tab called Repository Connection Information,
  - In some cases the ODI might ask to specify the folder, select Browse and follow this path `C:\Progarm Files\Java\jdk*` select the folder press OK, once the ODI is opening it will show a tab where you press NO.
- We will proceed to configure it with the following info, Press `Connect to work Repository` and follow:

Oracle Data Integrator Connection

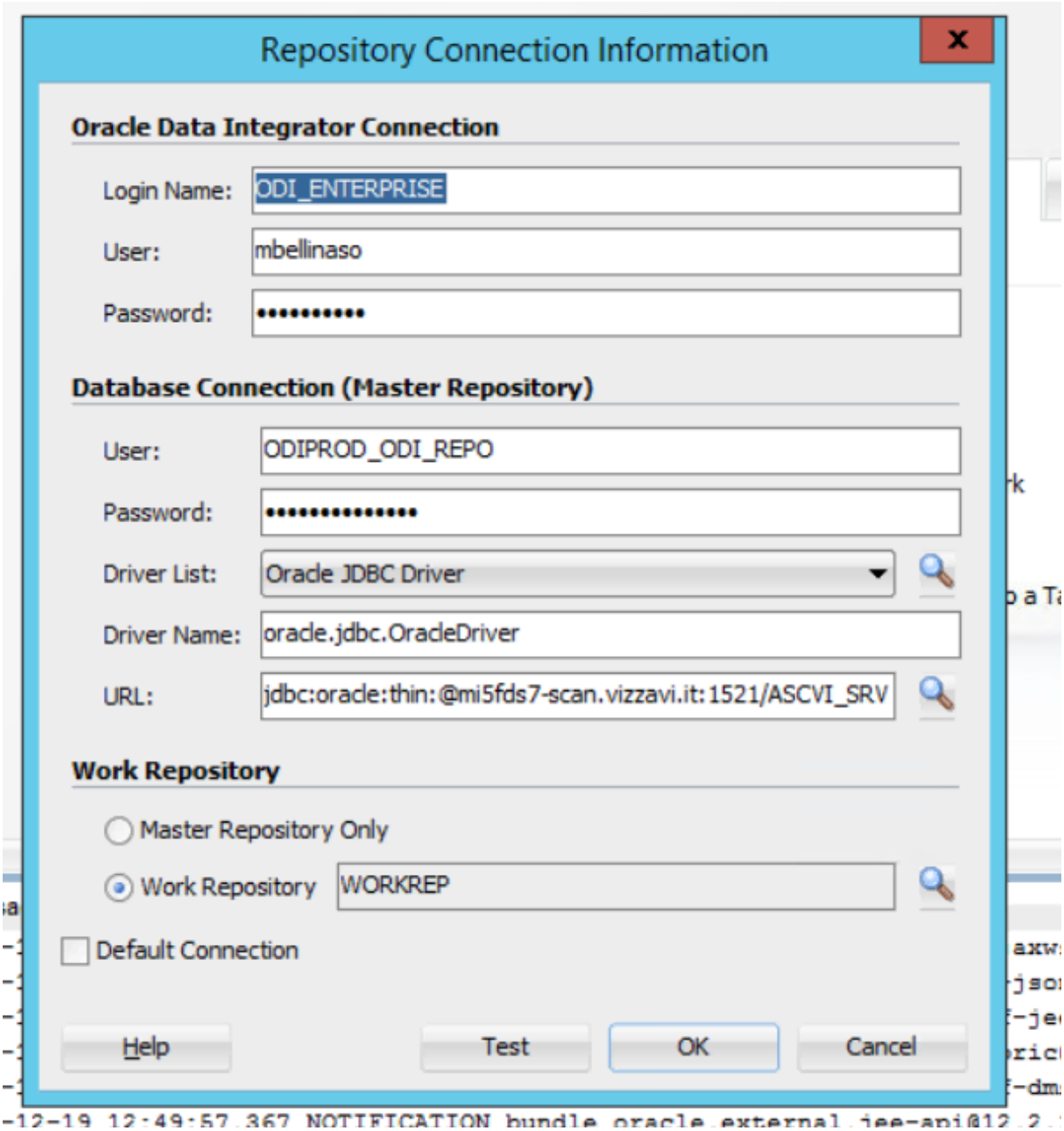
- Login Name → identifies the connection, it can be called as you wish.
- User → zz<youruser>
- Password → Use the one assigned

