Grau en Enginyeria Informàtica de Gestió i Sistemes d'Informació

MONITORBYTE: IMPLEMENTACIÓ D'UN SISTEMA DE MONITORITZACIÓ DE XARXA

Memòria

IVAN CAROL NAVAS

TUTORS: DR. LÉONARD JANER GARCIA
PERE BARBERAN AGUT

2022-2023

Dedicatòria

Dedico aquest treball a la meva família, en especial a la meva mare i avis materns.

També al meu professor i tutor Dr. Léonard Janer Garcia que ens ha deixat aquest any.

Agraïments

Vull agrair la confiança de Bytemaster per haver acceptat la col·laboració per dur a terme aquest projecte.

També al professorat del Tecnocampus per la docència durant el grau. En especial al Dr. Léonard Janer Garcia i Pere Barberan Agut per la seva ajuda durant la tutorització del projecte.

Resum

En l'actualitat, les infraestructures informàtiques són un pilar fonamental per les empreses. Aquestes solen estar en entorns controlats en els centres de processament de dades (CPD) i són crítiques. Necessiten estar sempre operatives. Per garantir la seva estabilitat, són necessaris en els sistemes de monitorització de xarxa. Aquest projecte consisteix en la implementació d'un software de monitorització compatible amb els protocols SNMP i IPFIX en la infraestructura de xarxa d'una empresa.

Resumen

En la actualidad, las infraestructuras informáticas son un pilar fundamental para las empresas. Estas suelen estar en entornos controlados en los centros de procesamiento de datos (CPD) y son críticas. Necesitan estar siempre operativas. Para garantizar su estabilidad, son necesarios sistemas de monitorización de red. Este proyecto consiste en la implementación de un software de monitorización compatible con los protocolos SNMP e IPFIX en la infraestructura de red de una empresa.

Abstract

Currently, IT infrastructures are a fundamental pillar for businesses. These are usually located in controlled environments in data centers and are critical. They need to be always operational. To ensure their stability, network monitoring systems are necessary. This project involves the implementation of monitoring software compatible with SNMP and IPFIX protocols in the network infrastructure of a company.

Índex

Índex de Figures

1. Introducció

Aquest projecte de fi de grau pretén ampliar la monitorització de la xarxa del CPD[1] de l'empresa BYTEMASTER SERVICIOS INFORMÁTICOS S.A. [1] per tal d'obtenir informació fiable per identificar i resoldre incidències més fàcilment.

Les empreses amb una infraestructura informàtica pròpia tenen el repte de gestionar-la i mantenir-la operativa per poder realitzar les seves activitats de negoci. Les empreses que ofereixen un SaaS[2], sobretot, necessiten tenir-la operativa les 24 hores del dia els 365 dies de l'any. Això provoca que qualsevol incidència o problema en la infraestructura que comprometi els seus serveis té un gran impacte en l'usuari final.

Així doncs, és imprescindible poder tenir indicadors que mostrin l'estat de la infraestructura. Aquests indicadors els poden proporcionar els sistemes de monitorització, per això són necessaris i útils. De sistemes de monitorització hi ha diferents tipus i poden utilitzar diferents protocols. Però l'objectiu sempre és el mateix, recollir informació d'equips (ús de CPU[3], ús de RAM[4], energia consumida, latències...) a temps real i guardar aquesta informació durant un període de temps determinat. D'aquesta manera es poden consultar les dades a temps real i amb anterioritat.

Les empreses no sempre disposen d'un sistema o sistemes de monitorització a l'alçada de la complexitat de la seva infraestructura. La raó és que per realitzar una bona implementació, a part d'escollir adequadament el *software*, s'ha de conèixer en profunditat la infraestructura i els seus serveis. A més, s'ha de dedicar força temps en validar la implementació. Això es tradueix en un cost que no sempre les empreses estan disposades a pagar.

[1] Centre de processament de dades
[2] Software as a service
[3] Central Processing Unit
[4] Random Access Memory

2. Marc teòric i anàlisi de referents

2.1 Context

Per tal d'entendre la infraestructura del CPD de Bytemaster s'ha estudiat les activitats de l'empresa i els serveis que aquesta manté.

Bytemaster és una empresa la qual la seva activitat principal és proporcionar un ERP[1], el "_b first". És un *software* que té present la cadena de processos d'un operador logístic i centralitza la seva gestió. A part, Bytemaster proporciona l'entorn "BOL", el qual és un entorn d'escriptori virtual *Windows* on els usuaris poden realitzar les tasques diàries del seu lloc de treball; gestió de correu, navegació i programes ofimàtics. També, el *software* "_b first" està disponible en aquests escriptoris virtuals i és la forma habitual d'accedir-hi. Actualment, el servei "BOL" té 3500 usuaris nominals i màxims de 1300 usuaris concurrents.

Altrament, hi ha altres serveis rellevants. Aquest són: sistema centralitzat de veu IP[2] per clients i treballadors, VPNs[3] de punt a punt, connexions "SSL-VPN" de *endpoints* al CPD, còpies de seguretat i *hosting* de webs. Així mateix, tots treballadors de Bytemaster necessiten accedir a recursos del CPD diàriament per poder realitzar les seves tasques diàries.

Tots els serveis són mantinguts per la plataforma en producció que hi ha al CPD i la majoria han d'estar disponibles les 24 hores del dia els 365 dies de l'any. A més a més, per la mateixa naturalesa del negoci dels clients, transitaris i operadors logístics, la inaccessibilitat a la plataforma en qualsevol dia i hora tingui un gran impacte.

Una infraestructura d'un CPD està constituïda per una gran quantitat de dispositius físics que interactuen entre si. A nivell d'infraestructura es pot diferenciar entre dos tipus de dispositius, els de xarxa (*routers*, *firewalls*, *switches* entre d'altres) i els dispositius finals (servidors físics, MVs[4] i cabines d'emmagatzematge entre d'altres). D'una banda, els dispositius de

[1] Enterprise Resource Planning
[2] Internet Protocol
[3] Virtual Private Network
[4] Màquina virtual

xarxa són aquells que proporcionen la interconnexió física dels equips finals perquè es pugin comunicar. També s'encarreguen de la lògica de la interconnexió, és a dir, les regles d'accés i les polítiques de seguretat perimetral entre dispositius finals. D'altra banda, els dispositius finals són aquells que necessiten ser interconnectats i compartir informació entre si. És a dir, són els que proporcionen els serveis necessaris per a l'activitat de l'empresa.

Tots aquests dispositius estan en un entorn compartit, això implica que un mal funcionament d'un d'aquests pot afectar a la resta. Sovint, no és fàcil trobar l'origen del problema o saber quin és. Com a conseqüència, els treballadors encarregats de mantenir la infraestructura poden tardar força en trobar la causa real del problema i començar a plantejar una solució. A més a més, la responsabilitat de la infraestructura sol recaure en diferents departaments i/o equips tècnics dificultant encara més l'eficiència de la resolució de la incidència.

Així doncs, un CPD és un entorn crític on hi ha un gran nombre de serveis convivint al mateix temps. Per mantenir tots aquests serveis són alhora necessaris un gran nombre de dispositius interconnectats entre si. En conseqüència, una falla en aquests pots ser molt difícil de detectar. Per aquest motiu, és necessari tenir un sistema de monitorització que pugui indicar quin és el problema o donar pistes d'on pot provenir.

2.2 Sistemes de monitorització existents

Actualment, Bytemaster ja disposa d'alguns sistemes de monitorització. Són els següents:

- **GMS (Global Management System):** És un *software* propietari del fabricant Sonicwall per gestionar els seus dispositius (principalment *firewalls*) de forma unificada així com la recol·lecció de dades dels dispositius. Concretament a Bytemaster s'utilitza exclusivament com a "Syslog Collector" [2] i s'obté la informació del *firewall* del CPD.

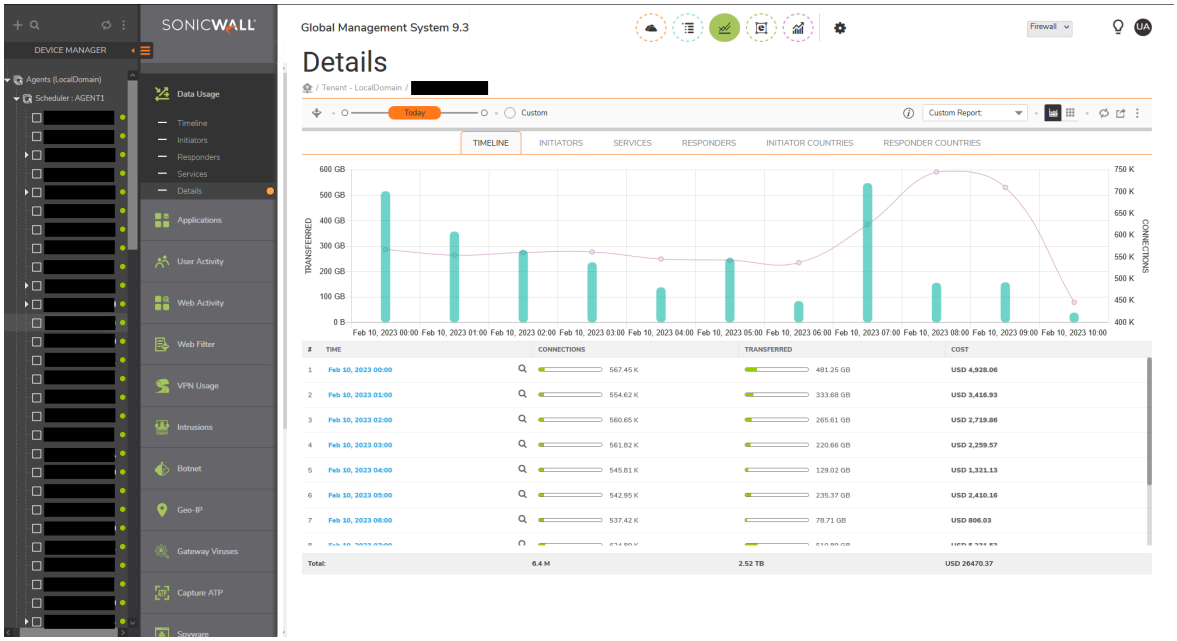


Fig. 2.1: Global Management System (GMS) de Bytemaster. Font: Elaboració pròpia.

- **LibreNMS:** *software open source* utilitzat per la monitorització via SNMP[5] dels equips de xarxa del CPD.

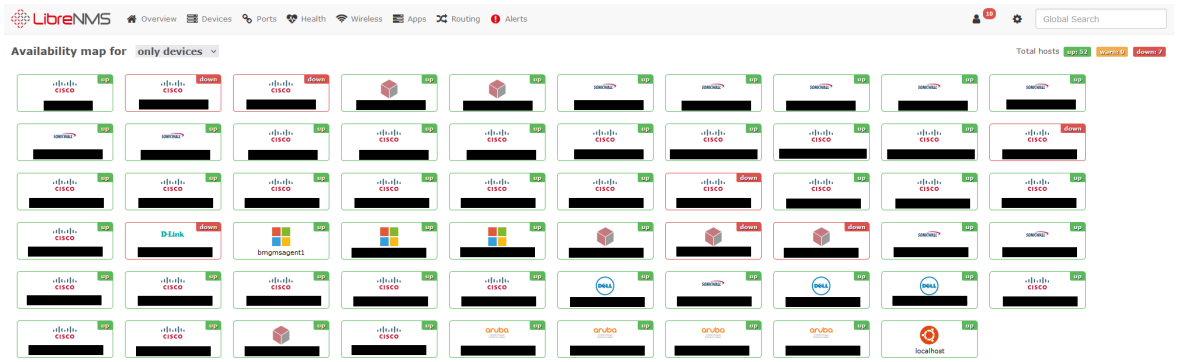


Fig. 2.2: LibreNMS de Bytemaster. Mapa de disponibilitat. Font: Elaboració pròpia.

[5] Simple Network Management Protocol

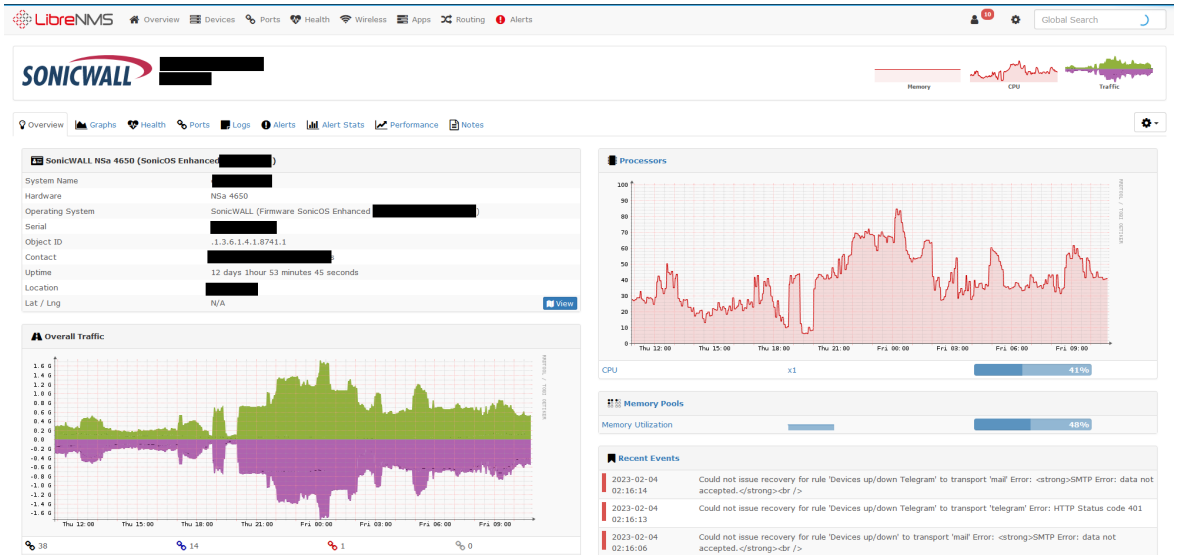


Fig. 2.3: LibreNMS de Bytemaster. Resum d'un *host*. Font: Elaboració pròpia.

- **Nagios Core:** *software open source* utilitzat per monitoritzar via ICMP[6] l'estat dels equips de xarxa i l'enviament d'alertes.

[6]Internet Control Message Protocol

Fig. 2.4: Nagios de Bytemaster. Grups de hosts. Font: Elaboració pròpia.

Aquests tres sistemes de monitorització es consideren insuficients per tal de tenir una visibilitat detallada de la salut de la xarxa del CPD. Falta informació rellevant dels *netflows*[7] del tràfic que travessa el firewall del CPD. A més, la gestió i manteniment dels *softwares open source* "Nagios Core" i "LibreNMS" no són simples ni escalables.

2.3 Topologia del CPD de Bytemaster

Cada empresa disposa d'una infraestructura pròpia i adaptada a les seves necessitats i recursos. Per complir amb els seus objectius, Bytemaster compte amb un *firewall* del fabri-

[7] Fluxos de tràfic IP

cant Sonicwall, model NSA 5700. En la figura 2.5 es poden apreciar les especificacions de l'equip.

Gen 7 NSa Series System Specifications

Firewall	NSa 2700	NSa 3700	NSa 4700	NSa 5700	NSa 6700
Operating system			SonicOS 7		
Interfaces	16x1GbE, 3x10G SFP+, 2 USB 3.0, 1 Console, 1 Mgmt. port	24x1GbE, 6x10G SFP+, 4x5G SFP+, 2 USB 3.0, 1 Console, 1 Mgmt. port	6 x 10G/5G/2.5G/1G (SFP+); 24 x 1GbE Cu 2 USB 3.0, 1 Console, 1 Mgmt. port	6 x 10G/5G/2.5G/1G (SFP+); 2x 10G/5G/2.5G/1G (Cu); 24 x 1GbE Cu 2 USB 3.0, 1 Console, 1 Mgmt. port	2x40G; 8x25G, 4 x10G/5G/2.5/1G SFP+, 4 x 10G/5G/2.5G/1G (Cu); 16 x 1GbE (Cu) 2 USB 3.0, 1 Console, 1 Mgmt. port
Storage	64GB M.2	128GB M.2	128GB	128GB	256GB M.2
Expansion	Storage Expansion Slot (Up to 256GB)	Storage Expansion Slot (Up to 256GB)	Storage Expansion Slot (Up to 1TB)	Storage Expansion Slot (Up to 1TB)	Storage Expansion Slot (Up to 1TB)
Logical VLAN and tunnel interfaces (maximum)	256	256	512	512	512
SSO Users	40,000	40,000	50,000	50,000	70,000
Access points supported (maximum)	512	512	512	512	512
Firewall/VPN Performance					
Firewall inspection throughput[1]	5.2 Gbps	5.5 Gbps	18 Gbps	28 Gbps	36 Gbps
Threat Prevention throughput[2]	3.0 Gbps	3.5 Gbps	9.5 Gbps	15 Gbps	19 Gbps
Application inspection throughput[2]	3.6 Gbps	4.2 Gbps	11 Gbps	18 Gbps	20 Gbps
IPS throughput[2]	3.4 Gbps	3.8 Gbps	10 Gbps	17 Gbps	20 Gbps
Anti-malware inspection throughput[2]	2.9 Gbps	3.5 Gbps	9.5 Gbps	16 Gbps	18.5 Gbps
TLS/SSL inspection and decryption throughput (DPI SSL)[2]	800 Mbps	850 Mbps	5 Gbps	7 Gbps	9 Gbps
IPSec VPN throughput[3]	2.10 Gbps	2.2 Gbps	11 Gbps	15 Gbps	19 Gbps
Connections per second	21,000	22,000	115,000	228,000	228,000
Maximum Connections (SPI)	1,500,000	2,000,000	4,000,000	5,000,000	8,000,000
MAX DPI-SSL Connections	125,000	150,000	350,000	350,000	750,000
Maximum connections (DPI)	500,000	750,000	2,000,000	3,500,000	6,000,000

Fig. 2.5: Especificacions del Sonicwall NSA 5700. Font: Elaboració pròpia.

Aquest equip està redundat per un altre firewall idèntic interconnectat directament i funcionen en mode actiu-passiu. És a dir, un dels dos sempre està actiu i realitza totes les taques (reenviament de paquets, inspecció de paquets, taules *cache* d'encaminament...) i l'altre està a l'espera (rol *standby*) d'agafar el rol d'actiu. Quan hi ha un canvi de rol s'anomena "salt de node". Per exemple, si l'equip "actiu" deixés de funcionar correctament. Els salts de node poden produir-se automàticament quan hi ha un mal funcionament o bé es poden provocar manualment. Això és útil per dur a terme tasques de manteniment o actualitzacions dels *firmwares*[8] dels equips sense afectar el servei. Per tal de tenir una redundància efectiva, totes les connexions (cables físics) dels equips estan connectats a *switches* diferents. Les

[8]Bloc d'instruccions de programa per a propòsits específics, gravats en una memòria de tipus no volàtil. Es pot interpretar com un tipus de Sistema Operatiu

interconnexions dels dos equips són simètriques.

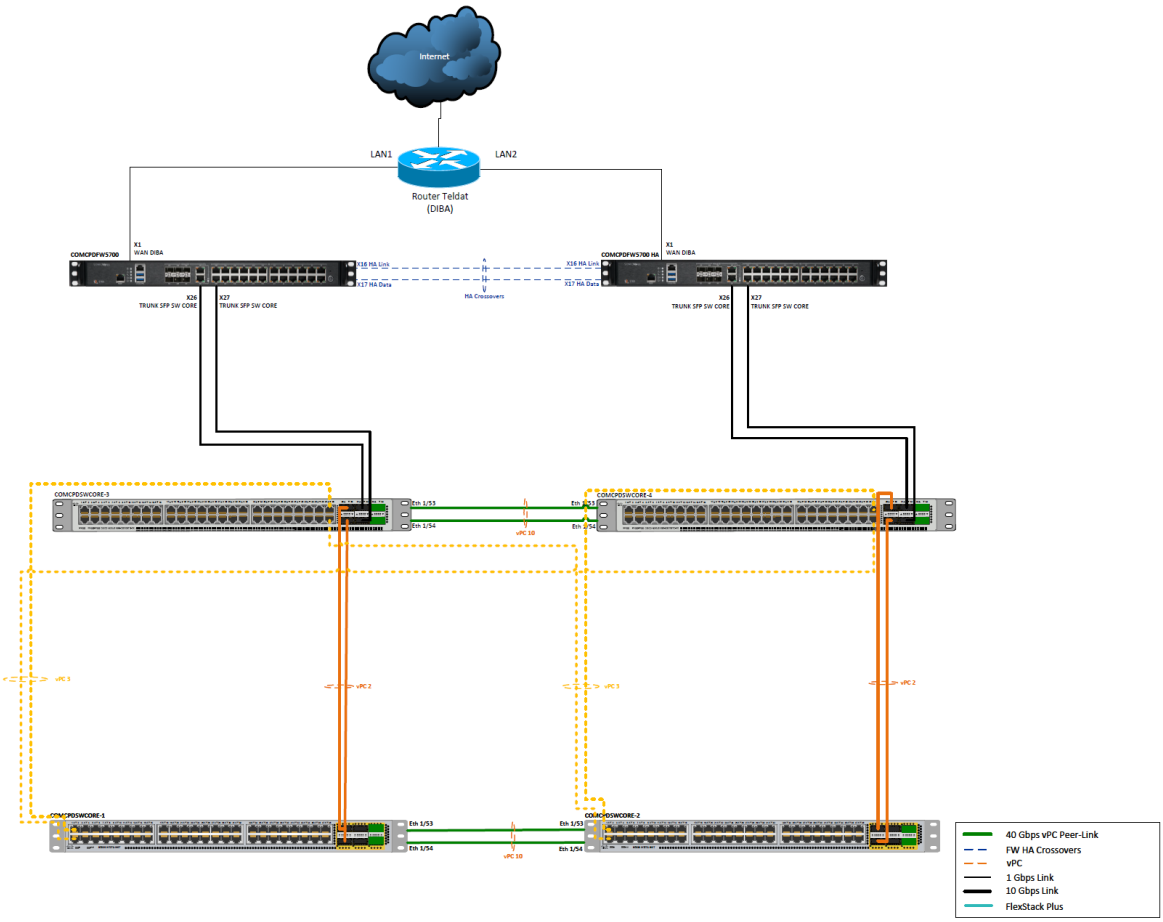


Fig. 2.6: Esquema físic de la topologia del CPD de Bytemaster. Font: Elaboració pròpia.

En la figura 2.6 es pot apreciar com els *firewalls* estan connectats a dos *switches* diferents (COMCPDSWCORE3 i COMCPDSWCORE4). Aquests són dos *switches* Cisco Nexus de la sèrie 9000 (model C93108TC-FX3P). Estan units mitjançant un *vPC domain*[9] que ofereix redundància entre ells. Així mateix, els *switches* COMCPDSWCORE1 i COMCPDSWCORE2 estan connectats als altres de la mateixa forma. Aquests dos últims són *switches* Cisco Nexus de la sèrie 3000 (model N3K-C3172TQ-10GT). Aquesta topologia proporciona la màxima redundància possible entre els equips. Per obtenir la redundància amb els servidors, les NIC[10] d'aquests estan degudament repartides entre els *switches* mitjançant *etherchannels*[11].

[9] vPC (Virtual Port Channel) domain s'usa per unir lògicament dos *switches* com un de sol
[10] Network Interface Card
[11] Permet l'agrupació lògica de diversos enllaços físics Ethernet

Pel que fa a la part lògica, existeixen vàries xarxes i *vlans*. El emphfirewall és l'únic *gateway*[12] de les xarxes, és a dir, tot el tràfic que va dirigit fora d'una xarxa ha de passar pel emphfirewall. Aplica al tràfic entre xarxes internes i evidentment cap a internet.

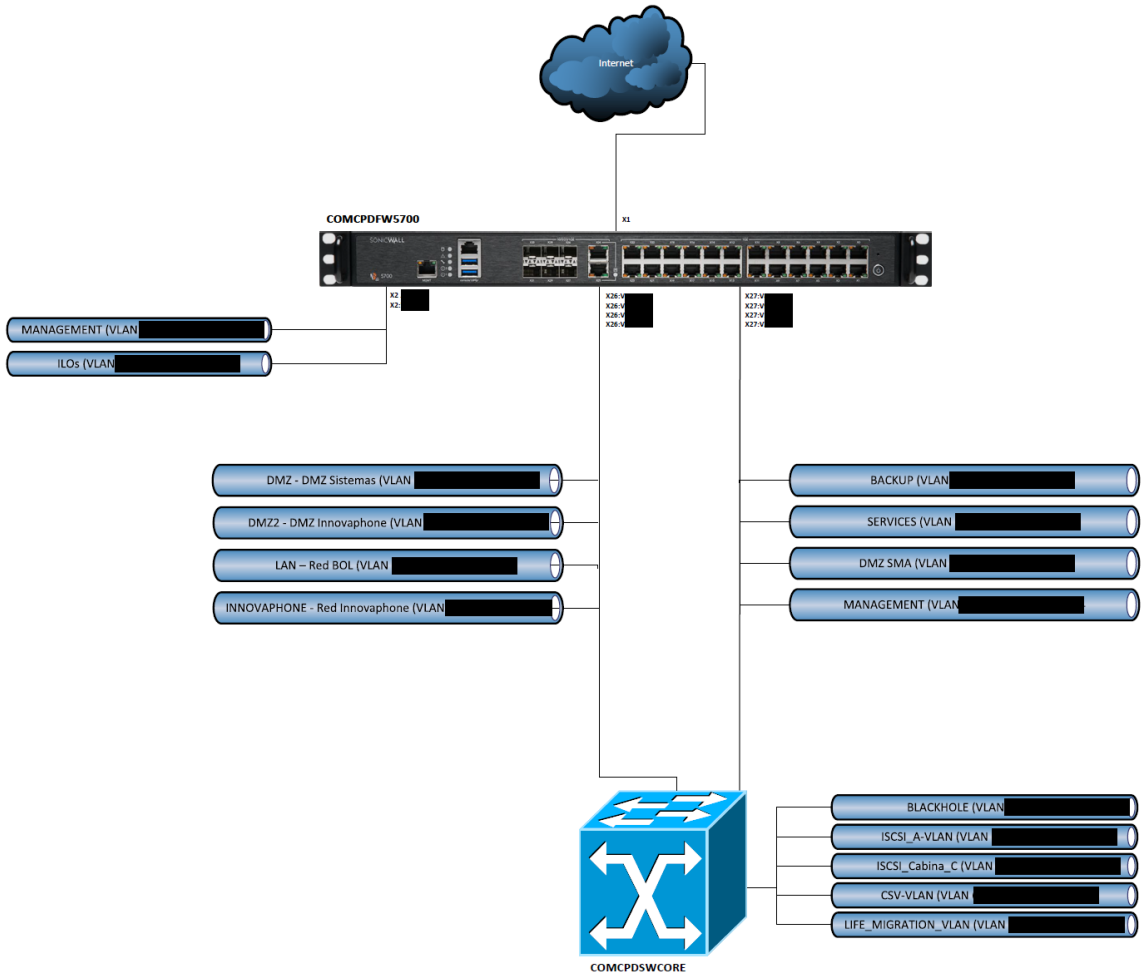


Fig. 2.7: Esquema lògic de la topologia del CPD de Bytemaster. Font: Elaboració pròpia.

Aquesta lògica té avantatges i inconvenients. L'inconvenient principal és que tot el tràfic entre les xarxes internes està obligat a passar pel *firewall*, això comporta que aquest tingui més càrrega de treball que si els *switches* s'encarreguessin d'encaminar el tràfic intern. Així que és necessari tenir un *firewall* amb més recursos. Altrament, l'avantatge principal és que en passar tot el tràfic intern pel *firewall* es poden crear polítiques més fàcilment i més granulars entre xarxes, que és el seu objectiu principal. Això s'anomena seguretat perimetral [3]. De retruc, això simplifica la monitorització entre xarxes ja que tot el tràfic passa pel

[12]Porta d'enllaç predeterminada

mateix node.

D'aquesta manera, gràcies a la funcionalitat del *firewall* d'enviar els *netflows* via protocol IPFIX[13], podem rebre la totalitat del tràfic des d'un sol node. Així doncs, el *software* escollit només haurà de rebre *netflows* d'un sol equip. Els fluxos del tràfic es poden veure a la figura 2.8.

