

Risoluzione dei problemi della VLAN nativa sulla modalità gestita Intersight

Sommario

[Introduzione](#)

[Prerequisiti](#)

[Requisiti](#)

[Componenti usati](#)

[Premesse](#)

[Risoluzione dei problemi](#)

[VMWare ESXi](#)

[VLAN nativa non configurata sulla vNIC, sugli uplink FI o sui dispositivi di rete upstream](#)

[Scenario 1. La VLAN nativa è configurata a livello di vNIC](#)

[Scenario 2. La VLAN nativa è configurata negli uplink FI](#)

[La VLAN nativa è configurata sulle vNIC, gli uplink FI e i dispositivi di rete upstream](#)

[Scenario 1. La VLAN nativa è configurata negli uplink FI, il dispositivo upstream non è configurato sulla vNIC](#)

[Scenario 2. La VLAN nativa è configurata sulla vNIC, ma il dispositivo upstream non è configurato negli uplink FI](#)

[Sistema operativo Windows Server](#)

[Acquisizione pacchetti](#)

[Scenario 1. La VLAN nativa è configurata negli uplink FI, ma non in vNIC](#)

[Scenario 2. La VLAN nativa è configurata sugli uplink FI e sulla vNIC](#)

[Scenario 3. La VLAN nativa è configurata a livello di sistema operativo e di vNIC](#)

[Informazioni correlate](#)

Introduzione

Questo documento descrive le opzioni di configurazione della VLAN nativa in un ambiente in modalità gestita da Cisco Intersight, evidenziando gli scenari comuni.

Prerequisiti

Requisiti

Cisco raccomanda la conoscenza dei seguenti argomenti:

- Conoscenze base dei server UCS (Unified Computing Systems)
- Conoscenze base di Intersight Managed Mode (IMM)
- Conoscenze base di ESXi e del sistema operativo Windows
- Nozioni di base sulle reti

Componenti usati

Le informazioni fornite in questo documento si basano sulle seguenti versioni software e hardware:

- Intersight Managed Mode (IMM)
- UCS X-215C-M8
- UCS-C240-M7SX
- 6536 Fabric Interconnect
- 6454 Fabric Interconnect
- Server serie X Firmware versione 5.3(0.240016)
- Fabric interconnect 6536 Firmware versione 4.3(5.25004)
- Firmware serie C per server versione 4.3(4.241063)
- Fabric interconnect 6536 Firmware versione 4.2(3m)

Le informazioni discusse in questo documento fanno riferimento a dispositivi usati in uno specifico ambiente di emulazione. Su tutti i dispositivi menzionati nel documento la configurazione è stata ripristinata ai valori predefiniti. Se la rete è operativa, valutare attentamente eventuali conseguenze derivanti dall'uso dei comandi.

Premesse

Le opzioni di configurazione della VLAN nativa in un ambiente in modalità Cisco Intersight-Managed hanno scenari comuni che portano al doppio tagging. In questo articolo vengono inoltre illustrate le procedure consigliate per la risoluzione dei problemi.

In Cisco UCS, gli adattatori NIC sono virtualizzati e presentati al sistema operativo tramite vNIC. Queste schede virtuali sono connesse a un'interfaccia Ethernet virtuale (vEthernet) che è generalmente configurata come porta trunk. La VLAN nativa viene usata per trasportare il traffico senza tag (o il traffico che non usa il tag 802.1Q) su una porta trunk.

A seconda del sistema operativo installato, può avere la capacità o meno di eseguire il tagging del proprio traffico. Ad esempio, VMWare ESXi è in grado di contrassegnare più VLAN. Per i sistemi operativi in cui il tagging VLAN non è disponibile o non è necessario, si consiglia di selezionare una VLAN nativa per la VLAN predefinita da usare per il traffico senza tag.

Risoluzione dei problemi

VMWare ESXi

VLAN nativa non configurata sulla vNIC, sugli uplink FI o sui dispositivi di rete upstream

nell'esempio, vengono usate le VLAN 470 e 72. Di seguito è riportato un esempio con uno scenario di lavoro.

- Nessuna VLAN nativa configurata negli uplink.

Profilo dominio:

Add VLANs

☐ Show VLAN ID Ranges

Q Search Filters 10 results

☐	VLAN ID	Name	Sharing Type	Primary VLAN ID	Multicast Policy	Auto Allow On Uplinks	
☐	1	default	None			Yes	...
☐	33	testrepro_33	None		multicast-IMM	No	...
☐	50	50	None		multicast-IMM	Yes	...
☐	55	55_55	None		multicast-IMM	Yes	...
☐	60	60_60	None		multicast-IMM	Yes	...
☐	69	VLAN	None		multicast-IMM	Yes	...
☐	70	VLAN	None		multicast-IMM	Yes	...
☐	72	Test-subnet-72_72	None		multicast-IMM	Yes	...
☐	201	test_201	None		multicast-IMM	Yes	...
☐	470	VLAN	None		multicast-IMM	Yes	...

