Università degli Studi di Camerino

Scuola di Scienze e Tecnologie

Corso di Laurea in Informatica (Classe L-31)

Open Source Network Security Monitoring Tools

Uno studio sull'importanza degli strumenti di monitoraggio delle reti

Laureando
Besjan Veizi

Matricola 97861

Relatore
Fausto Marcantoni

Correlatore
Marco Maccari

A.A. 2023/2024

Indice

Elenco dei codici

Elenco delle figure

Elenco delle tabelle

1. Introduzione

L'obiettivo principale dietro le attività dannose volte a compromettere la riservatezza, l'integrità e la disponibilità delle informazioni sono le infrstrutture di rete.
Mettendo da parte la componente di sicurezza delle informazioni, che merita un discorso a sè, un altro aspetto considerevole è capire esattamente come rendere operativo un programma di monitoraggio per proteggerla.
Il monitoraggio della rete è un processo IT critico in cui le componenti di rete, come router, switch, firewall, server e macchine virtuali, vengono monitorati per individuare guasti e prestazioni e valutati continuamente per mantenere e ottimizzare la loro disponibilità.

1.1 Motivazione

Le reti stanno crescendo in maniera cruciale e avere tutti i membri del team aziendale connessi e produttivi, richiede una rete sicura, reattiva e affidabile. Senza il monitoraggio della rete, il sistema si può paragonare ad un veicolo senza spie di avvertimento od allarmi acustici. Qualcosa potrebbe andare storto ma nella superficie tutto sembrerebbe a posto, e nessuno si accorgerebbe del problema se non quando si arriva all'arresto del sistema. La motivazione di questa tesi verte a mostrare come il monitoraggio della rete può prevenire l'accadere di ciò attraverso gli strumenti e le tecniche adatte, focalizzandoci di più nel mondo open source.

1.2 Obiettivi

Questa tesi verte allo studio del monitoraggio della rete, agli approcci principali che vengono presi e alle funzionalità chiave che gli strumenti di monitoraggio di rete offrono. In particolare, si cercherà di esprimere la loro efficacia in termini di uso delle risorse, accuratezza e tempo di risposta. Questi dati permetteranno di avere un modello per poter valutare le performance di un determinato strumento di monitoraggio e quindi comparare i punti di forza e di debolezza rispetto un'altro strumento. Data la natura vasta dell'argomento, sia in termini di tempo che di risorse che è possibile investire per trovare una soluzione che meglio si adegui alle proprie esigenze, l'obiettivo della tesi si concluderà con una simulazione di quello che potrebbe essere una aspetto reale. Partendo infatti da semplici esperimenti con gli applicativi che verranno mostrati, sarà possibile arrivare a usi pratici dimostrabili.

2. Monitoraggio della rete

2.1 Cos'è e a cosa serve il monitoraggio della rete

Il monitoraggio della rete ha radici storiche legate agli albori di Internet, quando negli anni '70-'80 gli amministratori delle reti iniziarono a sentire l'esigenza di nuovi approcci per supervisionare e gestire le performance dei sistemi sempre più complessi e distribuiti. Quando parliamo di monitoraggio di rete IT, o *network monitoring*, volgiamo infatti l'interesse verso criticità quali il rilevamento del calo delle prestazioni e presenza di guasti o malfunzionamenti delle componenti connesse nella rete. L'obiettivo principale è garantire prestazioni, affidabilità e sicurezza ottimali identificando problemi quali sovraccarico, interruzioni di rete o violazioni della sicurezza. Se e quando vengono rilevati questi problemi, gli amministratori di rete vengono prontamente avvisati tramite vari canali come e-mail, SMS o altri allarmi, consentendo rapide azioni correttive.

Il monitoraggio della rete è cruciale per diversi motivi:

1. **Sicurezza informatica:** permette di identificare attività sospette o malevole come attacchi DDoS, malware o intrusioni non autorizzate;
2. **Gestione delle performance:** aiuta a individuare colli di bottiglia nella rete e a migliorare la qualità del servizio (QoS) per gli utenti finali;
3. **Affidabilità e Disponibilità:** minimizza il tempo di inattività (*downtime*) attraverso il rilevamento tempestivo dei guasti e la risoluzione proattiva dei problemi;
4. **Riduzione dei costi:** una rete ben monitorata riduce il rischio di perdita di dati e i costi associati a guasti imprevisti.