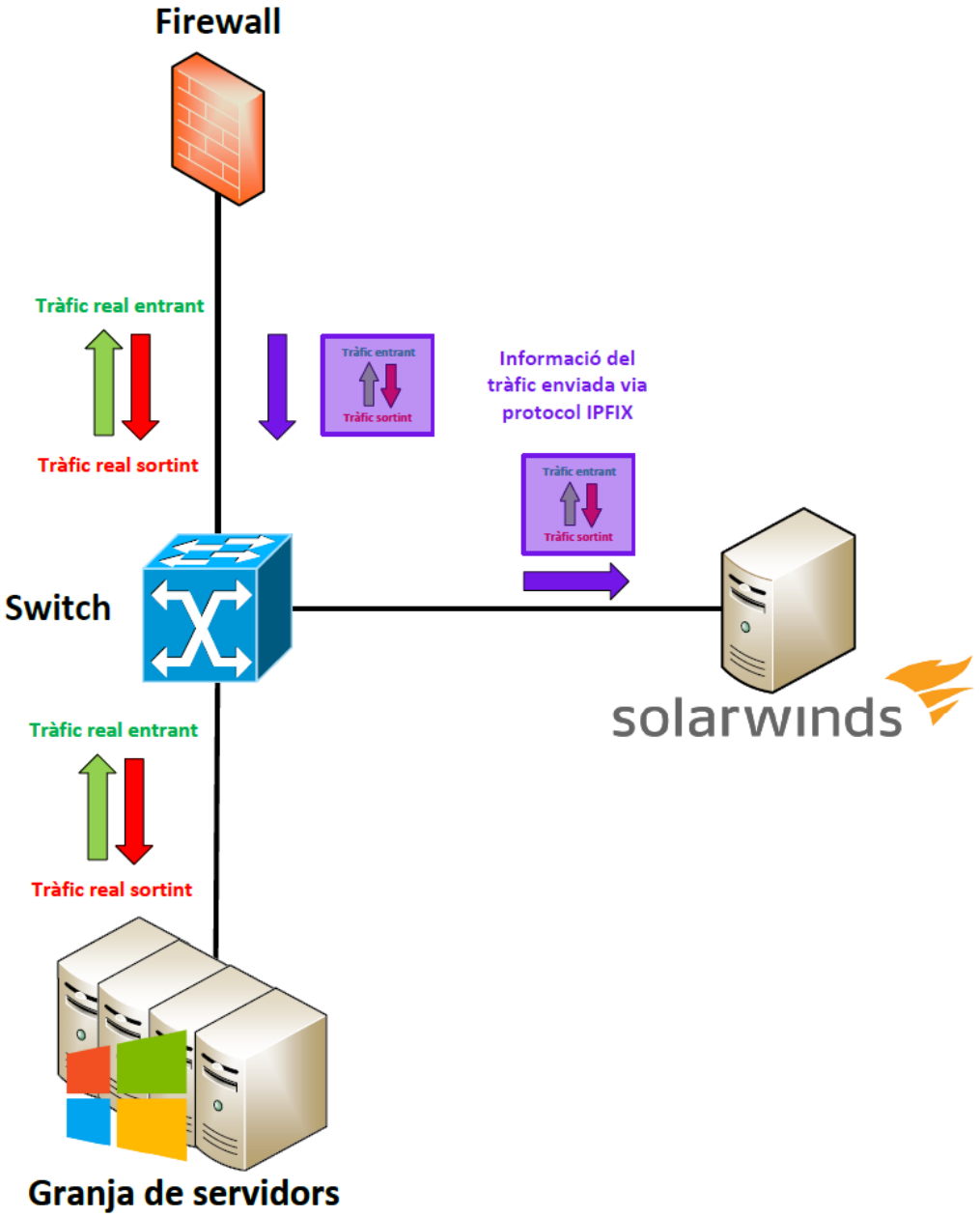


Fig. 2.8: Representació lògica dels *netflows* del CPD de Bytemaster. Font: Elaboració pròpia.

[13]IP Flow Information Export

3. Objectius i abast

3.1 Abast

Implementar un *software* de monitorització de tercers capaç de recol·lectar els *netflows* del tràfic IP que travessi pel *firewall* del CPD.

3.2 Objectius

3.2.1 Objectius del client: Bytemaster

- Aportar a Bytemaster un històric de dades de les connexions dins la xarxa del CPD que es puguin revisar amb anterioritat.
- Fer més eficient la cerca d'informació de monitorització de la xarxa del CPD.
- Deixar d'utilitzar dos sistemes actuals (LibreNMS i Nagios) per monitoritzar la xarxa del CPD i utilitzar només la nova implementació.

3.2.2 Objectius del producte: *Software* a implementar

- Escollir un *software* de tercers adequat per complir amb l'abast del projecte.
- La MV on s'implementarà el *software* elegit haurà de poder ser restaurada en cas que es comprometi totalment la instància en producció. És a dir, ha de tenir còpies de seguretat.

3.2.3 Objectius de l'usuari final: Tècnics del departament de comunicacions de Bytemaster

- Aportar a Bytemaster un sistema de monitorització de xarxa testejat que permeti als seus tècnics confiar en ell, és a dir, que sigui fiable.

- Aportar a Bytemaster un sistema de monitorització de xarxa que permeti als seus tècnics ser capaços d'identificar si hi ha o no un problema a la xarxa del CPD.
- El sistema de monitorització ha de ser usable per tècnics amb poca formació.

4. Metodologia

Degut a la naturalesa del projecte, la implementació d'un *software*, s'ha decidit aplicar una metodologia *Agile* [4]. La metodologia *Agile* està basada en els principis del *Agile Manifesto* [5]. Aquests manifesten la voluntat d'acceptar canvis en la planificació si aquests fan progressar el projecte pel bon camí. També, aposten per l'entrega continuada de valor, la col·laboració amb el client i cicles de desenvolupament on es reflexiona com ser més efectiu.

En ser un projecte acadèmic i alhora un empresarial, es mantindran reunions cada dues setmanes amb els respectius tutors per revisar l'avanç del projecte i contemplar possibles canvis.

Per mantenir un correcte flux d'informació amb el tutor acadèmic, s'han establert vàries eines de comunicació i gestió per aquest fi. Aquestes són:

- **Reunions virtuals:** Eina *Zoom* [6]. És convenient poder parlar cara a cara per tenir un intercanvi natural d'idees. Útil també per compartir escriptoris i facilitar la comprensió de les correccions del treball.
- **Comunicació:** Correu electrònic. Eina de comunicació estàndard per notificar reunions o missatges rellevants.
- **Gestió del projecte.** Eina *Teamwork* [7]. Útil per tenir una planificació a nivell general de les fases del projecte i anotar les tasques passades, presents i futures que es realitzen.
- **Intercanvi de fitxers:** Eina *Google Drive* [8]. Necessari per tenir un recurs comú per poder guardar i compartir fitxers rellevants pel projecte de qualsevol tipus.
- **Editor de documents:** Eina *Overleaf* [9]. Recurs principal per redactar i compartir documents de text basats en *Latex* [10]. Útil també per notificar correccions per part del tutor.

Per garantir que el client, específicament el tutor de Bytemaster, sigui un col·laborador més

del projecte i comprovi el seu progrés, s'han establert diverses eines de comunicació. Aquestes són:

- **Reunions virtuals:** Eina *Microsoft Teams* [11]. És convenient poder parlar cara a cara per explicar de forma natural el progrés del projecte. Útil també per compartir escriptoris.
- **Comunicació:** Correu electrònic. Eina de comunicació estàndard per notificar reunions o missatges rellevants.

Seguint la metodologia *Agile*, s'ha definit el següent flux de treball:

- **Anàlisis i investigació:** Recopilar informació, requisits i investigar possibles solucions.
- **Disseny:** Encaixar les possibles solucions amb els requisits.
- **Implementació:** Desenvolupar la solució dissenyada prèviament.
- **Verificació:** Comprovar si es compleixen el requisits.
- **Avaluació:** Avaluar els resultats. Verificar el que ha funcionat i el que no.

El flux de treball és circular i no només es recorre una vegada. Cada iteració pot ser una tasca o un conjunt d'elles i es poden repetir N vegades si es considera necessari. D'aquesta manera es pot polir en cada iteració el resultat final aportant més valor en cada una d'elles.

5. Desenvolupament

En aquest apartat es mostra el desenvolupament del projecte. Tenint en compte els seus requisits (5.1) i objectius (3.2), es mostra l'elecció del *software* així com la seva implementació (5.3, 5.4, 5.5 i 5.6) i validació (5.7).

5.1 Requisits funcionals i tecnològics

Per complir satisfactòriament amb els objectius del projecte s'han de complir diversos requisits funcionals i tecnològics.

5.1.1 Requisits funcionals

- El *software* ha de tenir una interfície gràfica amigable.
- El *software* ha de representar gràficament les dades de forma interactiva.
- El *software* ha de tenir un *dashboard*[1] personalitzable.
- El *software* ha de mantenir un històric de dades de mínim un mes.
- El *software* ha de poder enviar alertes per correu.
- El *software* no ha d'afectar de forma negativa a la plataforma en producció.

5.1.2 Requisits tecnològics

- El *software* ha de ser compatible amb el protocol IPFIX i SNMP.
- El *software* ha de ser compatible amb la virtualització sobre la plataforma *HyperV*[2].
- El *software* ha de ser robust i estar operatiu 24x7[3].
- El *software* ha de tenir l'opció de suport per part del fabricant.

[1] Tauler de control
[2] Hypervisor de Microsoft
[3] 24 hores del dia, els set dies de la setmana

- El *software* ha de tenir l'opció de recol·lectar paquets mitjançant *port mirroring*[4].
- El *software* ha de disposar de suficients recursos de *hardware* per funcionar correctament.
- La MV on està instal·lat el *software* ha de tenir còpies de seguretat.

5.2 Elecció del *software*

Per tal d'elegir el *software* adequat per aquest projecte s'han tingut presents els requisits funcionals i tecnològics descrits al apartat 5.1. En un primer anàlisis de mercat s'han seleccionat quatre possibles *softwares*:

- Solarwinds [12]
- Paessler PRTG [13]
- Plixer Scrutinizer [14]
- nProbe/nTop [15]

5.2.1 Solarwinds

Punts a favor:

- Àmplia comunitat d'usuaris.
- Llarga vida al mercat.
- Interfície molt amigable i personalitzable.
- Suport tècnic per part del fabricant.
- Modular, es poden instal·lar només els mòduls necessaris.

Punts en contra:

- Cost més elevat que algunes altres opcions.

[4]Consisteix en duplicar el tràfic d'un port d'un *switch* a un altre

- Només disponible en *Windows Server* i compatible amb *SQL Server*.
- Al ser tan personalitzable i tenir moltes opcions pot ser aclaparador.

5.2.2 Paessler PRTG

Punts a favor:

- Llarga vida al mercat.
- Interfície personalitzable.
- Suport tècnic per part del fabricant.

Punts en contra:

- Llicenciament vinculat a sondes. No és paga per equip sinó per servei a monitoritzar.
- Ja s'havia provat a Bytemaster, segons treballadors consultats no complia les expectatives.
- Complex d'aprendre a utilitzar-lo.

5.2.3 Plixer Scrutinizer

Punts a favor:

- Llarga vida al mercat.
- Bona relació qualitat/preu.
- Suport tècnic per part del fabricant.
- Compatibilitat amb camps únics IPFIX del fabricant Sonicwall, *firewall* actual del CPD de Bytemaster.

Punts en contra:

- Interfície gràfica antiquada.

- Ja s'havia provat a Bytemaster, segons treballadors consultats no complia les expectatives.

5.2.4 nProbe/nTop

Punts a favor:

- Llarga vida al mercat.
- Àmplia comunitat d'usuaris.
- És econòmic en ser *open source*.

Punts en contra:

- No té suport tècnic en ser *open source*.
- Interfície gràfica antiquada.
- Ja s'havia provat a Bytemaster, segons treballadors consultats no complia les expectatives.
- No compleix alguns requisits.

Analitzant tots els punts a favor i en contra de cada un dels *softwares* seleccionats inicialment, s'ha decidit instal·lar la solució *Solarwinds* per complir amb els objectius i els requisits del projecte.

5.3 Preparació del entorn

Per tal de tenir un entorn segur i controlat on instal·lar el *software* s'ha creat una nova xarxa, amb la corresponent *vlan*[5], en la topologia del CPD de Bytemaster. Veure figura 5.1. D'aquesta manera es poden controlar de forma perimetral els serveis permesos entre la xarxa de serveis on s'instal·larà el *Solarwinds* i la resta de xarxes en producció. Es poden apreciar les regles en la figura 5.2. Els serveis o protocols permesos són: SNMP, ICMP[6] i

[5]Virtual Local Area Network
[6]Internet Control Message Protocol

Syslog[7]. Aquests serveis s'han agrupat en un grup d'objectes al *firewall* per tal de simplificar la creació de les regles, veure figura 5.3.

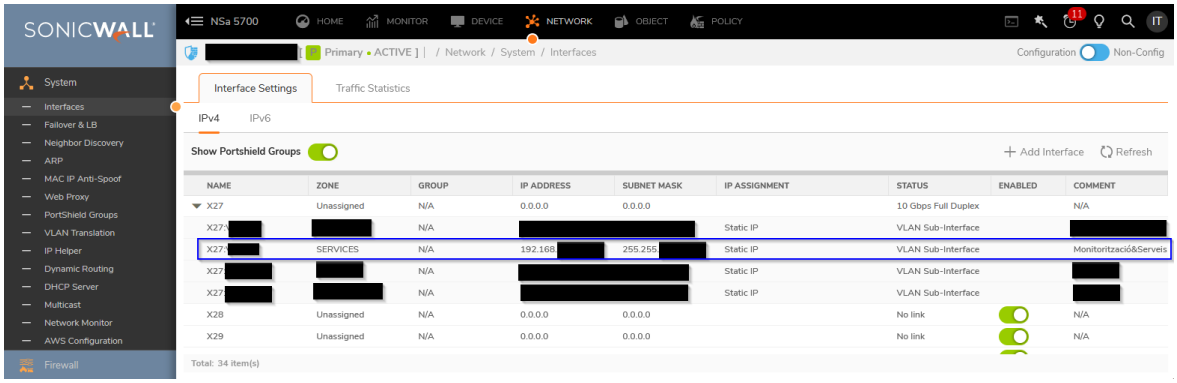


Fig. 5.1: Creació d'una nova interfície al *firewall* del CPD. Font: Elaboració pròpia.

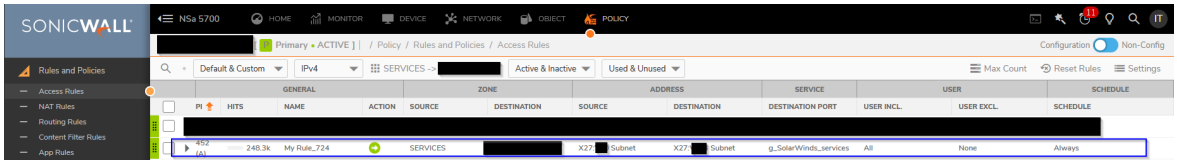


Fig. 5.2: Regla d'accés al *firewall* del CPD que permet els serveis. Font: Elaboració pròpia.

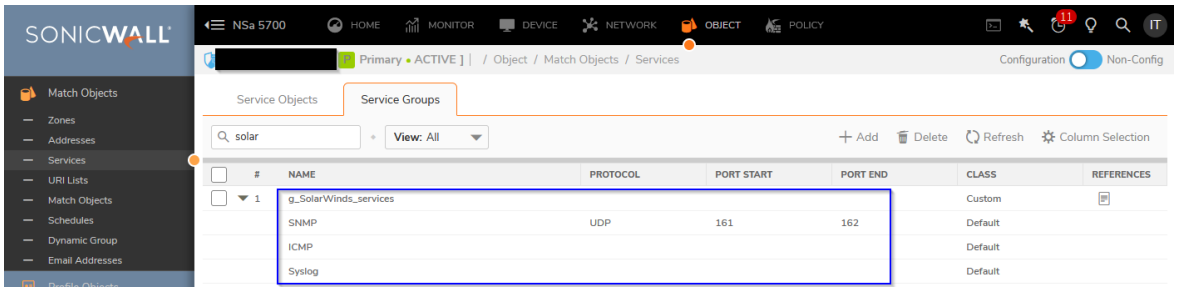


Fig. 5.3: Grup d'objectes de serveis del *firewall* del CPD. Font: Elaboració pròpia.

El servidor dedicat que s'utilitzarà per *hostejar*[8] el *Windows Server 2022 Datacenter* amb el rol de *hypervisor*[9] on s'executaran les MV és un *Dell PowerEdge R640*. Es poden veure els detalls de l'equip en la figura 5.6. Aquest té dos discs HDD[10] de 250 GB en RAID1[11] i dos discs SSD[12] de 500 GB en RAID1. Veure figura 5.4.

[7] Protocol estàndard IETF RFC 5424 per la recol·lecció de logs
[8] Capacitat d'allotjar MVs
[9] Capa de *software* per realitzar una virtualització de *hardware* que permet executar varis SO
[10] Hard Disk Drive
[11] Tipus de RAID, Redundant Array of Independent Disks
[12] Solid State Drive

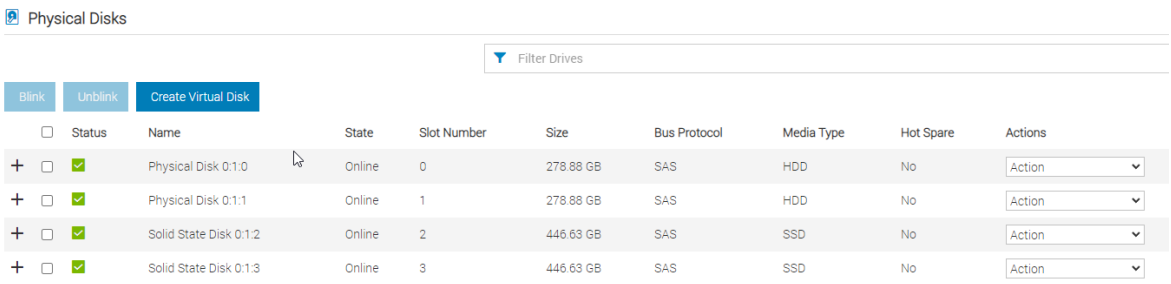


Fig. 5.4: Discs del *host*. Font: Elaboració pròpia.

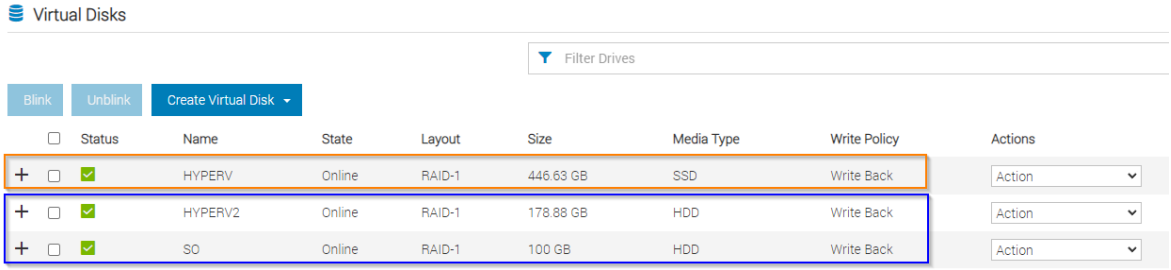


Fig. 5.5: RAIDs del *host*. Font: Elaboració pròpia.

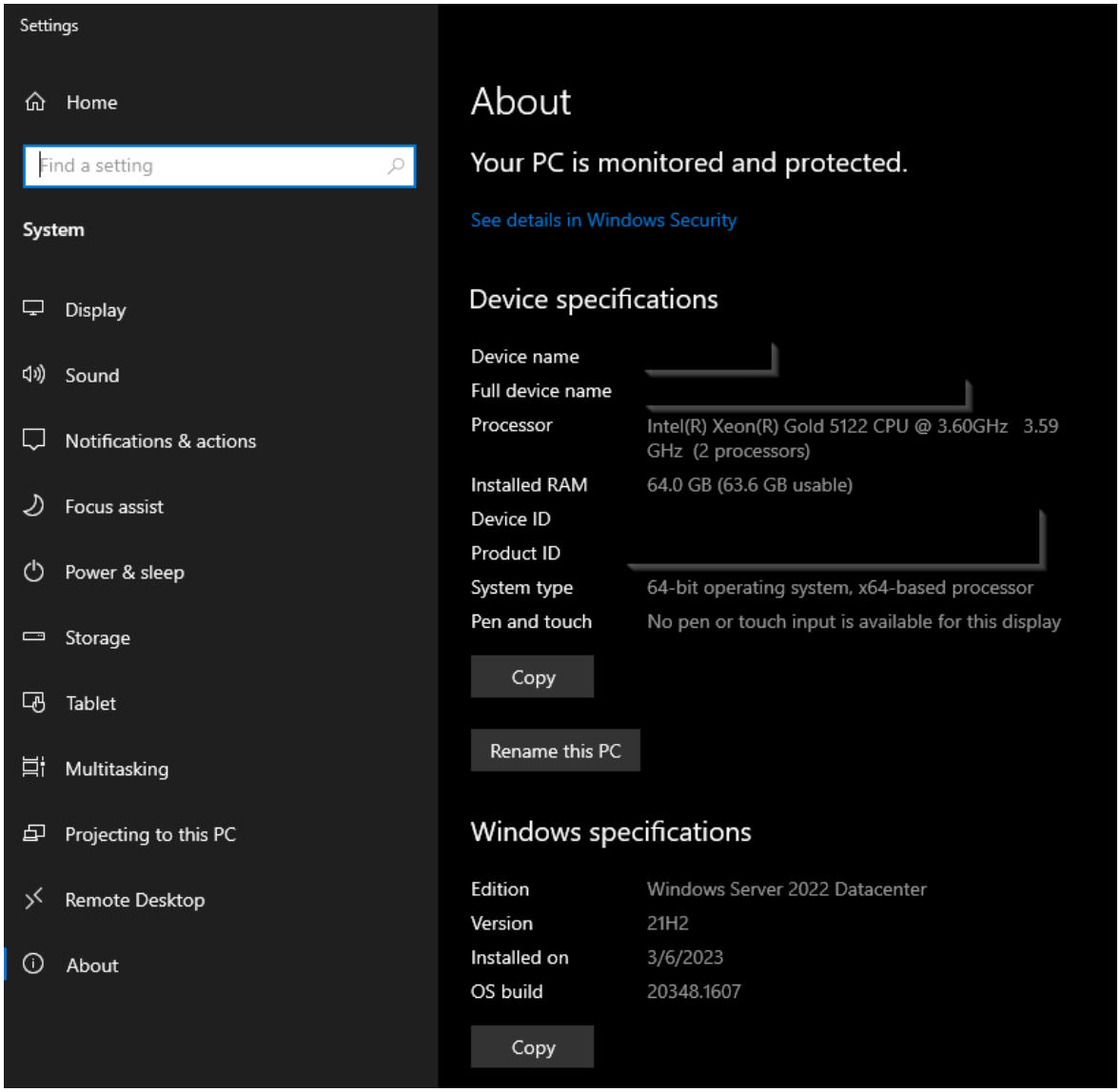


Fig. 5.6: Detalls del *Host*. Font: Elaboració pròpia.

Com es pot comprovar en la figura 5.5. El RAID1 de discs HDD té dues particions, una de 100 GB[13] i un altre de 180 GB. La primera és usada per crear un volum per allotjar el SO[14] i l'altre per poder allotjar MVs. El RAID1 de discs SSD serà una única partició amb un volum per allotjar MVs.

[13] gigabyte
[14] Sistema Operatiu

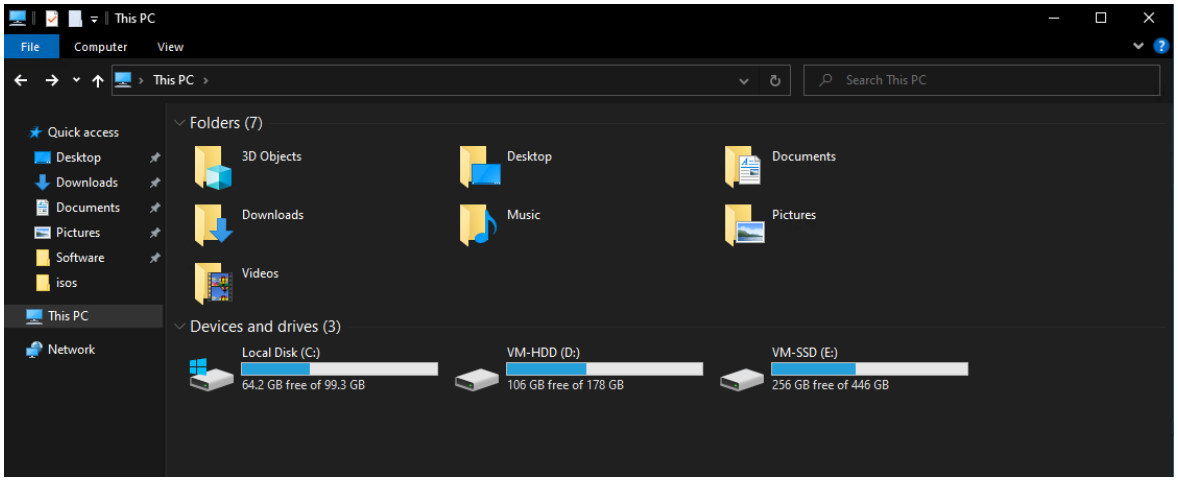


Fig. 5.7: Volums del *host*. Font: Elaboració pròpia.

En la pantalla de connexions de xarxa del servidor de la figura 5.8 es pot apreciar que el servidor disposa de quatre NICs, dues d'1 Gbps[15] i dues de 10 Gbps. Les dues primeres s'usen per crear un *teaming*[16] perquè el *host* tingui redundància. Veure figura 5.9. Les altres dues de 10 Gbps s'usen per crear un *virtual switch* [16] amb el mode *EmbeddedTeaming* [17] per tal de tenir redundància en les MV. Evidentment, una NIC de cada parell va connectada a un *switch* diferent. Els *switches* tenen configurat un *etherchannel*[17] per cada parell de NICs. Veure figura 5.10.

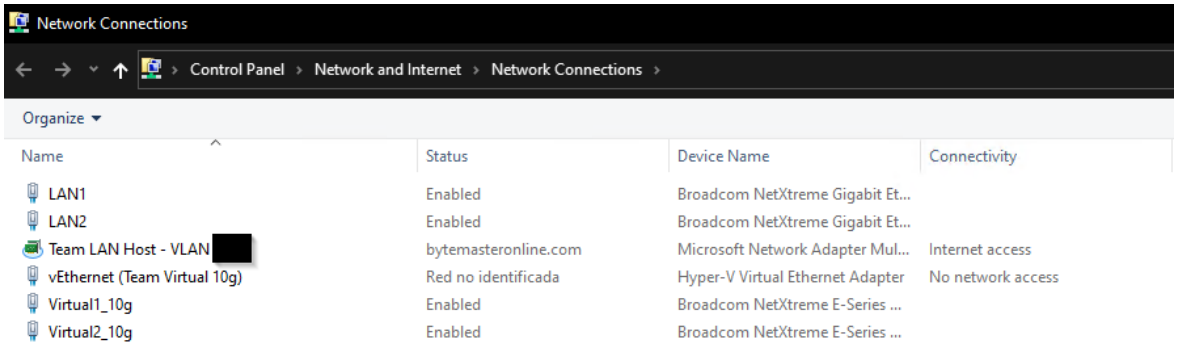


Fig. 5.8: NICs del *host*. Font: Elaboració pròpia.

[15] gigabit per segon
[16] Unió lògica de NICs
[17] Unió lògica de ports de *switch*

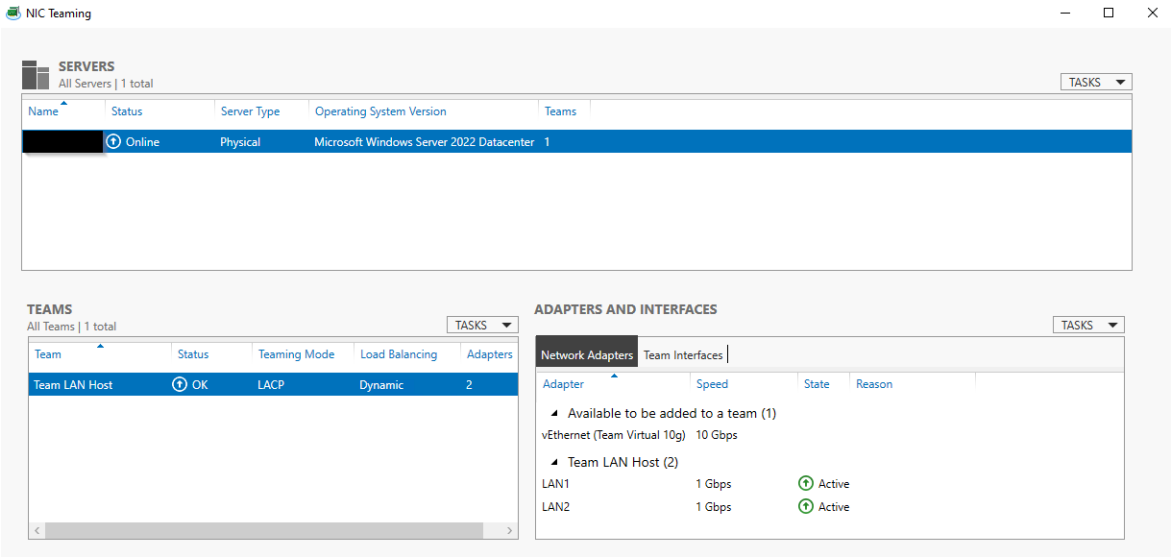


Fig. 5.9: *Teaming* del *host*. Font: Elaboració pròpia.

