

ntopInsight

An automatic tool for network identification and inventory @ LNS



Stefano Cannizzaro

Emidio Maria Giorgio

Motivazioni

- L'osservabilità della rete è un aspetto cruciale in un sito come LNS, la cui utenza prevede anche apparati sperimentali dislocati in sedi differenti da quella centrale.
- Necessità di rispettare le misure minime AGID – ABSC 1 (CSC1):
Inventario dei dispositivi autorizzati e non autorizzati
 - ABSC_ID 1.1.1 «***Implementare un inventario delle risorse attive***»
 - ABSC_ID 1.1.2 «***Implementare ABSC_ID 1.1.1 attraverso uno strumento automatico***»
 - ABSC_ID 1.1.3 «***effettuare il discovery dei dispositivi collegati alla rete con allarmi in caso di anomalie***»
- Riprogettare e aggiornare l'inventario degli asset informatici dei LNS ormai obsoleto e poco pratico 

Motivazioni

- La versione precedente dell'inventario era basata su un database + Arpwatch: alla scoperta di un nuovo mac address il sistema inseriva l'host nel database, associandolo ad un utente.
 - poche informazioni associabili all'host (IP, OS, Owner, mac address)
 - nessuna aggregabilità delle informazioni
 - Impossibile definire gruppi di host e responsabili
 - monitoraggio degli host attivi poco affidabile

Strumenti utilizzati

Per il monitoraggio:

- **ntopng**: strumento di discovery in tempo reale sviluppato dal team di *ntop* del prof. Luca Deri (UniPI)

Per la gestione degli asset:

- **Insight**: plugin della suite Atlassian Jira Service Management (ex Jira Service Desk) già in uso presso varie sezioni e laboratori dell'INFN.
- **Script python** su macchina pivot

ntopng: hosts attivi



- Dashboard
- Alerts
- Flows
- Hosts**
- Interface
- System
- Settings
- Developer
- Help

eth0

2.70 Mbit/s

2.90 Mbit/s

6

22,887 Flows

659

91

553 Devices

30,081 Flows

Q

Search



Devices

100
Filter Macs
Manufacturer
Device Type

Mac Address	Manufacturer	Device Type	Name	Hosts	ARP	Seen Since	Breakdown	Throughput	Traffic
00:0D:A2:BC:00:8E	Infra Technologies, Inc.	Computer	RES-C7-83-D4	1	318,938,030	133 days, 18:56:17	Sent	7.39 kbit/s	17.83 GB
D8:9E:F3:96:24:19	Dell Inc.	Computer	DESKTOP-JGG69EM	1	57,860,590	58 days, 04:24:55	Sent	75.91 kbit/s	3.43 GB
EC:D6:8A:01:ED:2B	Shenzhen JMicon Intelligent Technology Developmen	Unknown	EC:D6:8A:01:ED:2B	0	18,887,203	133 days, 18:56:17	Sent	383.89 bit/s	1.06 GB
08:F1:EA:80:79:4C	Hewlett Packard Enterprise	Computer	DESKTOP-SF84955	0	18,511,083	133 days, 18:56:15	Sent	0 bit/s	1.04 GB
EC:D6:8A:01:EE:C5	Shenzhen JMicon Intelligent Technology Developmen	Unknown	EC:D6:8A:01:EE:C5	0	12,330,798	133 days, 18:56:16	Sent	1.73 kbit/s	705.66 MB
08:2E:5F:1B:0A:87	Hewlett Packard	Computer	WORKGROUP	3	8,170,098	133 days, 18:56:17	Sent	191.95 bit/s	1.13 GB
00:04:96:83:60:84	Extreme Networks, Inc.	Router/Switch	00:04:96:83:60:84	0	7,474,133	133 days, 18:56:10	Sent	1.44 kbit/s	427.46 MB
00:04:96:9D:3A:2E	Extreme Networks, Inc.	Router/Switch	vr-mgmt.9d3a2e	1	6,081,988	133 days, 18:56:10	Sent	34.33 kbit/s	24.18 GB
2C:B8:ED:85:F4:98	SonicWall	Router/Switch	2C:B8:ED:85:F4:98	12	5,495,506	133 days, 18:56:17	Sent	191.95 bit/s	3.51 GB

ntopng web gui: host attivi

ntopng: hosts attivi



- Dashboard
- Alerts
- Flows
- Hosts**
- Interface
- System
- Settings
- Developer
- Help