Un altro motivo per cui il monitoraggio della rete è fondamentale, riguarda la **compliance normativa**. Infatti, in molte industrie, il monitoraggio della rete è necessario per conformarsi a regolamenti come:

- **Regolamento Generale sulla Protezione dei Dati (GDPR):** nell'Articolo 32 [1] viene richiesto alle organizzazioni di implementare misure tecniche e organizzative adeguate per garantire un livello di sicurezza adeguato al rischio, includendo la capacità di assicurare su base permanente la riservatezza, l'integrità, la disponibilità e la resilienza dei sistemi e dei servizi di trattamento.
- **ISO 27001:** specifica i requisiti per stabilire, implementare, mantenere e migliorare continuamente un sistema di gestione della sicurezza delle informazioni (SGSI). Essa include controlli relativi al monitoraggio e alla gestione delle reti per garantire la sicurezza delle informazioni. [2]

- **Direttiva NIS2:** La direttiva NIS2 impone alle organizzazioni di adottare misure di gestione del rischio per la sicurezza delle reti e dei sistemi informativi, inclusi il monitoraggio continuo, la gestione degli incidenti e la segnalazione tempestiva degli stessi alle autorità competenti. [3]

Importante è non cadere nel comune malinteso di considerare il monitoraggio della rete come attività di supporto alla sicurezza nel senso che impedisca l'accesso non autorizzato alla rete. Per queste attività, che hanno un loro aspetto di monitoraggio, ci spostiamo ai concetti di sistemi di rilevamento di intrusione (o **IDS**, *Intrusion Detection Systems*) e sistemi di prevenzione di intrusione (o **IPS**, *Intrusion Prevention Systems*). Diversamente, il network monitoring si concentra sull'osservazione continua delle prestazioni della rete, della disponibilità degli apparati e dei potenziali guasti che potrebbero presentarsi. Il monitoraggio di rete supporta un'ampia gamma di dispositivi come server, router, switch e persino *end devices*. Inoltre, potrebbe essere utilizzato in qualsiasi tipo di rete LAN (*Local Area Network*), WLAN (*Wireless Local Area Network*), VPN (*Virtual Private Network*) e persino WAN (*Wide Area Network*).

2.2 Le metriche di monitoraggio

Il monitoraggio di rete va di pari passo con il concetto di prestazione. Vanno dunque analizzati diversi parametri critici per poi arrivare a dare una valutazione della rete. Consideriamo quindi le seguenti metriche di prestazione:

- **tempo di risposta:** ovvero quanto tempo impiega un sistema a rispondere a una richiesta. Tempi di risposta elevati indicano congestione della rete o sovraccarico di uno o più dispositivi.

- **disponibilità:** indica la percentuale di tempo in cui un sistema è operativo ed accessibile. Avere un'alta disponibilità è fondamentale per le applicazioni mission-critical, ovvero le applicazioni il cui fallimento può comportare interruzioni significative, perdite finanziarie o persino un rischio di vita umana.

- **tempo di attività:** è il tempo totale in cui un sistema rimane funzionante senza interruzioni. Tipicamente viene misurato come una percentuale e un monitoraggio regolare assicura che i sistemi soddisfino gli standard di *uptime* richiesti.

- **carico di CPU:** indica la quantità di potenza di elaborazione in uso. Carichi CPU elevati possono portare a prestazioni più lente e possono segnalare la necessità di aggiornamenti hardware o bilanciamento del carico.

- **memoria usata:** indica il volume di RAM utilizzato. Un elevato utilizzo di memoria può causare rallentamenti delle applicazioni o crash del sistema.

- **larghezza di banda usata:** è la velocità con cui i dati vengono trasmessi sulla rete. Il monitoraggio della larghezza di banda aiuta a identificare i colli di bottiglia e a pianificare i miglioramenti della capacità.

Queste metriche assicurano collettivamente che le reti funzionino in modo efficiente e possano gestire i carichi di lavoro richiesti.

2.3 Approcci al monitoraggio

Per collezionare i dati dai dispositivi collegati nella rete e stilare le metriche di cui parlavamo nella sezione precedente, ci sono diversi approcci che vengono messi in atto dagli strumenti che fanno monitoraggio di rete.

2.3.1 Monitoraggio basato su SNMP

Simple Network Management Protocol (**SNMP**) [4] è un protocollo che opera allo strato applicativo OSI, ampiamente utilizzato per il monitoraggio e la gestione dei dispositivi di rete. Permette agli amministratori di rete di interrogare, monitorare e controllare i dispositivi da remoto, recuperando metriche sulle prestazioni e dati di sistema. L'SNMP funziona secondo un modello client-server. Di seguito elenchiamo i principali componenti:

- **SNMP Manager:** gestore che raccoglie i dati dai dispositivi. Esso è eseguito in un Network Management System;
- **SNMP Agent:** applicativo software in esecuzione sui dispositivi che risponde alle richieste (*SNMP Queries*) e invia notifiche asincrone (*SNMP Traps*);
- **Object Identifiers (OIDs):** indirizzi univoci che rappresentano diverse metriche per le prestazioni (es. utilizzo di CPU, larghezza di banda, etc.)
- **Management Information Base (MIB):** database strutturato consultato dall'agent e che definisce quali dati possono essere recuperati da un dispositivo;

Il monitoraggio basato su SNMP è uno strumento essenziale per gli amministratori di rete e di sistema per controllare le prestazioni dei dispositivi, rilevare guasti e ottimizzare l'infrastruttura. Tuttavia, anche se fornisce dati aggregati, l'SNMP non offre un'analisi approfondita del traffico della rete. Aumentando il numero di richieste SNMP, può causare picchi di CPU sui dispositivi di rete. D'altro canto, dato che il monitoraggio basato su SNMP funziona con un modello di polling (es. ogni 5 minuti), è possibile che si perdano picchi di traffico in tempo reale.