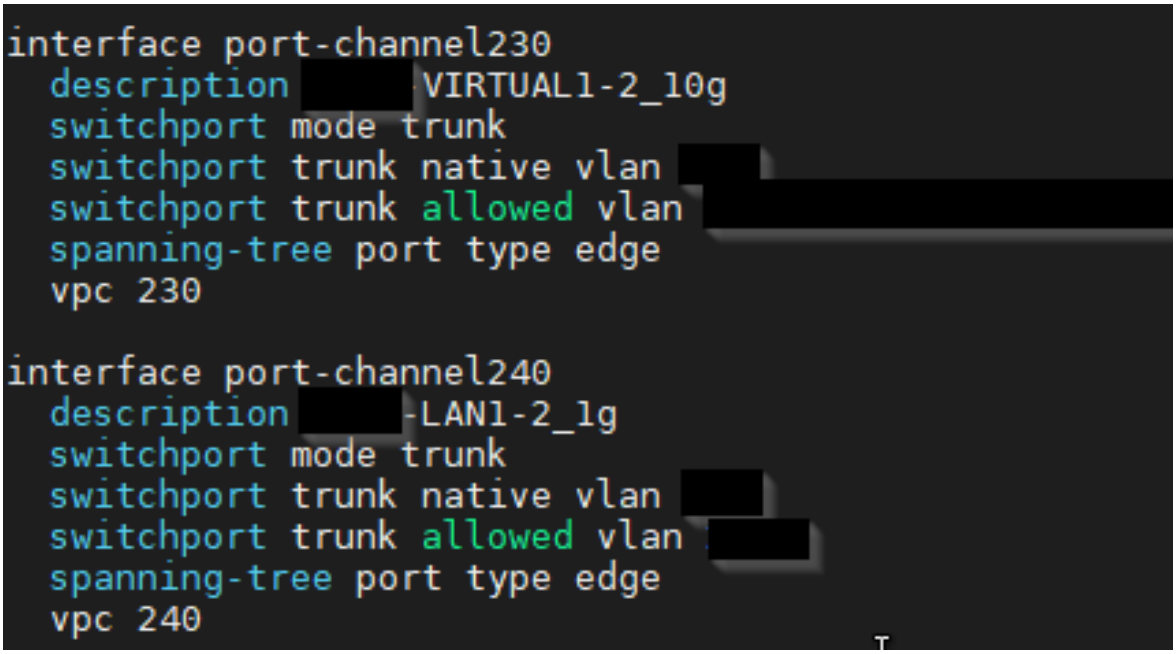


Fig. 5.10: *Etherchannels* dels *switches* pels *teamings* del *host*. Font: Elaboració pròpia.

5.4 Instal·lació del *software*: *Solarwinds*

Solarwinds disposa de dos tipus d'instal·lació:

- HCO (Hybrid Cloud Observability): Format "SaaS". Mode de llicenciament on es paga anualment per nombre de nodes. Inclou el suport i tots els mòduls del *software*.

- Mòduls: Mode de llicenciament on es paga una llicència perpètua pels mòduls del *software* desitjats i nombre de nodes. El suport s'ha de renovar anualment.

Per aquest projecte s'ha escollit la segona opció. Els mòduls escollits són el NPM (Network Performance Monitor) i NTA (NetFlow Traffic Analyzer). Amb aquest dos compleixen els objectius i requisits del projecte. Tenint present la dimensió de la infraestructura del CPD de Bytemaster, es compleixen els requisits de *Solarwinds* [18]. Seguint la guia d'instal·lació de *Solarwinds* [19], s'ha dividit la instal·lació en dues MVs. Veure figura 5.11.

- MV "SolarWindsPlataform": MV on hi han instal·lats els mòduls i la interfície gràfica.
- MV "SolarWindsSQL": MV on hi ha instal·lat el *SQL Server* per allotjar la base de dades de *Solarwinds*.

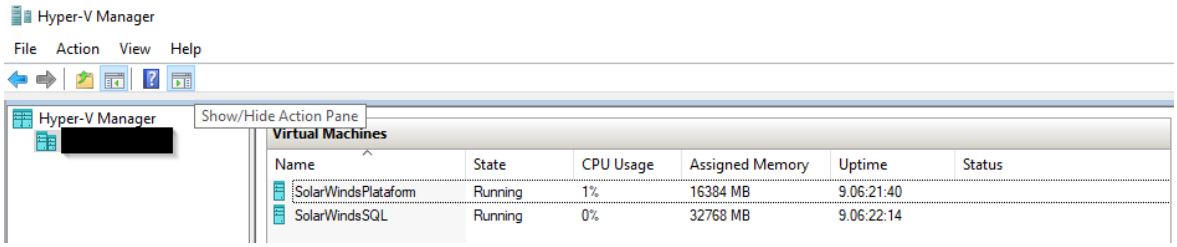


Fig. 5.11: MVs creades al HyperV del *host*. Font: Elaboració pròpia.

En les dues MVs s'ha instal·lat el SO *Windows Server 2022 (Standard)*. En la MV *SolarWindsPlataform* s'ha creat amb un disc virtual de 100 GB en el volum del *host* VM-HDD. Els detalls de la MV es poden veure en la figura 5.12 i els del disc en la 5.13. Aquest volum està creat sobre la segona partició del RAID1 de discs HDD. De les dues MV, és la que menys necessita els avantatges [20] dels discs SSD i menys espai d'emmagatzematge.

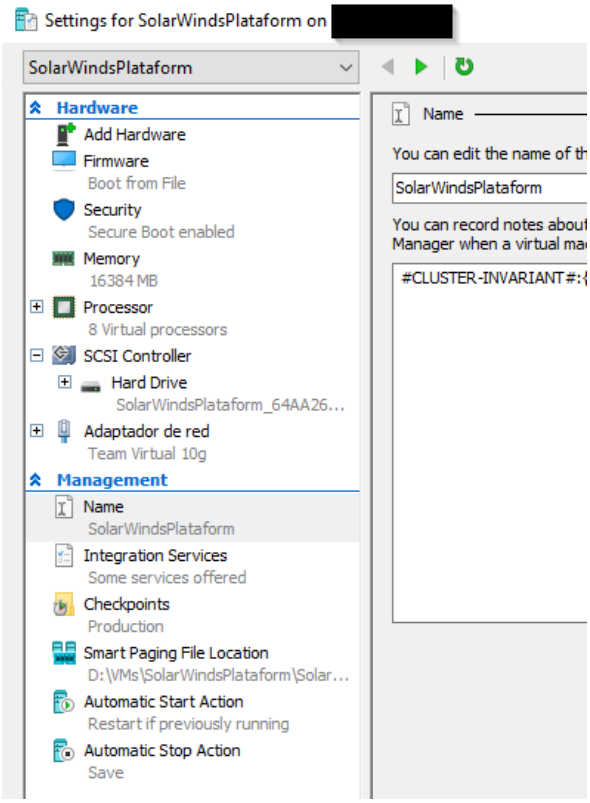


Fig. 5.12: Configuració del HyperV de la MV *SolarWindsPlataform*. Font: Elaboració pròpia.

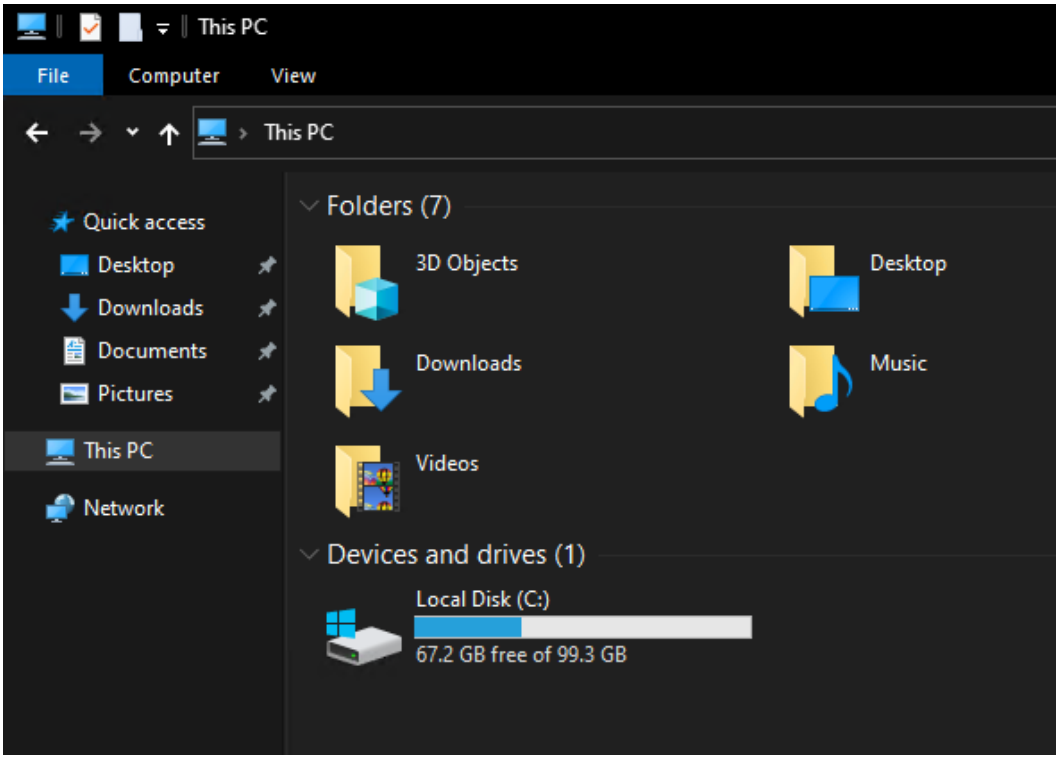


Fig. 5.13: Disc de la MV *SolarWindsPlataform*. Font: Elaboració pròpia.

La MV *SolarWindsSQL* (figura 5.14) s'ha creat sobre el volum VM-SSD, ja que és la que eventualment ocuparà més espai d'emmagatzematge degut a l'allotjament de la base de dades. A més, es beneficiarà dels avantatges dels discs SSD, molt important quan es tracta d'una instal·lació de *SQL Server*. Aquesta MV s'ha creat amb tres discs virtuals, un pel SO i dos pels directoris dels fitxers de la base de dades *logs* i *data*. Es pot comprovar en la figura 5.15. Per la naturalesa del funcionament del *SQL Server*, és una bona pràctica mantenir aquests directoris en diferents discs, tant virtuals com físics. En aquest cas, a falta de tenir més discs físics, en el servidor només compleix amb discs virtuals.

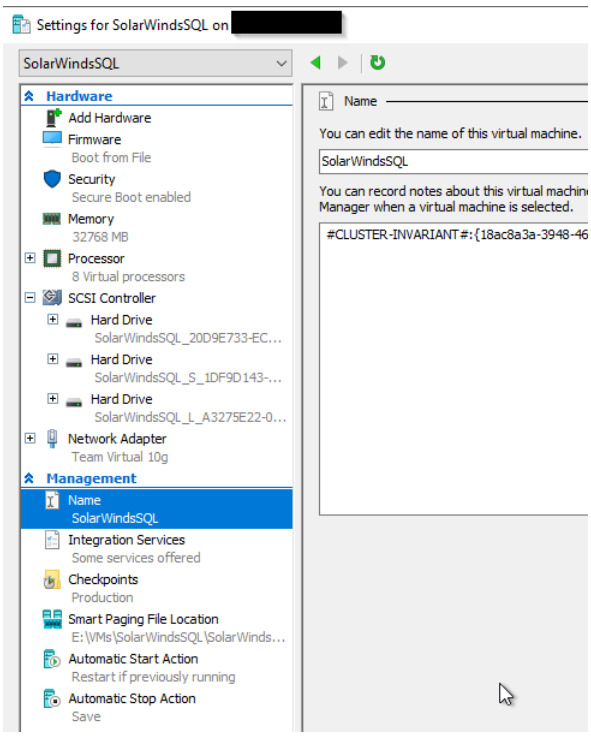


Fig. 5.14: Configuració de HyperV de la MV *SolarWindsSQL*. Font: Elaboració pròpia.

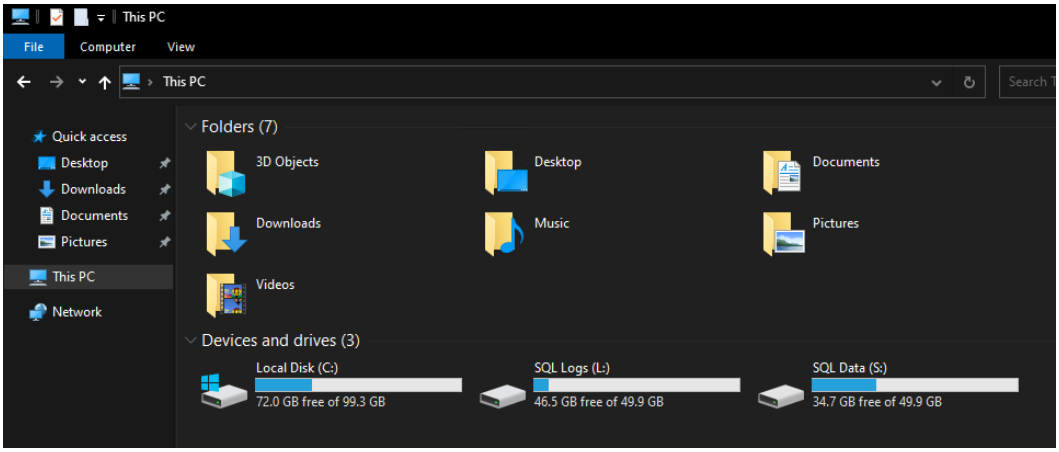


Fig. 5.15: Disc de la MV *SolarWindsSQL*. Font: Elaboració pròpia.

Amb les MVs correctament creades i configurades s'han instal·lat els *softwares Solarwinds* i *SQL Server* segons descrit anteriorment. Veure figures 5.16 i 5.17 respectivament.

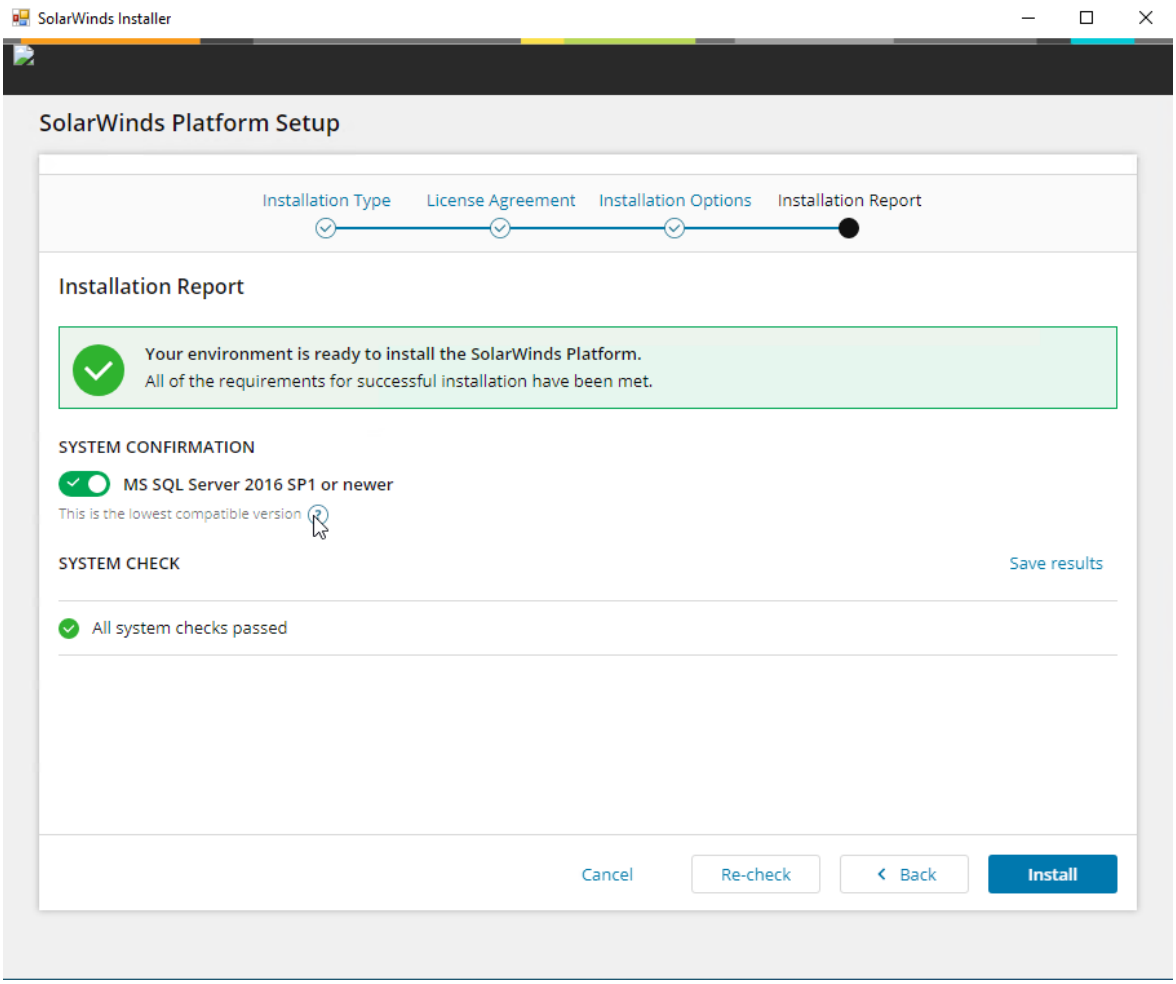


Fig. 5.16: Instal·lació del *Solarwinds* en la MV *SolarWindsPlataform*. Font: Elaboració pròpia.

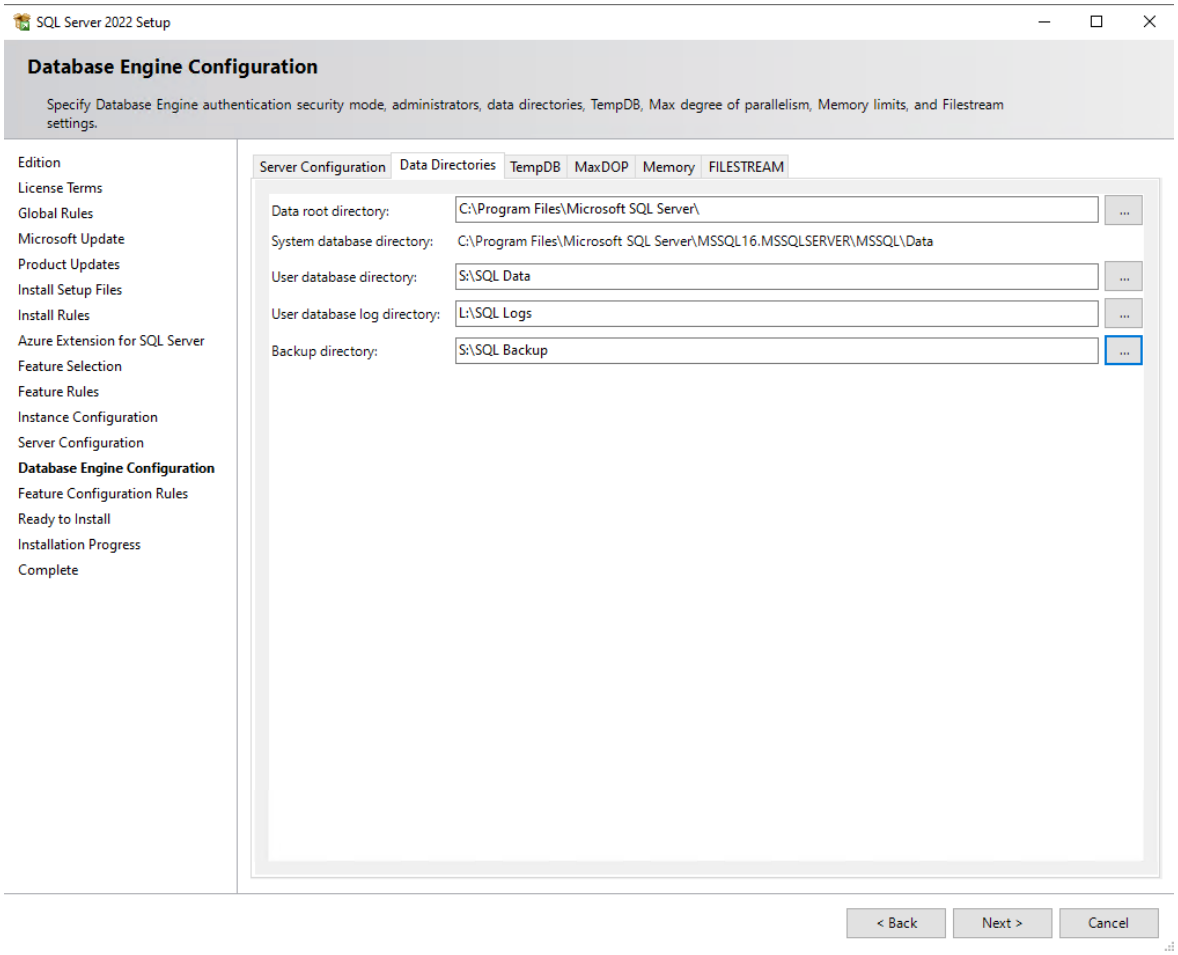


Fig. 5.17: Instal·lació del *SQL Server* en la MV *SolarWindsSQL*. Font: Elaboració pròpia.

5.5 Configuració del *Solarwinds*

La infraestructura de *networking* del CPD de Bytemaster consisteix en quatre *switches* Cisco Nexus i un *firewall* Sonicwall NSA 5700. Així doncs, aquests equips s'han afegit al *Solarwinds*. Per afegir un node simplement s'ha d'introduir la IP de l'equip i les credencials SNMPv3 (versió més segura del protocol) perquè els equips enviïn les dades al *Solarwinds*. Veure figures 5.18 i 5.19.

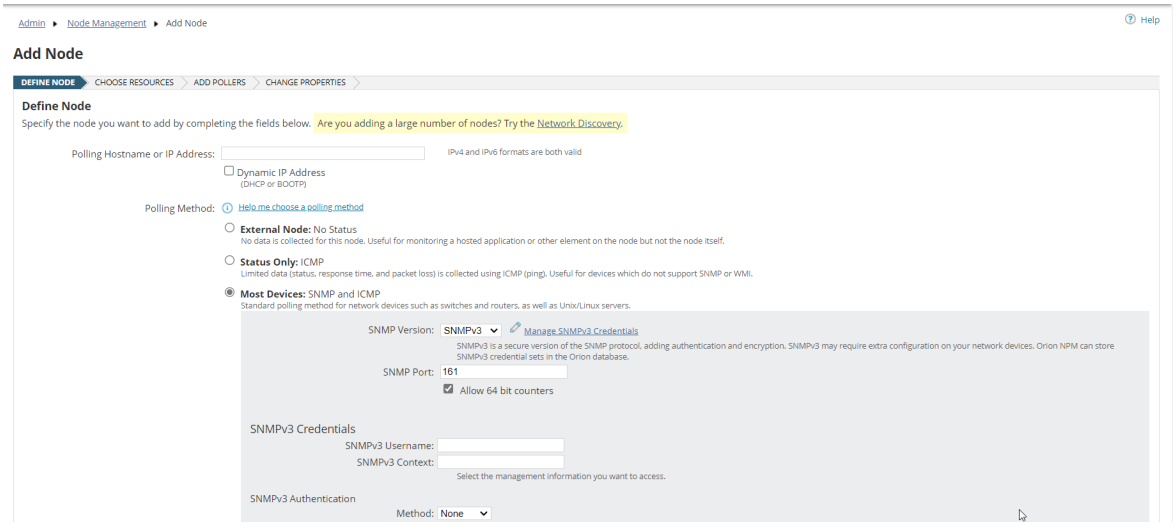


Fig. 5.18: Pantalla d'afegir node a *Solarwinds*. Font: Elaboració pròpia.

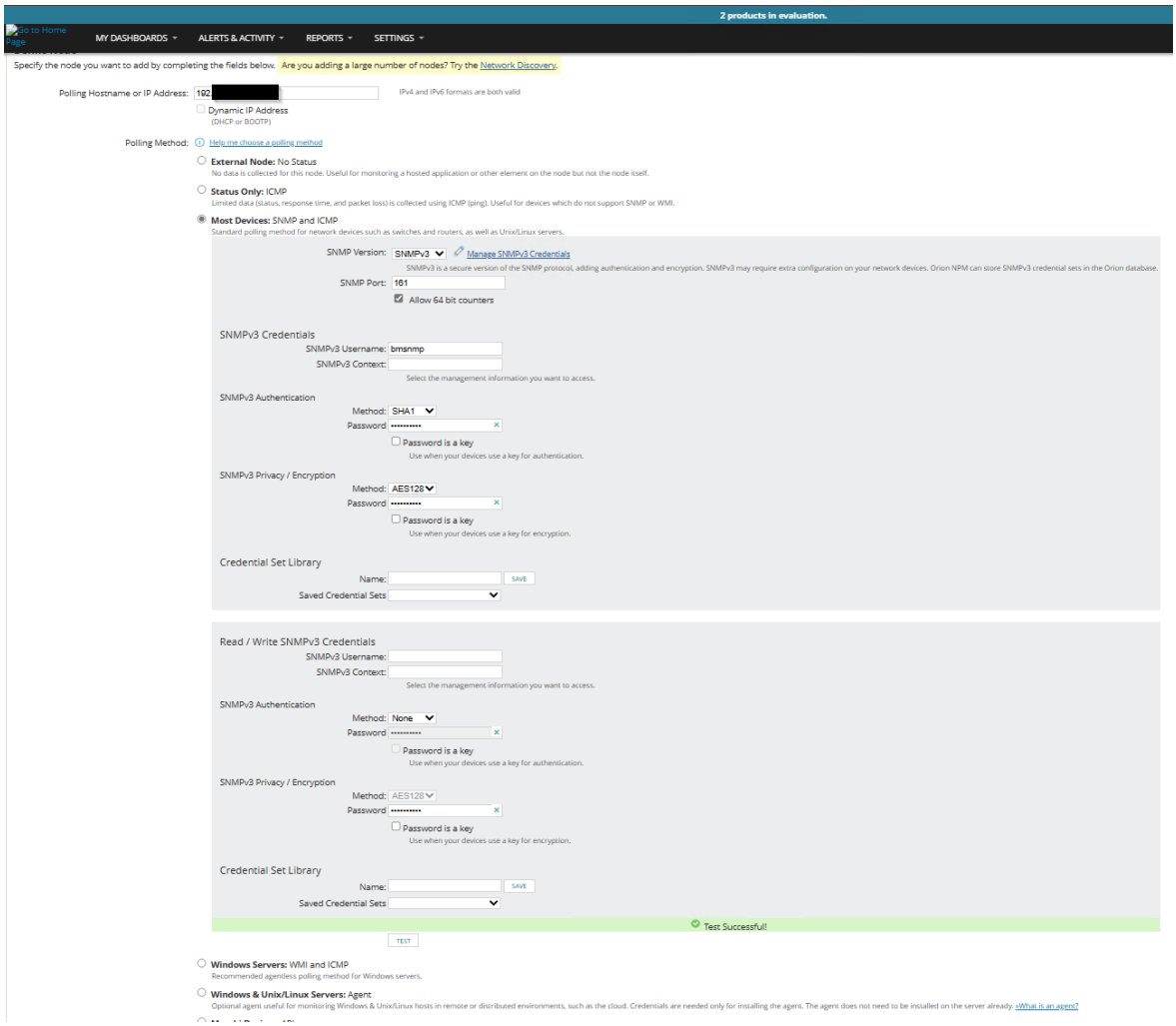


Fig. 5.19: Test satisfactori de les credencials SNMP a l'afegir un node a *Solarwinds*. Font: Elaboració pròpia.