Database Connection

- User → `ODIPROD_ODI_REPO`
- Password → Use the one given
- Driver List: `Oracle JDBC Driver`
- Driver Name: `oracle.jbdc.OracleDriver`
- URL: `jdbc:oracle:thin:@mi5fds7-scan:1521/ASCVI_SRV`

Work Repository

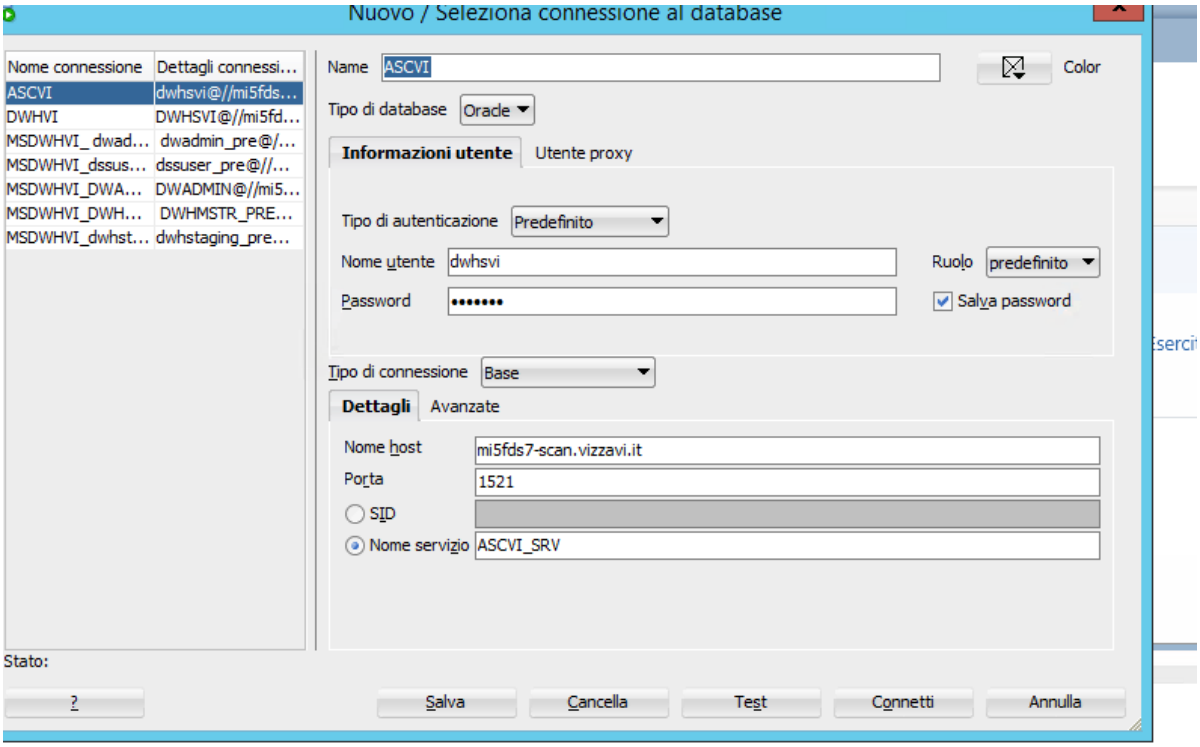
- Select the option Work Repository and press the search buttom then select the `WORKREP` option and press OK, it will prompt one last choice to store the info inside ODI press, select the second option `store password without secure wallet`
- Final result should be like the image below:


Repository Connection Information
Oracle Data Integrator Connection
Login Name:
ODI_ENTERPRISE
User:
mbellinaso
Password:
Database Connection (Master Repository)
User:
ODIPROD_ODI_REPO
Password:
Driver List:
Oracle JDBC Driver
Driver Name:
oracle.jdbc.OracleDriver
URL:
jdbc:oracle:thin:@mi5fds7-scan.vizzavi.it:1521/ASCVI_SRV
Work Repository
Master Repository Only
Work Repository
WORKREP
Default Connection
Help
Test
OK
Cancel

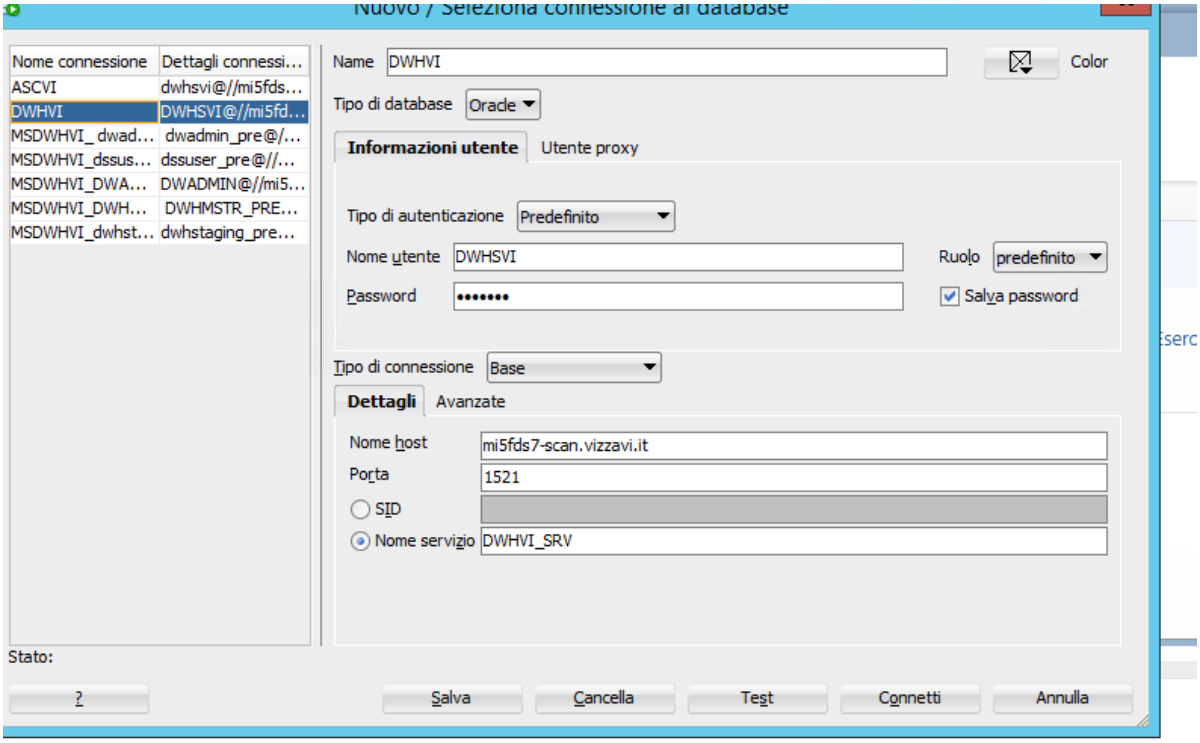
26.2.2. Oracle SQL Developer

once you have added the correct info test the connection no more than once for each session

- Press the green cross to the left to create a new session, you will do this twice for `ascvi` and `dwhvi`:
- Set the Name of the session as `ascvi`
  - Username `dwhsvi` and insert psw given, select the option safe password.
  - Hostname is `mi5fdsq7-scan.private.it`, port `1521`, and service name `ASCVI_SRV`
  - Final result should be like the image below:



- Set the Name of the session as `dwhvi`
  - Username `dwhsvi` and insert psw given, select the option safe password.
  - Hostname is `mi5fdsq7-scan.private.it`, port `1521`, and service name `DWHVI_SRV`
  - Final result should be like the image below:


Nuovo / Seleziona connessione al database
Nome connessione
Dettagli connessi...
ASCVI
dwhsvi@//mi5fds...
DWHVI
DWHSVI@//mi5fd...
MSDWHVI_ dwad...
dwadmin_pre@/...
MSDWHVI_dssus...
dssuser_pre@//...
MSDWHVI_DWA...
DWADMIN@//mi5...
MSDWHVI_DWH...
DWHMSTR_PRE...
MSDWHVI_dwhst...
dwhstaging_pre...
Name
DWHVI
Color
Tipo di database
Oracle
Informazioni utente
Utente proxy
Tipo di autenticazione
Predefinito
Nome utente
DWHSVI
Ruolo
predefinito
Password
Salva password
Tipo di connessione
Base
Dettagli
Avanzate
Nome host
mi5fds7-scan.vizzavi.it
Porta
1521
SID
Nome servizio
DWHVI_SRV
Stato:
?
Salva
Cancella
Test
Connetti
Annulla

27. Get_Users IUAM update monthly

This activity involves gminnms117 from `sys_kpi` user under the path `AccountReconciliation_GetUsers/AccountReconciliation`.

`cd Acc <Tab>`

This script will log into all the devices that in inventory has "Ade" "Yes" flag and takes notes of the accounts inside.
With the no option that log stays local in the machine, with the flag yes it's converted into a csv and pushed into IUAM machine.

It has to be done monthly by hand:

- You **cannot** put it at crontab
- You **cannot** use `nohup` or `screen` or any hang option

It must be run the first friday of the month in order to get the month change in the output.

- If the first friday of the month is not the first day of the month

The script must be executed manually and the session must be kept logged on. All commands start from the `/home/sys_kpi/AccountReconciliation_GetUsers/AccountReconciliation` because `./Get_Users` script location

27.1. Test weekly friday

To test the situation use the following commands:

You can use history to get the command: `ctrl+R no` *should return the command*

```
./GetUsers.sh  "Fast Delivery" "ade" "cron" "query/cron.sql" "no"
./GetUsers.sh  "SE SysAdmin" "ade" "cron" "query/cron.sql" "no"
```

As 20230804 FastDelivery takes around 5m and SE SysAdmin takes 1h.
As 20230825 FastDelivery takes around 5m and SE SysAdmin takes 1h40m

Check the output:

```
ls -1 output/Fast_Delivery/cron/ade/yyyymmdd.HH/tmp
ls -1 output/SE_SysAdmin/cron/ade/yyyymmdd.HH/tmp
```

Send an email to: manager2@consultant.telcoItalyomnitel.it; colleague@consulences.com; colleague@telcoItaly.com; elizabeth.spezzano2@consultant.telcoItalyomnitel.it

With Cc: boss@consultant.telcoItalyomnitel.it; boss2@consulences.com; manager@consulences.com; gabriele.saronni@telcoItaly.com; fabiana@telcoItaly.com

The mail subject will be: weeknumber - Get_Users - TEST - ADE

The mail body will be:
Here FastDelivery anomalies:
`ls -1 AccountReconciliation/output/Fast_Delivery/cron/ade/yyyymmdd.HH/tmp`
Here SESysAdmin anomalies:
`ls -1 AccountReconciliation/output/SE_SysAdmin/cron/ade/yyyymmdd.HH/tmp`

Now fetch the attachments, they need to be renamed as `csv` and downloaded:

As sys_kpi from gminnms117

```
cp
AccountReconciliation_GetUsers/output/Fast_Delivery/cron/ade/yyyymmdd.HH/result/system
s.accounts yyyymmdd_FD.csv
cp
AccountReconciliation_GetUsers/output/SE_SysAdmin/cron/ade/yyyymmdd.HH/result/systems.
accounts yyyymmdd_SA.csv
```