Rows per page 10 < 1 >

☒ Set Native VLAN ID

VLAN ID
1

Cancel Back Save

Via CLI:

FI-A

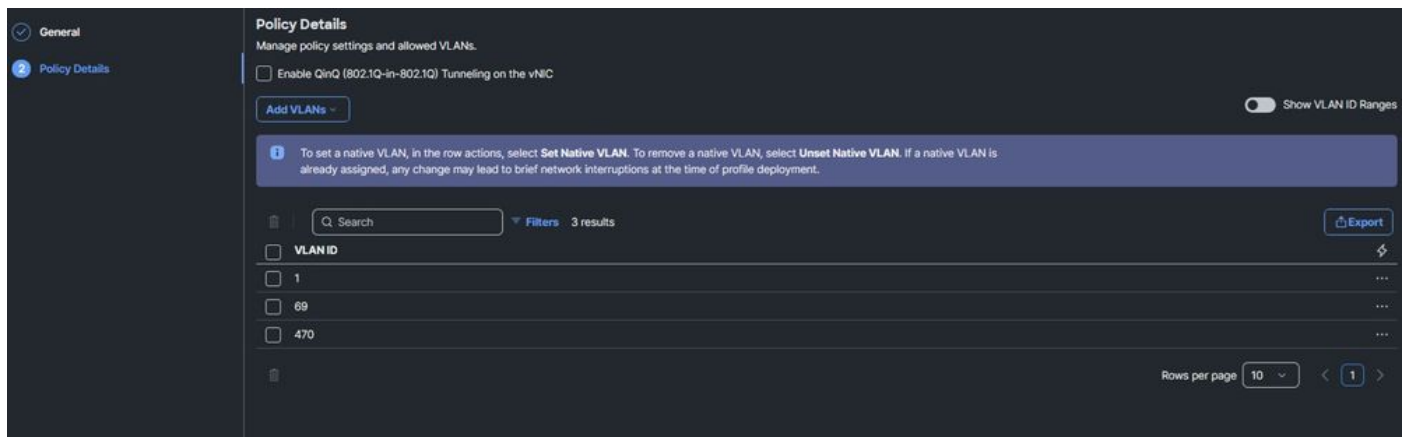
```
6536-A(nx-os)# show running-config interface ethernet 1/1
description Uplink PC Member
pinning border
switchport mode trunk
switchport trunk allowed vlan 1,50,55,60,69-70,72,201,470
```

FI-B

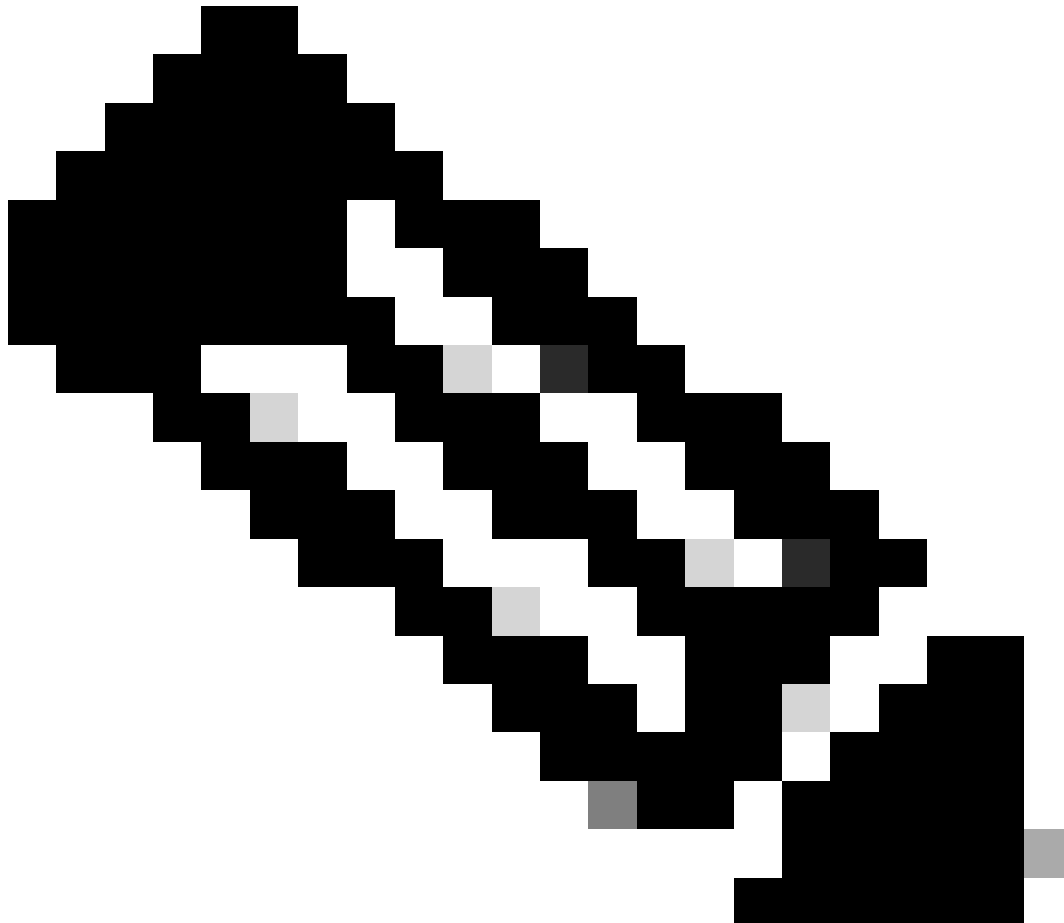
```
6536-B(nx-os)# show running-config interface ethernet 1/1
description Uplink PC Member
pinning border
switchport mode trunk
switchport trunk allowed vlan 1,50,55,60,69-70,72,201,470
```

- Nessuna configurazione VLAN nativa nelle vNIC

Criteri di gruppo rete Ethernet:



Via CLI:



Nota: È possibile visualizzare le reti Ethernet nei server attraverso il percorso Server > Inventario > Schede di rete, quindi selezionare la scheda VIC e fare clic su Interfacce.