Pel *Solarwinds* a cada equip físic se l'anomena node. Cada node pot tenir diferents *pollers*[18] que poden monitoritzar diferents serveis i protocols. Tots els equips de *networking* es monitoritzen via protocol SNMP i a més a més el *firewall* també via protocol IPFIX. Com s'ha comentat anteriorment, la implementació del *Solarwinds* consisteix en dos mòduls, el NPM i NTA. El primer és qui inclou la monitorització via SNMP i el tractament d'alertes. El segon, incorpora la capacitat de monitoritzar via IPFIX. Dels nodes monitoritzats via SNMP es rep informació bàsica dels equips. Això és de gran ajuda per valorar la salut dels mateixos equips, ja que aporta informació com: detalls de l'equip (nom, fabricant, model, versió de *firmware*...), estat de l'equip (si està operatiu o no), temps de resposta i latència, utilització de la CPU i RAM, estat de les interfícies físiques i lògiques (actives o caigudes), utilització de l'ample de banda de les interfícies i temperatura de l'equip entre d'altres. En les figures 5.20 i 5.21 es pot veure com *Solarwinds* representa aquest tipus d'informació.

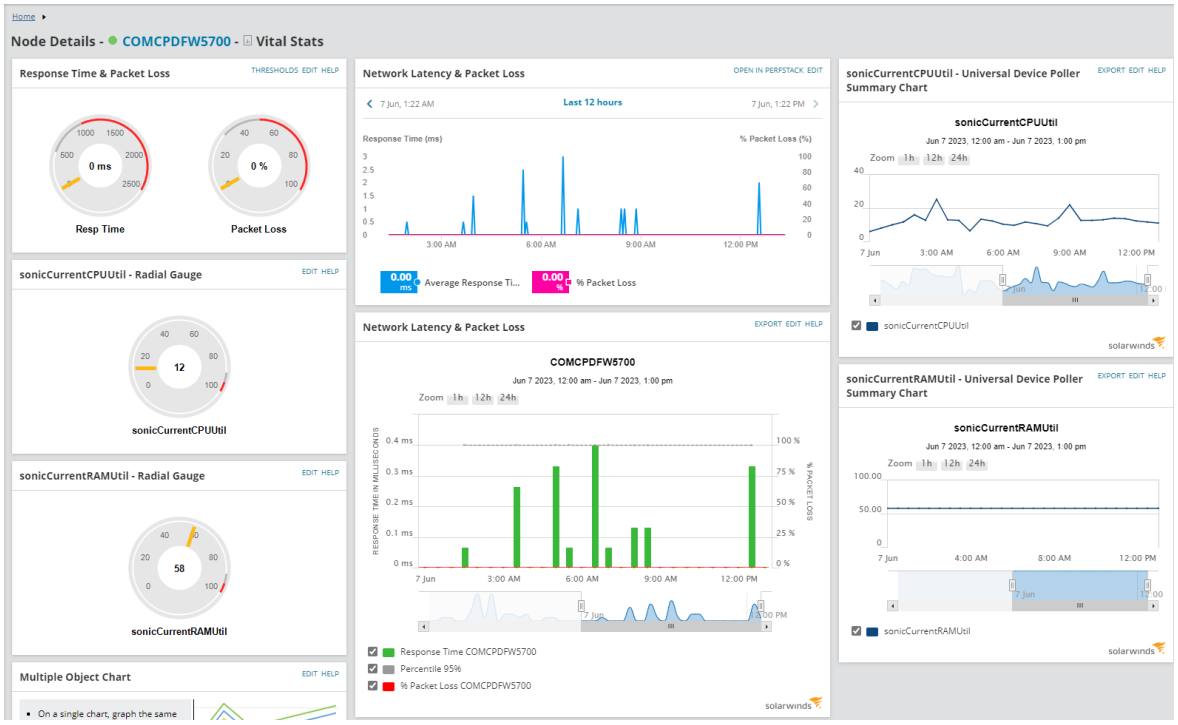


Fig. 5.20: Paràmetres de salut del *firewall* monitortizats via SNMP. Font: Elaboració pròpia.

[18]Part de *software* que envia una sol·licitud periòdica a un agent de dades de gestió

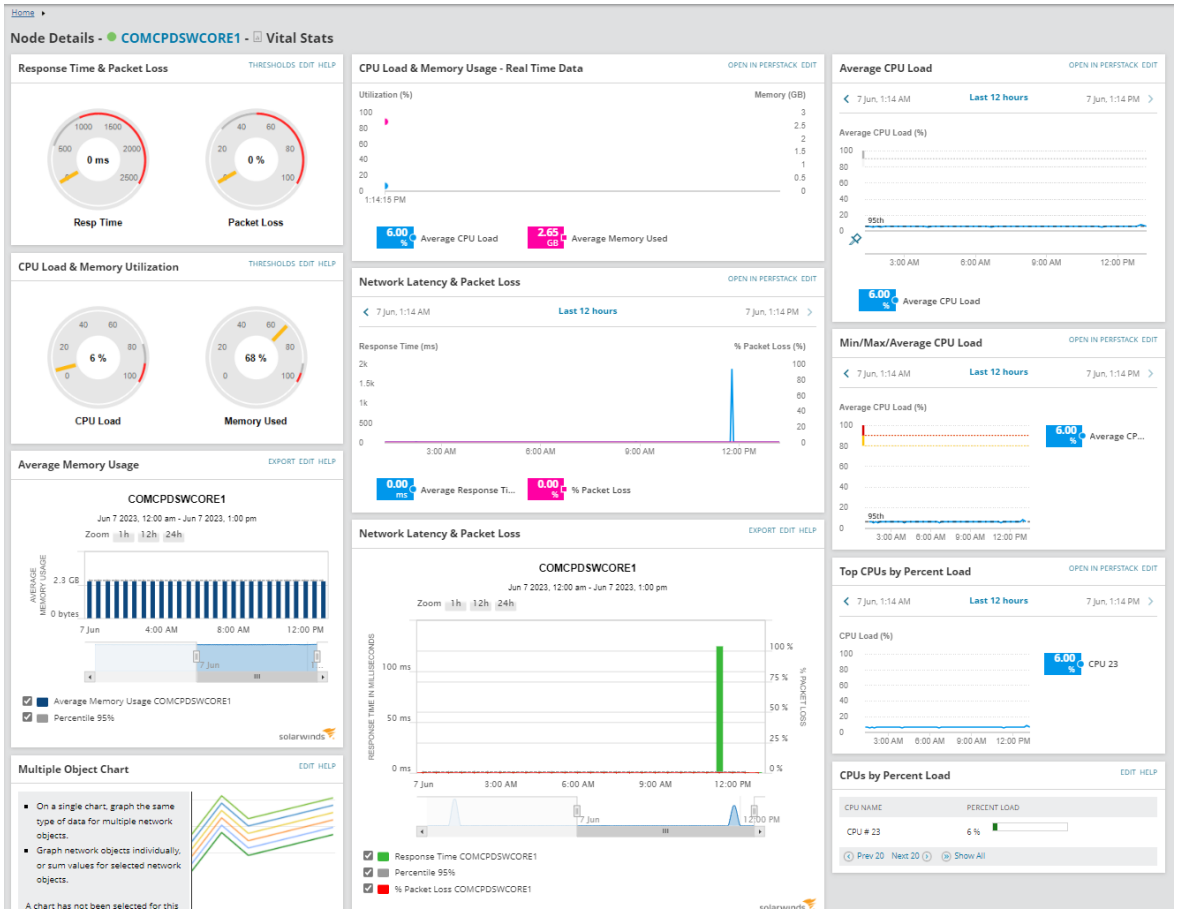


Fig. 5.21: Paràmetres de salut d'un switch Cisco Nexus monitortizats via SNMP. Font: Elaboració pròpia.

En el cas del *firewall*, també es monitoritza via IPFIX. A l'estar el node ja configurat al *Solarwinds*, simplement configurant el *firewall* perquè enviï els *flows* és suficient perquè el *software* pugui identificar a quin node pertany. Els paràmetres a configurar es mostren en la figura 5.22.

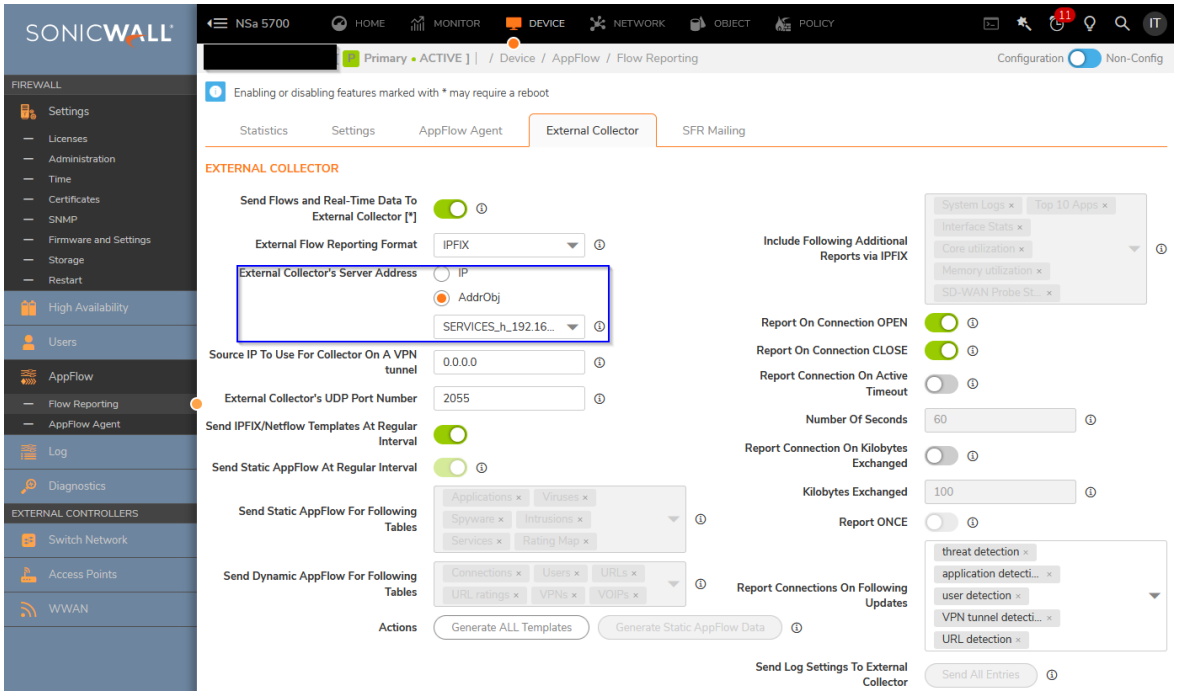


Fig. 5.22: Configuració del *firewall* per enviar dades al *Solarwinds* via IPFIX. Font: Elaboració pròpia.

Aquests *flows* del tràfic rebuts i representats gràficament pel *Solarwinds* aporten una nova capa de profunditat. Amb aquesta informació es pot veure el tràfic dels equips i serveis interns de la infraestructura (servidors físics i MVs principalment) i les conversacions que han tingut. D'aquesta manera es pot saber la quantitat de dades mogudes, la seva duració, l'emissor i receptor, el port utilitzat i el tipus d'aplicació. Veure figura 5.23.

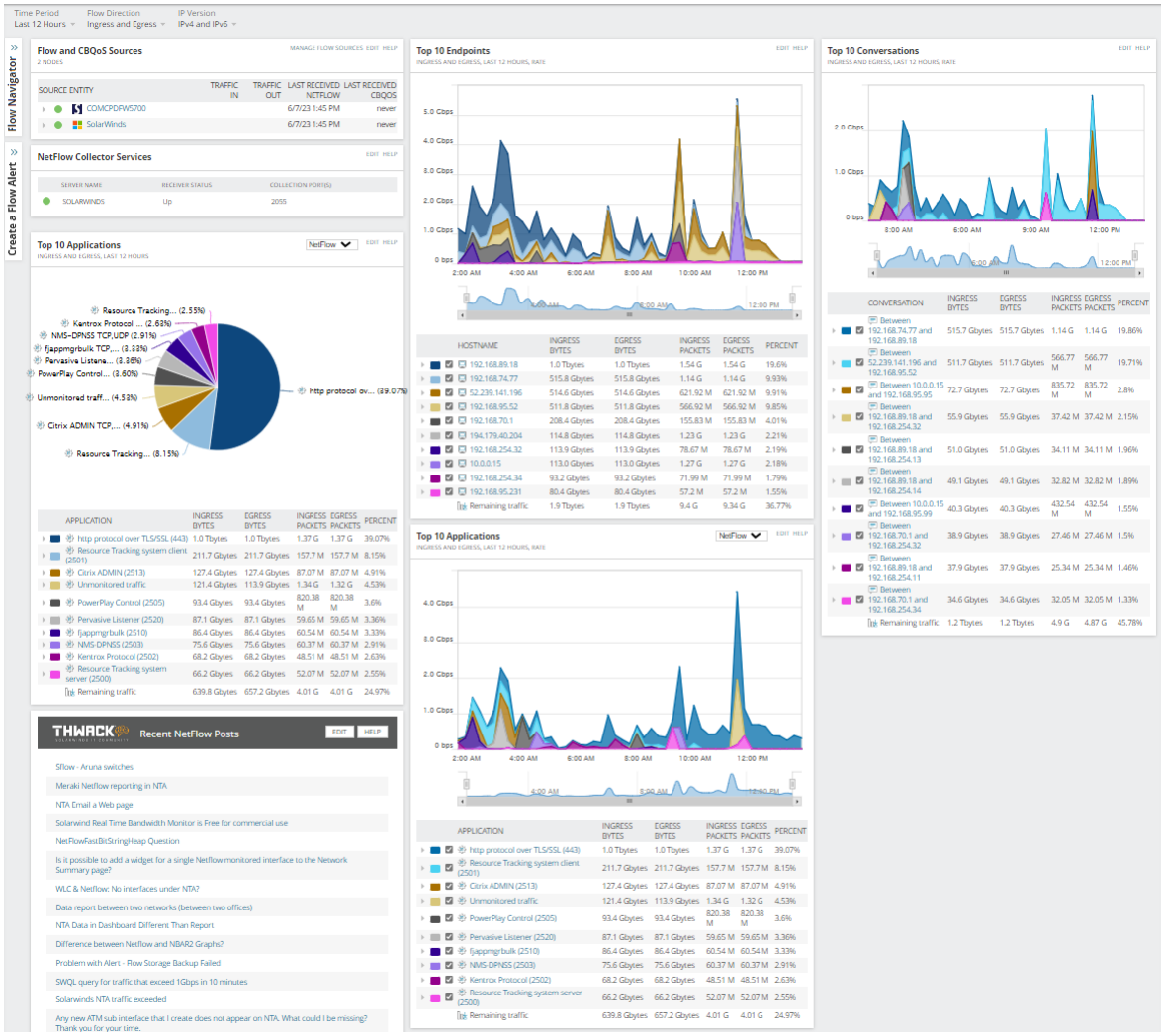


Fig. 5.23: Vista genèrica dels *flows* del *firewall* monitoritzats via IPFIX amb el mòdul NTA. Font: Elaboració pròpia.

A part d'afegir els equips de *networking*, que és l'objectiu principal, la mateixa MV *Windows* on està instal·lat el *Solarwinds* automàticament apareix com un node. Així doncs, es pot conèixer l'estat de la MV. Així mateix, també s'ha instal·lat un agent de *Solarwinds* on està instal·lada la base de dades, la MV *SolarWindsSQL*. Aquest agent és un executable que es pot descarregar des de la mateixa GUI[19] del *Solarwinds* (figura 5.24) i es pot instal·lar en màquines *Windows*. Aquest agent utilitza un protocol propi (figura 5.25) per enviar la informació a l'agent principal el qual està instal·lat el *Solarwinds*. D'aquesta manera, s'afegeix com a node la MV *SolarWindsSQL*. En ser màquines *Windows* es poden veure diferents paràmetres: detalls de l'equip (nom, SO i *hardware*), estat de l'equip (si està operatiu o no),

[19] Graphical User Interface

temps de resposta i latència, utilització de la CPU i RAM i l'emmagatzematge dels discs.

En la figura 5.26 es pot apreciar com es representen aquests paràmetres.

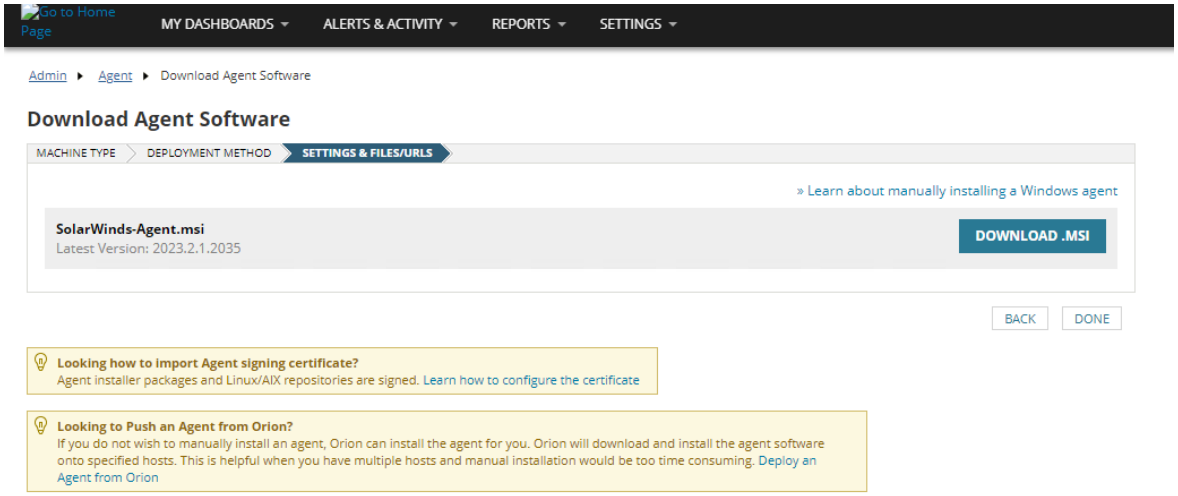


Fig. 5.24: Descarrega de l'agent des de la interfície gràfica del *Solarwinds*. Font: Elaboració pròpia.

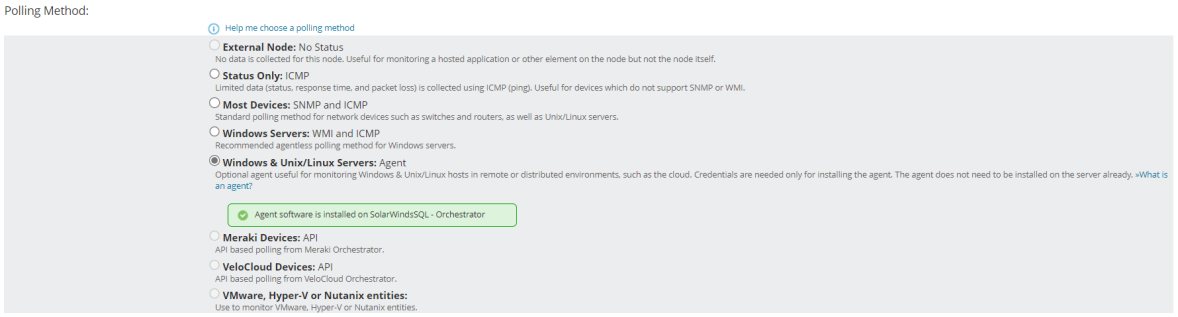


Fig. 5.25: Elecció del mètode de monitorització de l'agent de *Solarwinds*. Font: Elaboració pròpia.

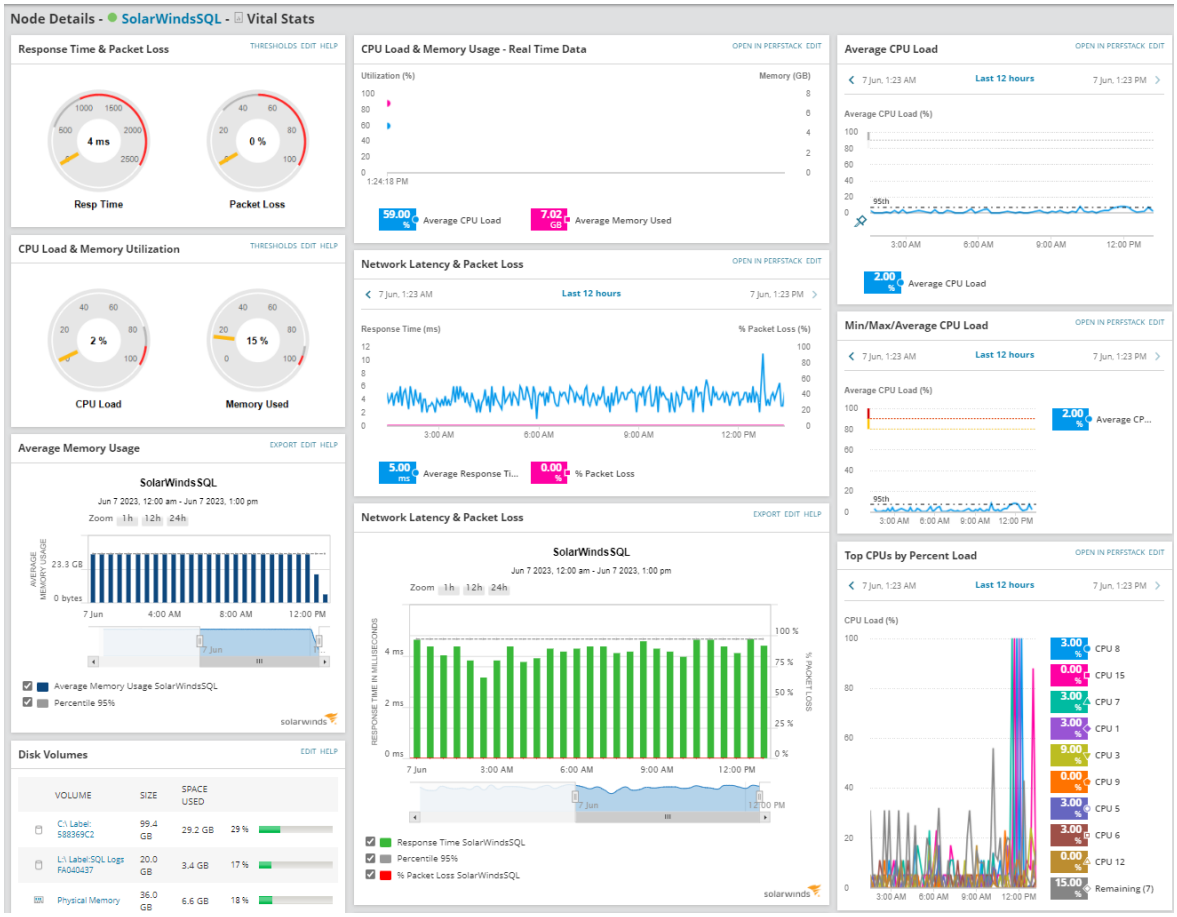


Fig. 5.26: Paràmetres de salut de la MV *SolarWindsSQL*. Font: Elaboració pròpia.

A part de poder consultar les dades a temps real, totes les dades que es reben són guardades per un període de temps raonable per poder consultar-les i analitzar-les a posteriori. Així mateix, es pot veure l'evolució dels volums de tràfic per poder detectar tendències, detectar carències de recursos o fer una auditoria d'algun tràfic sospitós que s'ha detectat a posteriori.

5.6 Personalització del *Solarwinds*

Tenint els nodes configurats i rebent les dades es necessari que aquestes siguin mostrades de la forma més clara i intuïtiva possible. *Solarwinds*, per si mateix, per defecte ja mostra la informació de forma simple i clara. Tot i això, cada infraestructura té les seves peculiaritats i necessitats pel qual sempre es pot afinar més segons les necessitats de cada usuari.

5.6.1 Personalització de *dashboards* i mapes

Per aconseguir personalitzar el *Solarwinds* a les necessitats de la infraestructura, els *dashboards* personalitzables són de gran utilitat. Així mateix, es pot adaptar cada tipus de menú segons convingui més. En la figura 5.30 es mostra com es pot editar-ne un.

Per tant, s'han personalitzat els *dashboards* que resumeixen l'estat de la infraestructura: Summary Home (figura 5.28), NPM Summary (figura 5.29) i NTA Summary (figura 5.23). També s'han personalitzat els *dashboards* dels paràmetres de salut dels equips vist en les figures 5.20 i 5.21. En la figura 5.27 es pot veure el menú de navegació entre *dashboards*.

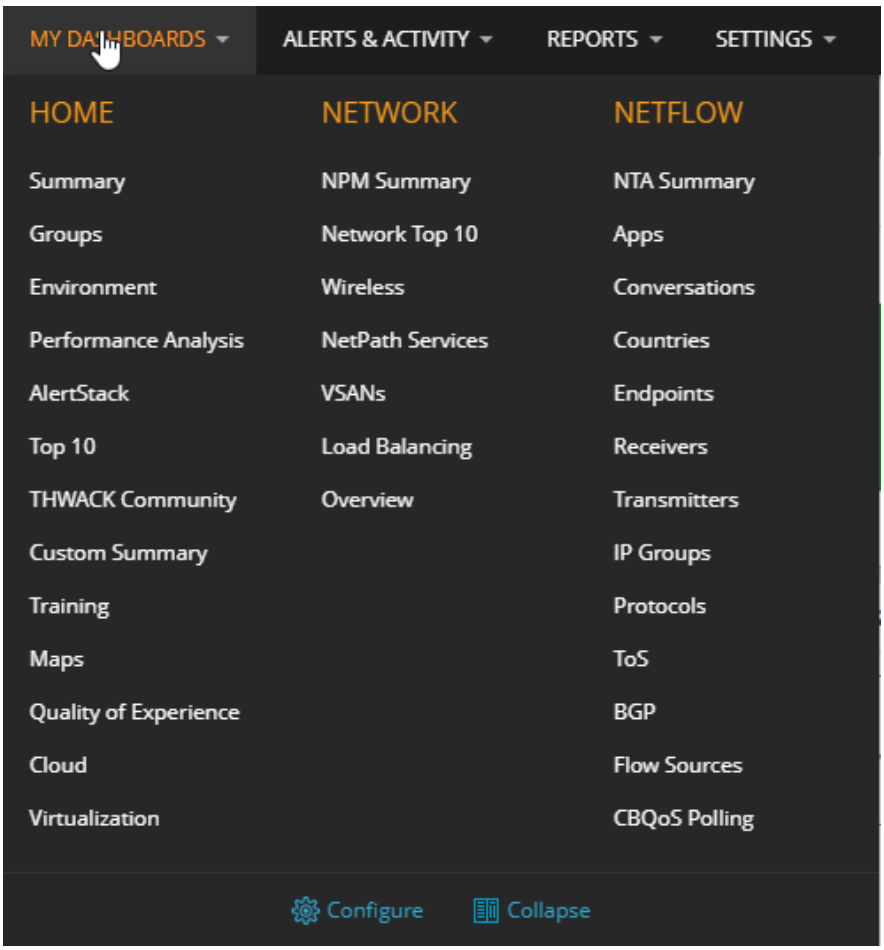


Fig. 5.27: Menú de navegació dels diferents *dashboards*. Font: Elaboració pròpia.