> delete any `csv` leftover from previous runs

27.2. Production, every first friday of the month

To execute it

You can use history to get the command: `ctrl+R yes` *should return the command*

```
./GetUsers.sh  "Fast Delivery" "ade" "cron" "query/cron.sql" "yes"
./GetUsers.sh  "SE SysAdmin" "ade" "cron" "query/cron.sql" "yes"
```

Check the output:

```
ls AccountReconciliation/output/Fast_Delivery/cron/ade/yyyymmdd.HH/tmp
ls AccountReconciliation/output/SE_SysAdmin/cron/ade/yyyymmdd.HH/tmp
```

As 20230804 FastDelivery keeps the same elapsed time while instead SysAdmin 40m

> The last output line should be an scplike output confirming the file has been pushed successfully

`Account-OS-SESysAdmin_ADE_yyyymm.csv 100% 966KB 965.6KB/s 00:00`

27.2.1. Extra trimming

- FastDelivery: `sed -i '/connection/d' Account-OS-Fast_Delivery_ADE_202404.csv` (sed -i '/;connection/d')
- SeSysAdmin:
  - `cd ~/AccountReconciliation_GetUsers/output/SE_SysAdmin/cron/ade/20240405.06/result`
  - `sed -i '/Comando\|completato\|con\|per\|utente/d' system.accounts`
  - `egrep -iwf ../../../../../../iuam_hosts.lst systems.accounts > Account-OS-SESysAdmin_ADE_202404.csv`
  - `awk -F';' '{print $1}' system.accounts | sort -u | wc -l`

As of 20240408 Fastdelivery has: 188 and SysAdmin 956 lines

27.2.2. In case of erros:

- Destination folder: `ssh sysadmin_sftp@10.971.225.176 ls -l /ACFSdisk/iuam_ade`
- expected output: `/ACFSdisk/iuam_ade`

In case the file is not there: you need to upload them manually:

- Account-OS-Fast_Delivery_ADE_yyyymm.csv
- Account-OS-SESysAdmin_ADE_yyyymm.csv

if csv not present:

```
cd
/home/sys_kpi/AccountReconciliation_GetUsers/output/SE_SysAdmin/cron/ade/yyyymmdd.hh/r
esult

cp systems.accounts Account-OS-SESysAdmin_ADE_yyyymm.csv
scp Account-OS-SESysAdmin_ADE_yyyymm.csv
sysadmin_sftp@10.971.225.176:/ACFSdisk/iuam_ade

cd
/home/sys_kpi/AccountReconciliation_GetUsers/output/Fast_Delivery/cron/ade/yyyymmdd.hh
/result

cp systems.accounts Account-OS-Fast_Delivery_ADE_yyyymm.csv
scp Account-OS-Fast_Delivery_ADE_yyyymm.csv
sysadmin_sftp@10.971.225.176:/ACFSdisk/iuam_ade

ssh sysadmin_sftp@10.971.225.176 ls -l /ACFSdisk/iuam_ade
```

Warn the team to run again the process

Send an e-mail to: DL-ServiceHelp@telcoItaly.com; With Cc: boss2@consulences.com; manager@consulences.com

```
potete proseguire con la lavorazione:

ssh sysadmin_sftp@10.971.225.176 ls -l /ACFSdisk/iuam_ade
-rw-rw-rw- 1 sysadmin_sftp   sftp_ade        379669 Feb 23 17:59 Account-OS-
Fast_Delivery_ADE_202402.csv
-rw-rw-rw- 1 sysadmin_sftp   sftp_ade        930697 Feb 23 17:58 Account-OS-
SESysAdmin_ADE_202402.csv
```

28. Periodic Process Restart

Example request

```
Buongiorno,
per forzare il ripristino della connessione verso la coda oracle,
si richiede di eseguire il restart con utenza "jsyssrv" del componente "logicmm" sui
due nodi "oss245 e oss246".
Grazie
```