GeneralInventoryUCS Server ProfileHCLTopologyMetricsConnectivity

Expand All

Motherboard

Boot

Management Controller

CPU's

Memory

Network Adapters

- Adapter UCSX-ME-V5Q50G_FCH28175L9
- Adapter UCSX-ML-V5Q50G_FCH2817742H

Storage Controllers

TPM

Adapter UCSX-ML-V5Q50G_FCH2817742H

GeneralInterfaces

DCE Interfaces

Name	OperState	IO Module Port	MAC Address
1	up	chassis-1-loc-2-muxhostport-port-29	EC:19:2E:56:5A:09
2	up	chassis-1-loc-2-muxhostport-port-30	EC:19:2E:56:5A:0A
3	up	chassis-1-loc-1-muxhostport-port-29	EC:19:2E:56:5A:0B
4	up	chassis-1-loc-1-muxhostport-port-30	EC:19:2E:56:5A:0C

NIC Interfaces

Name	MAC Address	QinQ VLAN	VIF ID	Active Oper State	Passive VIF ID	Passive Oper State	QoS Policy	Rate Limit (Mbps)
vNIC-A	00:25:85:01:00:34	-	800	Up	-	-	IMM-QOS	100000
vNIC-B	00:25:85:01:00:35	-	801	Up	-	-	IMM-QOS	100000

HBA Interfaces

Name	WWPN	VIF ID	Oper State	QoS Policy	Rate Limit (Mbps)
------	------	--------	------------	------------	-------------------

NO ITEMS AVAILABLE

FI-A

```
6536-A(nx-os)# show running-config interface vethernet 800
interface Vethernet800
  switchport mode trunk
  switchport trunk allowed vlan 1,69,470
```

FI-B

```
6536-B(nx-os)# show running-config interface vethernet 801
interface Vethernet801
  switchport mode trunk
  switchport trunk allowed vlan 1,69,470
```

- VLAN configurata nel sistema operativo:

Configure Management Network	VLAN (optional)
Network Adapters VLAN (optional) IPv4 Configuration IPv6 Configuration DNS Configuration Custom DNS Suffixes	470 A VLAN is a virtual network within a physical network. Because several VLANs can co-exist on the same physical network segment, VLAN configuration and partitioning is often more flexible, better isolated, and less expensive than flat networks based on traditional physical topology. If you are unsure how to configure or use a VLAN, it is safe to leave this option unset.

- Test ping riuscito:

```
C:\Users\ >ping 10.31.123.106

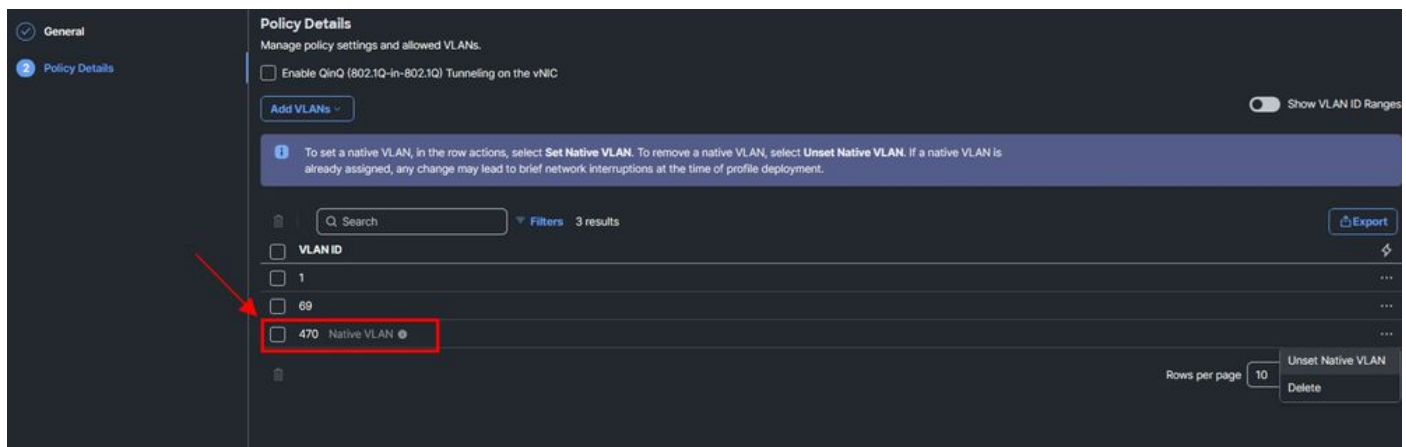
Pinging 10.31.123.106 with 32 bytes of data:
Reply from 10.31.123.106: bytes=32 time<1ms TTL=64
Reply from 10.31.123.106: bytes=32 time<1ms TTL=64
Reply from 10.31.123.106: bytes=32 time<1ms TTL=64
Reply from 10.31.123.106: bytes=32 time<1ms TTL=64

Ping statistics for 10.31.123.106:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 0ms, Average = 0ms
```

Scenario 1. La VLAN nativa è configurata a livello di vNIC

Se si configura la VLAN come nativa nel gruppo Ethernet Network, la connettività di rete potrebbe essere interrotta a causa di problemi di tagging della VLAN.