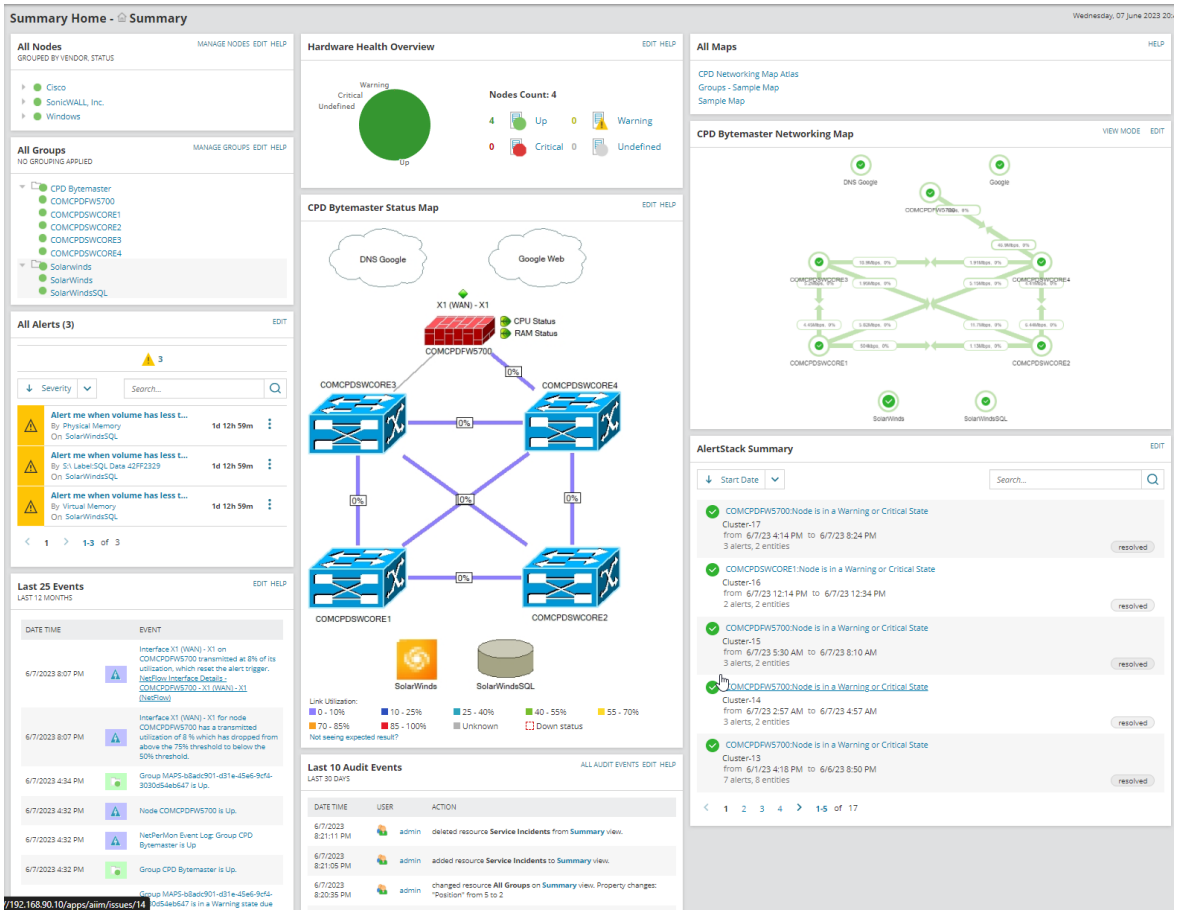


Fig. 5.28: *Dashboard* de *Summary Home*, pantalla inicial de la GUI. Font: Elaboració pròpia.

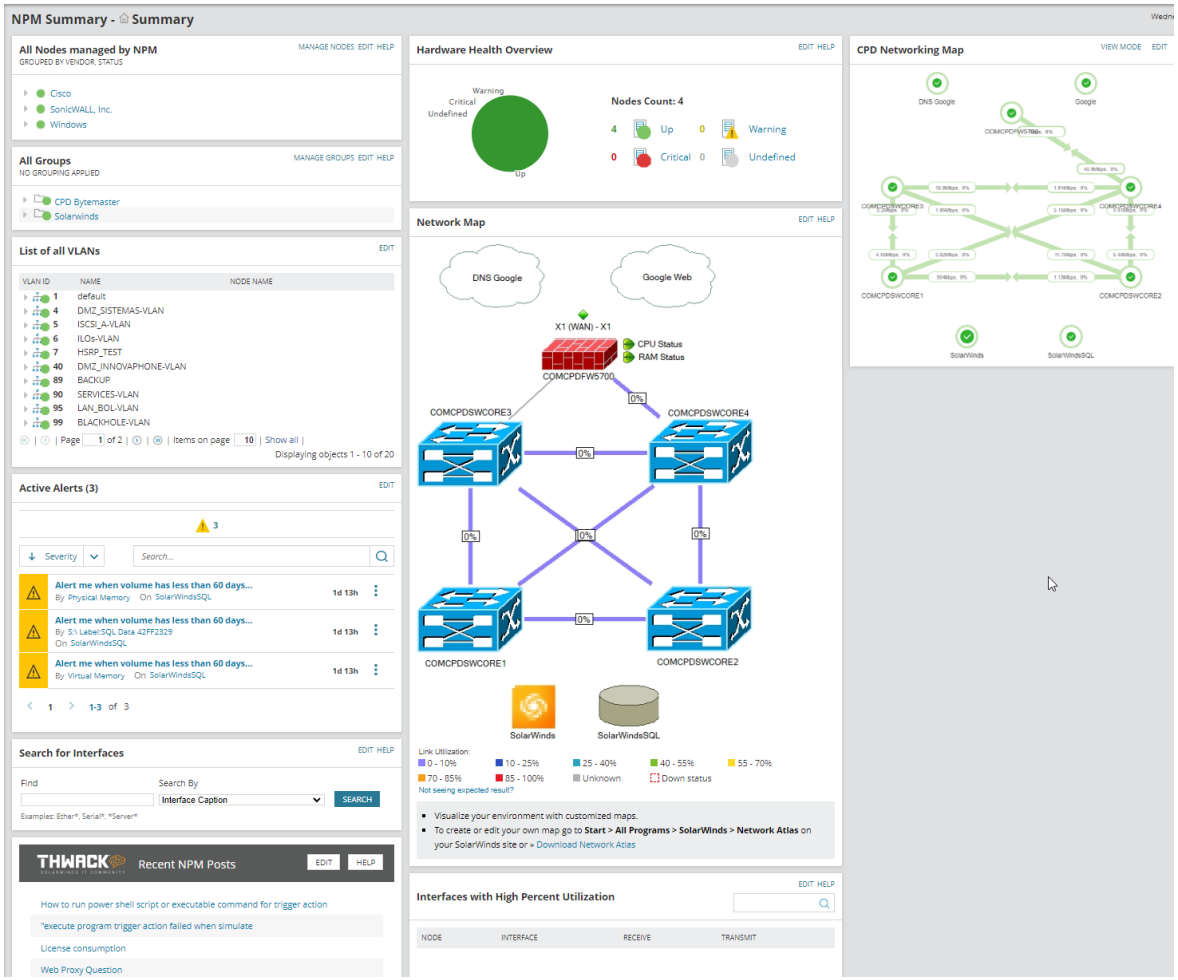


Fig. 5.29: *Dashboard* de *NPM Sumamry*, pantalla inicial del mòdul NPM. Font: Elaboració pròpia.

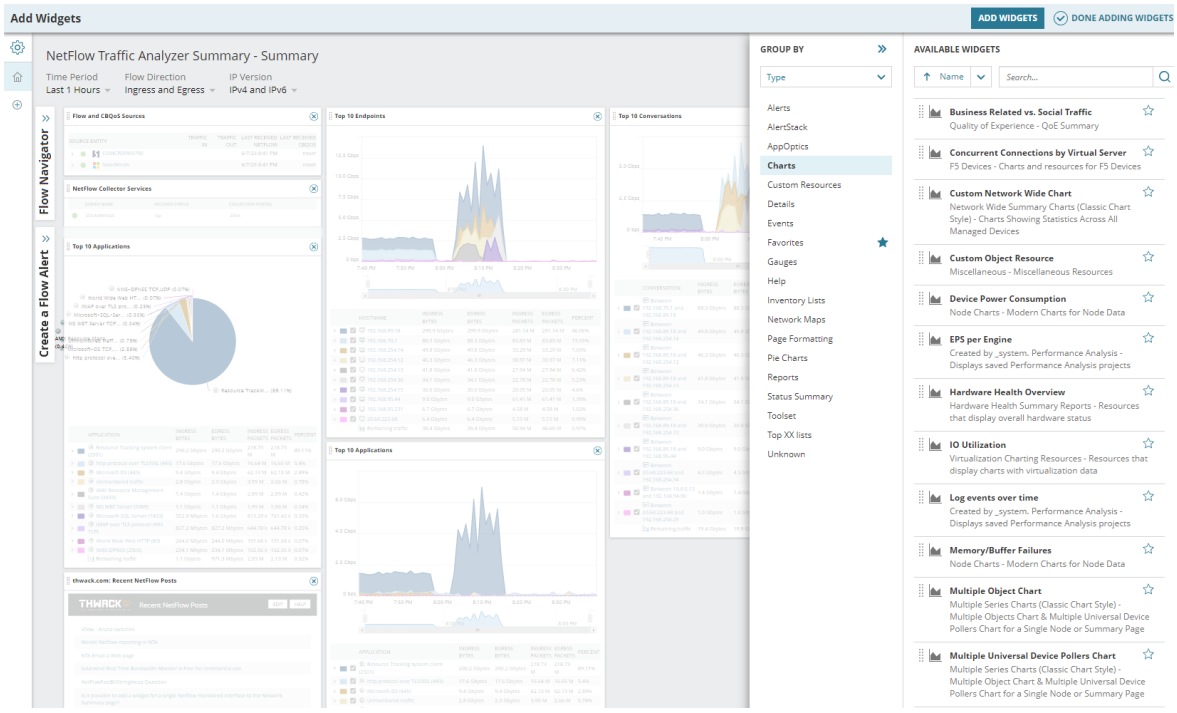


Fig. 5.30: Pantalla d'edició d'un *Dashboard*. Font: Elaboració pròpia.

Altrament a personalització dels *dashboards*, també s'han generat un parell de mapes. Es poden veure en les figures 5.31 i 5.32. Aquests informen de la distribució dels equips de xarxa i també del seu estat. Així com, la velocitat d'enllaç i la utilització d'aquest. Si el seu estat és d'avís o crític, els nodes del mapa canviaran de color a groc o vermell respectivament.

D'aquesta manera es pot identificar també de forma visual quins equips tenen alguna alerta o problema. En ser interactius, es pot accedir als detalls dels equips fent clic sobre les icones dels nodes. També s'han afegit els nodes de *Solarwinds* i *SolarwindsSQL*.

En la figura 5.33 es mostra el *software* d'edició utilitzat pel mapa de la figura 5.31.

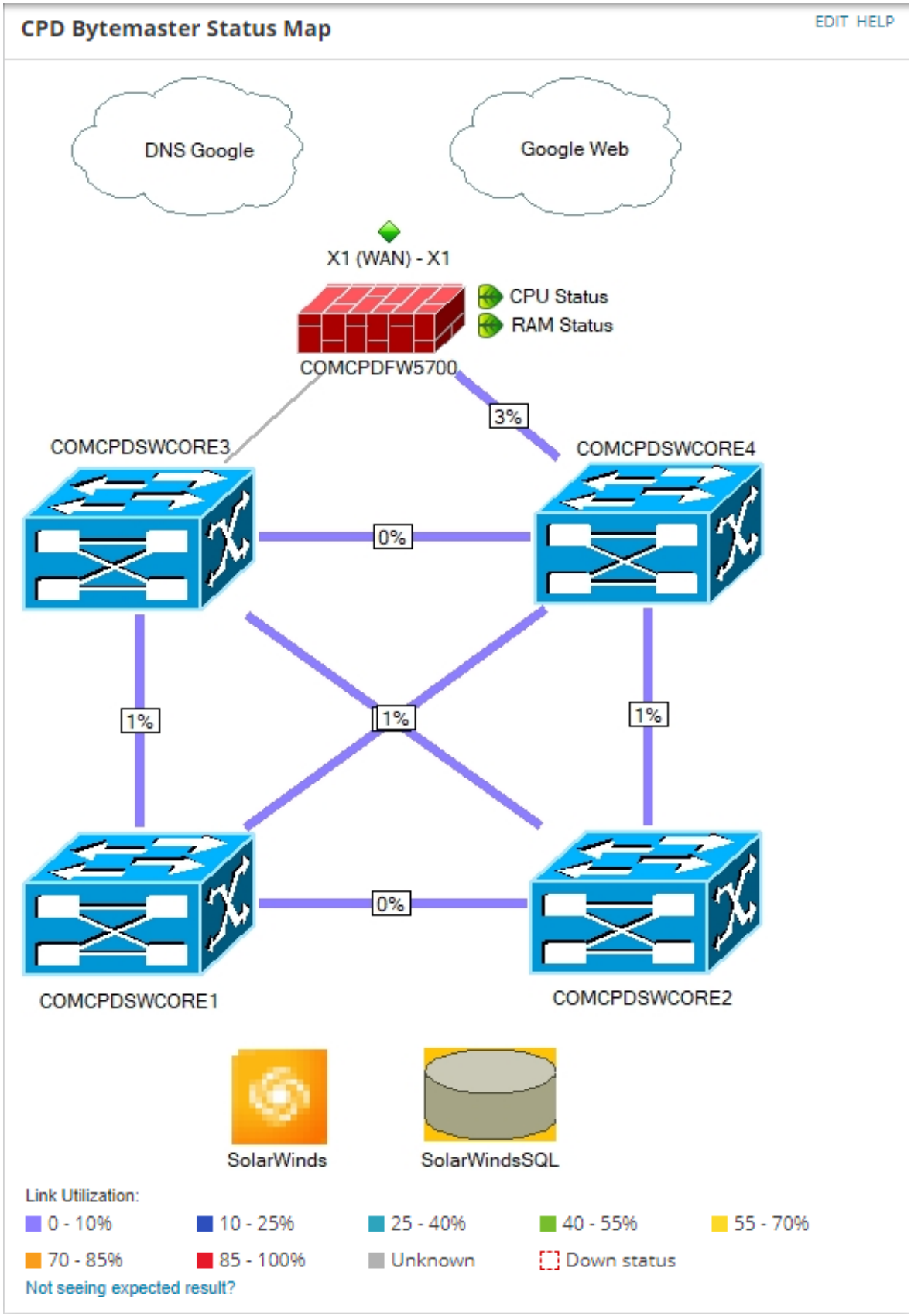


Fig. 5.31: Mapa d'estat del CPD de Bytemaster. Font: Elaboració pròpia.

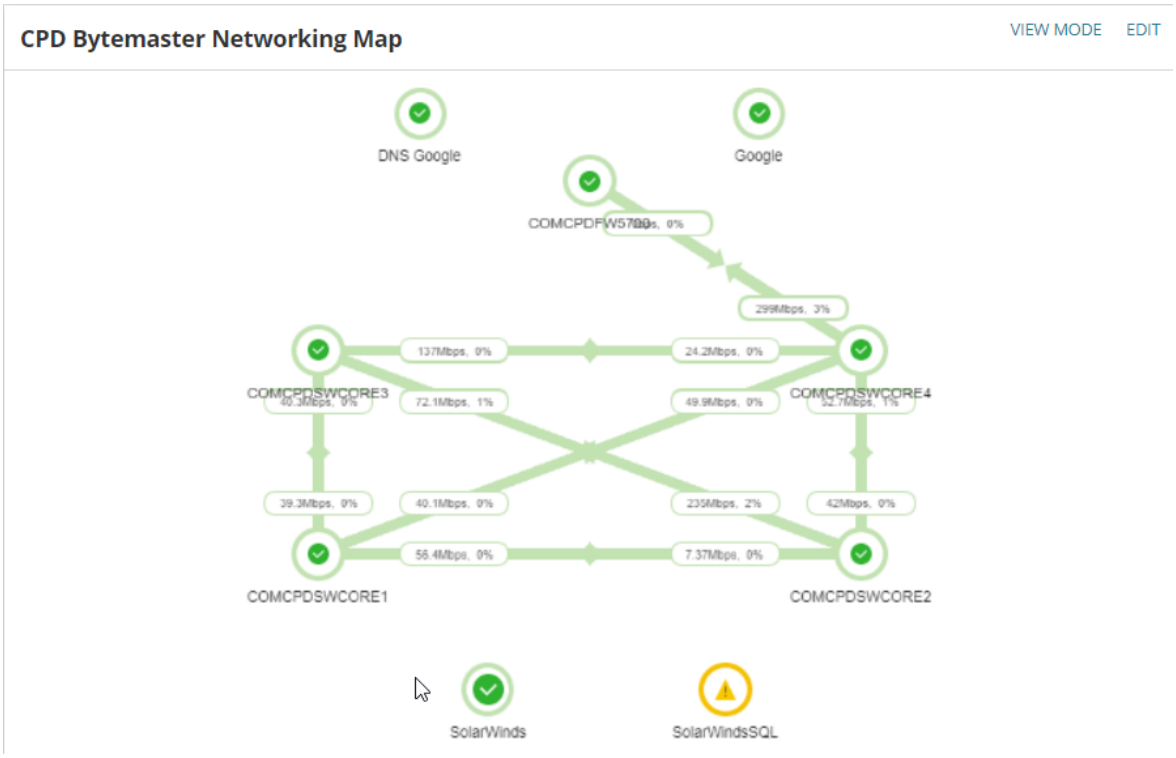


Fig. 5.32: Mapa de xarxa del CPD de Bytemaster. Font: Elaboració pròpia.

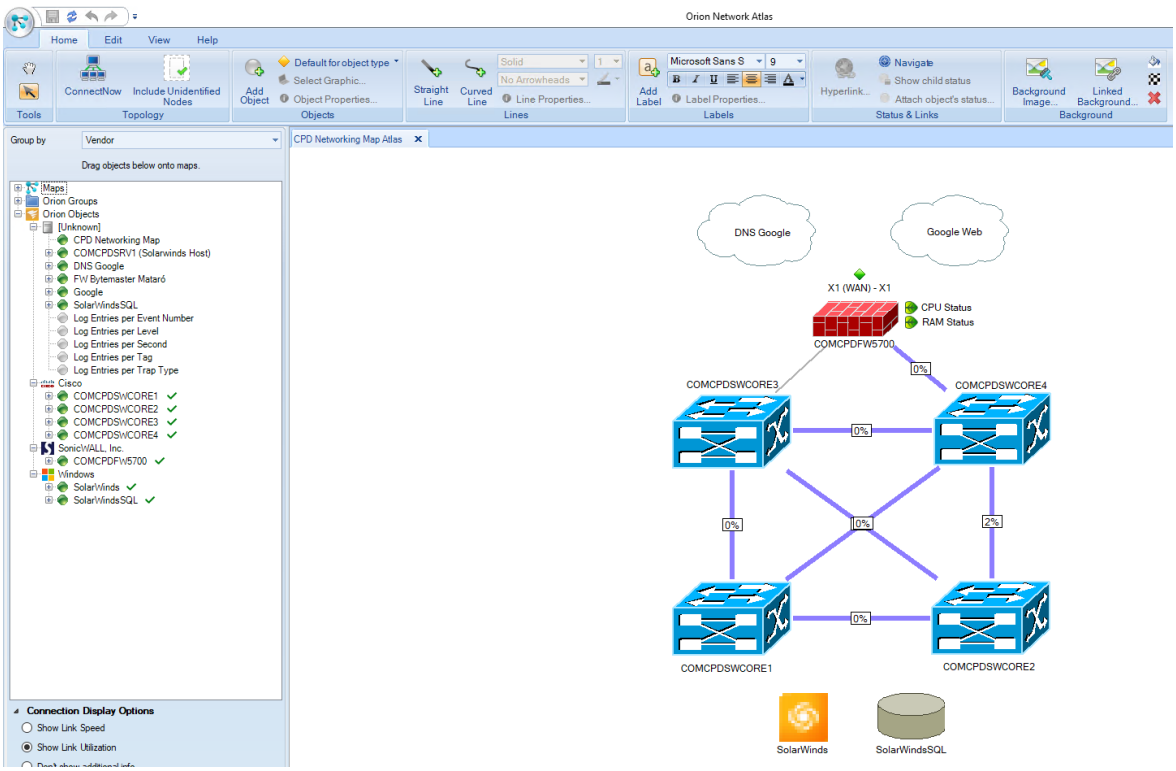


Fig. 5.33: *Software* Network Atlas, propietari de *Solarwinds* instal·lat en l'agent principal per generar els mapes. Font: Elaboració pròpia.

A més a més, els mapes permeten afegir un tipus d'objecte *probe*[20] anomenats *NetPath*. En aquest cas, apunten a dos serveis de *Google* (web i DNS[21]). Els *netpaths* són una característica del *Solarwinds* que permet traçar el camí fins al destí desitjat. Cada cert temps, 5-10 minuts, verifica si el recurs és accessible analitzant la seva latència i els paquets perduts. És força útil per concloure si hi ha algun problema dins la xarxa o fora. En mantenir un històric, si n'hi ha hagut algun amb anterioritat també es pot identificar. Veure figures 5.34 i 5.35.

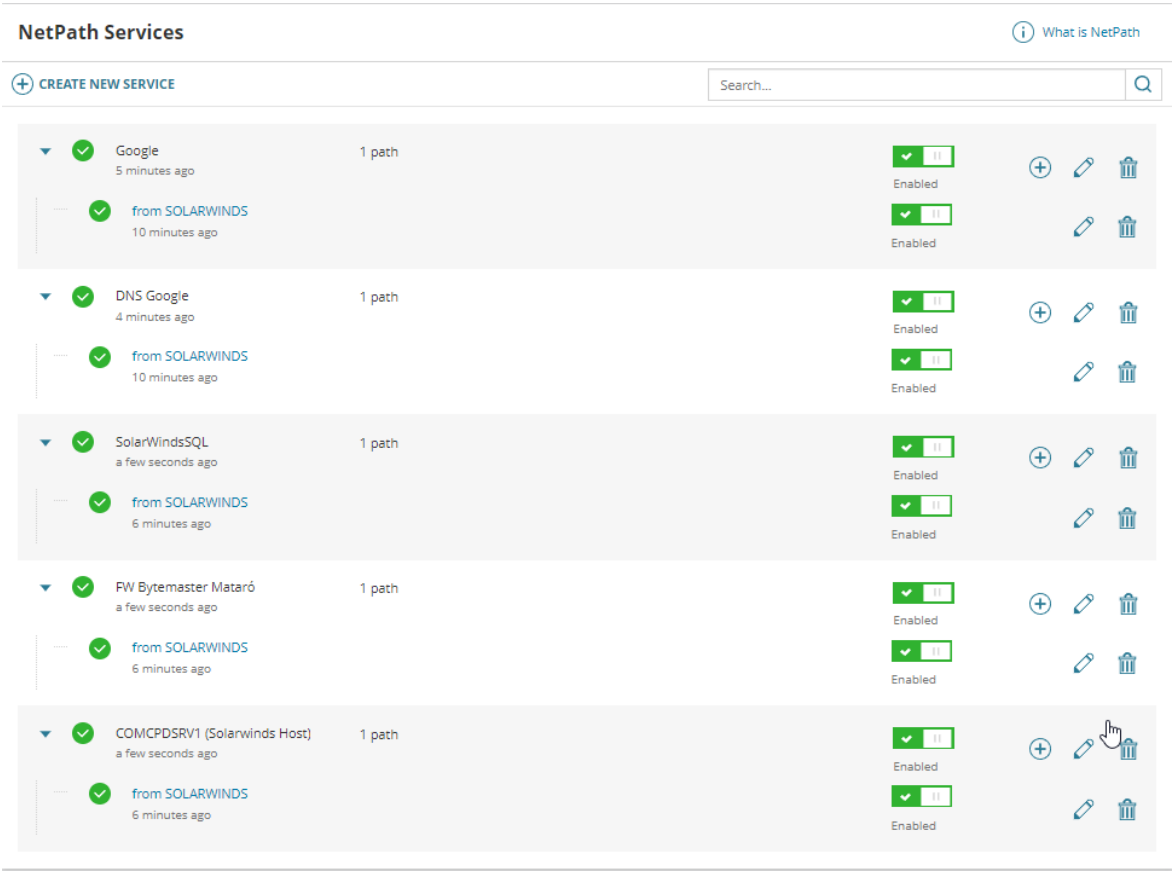


Fig. 5.34: Diferents *netpaths* útils configurats en el *Solarwinds*. Font: Elaboració pròpia.

[20]Sondes que verifiquen l'estat d'un recurs
[21]Domain Name Server

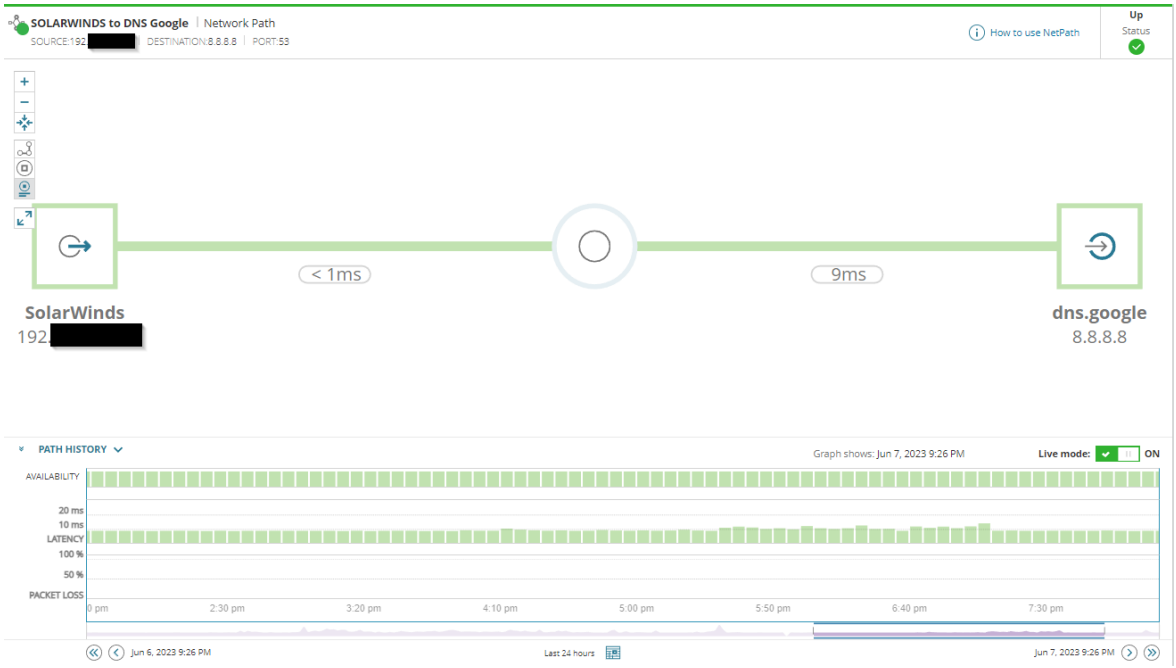


Fig. 5.35: *Netpath* cap a un DNS de Google amb el seu històric. Font: Elaboració pròpia.

5.6.2 Tractament d'alertes

Un dels objectius principals del projecte és tenir les dades del tràfic de la infraestructura disponibles i ben organitzades. Amb això, però, no és suficient per tenir un sistema sòlid de monitorització. És necessari un correcte tractament de les alertes.

La plataforma de Bytemaster opera les 24 hores del dia els 365 dies de l'any i no sempre hi ha un tècnic revisant l'estat de la plataforma. Ja sigui perquè sigui fora d'horari laboral o tingui altres tasques a realitzar durant aquesta. Així doncs, és imprescindible un sistema d'alertes que pugui avisar als tècnics d'aquelles casuístiques que siguin prou importants per a prestar-hi atenció.

En *Solarwinds*, una alerta es pot considerar com un missatge que es mostra en la GUI i queda enregistrat de forma automàtica quan és dona una condició o esdeveniment. Per exemple, un ventilador d'un *switch* deixa de funcionar. En aquest cas, el sistema detectarà que aquest ha deixat de funcionar i mostrarà un missatge avisant que ha succeït un esdeveniment rellevant. Les alertes tenen dues possibles categoritzacions o estats de severitat; avís (*Warning*) o crític (*Critical*). Es podrien afegir més tipus de severitat, però no s'ha trobat necessari. La severitat

és personalitzable, es pot escollir quin tipus de severitat es vol per cada esdeveniment i així adaptar-ho a les necessitats de cada plataforma.

En les figures 5.36 i 5.37 es mostren dos menús de personalització d'alertes.

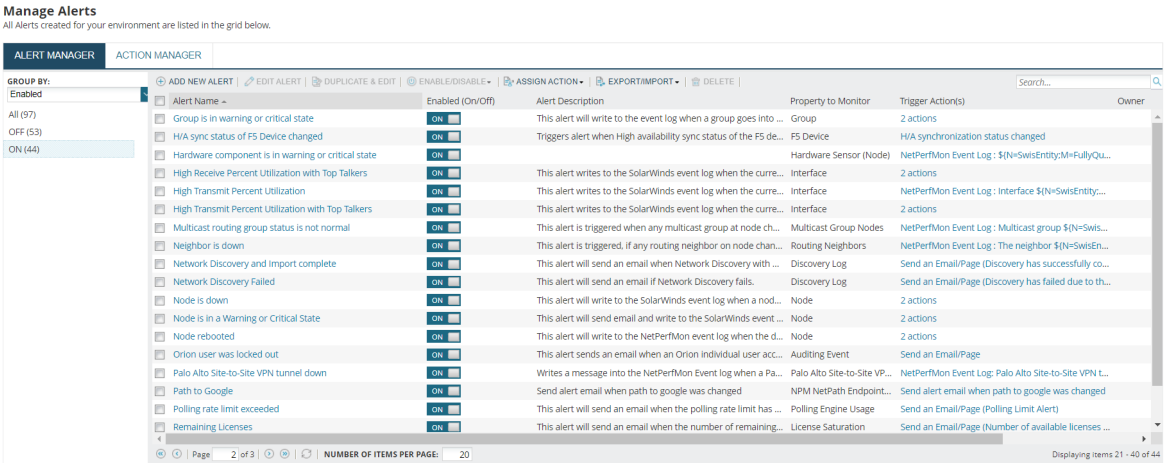


Fig. 5.36: Menú *Manage Alert* que permet crear alertes personalitzades o editar-les. Font: Elaboració pròpia.