eth0

2.70 Mbit/s

2.90 Mbit/s

6

22,887 Flows

659

91

553 Devices

30,081 Flows

Devices

100
Filter Macs
Manufacturer
Device Type

Mac Address	Manufacturer	Device Type	Name	Hosts	ARP	Seen Since	Breakdown	Throughput	Traffic
00:0D:A2:BC:00:8E	Infra Technologies, Inc.	Computer	RES-C7-83-D4	1	318,938,030	133 days, 18:56:17	Sent	7.39 kbit/s	17.83 GB
D8:9E:F3:96:24:19	Dell Inc.	Computer	DESKTOP-JGG69EM	1	57,860,590	58 days, 04:24:55	Sent	75.91 kbit/s	3.43 GB
EC:D6:8A:01:ED:2B	Shenzhen JMicon Intelligent Technology Developmen	Unknown	EC:D6:8A:01:ED:2B	0	18,887,203	133 days, 18:56:17	Sent	383.89 bit/s	1.06 GB
08:F1:EA:80:79:4C	Hewlett Packard Enterprise	Computer	DESKTOP-SF84955	0	18,511,083	133 days, 18:56:15	Sent	0 bit/s	1.04 GB
EC:D6:8A:01:EE:C5	Shenzhen JMicon Intelligent Technology Developmen	Unknown	EC:D6:8A:01:EE:C5	0	12,330,798	133 days, 18:56:16	Sent	1.73 kbit/s	705.66 MB
08:2E:5F:1B:0A:87	Hewlett Packard	Computer	WORKGROUP	3	8,170,098	133 days, 18:56:17	Sent	191.95 bit/s	1.13 GB
00:04:96:83:60:84	Extreme Networks, Inc.	Router/Switch	00:04:96:83:60:84	0	7,474,133	133 days, 18:56:10	Sent	1.44 kbit/s	427.46 MB
00:04:96:9D:3A:2E	Extreme Networks, Inc.	Router/Switch	vr-mgmt.9d3a2e	1	6,081,988	133 days, 18:56:10	Sent	34.33 kbit/s	24.18 GB
2C:B8:ED:85:F4:98	SonicWall	Router/Switch	2C:B8:ED:85:F4:98	12	5,495,506	133 days, 18:56:17	Sent	191.95 bit/s	3.51 GB

ntopng web gui: host attivi

ntopng: hosts attivi



- Dashboard
- Alerts
- Flows
- Hosts**
- Interface
- System
- Settings
- Developer
- Help

eth0

2.70 Mbit/s

2.90 Mbit/s

6

22,887 Flows

659

91

553 Devices

30,081 Flows

Devices

100
Filter Macs
Manufacturer
Device Type

Mac Address	Manufacturer	Device Type	Name	Hosts	ARP	Seen Since	Breakdown	Throughput	Traffic
00:0D:A2:BC:00:8E	Infra Technologies, Inc.	Computer	RES-C7-83-D4	1	318,938,030	133 days, 18:56:17	Sent	7.39 kbit/s	17.83 GB
D8:9E:F3:96:24:19	Dell Inc.	Computer	DESKTOP-JGG69EM	1	57,860,590	58 days, 04:24:55	Sent	75.91 kbit/s	3.43 GB

eth0

2.70 Mbit/s

3.10 Mbit/s

6

22,860 Flows

611

67

532 Devices

29,843 Flows

Mac: D8:9E:F3:96:24:19
Packets

Mac Address	D8:9E:F3:96:24:19 (Dell_96:24:19) [Show Hosts]		Computer
IP Address	172.16.14.250		
Name	DESKTOP-JGG69EM		Host Pool: Not Assigned
Device Type	Computer		
First / Last Seen	21/03/2022 10:10:28 [58 days, 04:33:13 ago]		18/05/2022 15:43:34 [00:07 ago]
Sent vs Received Traffic Breakdown	Sent		
First Observed On	04/02/2020 16:12:03		
Traffic Sent / Received	59,720,139 Pkts / 3.4 GB		1,411 Pkts / 155.4 KB
Address Resolution Protocol	ARP Requests	ARP Replies	
	57,939,298 Sent / 6 Received	15 Sent / 470 Received	

ntopng: hosts attivi



- Dashboard
- Alerts
- Flows
- Hosts**
- Interface
- System
- Settings
- Developer
- Help

eth0

2.70 Mbit/s

2.90 Mbit/s

6

22,887 Flows

659

91

553 Devices

30,081 Flows

Devices

100
Filter Macs
Manufacturer
Device Type

Mac Address	Manufacturer	Device Type	Name	Hosts	ARP	Seen Since	Breakdown	Throughput	Traffic
00:0D:A2:BC:00:8E	Infra Technologies, Inc.	Computer	RES-C7-83-D4	1	318,938,030	133 days, 18:56:17	Sent	7.39 kbit/s	17.83 GB
D8:9E:F3:96:24:19	Dell Inc.	Computer	DESKTOP-JGG69EM	1	57,860,590	58 days, 04:32:45	Sent	75.91 kbit/s	3.43 GB

eth0

2.70 Mbit/s

3.10 Mbit/s

6

22,860 Flows

611

67

532 Devices

29,843 Flows

Mac: D8:9E:F3:96:24:19
Packets

Mac Address

D8:9E:F3:96:24:19 (Dell_96:24:19) [Show Hosts]

Computer

IP Address

172.16.14.250

Name

DESKTOP-JGG69EM

Host Pool: Not Assigned

Device Type

Computer

First / Last Seen

21/03/2022 10:10:28 [58 days, 04:33:13 ago]