- Configurazione nel gruppo di reti Ethernet:



Via CLI:

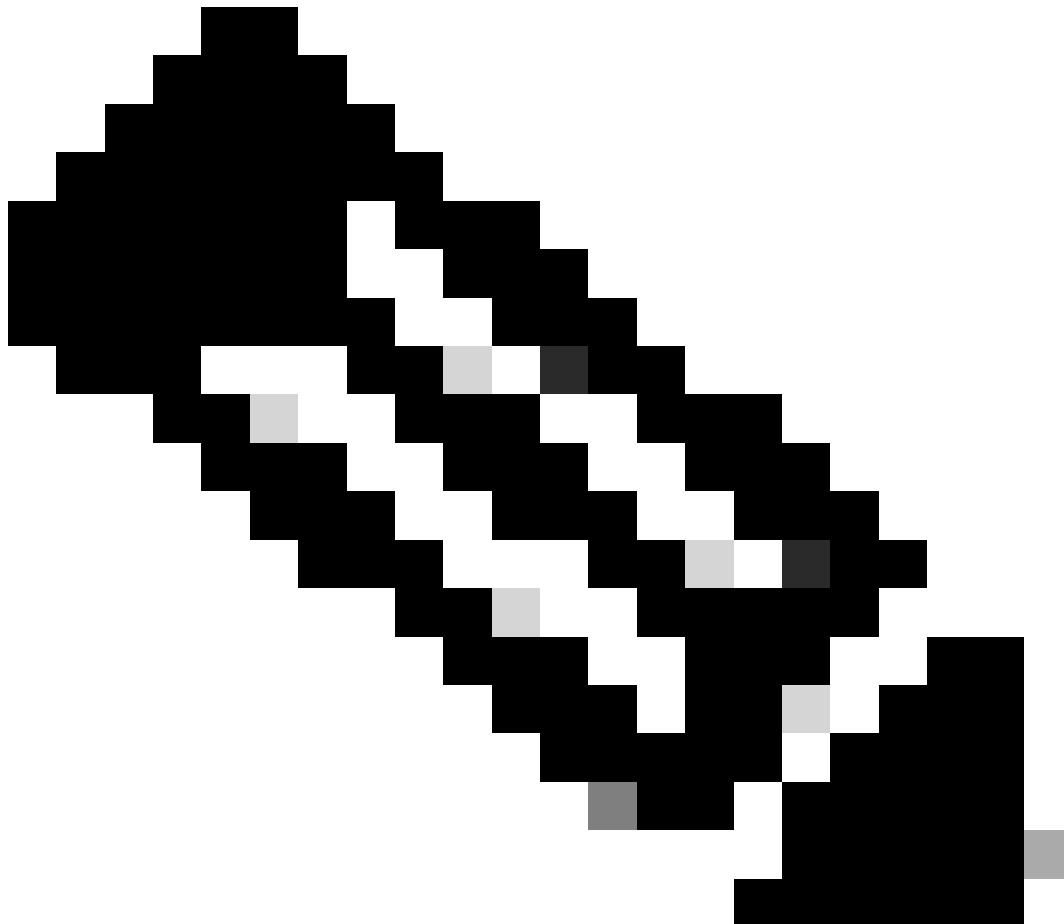
FI-A

```
6536-A(nx-os)# show running-config interface vethernet 800
interface Vethernet800
  switchport mode trunk
  switchport trunk native vlan 470 <<<<<<<<<<
  switchport trunk allowed vlan 1,69,470
```

FI-B

```
6536-B(nx-os)# show running-config interface vethernet 801
interface Vethernet801
  switchport mode trunk
  switchport trunk native vlan 470 <<<<<<<<<<
  switchport trunk allowed vlan 1,69,470
```

- Il test ping non è riuscito
-



Nota: Dopo aver rimosso la VLAN nativa dal gruppo di rete, la connettività viene ripristinata.

Scenario 2. La VLAN nativa è configurata negli uplink FI

- CLI VIa:

FI-A

```
6536-A(nx-os)# show running-config interface ethernet 1/1
description Uplink PC Member
switchport mode trunk
switchport trunk native vlan 470 <<<<<<<<<<
switchport trunk allowed vlan 1,50,55,60,69-70,72,201,470
```

FI-B

```
6536-B(nx-os)# show running-config interface ethernet 1/1
switchport mode trunk
switchport trunk native vlan 470 <<<<<<<<<<
switchport trunk allowed vlan 1,50,55,60,69-70,72,201,470
```

Se si tenta di eseguire il ping sul sistema operativo con la VLAN nativa configurata negli uplink, il test ping non ha esito positivo.

Per risolvere questo problema, è necessario rimuovere la VLAN dall'uplink e lasciare la VLAN configurata al livello del sistema operativo ESXi.

La VLAN nativa è configurata sulle vNIC, gli uplink FI e i dispositivi di rete upstream

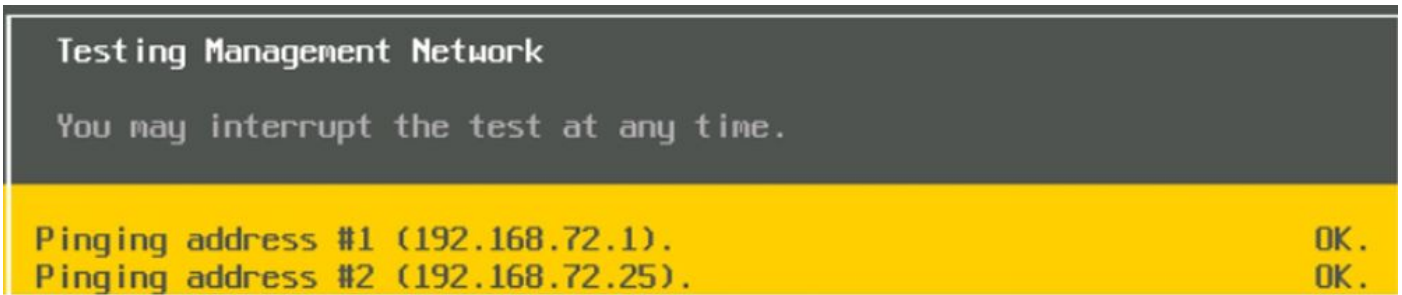
Per questo ripristino, è stata usata un'altra VLAN. La VLAN utilizzata è 72.