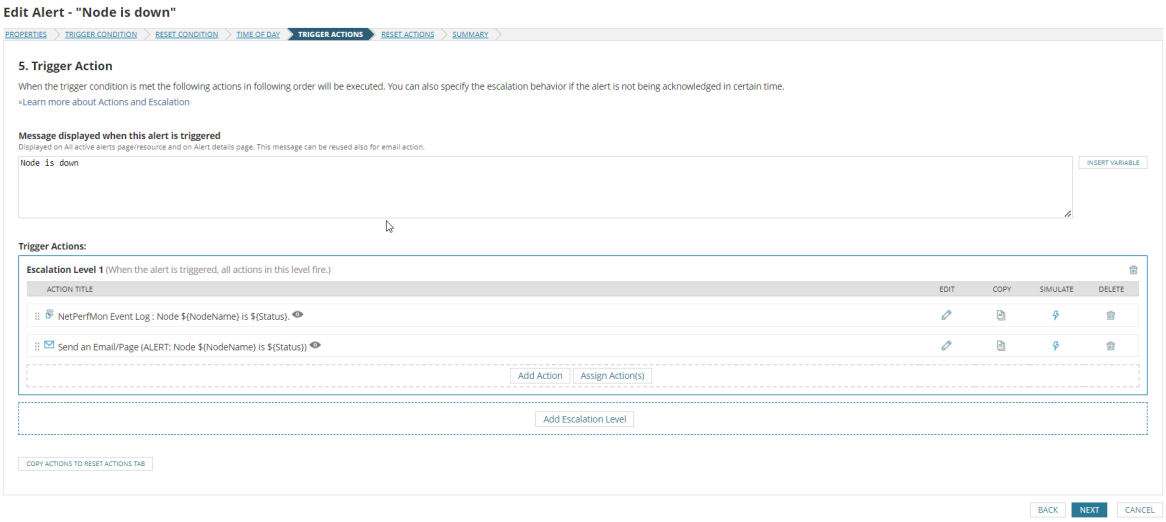


Fig. 5.37: Menú d'edició d'una alerta. Font: Elaboració pròpia.

La forma més ràpida de detectar una alerta és revisant els *Summary Dashboards* vists anteriorment, veure figures 5.28, 5.29. En aquests, si algun equip té alguna incidència, el seu nom o icona al mapa canviarà de color segons la severitat. Però això només és útil si l'esdeveniment que activa l'alerta està succeint en aquell moment. Si l'estat de l'equip s'ha restaurat, l'usuari no sabrà si hi ha succeït algun problema. Exceptuant que en el propi

dashboard hi ha una taula amb les últimes alertes.

Per poder veure en detall l'històric de les alertes *Solarwinds* disposa del menú *AlertStack*, figura 5.38. En aquest, es mostren les alertes que hi ha hagut de forma gràfica en un eix temporal.

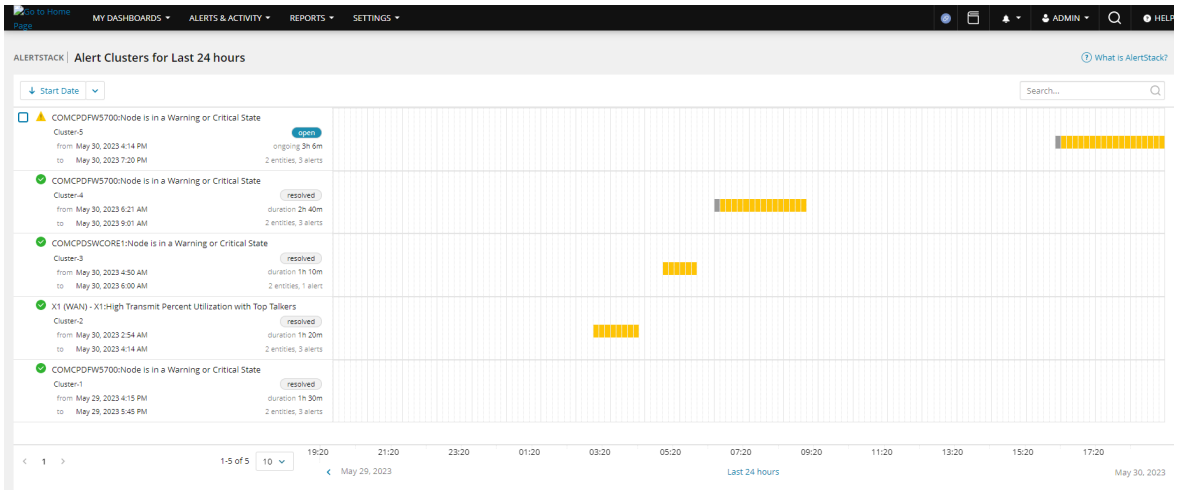


Fig. 5.38: Menú d'alertes *AlertStack*. Font: Elaboració pròpia.

Encara més, aquest mostra la duració de l'esdeveniment, la severitat, quan s'ha iniciat i quan s'ha acabat i si s'ha resolt o no. També disposa d'un cercador i un filtre per llistar les alertes. En cada alerta es pot fer clic i veure'n els detalls. Veure figura 5.39. Dins de la pestanya dels detalls, es mostren gràficament en l'eix temporal els diversos esdeveniments que s'han donat i es pot fer un seguiment al minut de quant ha durat cada un. Així mateix, també es mostren els equips involucrats.

Aquesta característica és molt útil pels tècnics que han de supervisar diàriament l'estat de salut de la plataforma, ja que ràpidament poden veure el que ha succeït anteriorment.

Fig. 5.39: Detalls d'una alerta del menú *AlertStack*. Font: Elaboració pròpia.

Els altres sistemes que té actualment Bytemaster: Nagios, LibreNMS i GMS envien les alertes via correu electrònic en diferents bústies compartides. Això provoca que identificar la duració de les incidències sigui més feixuc. Es necessita més temps i comprensió al ser necessari creuar la informació de diversos correus electrònics, dificultant així la tasca.

Solarwinds també disposa d'enviament d'alertes per correu electrònic. S'ha configurat que enviï les alertes més rellevants en una bústia compartida on tenen accés tots els tècnics del departament. Veure figures 5.40 i 5.41. D'aquesta manera s'augmenten les possibilitats de detectar més ràpidament si hi ha una incidència greu. Sabent això, es pot procedir a accedir a la GUI de *Solarwinds* per continuar amb la solució del problema. En aquest cas, però, les alertes enviades per correu només s'utilitzen per avisar que hi ha hagut alguna incidència, la revisió i l'anàlisi d'aquestes es poden realitzar més fàcilment des de la GUI.

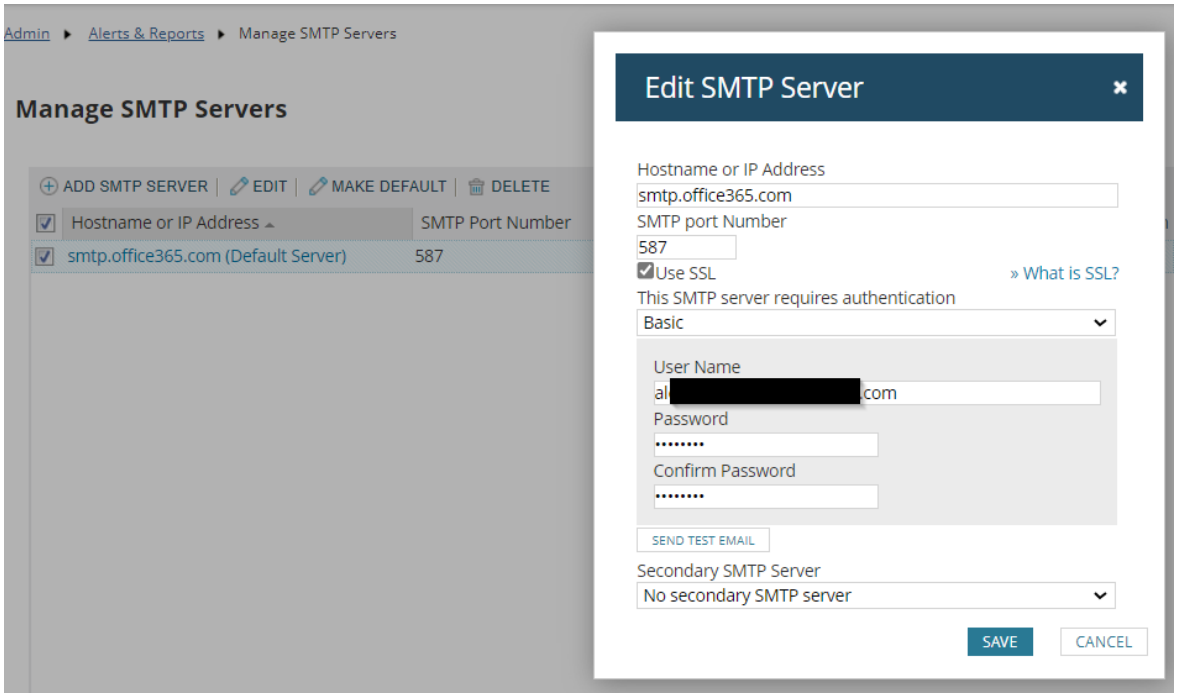


Fig. 5.40: Configuració del servidor de correu SMTP per l'enviament de correus electrònics des de *Solarwinds*. Font: Elaboració pròpia.

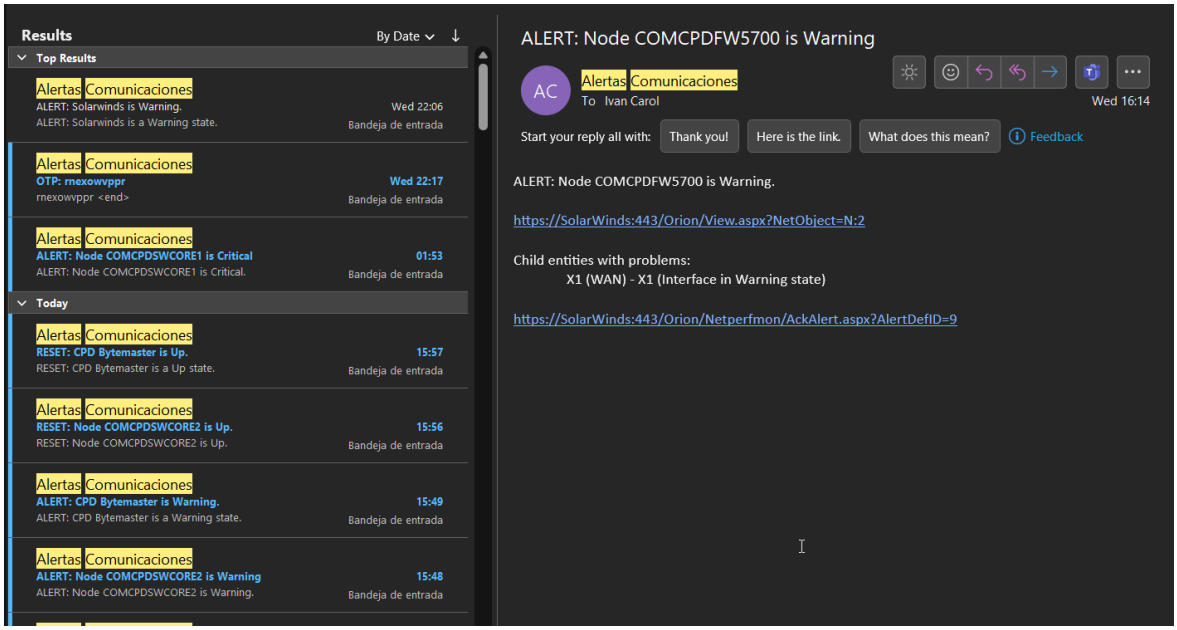


Fig. 5.41: Correus d'alertes de *Solarwinds*. Font: Elaboració pròpia.

5.6.3 Gestió d'alertes

La plataforma de *Solarwinds* és usada per més d'un tècnic. Els tècnics no tenen perquè comunicar-se entre ells en disposar de certa autonomia. Això pot provocar que dos o més

tècnics puguin veure una alerta simultàniament i revisar-ho a la vegada. En aquest cas, estarien solapant-se en la mateixa tasca malgastant un temps que es podria dedicar en dur a terme altres tasques. Per evitar-ho, *Solarwinds* disposa d'un sistema multiusuari el qual cada tècnic pot tenir el seu propi usuari. A més, el sistema d'alertes disposa d'un tractament personalitzat per usuari.

Quan es produeix una alerta, queda registrada independentment de si s'ha solucionat o no. *Solarwinds* anomena això una "Alerta activa". Aquesta alerta romandrà activa fins que un usuari la marqui com a reconeguda (*acknowledged*). En la figura 5.42 es mostra el menú d'alertes actives.

A més a més, els usuaris en tancar una alerta podran deixar una nota en forma de comentari com el que es veu en la figura 5.43. Aquesta nota pot servir per donar informació de com corregir una alerta en concret o per avisar al primer tècnic que l'ha resolt abans de tornar-ho a revisar. En disposar cada tècnic d'un usuari únic, quan es tanqui una alerta aquesta quedarà resolta i s'apreciarà qui l'ha marcat com a reconeguda. D'aquesta manera els tècnics poden veure quines alertes s'han revisat i per qui, així com quines alertes no han estat revisades.

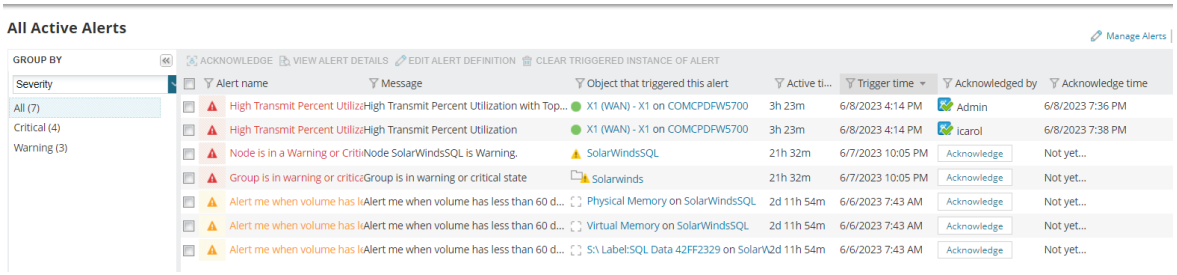


Fig. 5.42: Alertes actives. Notar que hi ha alertes tancades per usuaris diferents. Font: Elaboració pròpia.

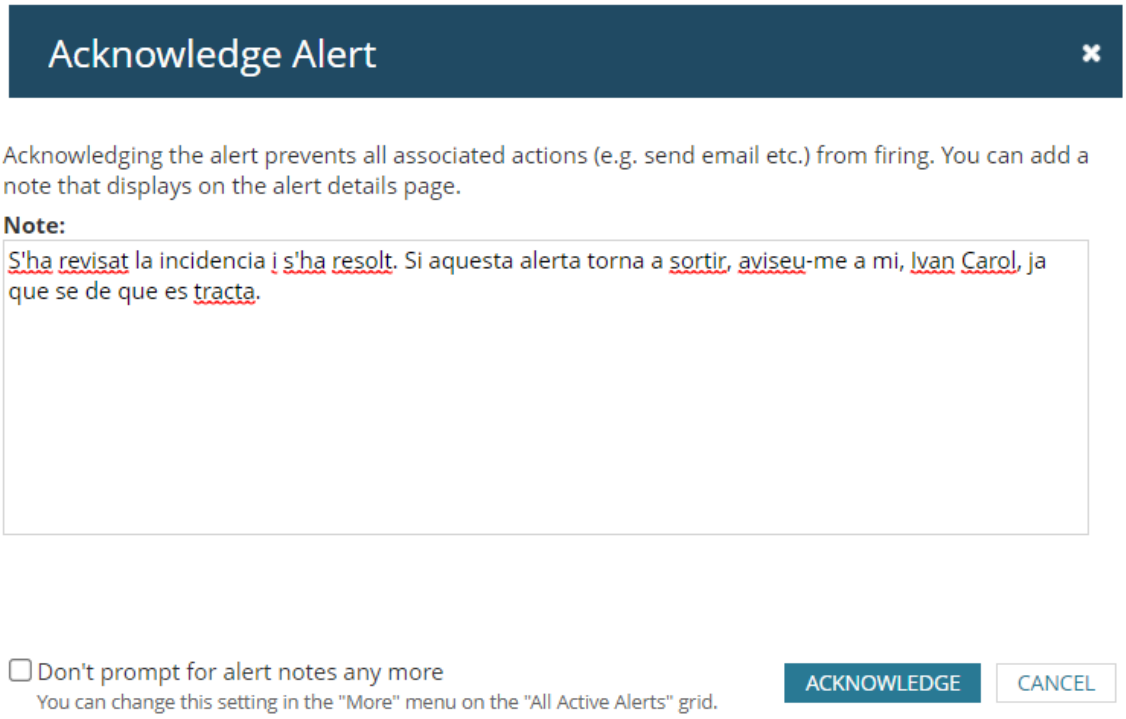


Fig. 5.43: Nota deixada per un usuari a tancar una alerta. Font: Elaboració pròpia.

A part d'usar els usuaris per la gestió d'alertes, aquesta funcionalitat també és útil per proporcionar a cada usuari els permisos que necessita. *Solarwinds* és força granular a l'hora d'assignar permisos als usuaris. També permet la creació de diversos tipus d'usuari, veure figura 5.44.

Es pot configurar que cada usuari només accedeix-hi a aquelles pestanyes que li són útils o necessita i permetre només la lectura de dades, evitant l'edició desitjada de nodes, objectes o mapes. Això comporta una capa extra de seguretat, evita que els usuaris més bàsics puguin comprometre l'estabilitat i el funcionament del *software*. En la figura 5.45 es pot apreciar una mostra de la varietat de permisos que se li poden assignar.

A més, el sistema registra amb esdeveniments les interaccions dels usuaris com es veu en la figura 5.46. Per tant, es pot realitzar una auditoria de les interaccions dels usuaris.

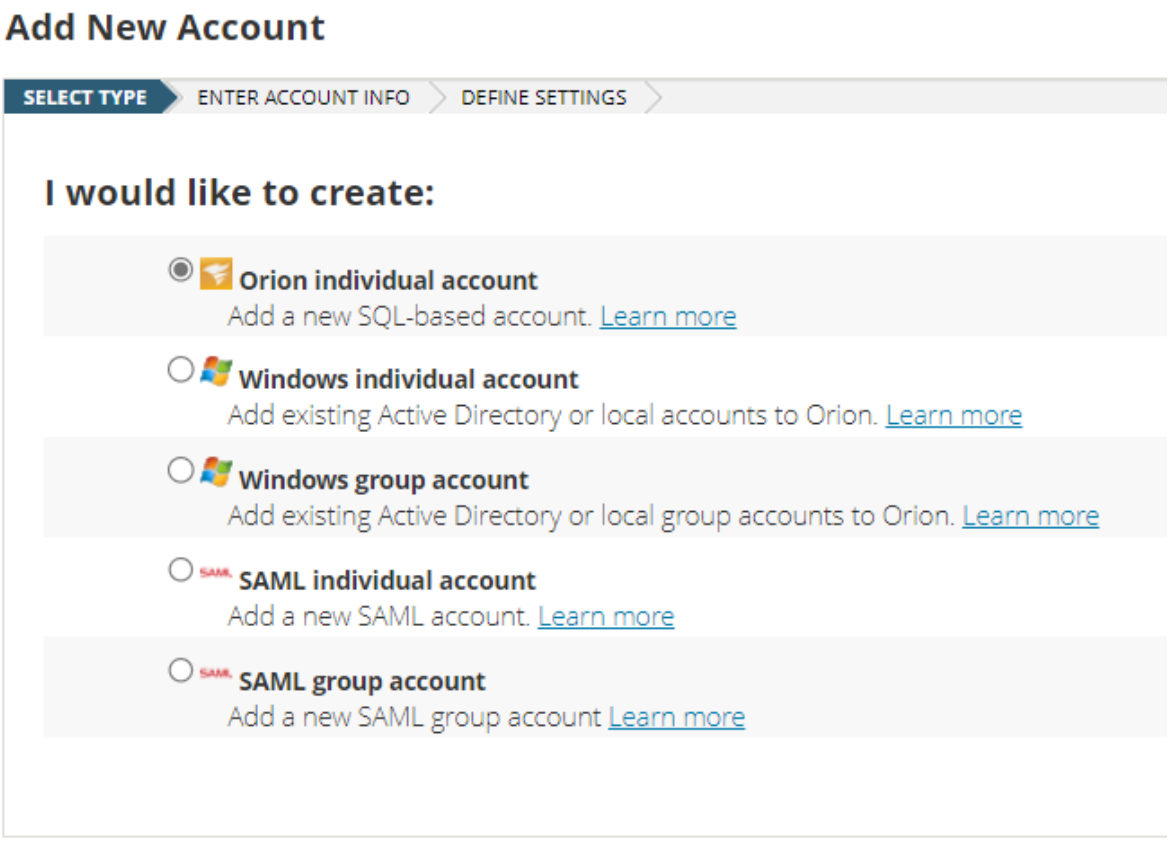


Fig. 5.44: Diferents tipus de creació d'usuari. Font: Elaboració pròpia.

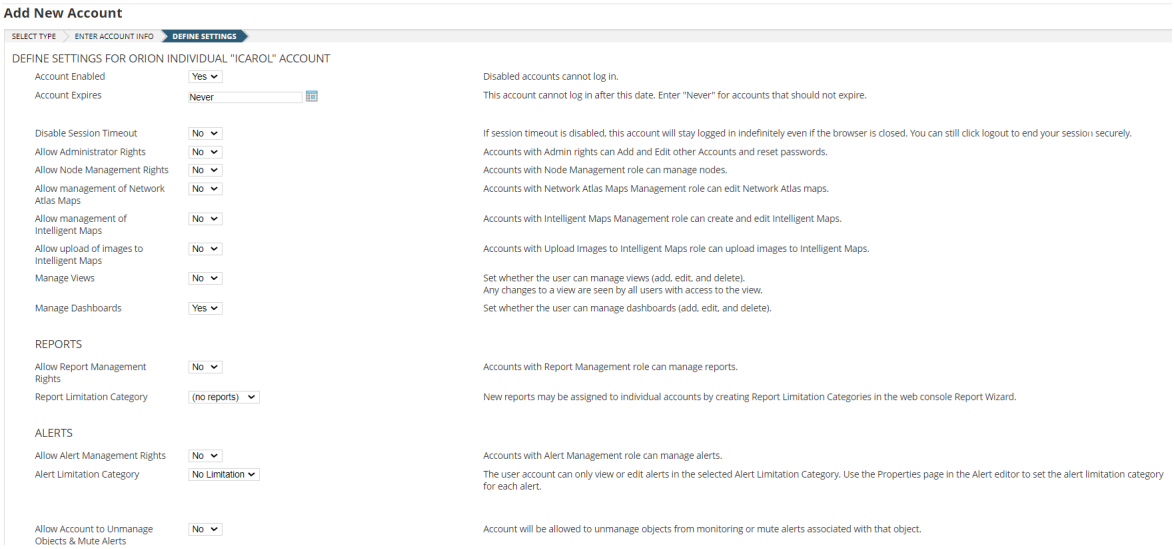


Fig. 5.45: Assignació de permisos d'usuari. Font: Elaboració pròpia.

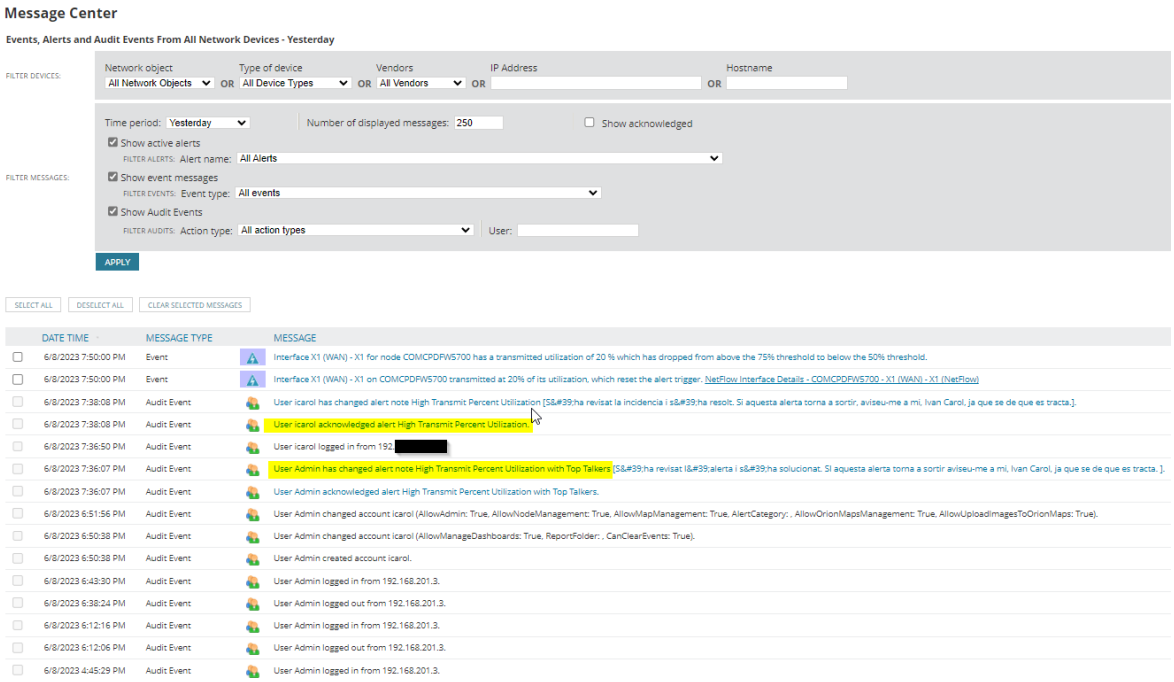


Fig. 5.46: Llista d'esdeveniments on es poden veure els canvis realitzats pels usuaris. Font: Elaboració pròpia.

5.7 Validació de la implementació

Aquest apartat té com a objectiu verificar la fiabilitat de la informació del *software*, és a dir, comprovar que les dades rebudes corresponen amb la realitat.

És important confirmar que les interpretacions que puguin fer de les dades corresponguin amb el tràfic real. Si no fos així, aquestes podrien dur a conclusions errònies i causar pèrdues de temps als tècnics en buscar problemes que no existeixin. Fins i tot, podria comportar en fer canvis en les configuracions dels equips que podrien afectar negativament a l'estabilitat del servei.

Per verificar empíricament aquesta casuística s'han realitzat les proves 5.7.1, 5.7.2 i 5.7.3. En aquestes, s'ha comprovat que la implementació de *Solarwinds* realitzada en la infraestructura de CPD mostra correctament el tràfic real que traspassa el *firewall*, és a dir, que correspon amb la realitat.

En conclusió, es pot assumir que les dades representades en el *Solarwinds* són confiables i es poden usar per extreure conclusions i prendre decisions.

5.7.1 Primera prova: Transferència amb el *software iperf3*

Per realitzar aquesta prova s'ha utilitzat el *software iperf3* [21]. Aquest és un *software open source* per realitzar proves d'estrès en xarxes IP les quals consisteixen en transferir el màxim de dades possible. *Iperf3* usa un mode client-servidor el qual ambdós tenen instal·lat el *software*. Per tal que la prova d'estrès tingui sentit convé que el client i el servidor estiguin a xarxes diferents, ja que d'aquesta manera tot el tràfic passarà pels seus respectius *gateways*.

Per aquesta prova, tant el client com el servidor estan a dues xarxes internes diferents, per tant, tot el tràfic passarà pel *firewall* (*gateway*) tal com s'ha explicat a l'apartat 2.3. Com el *firewall* és el dispositiu que envia les dades del tràfic, un cop acabada la prova s'hauria d'apreciar la informació al *Solarwinds*. Si es realitzés la prova en la mateixa xarxa, no es podria veure cap informació ja que ambdues màquines es comunicarien només a través dels *switches* a l'establir una comunicació de capa 2 (Mòdel OSI [22]).

Els resultats amb *iperf3* es poden veure en les figures 5.49 i 5.50.