18/05/2022 15:43:34 [00:07 ago]

Sent vs Received Traffic Breakdown

Sent

First Observed On

04/02/2020 16:12:03

Traffic Sent / Received

59,720,139 Pkts / 3.4 GB

1,411 Pkts / 155.4 KB

Address Resolution Protocol

ARP Requests

ARP Replies

Insight


INFN Service Desk

Dashboards ▾
Projects ▾
Issues ▾
Insight ▾
Create

Search

Search objects
Overview
Graph
Object Schema ▾

LNS IT Asset
Object Schema for LNS IT

Search object types

- People&Groups
- Network Assets
- Datacenter
- Datacenter Portopalo
- Datacenter Porto
- CdC Electronics Asset
- ntop discovered hosts
- Discovered hosts (1168)
- Location (41)

Discovered hosts
Gli host scoperti dai discovery con NTOP

Filter Search
Advanced
50

Create Object
Objects
Attributes
Graph
Object Type ▾

Name ↕

- IOMV-LNS-SHARE-Services - SMB/CIFS
- Ipc-cirrone-01 [18:31:bf:cc:26:0d]
- "fisichella-lns [34:17:eb:a7:ed:4d]
- #macbook-pro-di-davide-bandieramonte
- \$50-34-10-70.1 Time Capsule di ASFIN2
- %BrukerPSCU2-2 Web-based Configuration
- 'CONTROLTARGETPC Web-based Configuration
- 'Desktop remoto di ciccio su smo-analisi
- 'DESKTOP-JI9TI0J Web-based Configuration
- 'INFN-7C6DE106A0 Web-based Configuration

LNS IT Asset / ... / Discovered hosts / LNSIT05-7939
IOMV-LNS-SHARE-Services - SMB/CIFS

Edit
Comment
More ▾
Object Graph

Details

- Name IOMV-LNS-SHARE-Services - SMB/CIFS
- IP 172.16.50.23
- hostName IOMV-LNS-SHARE-Services - SMB/CIFS
- MAC_ADDRESS F8:BC:12:72:3C:A5
- Registered OK

Activity

- Comments History

There are no comments yet on this object

Comment

Dates

- Created 26/Mar/20 18:18
- Updated 12/Feb/21 16:59

Inbound References

- 1 Computer

Attachments

Drop files to attach
The maximum File upload size is 10.0 MB.

Attach Files

There are no attachments

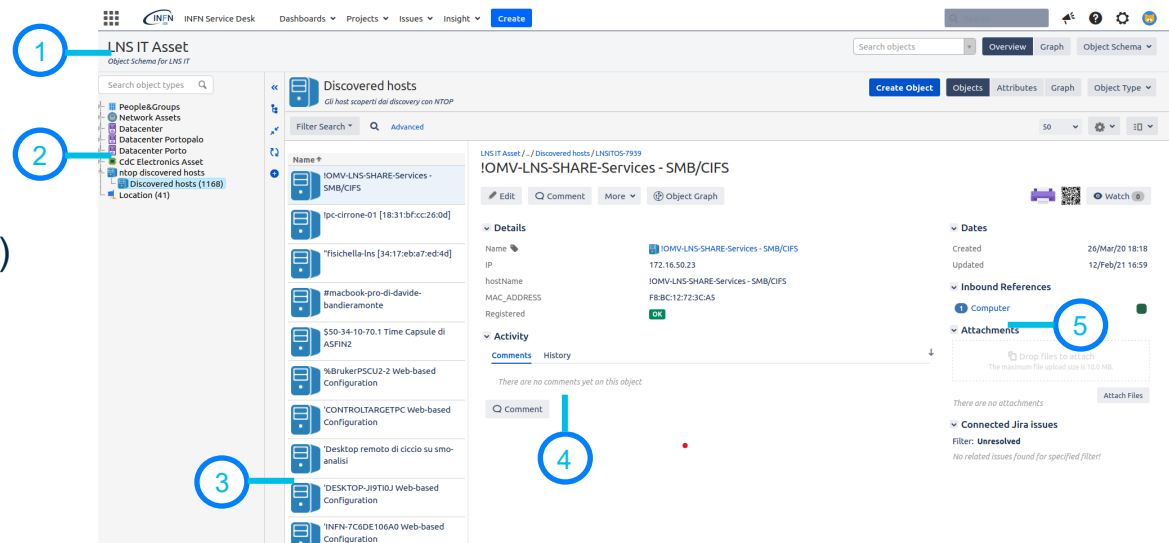
Connected Jira issues

Filter: **Unresolved**

No related issues found for specified filter!