- Servers can be accessed from itmi3pans001, or using mobaXterm saved sessions
- log as the requested user, "jsyssrv"
- Run a `find / -name <indicated_service>*` to find service path. Usually something like `path_to_service/bin/`
- Verify service status with one of the following `./service.sh check` or `./service.sh status`
  - Check if the service has the following commands available; `./service.sh restart`, `./service.sh stop`, `./service.sh graceful-restart`
  - You can run `./service.sh` without commands in order to discover possibilities

If there's no stop command or it refuses to die

- Determine the PID (Process ID) using `ps aux | serviceName`
- Kill it: `kill -9 PID`
- Restart service `./service.sh start`
  - Repeat the process in all the requested servers
- Reply to the request

28.1. Restore All Services On Servers

Example request

```
Good Morning,
We have observed that since XXX yesterday ALL services on XXX servers have stopped
working as if a kill of all processes was done.

Could you please provide an audit and turn all services back on?
Grazie
```

- Servers can be accessed from itmi3pans001, or using mobaXterm saved sessions
- Inside the path `/var/tmp/` check the owner of the script named `ossXXX_start_all.sh`
- Log as the requested user and run the script named `ossXXX_start_all.sh`

28.2. Transaction manager

Example request

```
Buongiorno,
a seguito di questo allarme vi chiedo di provvedere a fare il restart del
transactionmanager del nodo oss245
Grazie
```

- Servers can be accessed from itmi3pans001, or using mobaXterm saved sessions
- The server is listed this time: oss245
  - Beware that this is twin with oss246
- log as the requested user, in this case it's not told but it's `jsyssrv`
- The steps are the following

Log as `jsyssrv` from `ansysad` user. In case you log from moba sessions, type `exit` or ctrl+d to revert back to ansysad from root

```
sudo su - jsyssrv
cd /app/jsyssrv/jboss-as-7.1.1.Final/bin/
./transactionmanager.sh stop
./transactionmanager.sh start
```

if you encounter the following:

```
jsyssrv@oss246:/app/jsyssrv/jboss-as-7.1.1.Final/bin# ./transactionmanager.sh start

[INFO] - Checking transactionmanager status
[INFO] - PID file trovato (6002) - Verifico se c'Ã¨ un processo di transactionmanager
```

```
attivo
[WARN] - Questa istanza di transactionmanager sembra essere ancora attiva
[WARN] - Aspetta ancora qualche secondo prima di tentare un riavvio
[ALERT] - Se invece sei proprio sicuro di cosa stai facendo, esegui: kill -9 6002 6045
```

Run the suggested command: `kill -9 6002 6045` which is different every time

> It is most likely that after confirming the restart on oss245 another mail will follow asking for the same activity on oss246

28.3. Memobarring

- Servers can be accessed from itmi3pans001, or using mobaXterm saved sessions
  - oss256
  - oss257
  - oss258
- become `su - memobarring`
- The path is: `/app/barringws/fsb/memobarring`
- Run `./barringws stop`
- Run `./barringws start`

28.4. King Kong FDCGW

Example request

```
Ciao,

dopo il patching di questa mattina  il processo Kong risulta spento.
Potete forzare un update del servizio ?
Collegarsi su un nodo di docker ( mi5fdsx006 o mi5fdsx007 ) con l utenza jsyssrv e
dare il comando
docker service update fdcgw_kong
Se non funziona provate a eseguire questa procedura:
docker service scale fdcgw_kong=0
docker service scale fdcgw_kong=1
docker service scale fdcgw_kong=2

Nota:
Per verificare che sia tutto a posto  potete usare il comando: `docker service ls`

Dovrebbe mostrare 2 istanze di fdcgw_kong attive
```

- The server can be accessed from itmi3pans001, or using mobaXterm saved sessions
- Log into either of the asked ones but don't do the activity on both
- **Don't** use `docker service update fdcgw_kong`
- Run the other commands direcly one after the other
- Check with `docker service ls`

28.5. Restart Agent inside ODI Devices

Example request

```
Ciao,
Venerdì scorso non ci siamo accorti che con il ripristino della MI5FDSQ021 non si è
provveduto a riattivare l agente ODI oraclediagent1.
Si chiede quindi di provvedere il prima possibile.
```