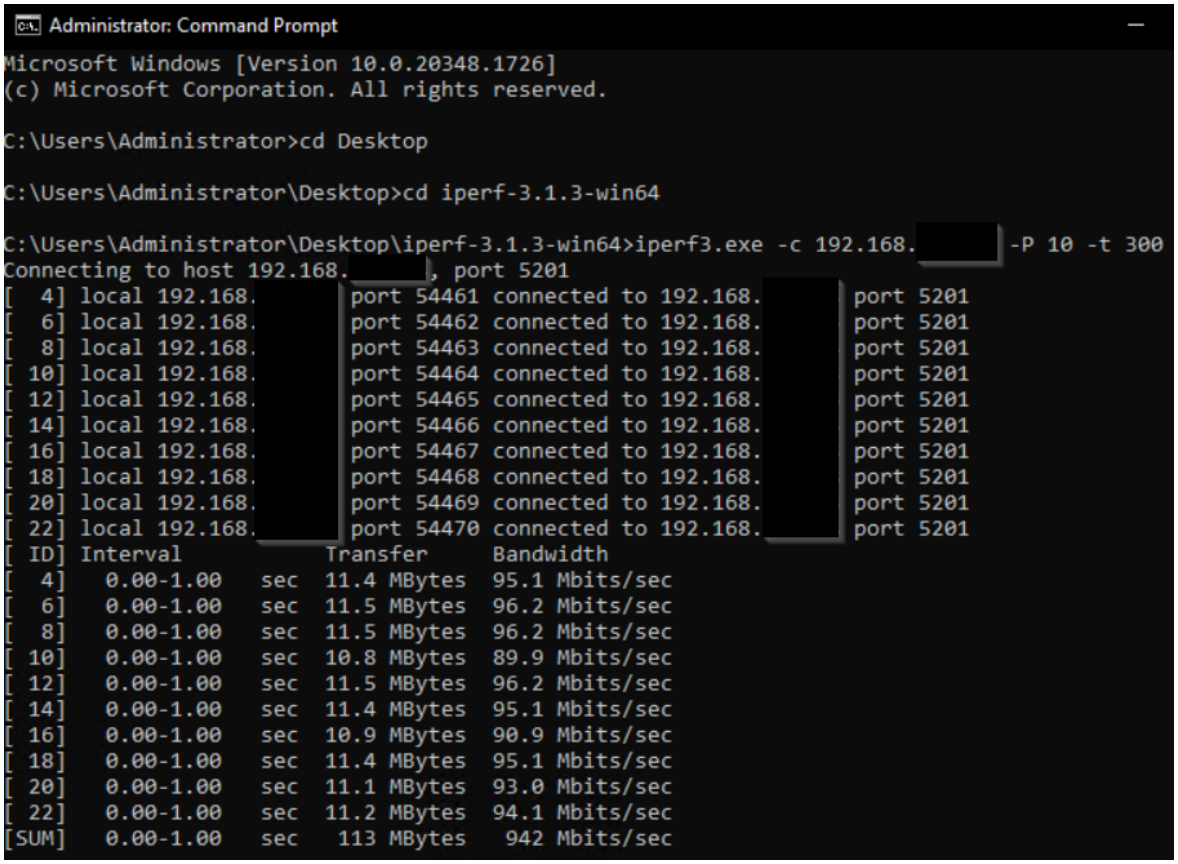


Fig. 5.47: Comanda per executar la prova des del client. Font: Elaboració pròpia.

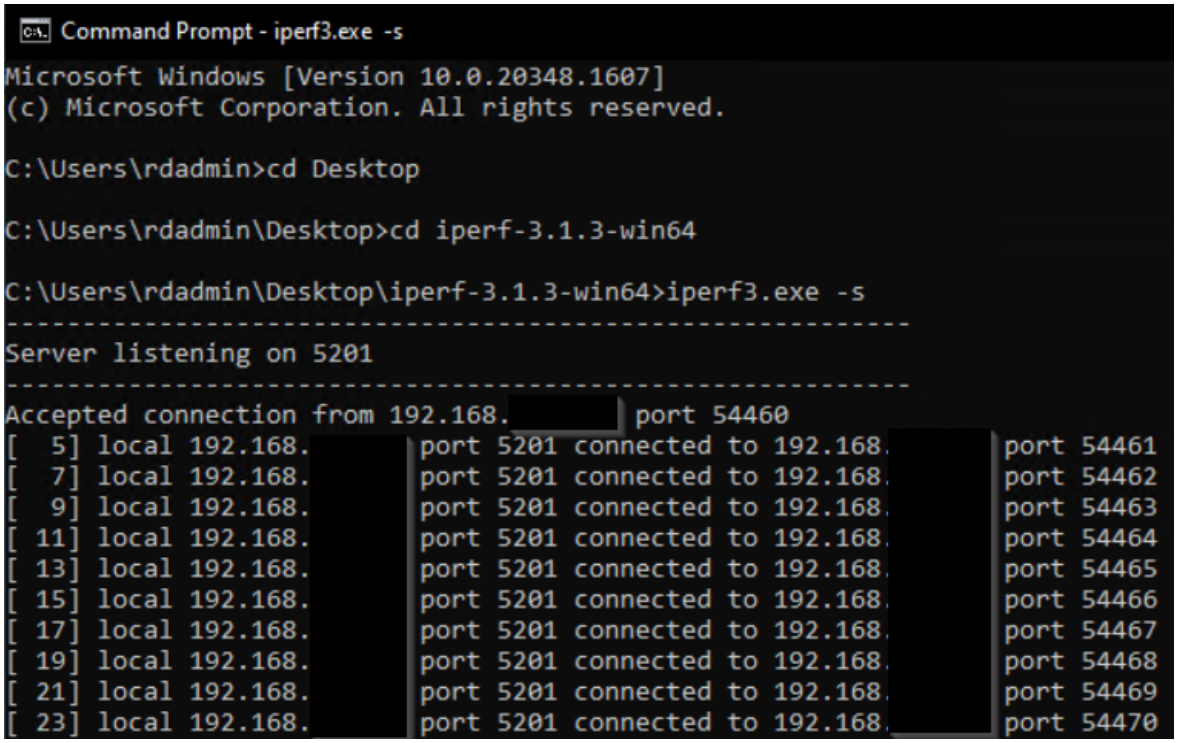


Fig. 5.48: Comanda per executar la prova des del servidor. Font: Elaboració pròpia.

En la figura 5.47 es pot veure que s'ha executat la comanda per iniciar la prova. Aquesta realitza 10 connexions independents durant un període de 5 minuts (300 segons). Es paral·lelitzen les connexions per tal d'aprofitar el màxim d'amplada de banda possible.

```
[ ID] Interval           Transfer     Bandwidth
[  4]   0.00-300.00 sec  3.42 GBytes  97.9 Mbits/sec                  sender
[  4]   0.00-300.00 sec  3.42 GBytes  97.9 Mbits/sec                  receiver
[  6]   0.00-300.00 sec  3.55 GBytes   102 Mbits/sec                  sender
[  6]   0.00-300.00 sec  3.55 GBytes   102 Mbits/sec                  receiver
[  8]   0.00-300.00 sec  3.38 GBytes  96.9 Mbits/sec                  sender
[  8]   0.00-300.00 sec  3.38 GBytes  96.9 Mbits/sec                  receiver
[ 10]   0.00-300.00 sec  3.23 GBytes  92.5 Mbits/sec                  sender
[ 10]   0.00-300.00 sec  3.23 GBytes  92.5 Mbits/sec                  receiver
[ 12]   0.00-300.00 sec  3.40 GBytes  97.5 Mbits/sec                  sender
[ 12]   0.00-300.00 sec  3.40 GBytes  97.5 Mbits/sec                  receiver
[ 14]   0.00-300.00 sec  3.10 GBytes  88.9 Mbits/sec                  sender
[ 14]   0.00-300.00 sec  3.10 GBytes  88.9 Mbits/sec                  receiver
[ 16]   0.00-300.00 sec  3.26 GBytes  93.4 Mbits/sec                  sender
[ 16]   0.00-300.00 sec  3.26 GBytes  93.4 Mbits/sec                  receiver
[ 18]   0.00-300.00 sec  3.13 GBytes  89.5 Mbits/sec                  sender
[ 18]   0.00-300.00 sec  3.13 GBytes  89.5 Mbits/sec                  receiver
[ 20]   0.00-300.00 sec  3.09 GBytes  88.5 Mbits/sec                  sender
[ 20]   0.00-300.00 sec  3.09 GBytes  88.5 Mbits/sec                  receiver
[ 22]   0.00-300.00 sec  3.27 GBytes  93.6 Mbits/sec                  sender
[ 22]   0.00-300.00 sec  3.27 GBytes  93.6 Mbits/sec                  receiver
[SUM]   0.00-300.00 sec  32.8 GBytes   940 Mbits/sec                  sender
[SUM]   0.00-300.00 sec  32.8 GBytes   940 Mbits/sec                  receiver

iperf Done.
```

Fig. 5.49: Resultat de la primera prova amb *iperf3*. Font: Elaboració pròpia.

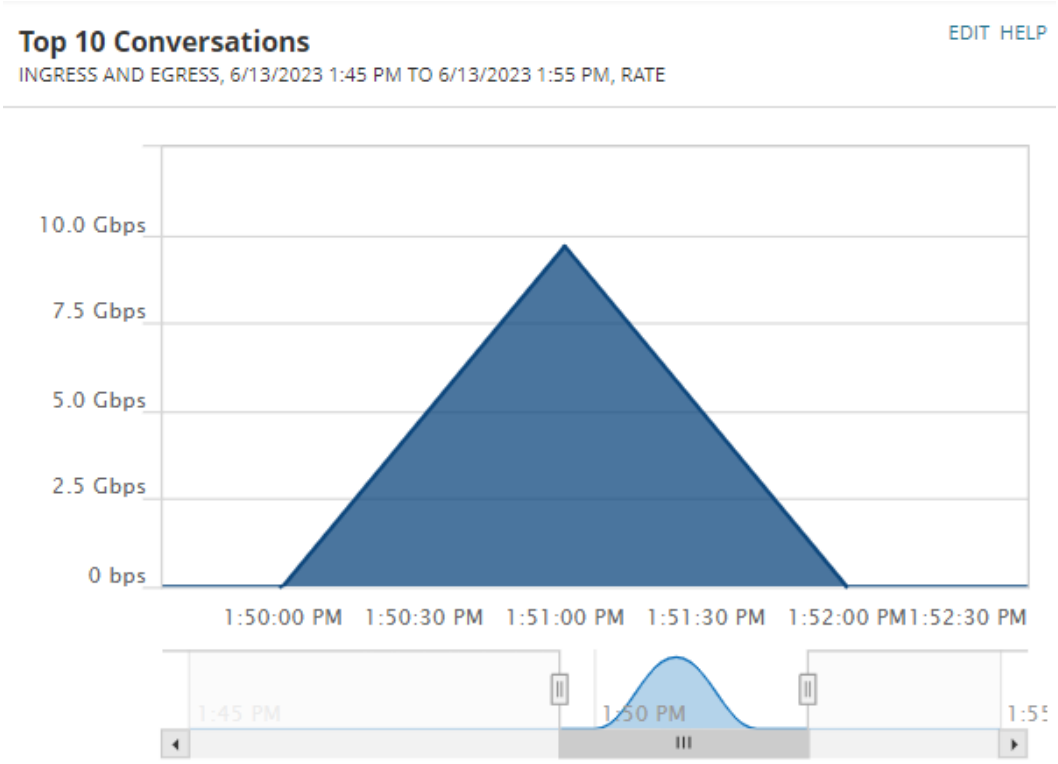
```
[ ID] Interval           Transfer     Bandwidth
[  4]   0.00-300.00 sec  3.39 GBytes  97.0 Mbits/sec                  sender
[  4]   0.00-300.00 sec  3.39 GBytes  97.0 Mbits/sec                  receiver
[  6]   0.00-300.00 sec  3.44 GBytes  98.5 Mbits/sec                  sender
[  6]   0.00-300.00 sec  3.44 GBytes  98.5 Mbits/sec                  receiver
[  8]   0.00-300.00 sec  3.21 GBytes  91.9 Mbits/sec                  sender
[  8]   0.00-300.00 sec  3.21 GBytes  91.9 Mbits/sec                  receiver
[ 10]   0.00-300.00 sec  3.24 GBytes  92.9 Mbits/sec                  sender
[ 10]   0.00-300.00 sec  3.24 GBytes  92.9 Mbits/sec                  receiver
[ 12]   0.00-300.00 sec  3.28 GBytes  93.8 Mbits/sec                  sender
[ 12]   0.00-300.00 sec  3.28 GBytes  93.8 Mbits/sec                  receiver
[ 14]   0.00-300.00 sec  3.33 GBytes  95.4 Mbits/sec                  sender
[ 14]   0.00-300.00 sec  3.33 GBytes  95.4 Mbits/sec                  receiver
[ 16]   0.00-300.00 sec  3.18 GBytes  91.2 Mbits/sec                  sender
[ 16]   0.00-300.00 sec  3.18 GBytes  91.2 Mbits/sec                  receiver
[ 18]   0.00-300.00 sec  3.20 GBytes  91.7 Mbits/sec                  sender
[ 18]   0.00-300.00 sec  3.20 GBytes  91.7 Mbits/sec                  receiver
[ 20]   0.00-300.00 sec  3.22 GBytes  92.1 Mbits/sec                  sender
[ 20]   0.00-300.00 sec  3.22 GBytes  92.1 Mbits/sec                  receiver
[ 22]   0.00-300.00 sec  3.22 GBytes  92.1 Mbits/sec                  sender
[ 22]   0.00-300.00 sec  3.22 GBytes  92.1 Mbits/sec                  receiver
[SUM]   0.00-300.00 sec  32.7 GBytes   937 Mbits/sec                  sender
[SUM]   0.00-300.00 sec  32.7 GBytes   937 Mbits/sec                  receiver

iperf Done.
```

Fig. 5.50: Resultat de la segona prova amb *iperf3*. Font: Elaboració pròpia.

En la figura 5.49 es pot veure el resultat de la prova. En ella es pot apreciar la velocitat

mitjana de transferència i la quantitat de dades transferides.

Un cop realitzada la prova, s'ha procedit a revisar el *Solarwinds*. Per tal de comprovar si aquest tràfic és visible, s'ha filtrat per les IP d'ambdues màquines i per l'interval de temps el qual s'ha realitzat. Així doncs, les gràfiques a continuació mostren la transferència.



CONVERSATION	INGRESS BYTES	EGRESS BYTES	INGRESS PACKETS	EGRESS PACKETS	PERCENT
Between TestVM and 192.168.[redacted]	36.3 Gbytes	36.3 Gbytes	24.23 M	24.23 M	100%
COMCPDFW5700	36.3 Gbytes	36.3 Gbytes	24.23 M	24.23 M	
X27[redacted] (SERVICES) - X27:[redacted]	36.3 Gbytes	0 bytes	24.23 M	0	
X27:[redacted] (MANAGEMENT) - X27:[redacted]	0 bytes	36.3 Gbytes	0	24.23 M	
Remaining traffic	0 bytes	0 bytes	0	0	0%

Fig. 5.51: Gràfica amb la informació del tràfic d'ambdues proves amb *iperf3*. Font: Elaboració pròpia.

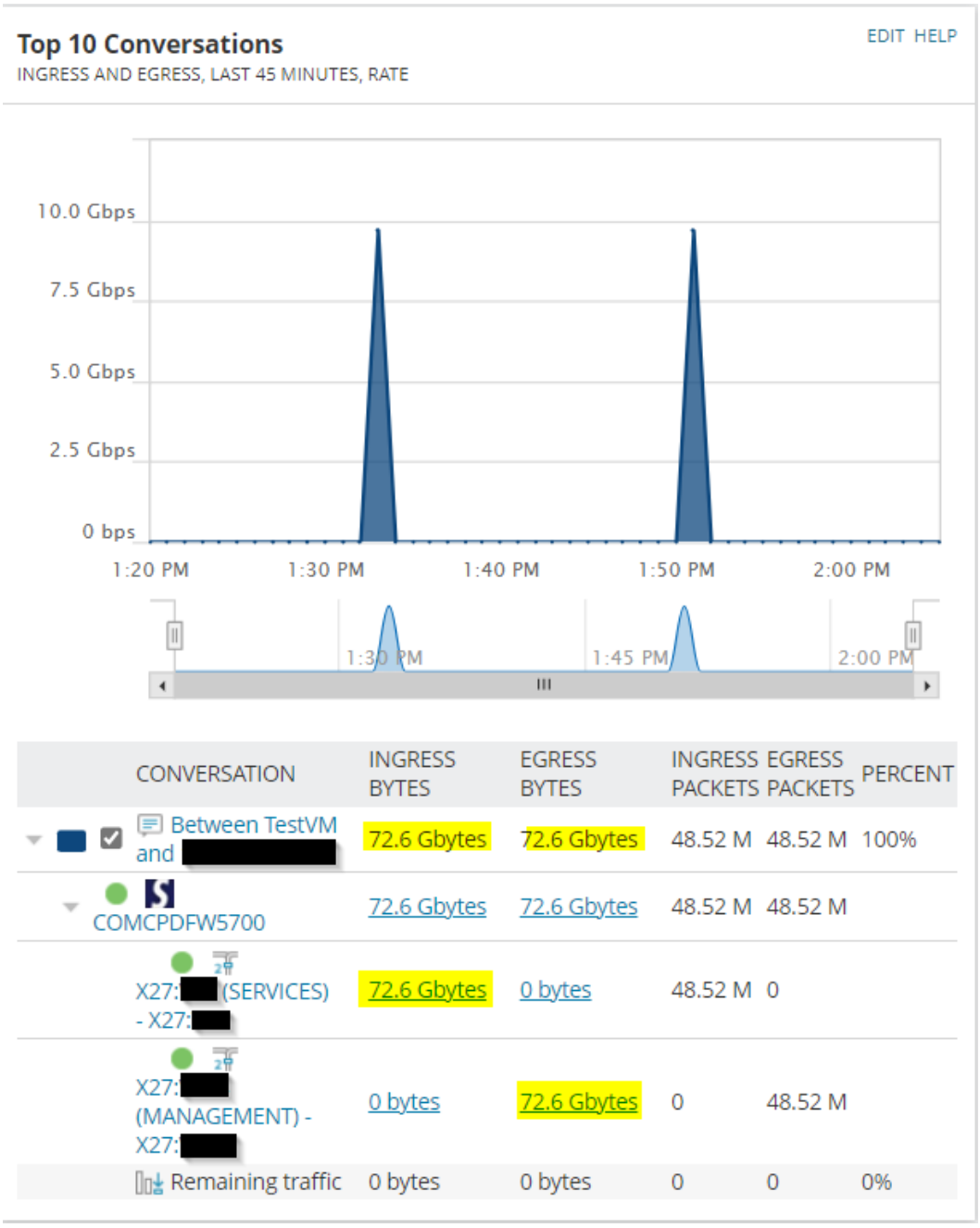


Fig. 5.52: Gràfica amb la informació del tràfic de la segona prova amb *iperf3*. Font: Elaboració pròpia.

En la figura 5.51 es pot apreciar dos pics. La mateixa prova s'ha realitzat dues vegades deixant uns minuts de separació entre elles per comprovar-ne la fiabilitat. En la figura 5.52 es pot veure ampliada la segona prova. En ella es pot comprovar que la quantitat de dades transferida s'aproxima molt a la donada per iperf3. Aquesta variació és normal a causa del fet que *Solarwinds* té en copte les capçaleres IP i el resultat de *iperf3* no, aquest últim només mostra la suma de la informació útil dels paquets enviats.

Després de corroborar els resultats es pot concloure que la prova és satisfactòria.

5.7.2 Segona prova: Transferència utilitzant el protocol SMB

En aquesta prova s'ha realitzat una transferència via SMB[22], entre dos sistemes *Windows*. La mida del fitxer és de 24 GB, quantitat prou gran per una prova com aquesta. Per fer això, s'ha creat una carpeta compartida [23] en un dels equips per poder transferir el fitxer des de l'altre. En la figura 5.53 es mostra la mida del fitxer i la ruta destí des de l'equip origen.

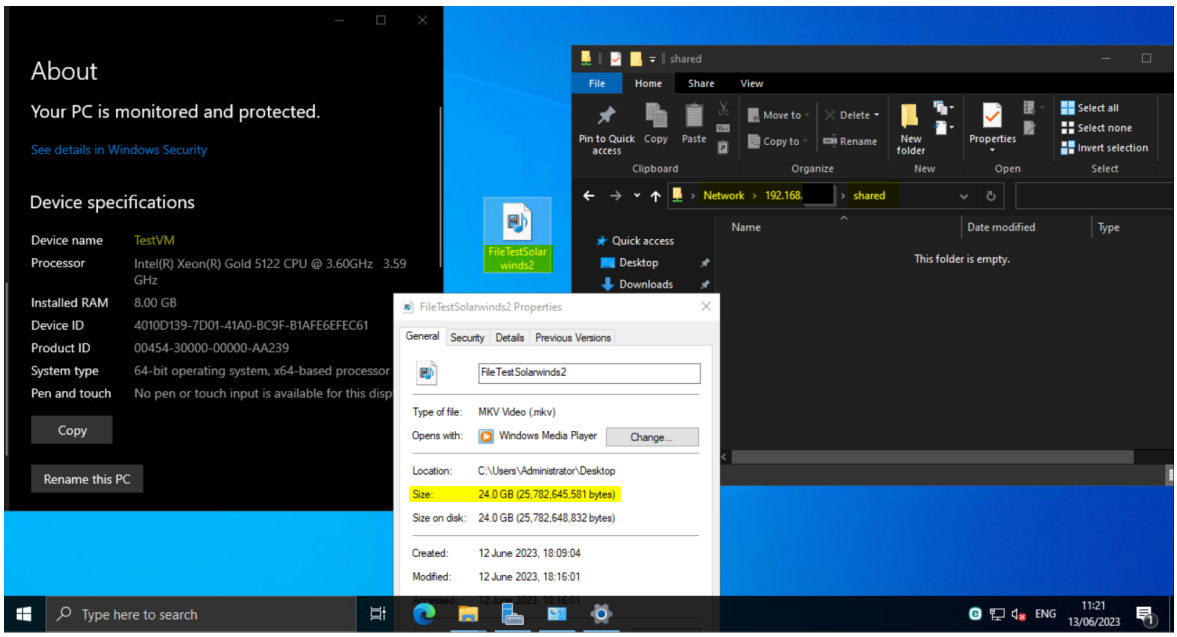


Fig. 5.53: Captura de la ruta on s'ha copiat el fitxer. Font: Elaboració pròpia.

Durant la transferència es pot veure la velocitat real, figura 5.54.

[22] Server Message Block

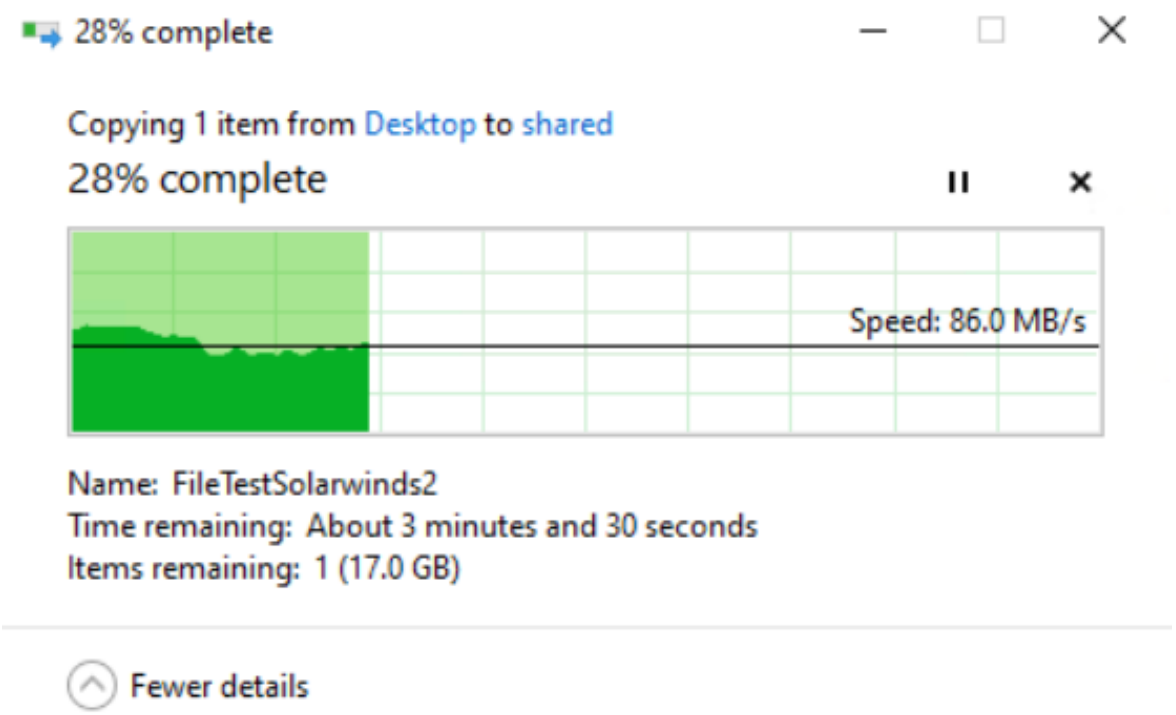


Fig. 5.54: Velocitat de transferència mostrada en *Windows*. Font: Elaboració pròpia.

Un cop acabada la transferència, figura 5.55, es pot comprovar al *Solarwinds* si ha quedat enregistrada. Per facilitar la cerca s'ha filtrat per les IP d'origen i destí, veure figura 5.56.

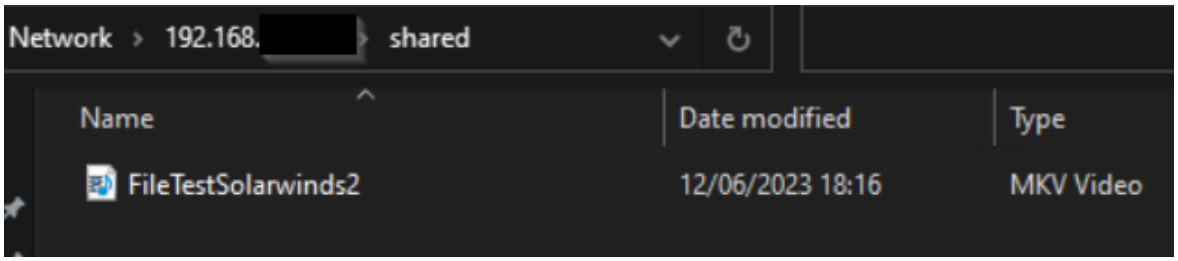


Fig. 5.55: Fitxer copiat en la ruta final. Font: Elaboració pròpia.

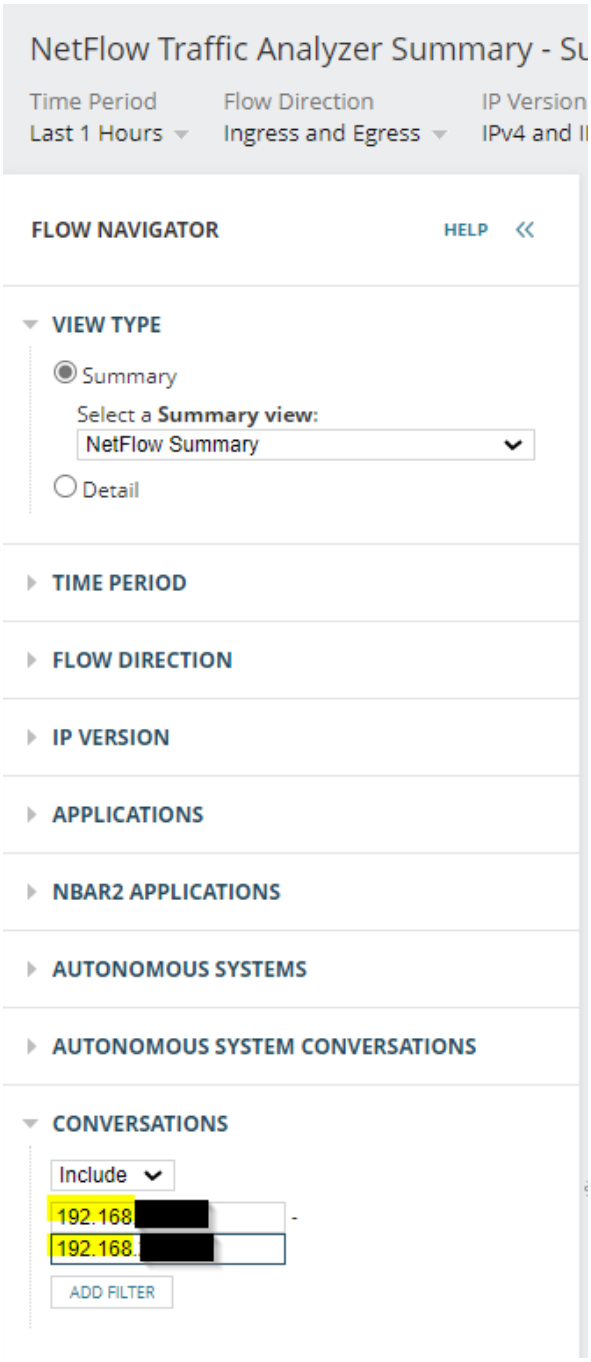


Fig. 5.56: Filtre a *Solarwinds* amb les IP origen i destí. Font: Elaboració pròpia.