Considerazioni:

1. La VLAN 72 è configurata come nativa nel nostro DG Catalyst
2. La VLAN 72 è configurata come nativa nel dispositivo Nexus
3. La VLAN 72 è configurata come nativa negli uplink FI
4. La VLAN 72 è configurata come nativa nelle vNIC
5. La VLAN non ha tag nel sistema operativo:

Configure Management Network	VLAN (optional)
Network Adapters VLAN (optional) IPv4 Configuration IPv6 Configuration DNS Configuration Custom DNS Suffixes	Not set A VLAN is a virtual network within a physical network. Because several VLANs can co-exist on the same physical network segment, VLAN configuration and partitioning is often more flexible, better isolated, and less expensive than flat networks based on traditional physical topology. If you are unsure how to configure or use a VLAN, it is safe to leave this option unset.

Se si seguono queste considerazioni e si prova il ping, si osserverà che il ping funziona come previsto:



Acquisizione dei pacchetti a livello di sistema operativo:

Un altro modo per verificare se il data plane funziona come previsto consiste nell'acquisire un pacchetto a livello di sistema operativo. In questo articolo sulla risoluzione dei problemi è stato utilizzato lo strumento pktcap-uw per acquisire il traffico che passa attraverso le schede di rete fisiche. Ad esempio:

```
pktcap-uw --uplink vmnic0 --dir 2 -o /vmfs/volumes/datastore1/pcaps/nativeworking.pcap -i icmp:
```

No.	Time	Source	Destination	Protocol	Length	Info
→ 1	0.000000	10.31.123.45	192.168.72.25	ICMP	74	Echo (ping) request id=0x000a, seq=12681/35121, ttl=127 (reply in 2)
← 2	0.000112	192.168.72.25	10.31.123.45	ICMP	74	Echo (ping) reply id=0x000a, seq=12681/35121, ttl=64 (request in 1)
7	1.018514	10.31.123.45	192.168.72.25	ICMP	74	Echo (ping) request id=0x000a, seq=12682/35377, ttl=127 (reply in 8)
8	1.018625	192.168.72.25	10.31.123.45	ICMP	74	Echo (ping) reply id=0x000a, seq=12682/35377, ttl=64 (request in 7)

acquisizione ELAM:

L'acquisizione ELAM può essere utile quando si risolvono problemi relativi alla VLAN nativa; lo strumento consente di visualizzare in tempo reale i pacchetti inoltrati a livello ASIC. Non interrompe il data plane. Per la risoluzione dei problemi, è necessario focalizzare l'attenzione solo sull'indirizzo MAC e IP del dispositivo di origine e di destinazione".

Esempio di funzionamento dei pacchetti:

```
root@IMM-SAAS-MXSVLAB-6536-A(nx-os)# attach module 1
root@module-1# debug platform internal tah elam asic 0
root@module-1(TAH-elam)# trigger init asic 0 slice 1 lu-a2d 1 in-select 6 out-select 0
Slot 1: param values: start asic 0, start slice 1, lu-a2d 1, in-select 6, out-select 0
root@module-1(TAH-elam-inse16)# set outer ipv4 src_ip 192.168.72.25 dst_ip 192.168.72.1
root@module-1(TAH-elam-inse16)# start
root@module-1(TAH-elam-inse16)# report
HEAVENLY ELAM REPORT SUMMARY
slot - 1, asic - 0, slice - 1
=====
```

Incoming Interface: Eth1/10
Src Idx : 0x1001, Src BD : 72
Outgoing Interface Info: dmod 1, dpid 72
Dst Idx : 0x601, Dst BD : 72

Packet Type: IPv4

Dst MAC address: B0:8B:CF:C8:A2:6B
Src MAC address: 00:25:B5:01:00:34
.1q Tag0 VLAN: 72, cos = 0x0

Dst IPv4 address: 192.168.72.1
Src IPv4 address: 192.168.72.25

```
Ver      = 4, DSCP      = 0, Don't Fragment = 0
Proto    = 1, TTL       = 64, More Fragments = 0
Hdr len  = 20, Pkt len  = 84, Checksum      = 0xc0a9
```

```
L4 Protocol : 1
ICMP type   : 8
ICMP code   : 0
```

Drop Info:

```
LUA:
LUB:
LUC:
LUD:
Final Drops:
```

```
vntag:
vntag_valid : 1
vntag_vir   : 195
vntag_svif  : 195
```

Nell'output ottenuto, è evidente che src e dst si trovano sulla VLAN 72. Ciò è previsto perché si sa che si sta utilizzando la VLAN 72 come porta nativa in tutti i percorsi ed è arrivata sulla porta ethernet 1/10, destinata all'interfaccia dpid 72, dpid è l'identificatore interno della porta ASIC e il mapping può essere trovato utilizzando show interface hardware-mapping:

```
6536-A(nx-os)# show interface hardware-mappings
```

Name	Ifindex	Smod	Unit	HPort	FPort	NPort	VPort	Slice	SPort	SrcId	MacId	MacSP	VIF	Block	BlkSrcID
Eth1/1	1a000000	1	0	72	255	0	-1	1	0	0	18	0	1537	0	0

```
6536-A(nx-os)# show hardware internal tah interface ethernet 1/1
```

```
#####
```

```
IfIndex: 0x1a000000
```

```
DstIndex: 6144
```

```
IfType: 26
```

```
Asic: 0
```

```
Asic: 0
```

```
AsicPort: 72
```

```
SrcId: 0
```

```
Slice: 1
```

```
PortOnSlice: 0
```

```
Table entries for interface Ethernet1/1
```

In base alle informazioni ottenute nel comando show interface hardware-mappings, la porta di destinazione è la porta Ethernet 1/1 che è uno degli uplink nel dominio UCS.