- Log inside the required server or servers from EAG
- From Command Prompt go inside this path `C:\Oracle\Middleware\Oracle_Home\user_projects\domains\base_domain\bin`
- Run this command `startComponent.cmd OracleDIAgent1`
- You will be asked to insert a password regading the Node Manager Oracle ODI MI5FDODI01 and MI5FDODI02, stored inside the inventory

Remember the agents are: OracleDIAgent1 - MI5FDSQ021 and OracleDIAgent2 - MI5FDSQ022

28.6. Restart ERIF LEGACY

If you are not already, log in with the erif utility

- Enter inside the "ER_IF" directory: `cd /app/erif/ER_IF`
  - Stop ERIF Legacy: `./jbctl -c stop -e it -s settings_solaris.sh`
  - Start ERIF Legacy: `./jbctl -c start -e it -s settings_solaris.sh`

Nodes are oss250-oss251-oss252-oss253-oss254-oss255

28.7. Restart kplexgw

If you are not already, log in with the jboss utility

- Enter inside the "kplexgw" directory: `cd /app/jboss/wildfly-18.0.1.Final_Kplex/bin`
  - Stop kplexgw: `./kplexgw.sh stop`

The stopping process typically lasts between 5 to 15 minutes. To ensure it has stopped, simply rerun the previous command.

- Start kplexgw: `./kplexgw.sh start`

Nodes are oss259-oss260. Restart one at a time

29. TiT Activities and Updates

Mail Object: telcoItaly - TiTCare - Request - Aggiornamento Report TIT

```
Request's description:

Good morning,
At the customer's request, to make a new report visible, we kindly ask you to perform
the following update on the production database:

use IM_1_HintIntranet
update [RES-02L-] set rpt_profili= '111, 144, TLCC, 997, 172' where I_ID = 67823719

Thank you.
```

- Log inside the required server or servers from EAG, usually indicated in the mail
- Open Microsoft SQL Server Management Studio
- You will be asked to log in as a user, in this case use 'sa' and insert the password
- Open the Databases folder, and once inside do right click inside the `IM_1_HintIntranet` database, select new query
- Once it opens the SQLQuery, paste the script given, select all, and press Execute.

30. Doorway Updates

Mail Object: telcoItaly Applicazione Doorway - change

```
Request's description:
Impacted URLs:
doorway.telcoItaly.co.uk

Impacted services:
telcoItaly Doorway

Machines impacted:
osx262v

Request Description:
== STEP #1 - Back-up filesystem.
Make backups

== STEP #2 - Downloading updates.
Download the attached package tda-registry_update.zipper

== STEP #3 - Update filesystem for change VF root implementation.
Copy the contents of the tda-registry_update.zip per package (where directories and
files are already properly organized) to the /app/telcoItaly/tda-registry folder where
the application is installed

== STEP #4 - Clearing Cache.
Empty the contents of the folder to follow by running the command:
rm -rf /app/telcoItaly/tda-registry/var/cache/twig/*

== STEP #5 - Vendor-side testing.
Notify successful execution of STEP #3 and wait for confirmation from the vendor
before concluding the change
```

Backup

- From EAG open Egde Browser, using the vmware vCenter
- In the search bar type `osx262v`
- Once the info is displayed, go to actions, take snapshots and make a snapshot of the machine

if there are older snapshots regarding this activity delete them

- Control that the process is completed

Update

- Log inside the required server `osx262v`
- As `root` copy the files in the correspondent folder
  - Example:

```
cp -o /home/ansysad/tda-registry_update/lib/User/UserController.php
/app/telcoItaly/tda-registry/lib/User/
cp -o /home/ansysad/tda-registry_update/scripts/DeactivateUsers.php
/app/telcoItaly/tda-registry/scripts/
```

- Clear the cache with the command indicated
- Answer the mail saying that the activity is completed

FB fabiana.coworker@consulences.com & GS gabriele.saronni@consulences.com