Insight

1. **Object schema:** il nome del Progetto
2. **Object types:** containers per i vari oggetti ognuno con le proprie caratteristiche (attributi)
3. **Objects:** l'asset vero e proprio
4. **Attributes:** caratteristiche che definiscono l'oggetto
5. **References:** relazioni e dipendenze fra oggetti



Insight web gui

ntopInsight

- *ntopInsight è un sistema costituito da un insieme di script in linguaggio python che interfacciano in modo sicuro ntopng e Insight, allo scopo di monitorare lo stato di attività della rete locale dei Laboratori Nazionali del Sud e nello stesso tempo realizzare un inventario degli asset informatici attivi che venga riempito ed aggiornato in maniera automatica.*
- **Crea corrispondenza tra attributi di ntopng ed Insight**
- **Partendo dai template IT predefiniti di Insight, è stato definito un personale Object Schema per riflettere l'organizzazione logica degli host LNS e gli attributi ritenuti utili**

ntopInsight vs Insight Discovery

- Insight Discovery: strumento di scanning della rete, estrae dettagliate informazioni per ogni asset che possono essere importate nel db di Insight.
- Vantaggio: sistema di inventario è integrato con il sistema di monitoraggio; versione con *agent* e *agent-less* per host non sempre on-line
- Svantaggio: deve essere installato nella rete da monitorare, mentre l'istanza in uso INFN è installata on-premise sui server nazionali

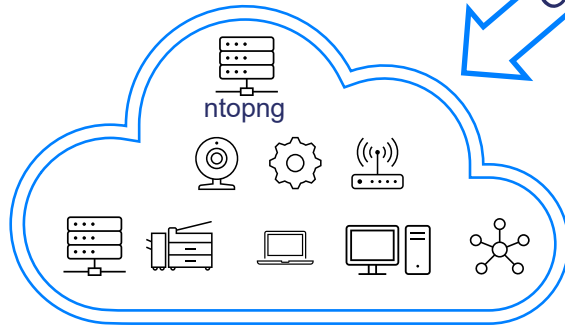
ntopInsight: REST-API

- ntopng ed Insight usano REST-API per l'integrazione con applicazioni standalone o web.
- Forniscono accesso alle risorse via percorsi URI per identificare una risorsa.
- Le REST API di Insight ed ntopng usano JSON come formato di comunicazione e i metodi standard HTTP (GET, PUT, POST, DELETE)
- L'autenticazione ed autorizzazione all'accesso avviene tramite Personal Access Token.

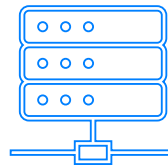
ntopInsight: schema

ntopng endpoint – API Version 2.0

- Download host attivi:
http://localhost:3000/luad/do_export_data.lua



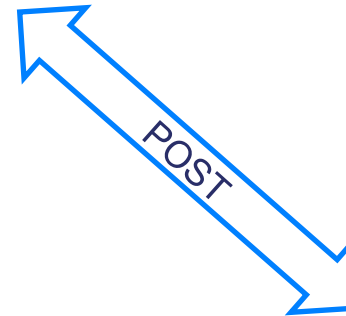
Rete LNS



Macchina pivot

Insight endpoint – API Version 1.0

- Creazione degli oggetti:
<https://servicedesk.infn.it/rest/insight/1.0/object/create>



Insight

ntopInsight

- Definisce una corrispondenza tra attributi di ntopng e quelli richiesti in Insight
- La macchina pivot:
 - Schedula ed esegue gli script per la comunicazione tra ntopng e Insight ed il download/upload dei dati
 - Esegue manipolazioni e controlli sui dati
 - Contiene la copia principale dell'inventario, ovvero la lista degli host sotto forma di file json. La stessa copia esiste anche su Insight.
- I risultati dei task che vengono eseguiti sulla copia locale del json vengono trasferiti giornalmente su Insight.
- Vantaggi di questo approccio:
 - Limitazione degli accessi su Insight
 - Possibilità di effettuare facilmente tutte le manipolazioni ed i controlli del file json via script python
 - Indipendenza da Insight

ntopInsight: attributi

```
"hosts": {
  "172.16.98.110": {
    "bridge.ingress_drops.packets": 0,
    "udp.bytes.rcvd": 255,
    "throughput_trend_pps": 3,
    "seen.last": 1581583793,
    "is_broadcast": false,
    "childSafe": false,
    "tcp.packets.lost": 0,
    "drop_all_host_traffic": false,
    "tcp.packets.out_of_order": 0,
    "tcp.packets.rcvd": 29,
    "tcp.packets.retransmissions": 0,
    "other_ip.bytes.rcvd": 0,
    "duration": 751674,
    "systemhost": false,
    "dhcpHost": true,
    "os": "",
    "icmp.packets.sent": 0,
    "country": "",
    "throughput_pps": 0,
    "asn": 0,
    "tcp.bytes.rcvd": 2146,
    "other_ip.packets.sent": 0,
    "ip": "172.16.98.110",
    "has_blocking_shaper": false,
    "seen.first": 1580832120,
    "privatehost": true,
    "bridge.egress_drops.packets": 0,
    "tcp.packets.sent": 0,
    "flows.as_client": 1633,
    "asname": "",
    "active_http_hosts": 0,
    "active_flows.as_client": 1,
    "local_network_name": "172.16.0.0/16",
    "icmp.bytes.rcvd": 0,
    "bytes.sent": 393239,
    "city": "",
    "vlan": 0,
    "devtype": 3,
    "longitude": 0,
    "hiddenFromTop": false,
    "icmp.packets.rcvd": 0,
    "is_blacklisted": false,
    "bytes.rcvd": 2401,