Scenario 1. La VLAN nativa è configurata negli uplink FI, il dispositivo upstream non è configurato sulla vNIC

Questa volta, è evidente che la richiesta ICMP smette di funzionare, come previsto, perché la VLAN nativa è stata rimossa dalle vNIC:

Acquisizione ELAM.

In questo caso, non sarà possibile eseguire il ping e se si tenta di utilizzare l'indirizzo IP dell'origine e della destinazione, il comando non funzionerà perché non è presente alcuna connessione. In questo caso particolare, impostare gli indirizzi MAC come filtro per ottenere ulteriori informazioni:

```
root@module-1(TAH-elam-inse16)# set outer 12 src_mac 00:25:B5:01:00:34 dst_mac ff:ff:ff:ff:ff:ff
root@module-1(TAH-elam-inse16)# start
root@module-1(TAH-elam-inse16)# report
HEAVENLY ELAM REPORT SUMMARY
slot - 1, asic - 0, slice - 1
=====
```

```
Incoming Interface: Eth1/10
Src Idx : 0x1001, Src BD : 1
Outgoing Interface Info: dmod 1, dpid 72
Dst Idx : 0x601, Dst BD : 72
```

Packet Type: ARP

```
Dst MAC address: FF:FF:FF:FF:FF:FF
Src MAC address: 00:25:B5:01:00:34
.lq Tag0 VLAN: 1, cos = 0x0
```

```
Target Hardware address: 00:00:00:00:00:00
Sender Hardware address: 00:25:B5:01:00:34
Target Protocol address: 192.168.72.1
Sender Protocol address: 192.168.72.25
ARP opcode: 1
```

Drop Info:

```
LUA:
LUB:
LUC:
LUD:
Final Drops:
```

```
vntag:
vntag_valid    : 1
vntag_vir     : 195
vntag_svif    : 195
```

6536-A(nx-os)# show interface hardware-mappings

```
-----
Name      Ifindex  Smode Unit  HPort  FPort  NPort  VPort  Slice  SPort  SrcId  MacId  MacSP  VIF   Block  BlkSrcID
-----
Eth1/1    1a000000  1     0      72     255    0      -1     1      0      0     18     0     1537  0      0
```

È possibile vedere la VLAN per l'indirizzo MAC 00:25:B5:01:00:34 (vNIC-A) che sta utilizzando la VLAN 1. Questa condizione non è corretta perché è necessario usare la VLAN 72.

Scenario 2. La VLAN nativa è configurata sulla vNIC, ma il dispositivo upstream non è configurato negli uplink FI

Acquisizione ELAM:

```
root@module-1(TAH-elam-inse16)# set outer 12 src_mac 00:25:B5:01:00:34 dst_mac ff:ff:ff:ff:ff:ff
root@module-1(TAH-elam-inse16)# start
root@module-1(TAH-elam-inse16)# report
HEAVENLY ELAM REPORT SUMMARY
slot - 1, asic - 0, slice - 1
=====
```

```
Incoming Interface: Eth1/10
Src Idx : 0x1001, Src BD : 72
Outgoing Interface Info: met_ptr 0
```

Packet Type: ARP

```
Dst MAC address: FF:FF:FF:FF:FF:FF
Src MAC address: 00:25:B5:01:00:34
.lq Tag0 VLAN: 72, cos = 0x0
```

```
Target Hardware address: 00:00:00:00:00:00
Sender Hardware address: 00:25:B5:01:00:34
Target Protocol address: 192.168.72.1
Sender Protocol address: 192.168.72.25
ARP opcode: 1
```

Drop Info:

```
LUA:
LUB:
LUC:
LUD:
Final Drops:
```

```
vntag:
vntag_valid    : 1
vntag_vir      : 195
vntag_svif     : 195
```