En la figura 5.57, es pot comprovar al *Solarwinds* que quantitat de dades transmeses coincideix amb la mida del fitxer enviat entre ambdós equips. Així mateix, la duració de la transferència representada gràficament correspon amb el temps que ha durat la prova.

Per tant, podem concloure que aquesta prova ha estat satisfactòria.

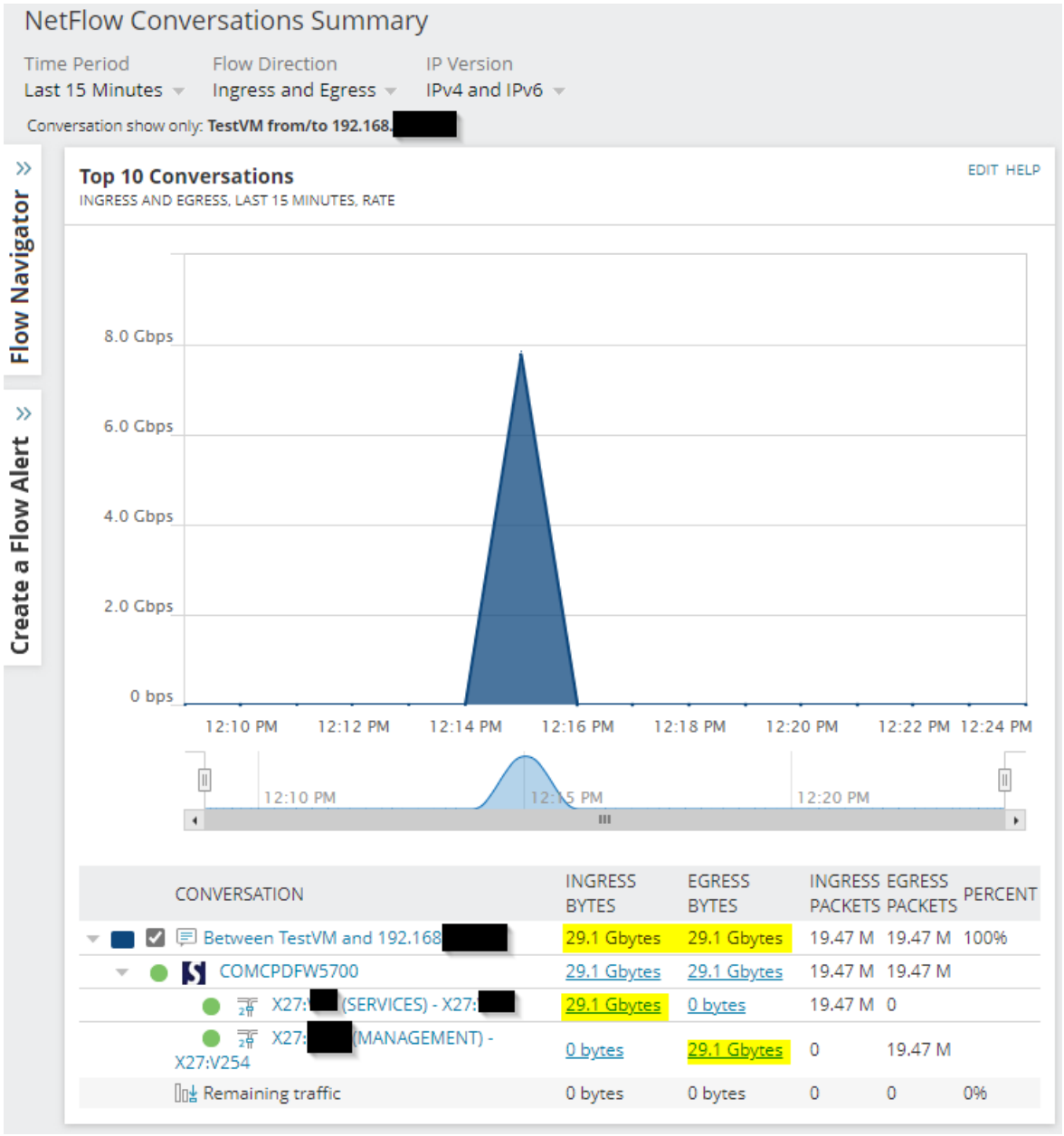


Fig. 5.57: Gràfica de *Solarwinds* amb la informació del tràfic de la prova. Font: Elaboració pròpia.

5.7.3 Tercera prova: Transferència utilitzant el protocol FTP

En aquesta prova s'ha transferit el fitxer de la prova anterior mitjançant el protocol FTP[23]. En ser un protocol client-servidor, per transferir un fitxer es necessita tenir un equip amb el rol de servidor i l'altre amb el rol de client. Per poder dur a terme aquesta prova s'ha activat el rol d'FTP [24] en un equip i s'ha instal·lat un client FTP en l'altre, concretament

[23]File Transfer Protocol

el *software Filezilla* [25]. En la figura 5.58 es pot veure com s'ha establert una connexió des del *Filezilla* amb el servidor FTP.

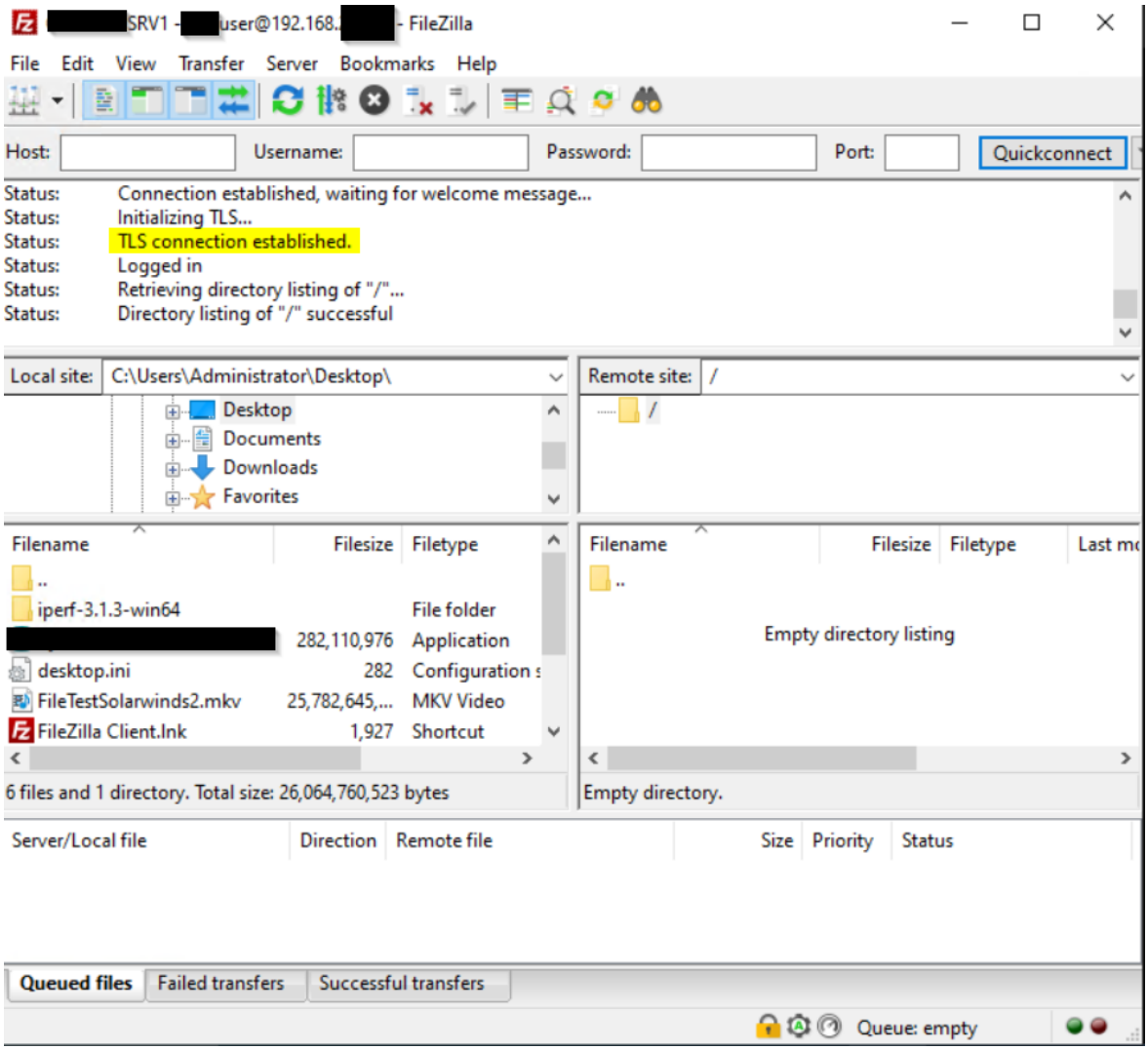


Fig. 5.58: Client FTP *Filezilla*. Connexió establerta amb el servidor. Font: Elaboració pròpia.

Per transferir el fitxer, és suficient en arrossegar el fitxer amb el ratolí a la carpeta remota. Així doncs, per una banda, en la figura 5.59 es pot veure la realització de la transferència i la seva velocitat. D'altra banda, en la figura 5.60, es mostra com s'ha completat la transferència.

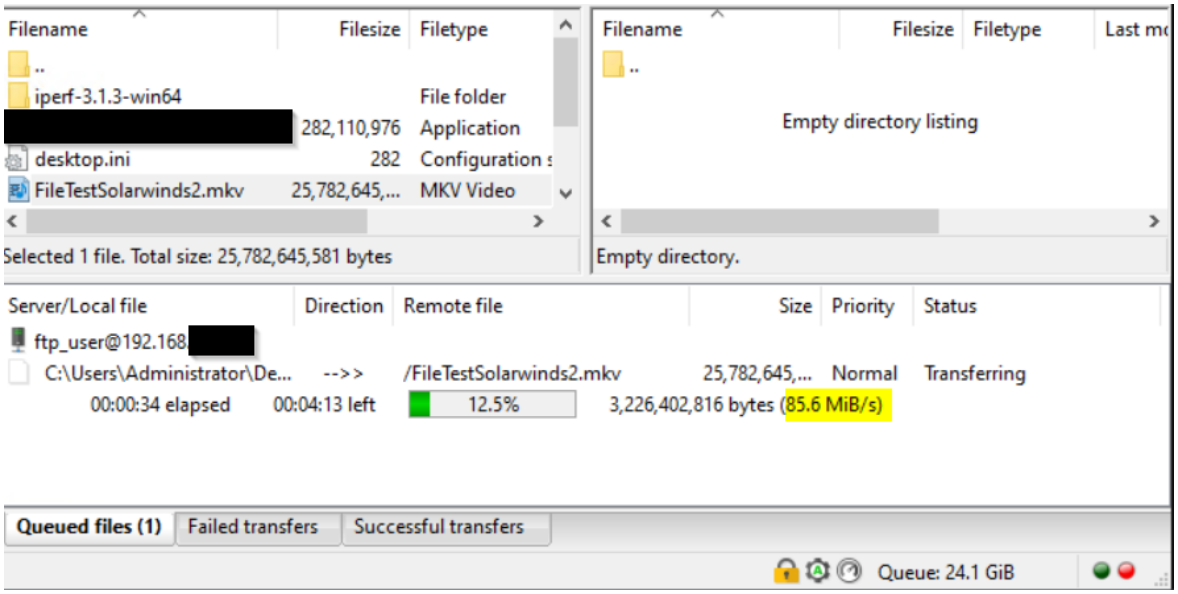


Fig. 5.59: Client FTP *Filezilla*. Velocitat de la transferència. Font: Elaboració pròpia.

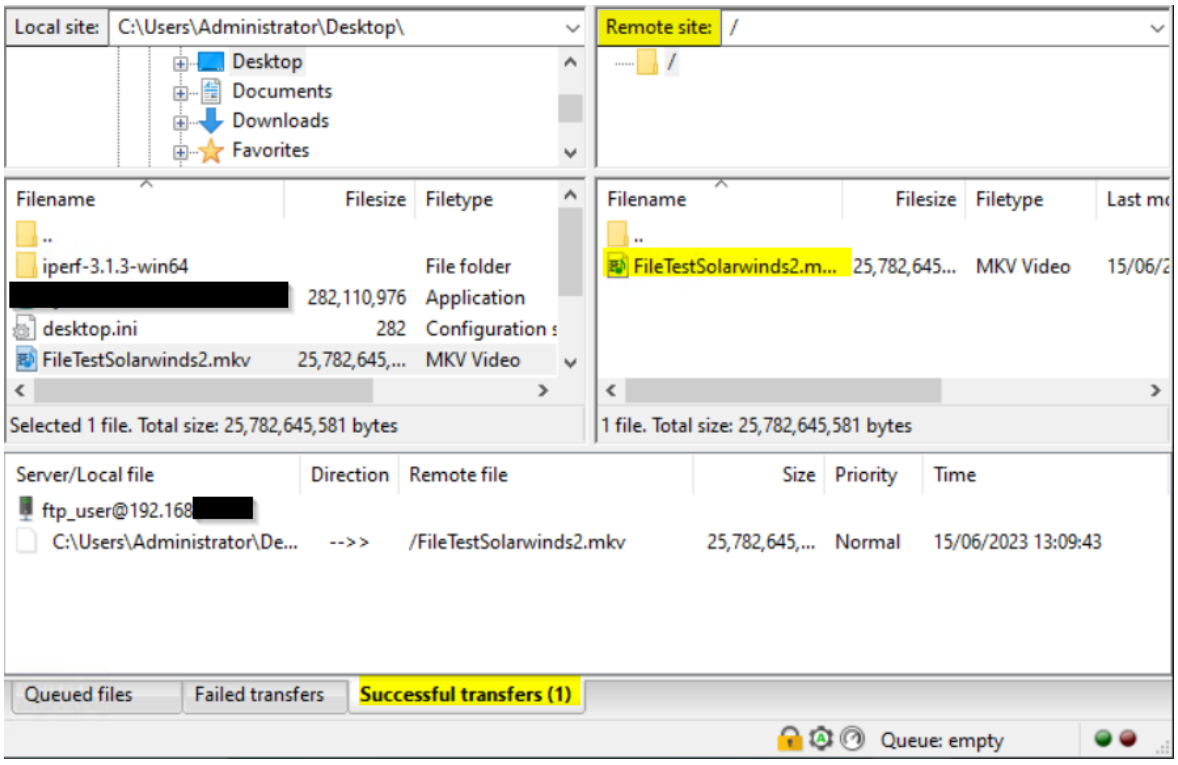


Fig. 5.60: Client FTP *Filezilla*. Transferència completada. Font: Elaboració pròpia.

Un cop realitzada la transferència s'ha comprovat al *Solarwinds* si l'ha detectat. En la figura 5.61 es pot comprovar com efectivament el *software* ha estat capaç de detectar i enregistrar la informació.

Aquesta concorda amb la transferència realitzada. Així doncs, la prova ha estat satisfactòria.

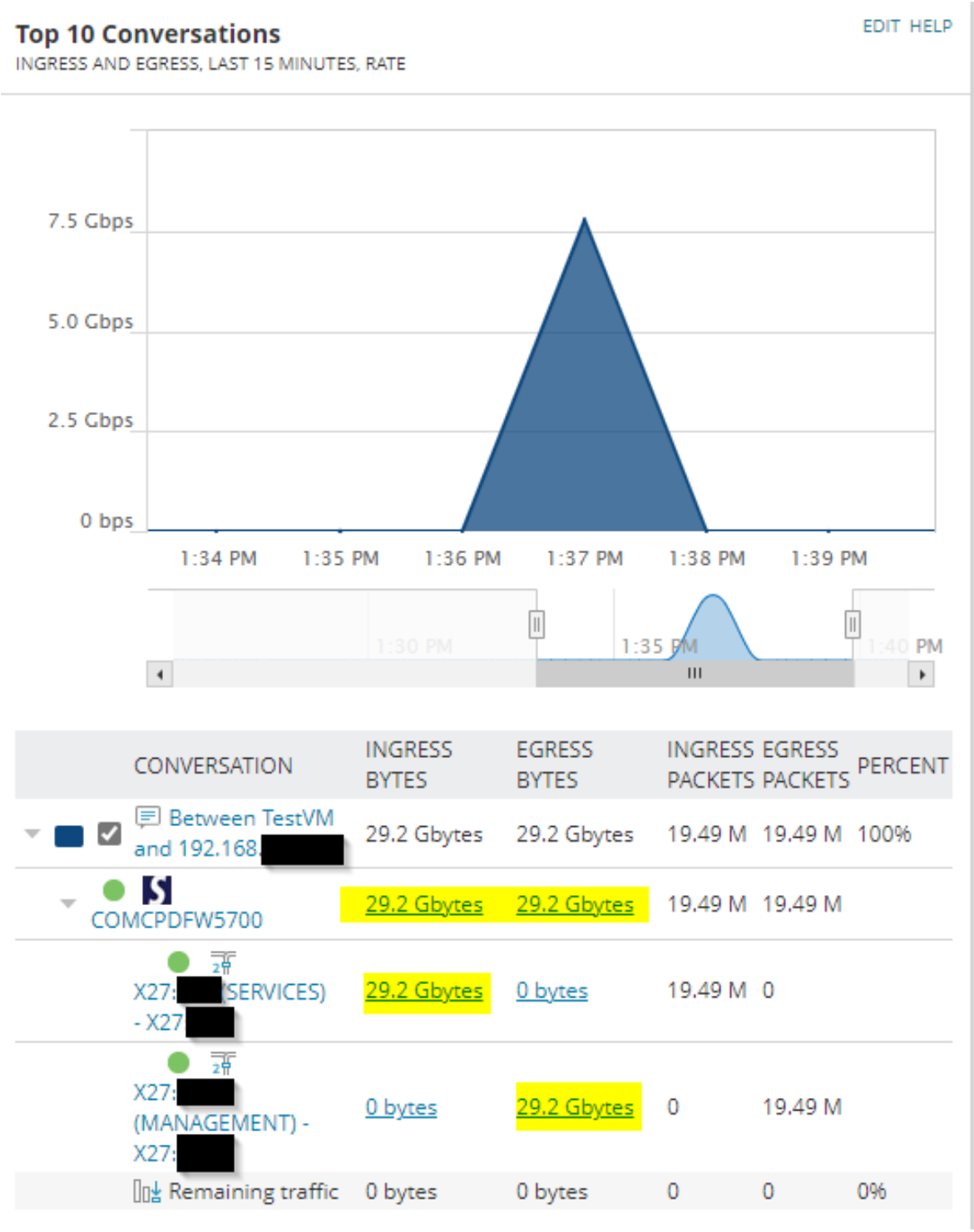


Fig. 5.61: Gràfica de *Solarwinds* amb la informació del tràfic de la prova. Font: Elaboració pròpia.

6. Anàlisi de resultats, conclusions i possibles ampliacions

6.1 Conclusions

L'objectiu principal d'aquest projecte era trobar i escollir una solució de *software* de monitorització de xarxes existent en el marcat que suportes el protocol SNMP i IPFIX. Es volia aportar a l'equip tècnic de Bytemaster una solució que els permetés una major comprensió de la salut de la infraestructura del CPD i alhora reduir el temps que hi dediquen.

Després de buscar i analitzar varies possibles solucions en el mercat que podrien complir amb els objectius i requisits de projecte s'ha escollit el *software Solarwinds*, específicament els seus mòduls NPM i NTA. Els punts més rellevants per la seva elecció han estat la llarga duració en el mercat, la comunitat d'usuaris i l'existència de suport per part del fabricant. Aquest últim punt és crític per poder mantenir la implementació en el temps, ja que no és viable que tots els tècnics tinguin coneixements avançats d'un *software* de tercers. Tenint suport, sempre es té l'opció de parlar amb el fabricant per poder resoldre els dubtes i problemes que es puguin produir.

Per la naturalesa del *software*, la implementació del *Solarwinds* s'ha realitzat en un servidor físic del CPD dedicat per aquest ús. Aquesta implementació ha comportat l'elecció del *hardware* del servidor segons els requisits del *software* i la seva correcta preparació per tenir un entorn de virtualització adequat. Per preparar un entorn així, i més en una infraestructura en producció, s'han de tenir o aprendre uns coneixements avançats de sistemes. Per aquest motiu s'ha de tenir present a l'hora de prendre la decisió d'instal·lar un *software on premise*[1].

Un cop instal·lat el *Solarwinds*, s'ha vist la complexitat del *software* i la dificultat d'adaptar-lo a les necessitats de la infraestructura. Per poder personalitzar-lo, s'ha de tenir un coneixement profund de la infraestructura a monitoritzar. Durant aquest procés, s'han trobat dificul-

[1] On-premise significa en català "a les instal·lacions pròpies" i es refereix a la utilització de servidors propis en l'entorn de l'empresa.

tats en configurar algunes funcionalitats. Una d'elles era un dels objectius secundaris, monitoritzar l'estat de les VPN via SNMP per tal de poder prescindir del *software* Nagios. Això no ha estat possible ja que existeix una incompatibilitat en la lectura de dades via SNMP entre *Solarwinds* i el fabricant de *firewalls* Sonicwall. Altrament, el *software* LibreNMS del que ja disposava Bytemaster no és necessari i es podria eliminar.

Tenint el *Solarwinds* configurat també s'ha millorat el tractament d'alertes i la seva gestió. Amb aquesta nova funcionalitat, que no es disposava anteriorment a Bytemaster, ha reduït el temps necessari per poder determinar si hi ha un problema important en la infraestructura. De la mateixa manera, també s'ha facilitat poder traçar els orígens de les incidències en disposar d'informació creuada de diversos dispositius en una mateixa plataforma.

En conclusió, es pot dir que el resultat final del projecte és satisfactori. S'han complert la majoria d'objectius i requisits que s'havien plantejat a l'inici del projecte. El resultat final soluciona allò que es necessitava que es resolgués. Així doncs, Bytemaster ja disposa d'una plataforma robusta i pràctica que permet als seus tècnics identificar i gestionar més fàcilment les possibles incidències que puguin sorgir en la seva infraestructura del CPD.

6.2 Possibles ampliacions

6.2.1 Còpies de seguretat

Un dels objectius secundaris era poder restaurar les MVs de *Solarwinds* si aquestes es veien compromeses. No s'ha realitzat durant projecte ja que era necessària la col·laboració del tècnic responsable del departament de sistemes de Bytemaster. Per incompatibilitats de calendari no s'ha pogut trobar el temps necessari abans de la finalització d'aquest projecte. Tot i així, Bytemaster ja disposa d'una solució de còpies de seguretat per MVs, el *software Veeam Backup* [26]. Eventualment les MVs de *Solarwinds* s'hi podrien afegir.

6.2.2 Monitorització d'interfícies VPN via SNMP

Un altre dels objectius secundaris era prescindir del *software* Nagios, que entre altres funcionalitats, envia alertes via correu electrònic quan cau un túnel VPN del *firewall* del CPD. Teòricament, aquesta funcionalitat era possible amb *Solarwinds* en disposar de monitorització via SNMP. Durant la realització d'aquest projecte s'ha vist una incompatibilitat en la lectura OID[2] de l'estat de les interfícies VPNs per part de *Solarwinds*. Sonicwall presenta aquests valors amb una taula i *Solarwinds* no pot llegir-la, només llegeix valors enters.

S'ha trobat una alternativa per poder monitoritzar l'estat de les VPN amb aquests dos fabricants tot i que requereix canvis en les configuracions de les VPNs. Per poder complir amb el calendari del projecte s'ha descartat aquesta opció. Tot i així, no es descarta que en un futur s'apliquin aquests canvis.

6.2.3 Ampliació de mòduls del *Solarwinds*

L'abast de la monitorització de xarxa d'aquest projecte es centrava en els equips de xarxa i el tràfic que es podia analitzar mitjançant el protocol IPFIX. Però la complexitat d'un entorn en producció va més enllà, hi ha recursos que és convenient que és monitoritzin amb més detall com podrien ser els servidors físics, les bases de dades i les MV.

Així doncs, disposant d'una implementació funcional del *software Solarwinds* es podrien instal·lar més mòduls per obtenir encara més informació. El més interessant seria el mòdul SAM ("Server & Application Monitor"). Aquest permet recollir en detall i de forma escalable la informació dels servidors i dels serveis que aquests ofereixen.

[2]En el protocol SNMP, OID significa "Object Identifier"

Bibliografia

[1] Bytemaster, "Bytemaster acelera la transformación digital del sector logístico," Disponible a https://www.bytemaster.es/ (10/02/2023).

[2] Solarwinds, "What is syslog?" Disponible a https://www.solarwinds.com/resources/it-glossary/syslog (13/06/2023).

[3] G. Arellano, "Seguridad perimetral," *Sitio Web: http://cisco. frcu. utn. edu. ar*, 2005.

[4] Lucidspark, "Agile methodology: What it is, how it works, and why it matters," Disponible a https://lucidspark.com/blog/what-is-agile-methodology (10/02/2023).

[5] M. Fowler, J. Highsmith *et al.*, "The agile manifesto," *Software development*, vol. 9, no. 8, pp. 28–35, 2001.

[6] Zoom, "Zoom," Disponible a https://zoom.us/ (13/06/2023).

[7] Teamwork, "Eina teamwork," Disponible a https://www.teamwork.com/ (13/06/2023).

[8] Google, "Eina google drive," Disponible a https://www.google.com/drive/ (13/06/2023).

[9] Overleaf, "Eina overleaf," Disponible a https://www.overleaf.com/ (13/06/2023).

[10] Latex, "Latex," Disponible a https://www.latex-project.org/ (13/06/2023).

[11] Microsoft, "Eina microsoft teams," Disponible a https://www.microsoft.com/en-us/microsoft-teams/group-chat-software (13/06/2023).

[12] Solarwinds, "Web solarwinds," Disponible a https://www.solarwinds.com/ (20/04/2023).

[13] P. PRTG, "Web paessler prtg," Disponible a https://www.paessler.com/prtg (20/04/2023).

[14] P. Scrutinizer, "Web plixer scrutinizer," Disponible a https://www.plixer.com/products/scrutinizer/ (20/04/2023).

[15] nProbe/nTop, "Web nprobe/ntop," Disponible a https://www.ntop.org/products/netflow/nprobe/ (20/04/2023).

[16] Microsoft, "Com configurar un virtual switch," Disponible a https://learn.microsoft.com/en-us/windows-server/virtualization/hyper-v/get-started/create-a-virtual-switch-for-hyper-v-virtual-machines?tabs=hyper-v-manager (13/06/2023).

[17] ——, "Windows teamings," Disponible a https://learn.microsoft.com/en-us/windows-server/networking/technologies/hpn/hpn-software-only-features (13/06/2023).

[18] Solarwinds, "Solarwinds platform requirements," Disponible a https://documentation.solarwinds.com/en/success_center/orionplatform/content/core-orion-requirements-sw1916.htm (20/04/2023).

[19] ——, "Install solarwinds platform products in a new environment," Disponible a https://documentation.solarwinds.com/en/success_center/orionplatform/content/install-new-deployment.htm (20/04/2023).

[20] K. González Becerril, "Estudio comparativo para demostrar las ventajas y desventajas de las unidades de almacenamiento: Disco duro y unidad de estado sólido," 2019.

[21] iperf3, "Web iperf3," Disponible a https://iperf.fr/iperf-download.php (13/06/2023).

[22] W. M. Moreno, "El modelo osi," *Recuperado de https://d1wqtxts1xzle7. cloudfront. net/48988821/01_modelo_OSI_v2-with-cover-pagev2. pdf*, 2003.

[23] Microsfot, "How to create a shared folder," Disponible a https://support.microsoft.com/en-us/windows/file-sharing-over-a-network-in-windows-b58704b2-f53a-4b82-7bc1-80f9994725bf#ID0EBD=Windows_10 (13/06/2023).

[24] Microsoft, "Creating a new ftp site in iis 7," Disponible a https://learn.microsoft.com/en-us/iis/publish/using-the-ftp-service/creating-a-new-ftp-site-in-iis-7 (13/06/2023).

[25] Filezilla, "Web filezilla," Disponible a https://filezilla-project.org/ (13/06/2023).

[26] V. Backup, "Web veeam backup," Disponible a https://www.veeam.com/vm-backup-recovery-replication-software.html (13/06/2023).