```

Estratto del json di ntopng

```
"172.16.62.75": {
  "name": "SL1",
  "mac": "00:80:F4:E4:7C:C1",
  "ip": "172.16.62.75",
  "seen.first": "Thu May 12 15:01:42 2022",
  "seen.last": "Thu May 12 15:06:30 2022"
},
"172.16.30.241": {
  "name": "iDRAC-JPCR1H2",
  "mac": "54:48:10:F7:E4:A2",
  "ip": "172.16.30.241",
  "seen.first": "Mon May 16 14:45:15 2022",
  "seen.last": "Mon May 16 14:45:15 2022"
},
"172.16.15.80": {
  "name": "172.16.15.80",
  "mac": "98:F2:B3:07:9B:2",
  "ip": "172.16.15.80",
  "seen.first": "Mon May 16 20:04:55 2022",
  "seen.last": "Mon May 16 20:04:55 2022"
},
"172.16.20.80": {
  "name": "MBP-di-Giuseppe",
  "mac": "A0:CE:C8:F3:F1:7",
  "ip": "172.16.20.80",
  "seen.first": "Mon May 16 20:04:55 2022",
  "seen.last": "Mon May 16 20:04:55 2022"
},
"172.16.15.225": {
  "name": "km3ceph-01",
  "mac": "54:A0:50:88:94:7",
  "ip": "172.16.15.225",
  "seen.first": "Mon May 16 20:04:55 2022",
  "seen.last": "Mon May 16 20:04:55 2022"
},
"172.16.31.16": {
  "name": "DOMINO_1BC2",
  "mac": "00:D0:F3:02:1B:C2",
  "ip": "172.16.31.16",
  "seen.first": "Mon May 16 21:08:00 2022",

```

json di ntopng filtrato

LNSIT Asset / .. / Discovered hosts / LNSITOS-11880

DESKTOP-K5ISN30

Edit Comment More Object Graph

Details

Name	DESKTOP-K5ISN30
IP	172.16.15.140
hostName	DESKTOP-K5ISN30
MAC_ADDRESS	8C:16:45:E2:9E:C5
seen first	Wed Apr 27 08:07:39 2022
seen last	Wed Apr 27 08:48:40 2022

ntopInsight

Le REST API usano file json come formato di comunicazione, pertanto nella creazione di un oggetto su Insight il campo *data* dei metodi HTTP deve contenere il json nel corretto formato indicando:

- Il *typeld* dell'oggetto

- *Il typeld è identificabile dalla url del service desk nel momento in cui si crea un oggetto template dalla web gui*

- Tutti gli attributi identificati dal loro ID

- *Per ogni attributo creato nella web gui, Insight genererà un ID che andrà scritto nel json per la creazione o modifica via REST API dell'oggetto*

ntopInsight

Ad esempio gli oggetti LNS con *typeId* = 575 sono definiti dagli attributi di interesse

Attributo	Id
name	2319
IP	2339
hostname	2340
mac address	2341
seen first	3606
seen last	3607

```
{
  "attributes": [
    {
      "objectTypeAttributeId": 2319,
      "objectAttributeValues": [
        {
          "value": "DESKTOP-K5ISN30"
        }
      ]
    },
    {
      "objectTypeAttributeId": 2339,
      "objectAttributeValues": [
        {
          "value": "172.172.172.172"
        }
      ]
    },
    {
      "objectTypeAttributeId": 2340,
      "objectAttributeValues": [
        {
          "value": "DESKTOP-K5ISN30"
        }
      ]
    },
    {
      "objectTypeAttributeId": 2341,
      "objectAttributeValues": [
        {
          "value": "8C:16:45:E2:9E:C5"
        }
      ]
    },
    {
      "objectTypeAttributeId": 3606,
      "objectAttributeValues": [
        {
          "value": "Fri Sep 17 09:42:05 2021"
        }
      ]
    },
    {
      "objectTypeAttributeId": 3607,
      "objectAttributeValues": [
        {
          "value": "Fri Sep 17 12:23:30 2021"
        }
      ]
    }
  ]
},
"objectTypeId": 575
}
```

ntopInsight: processi schedulati

Macchina pivot: script schedulati giornalieri

- Con frequenza fissa (10 min) interroga ntopng: genera e conserva istantanee (json) filtrate, degli host attivi @LNS

Macchina pivot: script schedulati giornalieri

- Tra un download ed il successivo viene effettuato il confronto tra il json storico locale ed il nuovo json che può contenere o meno nuovi host

Macchina pivot: script schedulati giornalieri – nuovi host trovati

- Viene aggiornato il json locale
- Creazione nuovo file json contenente solo i nuovi host del giorno
- Notifiche mail a SD agent (validazione findings in tempo reale)