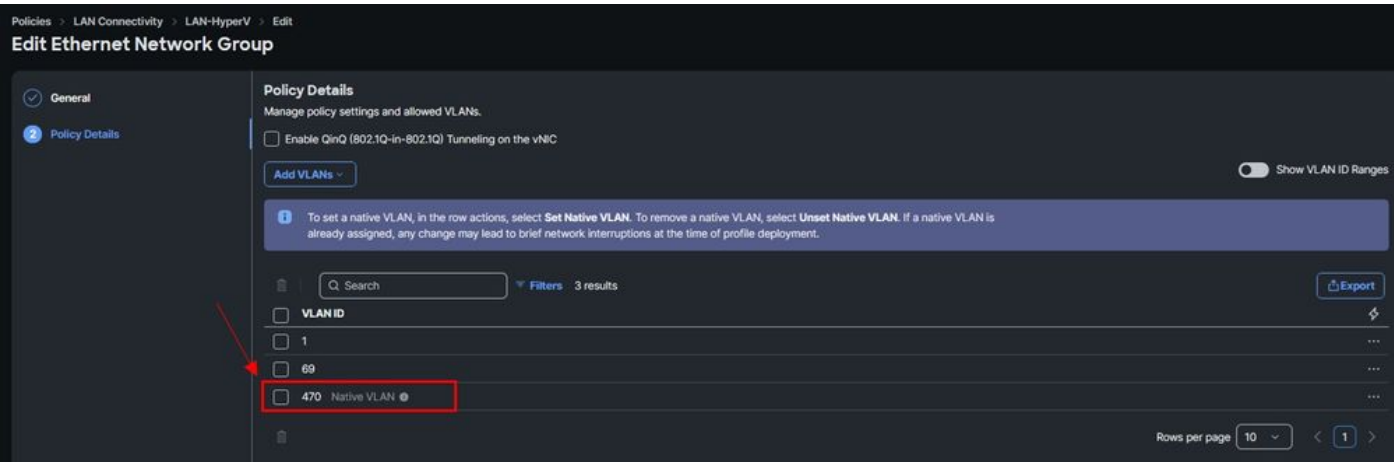
Nell'output, è evidente che si sta utilizzando la VLAN 72 corretta. Tuttavia, se si controlla la configurazione nell'uplink, si osserverà che la VLAN nativa non è configurata:

```
6536-A(nx-os)# show running-config interface ethernet 1/1
description Uplink PC Member
switchport mode trunk
switchport trunk allowed vlan 1,50,55,60,69-70,72,201,470
```

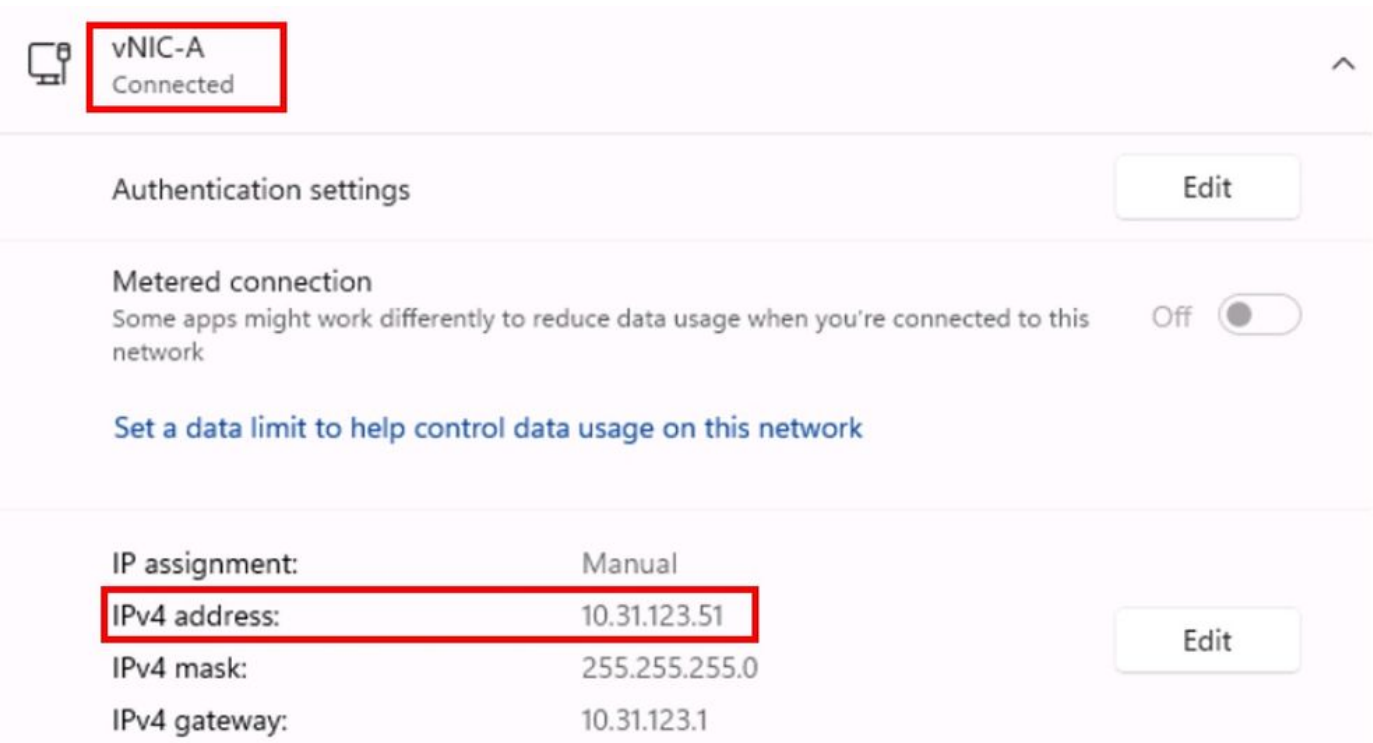
Sistema operativo Windows Server

Il problema della VLAN nativa può essere presente anche nel sistema operativo Windows, in genere perché la VLAN nativa non ha tag sulla vNIC.