Macchina pivot: script schedulati giornalieri

- Fine giornata lavorativa viene effettuato l'upload su Insight

ntopInsight: attività SD agent

Agente Service Desk: notifiche mail

- Riceve notifiche sui nuovi host in tempo reale (effettua controlli del caso su eventuali anomalie)



Agente Service Desk: notifiche mail

- Riceve notifiche sugli host di cui è stato fatto l'upload su Insight



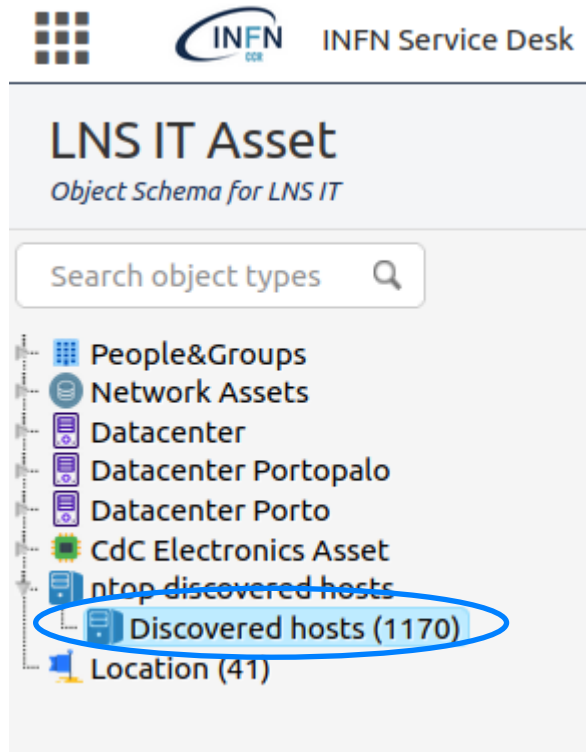
Agente Service Desk: organizza l'inventario

- etichetta organizza ed assegna i nuovi host nei vari rami dell'inventario
- Crea dipendenze e relazioni : aggregabilità delle informazioni

ntopInsight: popolamento

Discovered hosts

Discovered hosts



Attributi del nuovo oggetto

LNSITAsset / .. / Discovered hosts / LNSITOS-11880

DESKTOP-K5ISN3O

[Edit](#) [Comment](#) [More](#) [Object Graph](#)

Details

Name	DESKTOP-K5ISN3O
IP	172.16.15.140
hostName	DESKTOP-K5ISN3O
MAC_ADDRESS	8C:16:45:E2:9E:C5
seen first	Wed Apr 27 08:07:39 2022
seen last	Wed Apr 27 08:48:40 2022

ntopInsight

Tutti i nuovi oggetti vanno collocati nel ramo *Discovered hosts*, successivamente, guidato dalle notifiche, l'agente del service desk procede manualmente all'assegnazione della risorsa di rete creando così tutte le relazioni e le dipendenze tra gli oggetti

In ogni caso il ramo *Discovered hosts* contiene la situazione aggiornata degli host attivi.

LNS IT Asset
Object Schema for LNS IT

Search object types

- People&Groups
 - Utenti (109)
 - Workgroup (28)
- Network Assets
 - Host
 - Computer (97)
 - Experiment computer (20)
 - Laptop wired (21)
 - Printer (23)
 - Experiment Printer (1)
 - Experiment Instruments (10)
 - Other device (22)
 - IP camera (47)
 - Switch (3)
 - Hypervisor (4)
 - Virtual Machine (10)
 - Server (6)
 - Out of Band (2)
 - Rack
 - AccessPoint (32)
 - Firewall (2)
 - Asset Details
 - Datacenter
 - Datacenter Portopalo
 - Datacenter Porto
 - CdC Electronics Asset
 - ntop discovered hosts
 - Discovered hosts (1170)
 - Location (41)

Discovered hosts
Gli host scoperti dai discovery con NTOP

Filter Search Advanced

Name
!OMV-LNS-SHARE-Services - SMB/CIFS
!pc-cirrone-01 [18:31:bf:cc:26:0d]
*fisichella-Ins [34:17:eb:a7:ed:4d]
#macbook-pro-di-davide-bandieramonte
\$50-34-10-70.1 Time Capsule di ASFIN2
%BrukerPSCU2-2 Web-based Configuration
*CONTROLTARGETPC Web-based Configuration
*Desktop remoto di ciccio su smo-analisi
*DESKTOP-JI9TI0J Web-based Configuration
*INFN-7C6DE106A0 Web-based Configuration
050-34-10-70.1 AirPort Time

LNS IT Asset / - / Discovered hosts / LNSITOS-7939

!OMV-LNS-SHARE-Services -

Edit Comment More

Details

Name

IP 1

hostName !

MAC_ADDRESS F

Registered

Activity

Comments History

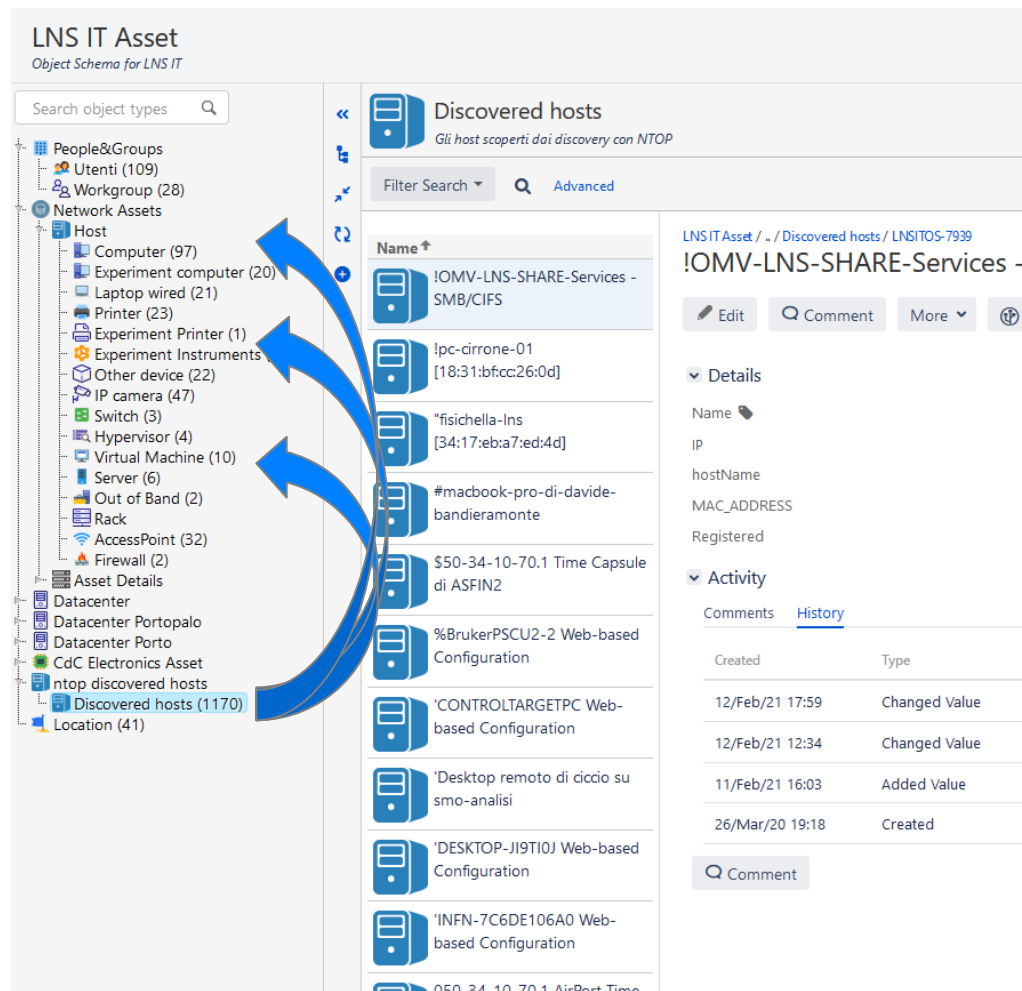
Created	Type
12/Feb/21 17:59	Changed Value
12/Feb/21 12:34	Changed Value
11/Feb/21 16:03	Added Value
26/Mar/20 19:18	Created

Comment

ntopInsight

Tutti i nuovi oggetti vanno collocati nel ramo *Discovered hosts*, successivamente, guidato dalle notifiche, l'agente del service desk procede manualmente all'assegnazione della risorsa di rete creando così tutte le relazioni e le dipendenze tra gli oggetti

In ogni caso il ramo *Discovered hosts* contiene la situazione aggiornata degli host attivi.



LNS IT Asset
Object Schema for LNS IT

Search object types

- People&Groups
 - Utenti (109)
 - Workgroup (28)
- Network Assets
 - Host
 - Computer (97)
 - Experiment computer (20)
 - Laptop wired (21)
 - Printer (23)
 - Experiment Printer (1)
 - Experiment Instruments
 - Other device (22)
 - IP camera (47)
 - Switch (3)
 - Hypervisor (4)
 - Virtual Machine (10)
 - Server (6)
 - Out of Band (2)
 - Rack
 - AccessPoint (32)
 - Firewall (2)
 - Asset Details
 - Datacenter
 - Datacenter Portopalo
 - Datacenter Porto
 - CdC Electronics Asset
 - ntop discovered hosts
 - Discovered hosts (1170)
 - Location (41)

Discovered hosts
Gli host scoperti dai discovery con NTOP

Filter Search Advanced

Name

- !OMV-LNS-SHARE-Services - SMB/CIFS
- lpc-cirrone-01 [18:31:bf:cc:26:0d]
- *fisichella-Ins [34:17:eb:a7:ed:4d]
- #macbook-pro-di-davide-bandieramonte
- \$50-34-10-70.1 Time Capsule di ASFIN2
- %BrukerPSCU2-2 Web-based Configuration
- *CONTROLTARGETPC Web-based Configuration
- *Desktop remoto di ciccio su smo-analisi
- *DESKTOP-JI9TI0J Web-based Configuration
- *INFN-7C6DE106A0 Web-based Configuration
- 050-34-10-70.1 AirPort Time

LNS IT Asset / - / Discovered hosts / LNSITOS-7939

!OMV-LNS-SHARE-Services -

Edit Comment More

Details

Name

IP 1

hostName !