Per questo scenario, è stata utilizzata la VLAN nativa 470:



La vNIC utilizzata è connessa in Windows:



Acquisizione pacchetti

Se si tenta di eseguire il ping sulla rete, si osserverà che l'acquisizione dei pacchetti funziona come previsto, in quanto la VLAN nativa è contrassegnata nella vNIC:

No.	Time	Source	Destination	Protocol	Length	Info
1632	157.599402	10.31.123.45	10.31.123.51	ICMP	74	Echo (ping) request id=0x000a, seq=29175/63345, ttl=128 (reply in 1632)
1632	157.599645	10.31.123.51	10.31.123.45	ICMP	74	Echo (ping) reply id=0x000a, seq=29175/63345, ttl=128 (request in 1631)
1634	157.881196	10.61.94.90	10.31.123.51	ICMP	74	Echo (ping) request id=0x0002, seq=6442/10777, ttl=106 (reply in 1635)
1635	157.881469	10.31.123.51	10.61.94.90	ICMP	74	Echo (ping) reply id=0x0002, seq=6442/10777, ttl=128 (request in 1634)

Scenario 1. La VLAN nativa è configurata negli uplink FI, ma non in vNIC

- Livello vNIC:

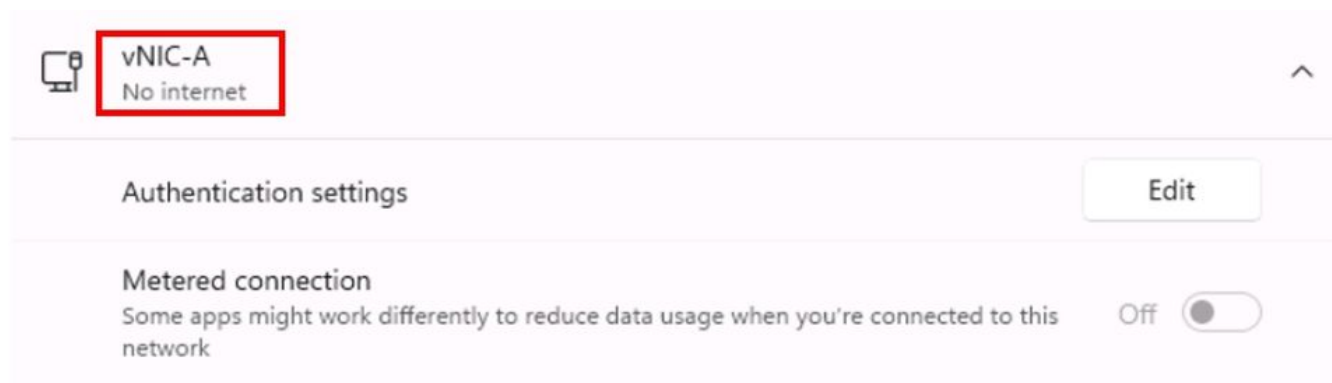
```
6454-A(nx-os)# show running-config interface vethernet 801
interface Vethernet801
  switchport mode trunk
  switchport trunk allowed vlan 1,69,470
```

- Livello FI-A:

```
6454-A(nx-os)# show running-config interface ethernet 1/15-16
interface Ethernet1/15
  description Uplink PC Member
  switchport mode trunk
  switchport trunk native vlan 470 <<<<<<<<<<
  switchport trunk allowed vlan 1,69-70,72,470

interface Ethernet1/16
  description Uplink PC Member
  switchport mode trunk
  switchport trunk native vlan 470 <<<<<<<<<<
  switchport trunk allowed vlan 1,69-70,72,470
```

La vNIC utilizzata non è connessa in Windows:



Se si tenta di eseguire il ping, è previsto che non possa funzionare.

Scenario 2. La VLAN nativa è configurata sugli uplink FI e sulla vNIC

- Livello vNIC:

```
6454-A(nx-os)# show running-config interface vethernet 801
```

```
interface Vethernet801
  switchport mode trunk
  switchport trunk native vlan 470 <<<<<<<<<<
  switchport trunk allowed vlan 1,69,470
```

- Livello FI-A:

```
IMM-SAAS-MXSVLAB-6454-A(nx-os)# show running-config interface ethernet
interface Ethernet1/15
  description Uplink PC Member
  switchport mode trunk
  switchport trunk native vlan 470 <<<<<<<<<<
  switchport trunk allowed vlan 1,69-70,72,470

interface Ethernet1/16
  description Uplink PC Member
  switchport mode trunk
  switchport trunk native vlan 470 <<<<<<<<<<
  switchport trunk allowed vlan 1,69-70,72,470
```

Questa configurazione non consente la connettività. Si prevede che non si riceva una risposta quando si esegue un test ping.

Scenario 3. La VLAN nativa è configurata a livello di sistema operativo e di vNIC

- Lato sistema operativo:

NIC Teaming ✕

New team interface

VLAN 470 - VLAN 470

Team: VLAN 470

Type: Primary interface

VLAN membership

☐ **Default**
The default interface handles all traffic that is not claimed by other VLAN-specific interfaces.

☒ **Specific VLAN:** 

- Livello vNIC:

```
6454-A(nx-os)# show running-config interface vethernet 801
interface Vethernet801
  switchport mode trunk
  switchport trunk native vlan 470 <<<<<<<<<<
  switchport trunk allowed vlan 1,69,470
```

- Il test ping non funziona e la connettività non è disponibile.

Informazioni correlate

- [Guida alla configurazione della modalità gestita di Cisco Intersight](#)
- [Cisco Configure ELAM su UCS](#)
- [Acquisizione dei pacchetti su ESXi con lo strumento pktcap-uw](#)

Informazioni su questa traduzione

Cisco ha tradotto questo documento utilizzando una combinazione di tecnologie automatiche e umane per offrire ai nostri utenti in tutto il mondo contenuti di supporto nella propria lingua. Si noti che anche la migliore traduzione automatica non sarà mai accurata come quella fornita da un traduttore professionista. Cisco Systems, Inc. non si assume alcuna responsabilità per l'accuratezza di queste traduzioni e consiglia di consultare sempre il documento originale in inglese (disponibile al link fornito).