MAC_ADDRESS F

Registered

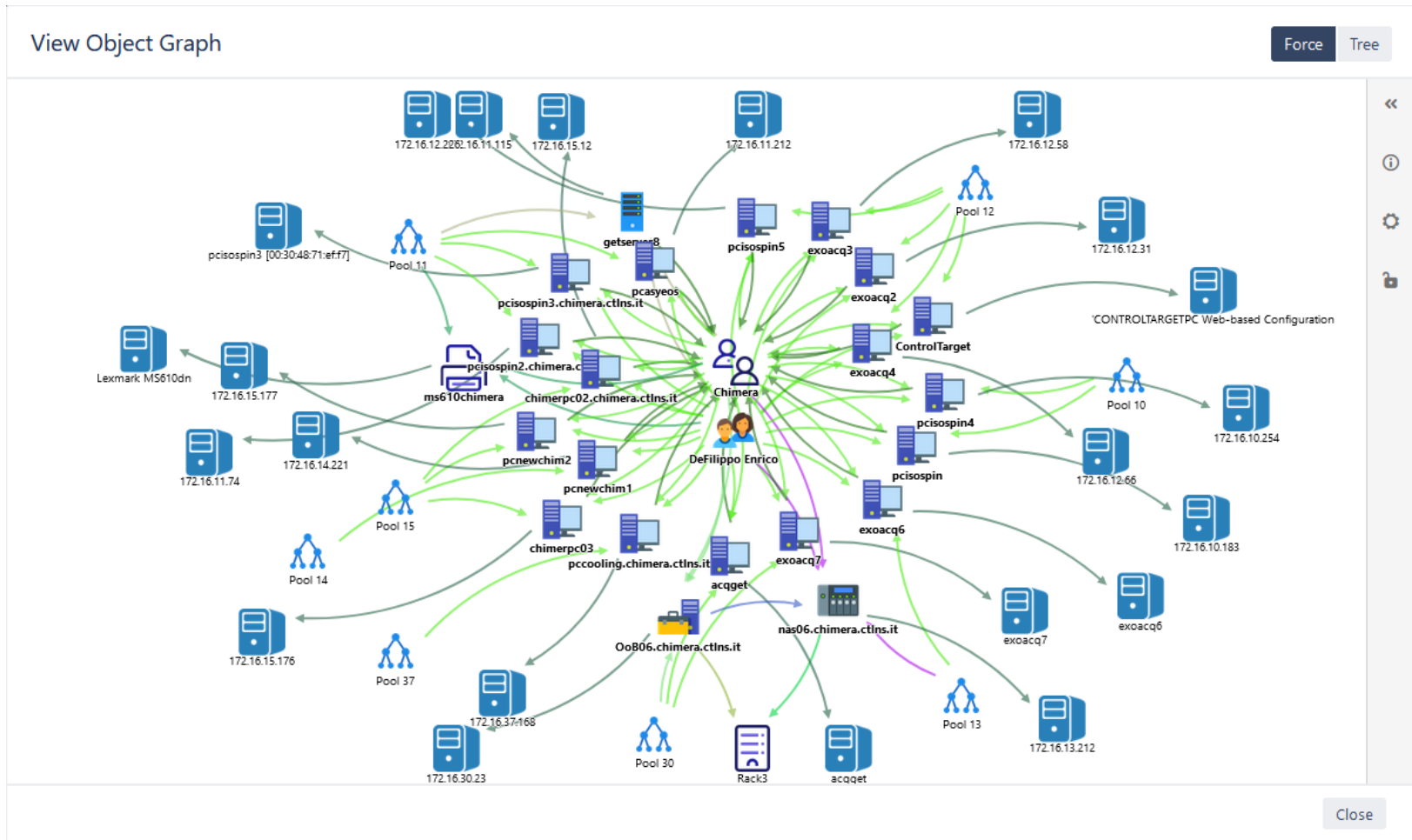
Activity

Comments History

Created	Type
12/Feb/21 17:59	Changed Value
12/Feb/21 12:34	Changed Value
11/Feb/21 16:03	Added Value
26/Mar/20 19:18	Created

Comment

ntopInsight aggregabilità: esempio esperimento Chimera



Sviluppi futuri

- **Macchina pivot: script schedulati con minor frequenza**
 - Confronto informazioni tra la lista degli host locale e ultimi download per verificare
 - Congruenza ip-mac address
 - Last seen (host non più attivi)
- Migliore leggibilità degli hostname attraverso DNS locale (per adesso ntop rileva IP o NetBIOS)

Grazie