2.3.2 Remote Monitoring (RMON)

Remote Monitoring (o **RMON**) è un'estensione all'approccio del monitoraggio basato su SNMP, a differenza però che esso si basa su un *monitoraggio proattivo*. Viene quindi ridotta la dipendenza dall'interrogazione continua dei dispositivi d'interesse poiché passiamo ad un architettura basata sui ***probe***. Infatti, secondo la prima versione di RMON (RMONv1) [4], nei dispositivi connessi in rete, solitamente switch, router e firewall, viene installato un modulo hardware o software (il probe) che ha il compito di raccogliere il traffico di rete e memorizza i dati nella sua Management Information Base (MIB). I dati vengono elaborati localmente dal probe, che applica filtri e calcola metriche aggregate (es. utilizzo di banda, tasso di errore, etc.): ciò riduce il polling continuo che invece avviene nell'approccio di monitoraggio basato su SNMP.

Il probe quindi, invia automaticamente avvisi o registra eventi quando vengono superate soglie predefinite, senza bisogno di interrogazioni. Dall'altro lato, il RMON Manager, un sistema centrale che comunica con i RMON probe, richiede report dettagliati on-demand e visualizza le statistiche di rete. Il gestore analizza gli allarmi e i

registri eventi per il troubleshooting.
RMON ha un'altra versione (RMONv2) [5] in cui i dati aggregati dai RMON probe presentano ulteriori metriche avanzate che contribuiscono al monitoraggio del livello applicativo, supportano le VLAN e permettono un'analisi basata su IP.
Il Remote Monitoring presenta una configurazione complessa che richiede un po' di esperienza per essere impostato come approccio per monitoraggio della rete. Inoltre bisogna considerare che non tutti i dispositvi supportano RMON nativamente. Ciò vale per dispositivi di rete low-end and consumer-grade (es. home access-point/routers o modem e gateways distribuiti dagli ISP locali) ma anche per dispositivi enterprise *virtualized e cloud-based*. Nel primo caso i dispositivi danno priorità all'accessibilità e alla semplicità rispetto alle funzionalità di monitoraggio avanzate. Non dispongono delle risorse di CPU e memoria necessarie per l'analisi e l'archiviazione dei pacchetti RMON. Mentre spostandoci al mondo virtualizzato o basato su cloud, i venditori offrono soluzioni interne di monitoraggio, es. API-driven monitoring e dashboard di report in cloud per ridurre la necessità di configurare i dispositivi e supportare i RMON probe. Infine, bisogna tenere in considerazione che l'archiviazione storica da parte dei RMON probe per motivi di analisi delle tendenze di rete e la creazione degli report utili al gestore RMON, anche se minore del monitoraggio SNMP, ha comunque un impatto sulle prestazioni dei dispositivi.

2.3.3 Analisi del Traffico Basata sui Flussi (NetFlow, sFlow, IPFIX)

L'analisi del traffico basata sui flussi è un approccio al monitoraggio della rete che raccoglie dati dettagliati sul traffico, inclusi gli indirizzi IP, i protocolli, le porte e i volumi dei dati trasferiti, ma non l'intero payload.

Di base abbiamo tre componenti chiave:

- **Esportatore di Flussi (*Flow Exporter*):** identifica e raccoglie i dati sui flussi di traffico (es. IP sorgente/destinazione, porta, protocollo, dimensione pacchetti, etc.) e invia i record dei flussi al collector;
- **Collettore di Flussi (*Flow Collector*):** riceve i dati dal Flow Exporter, li archivia e organizza in flussi per analisi successiva;
- **Analizzatore di Flussi (*Flow Analyzer*):** interpreta i dati organizzati dal Collector per fornire insight sulla rete, quindi identifica problemi di traffico, congestioni e attività sospette

NetFlow, **sFlow** e **IPFIX** sono tre protocolli utilizzati per il monitoraggio e l'analisi del traffico di rete. Ognuno offre approcci distinti nella raccolta e nell'analisi dei dati di rete. [6]

- **Netflow:** è stato sviluppato da Cisco, quindi è un protocollo proprietario per la raccolta di informazioni sul traffico IP che attraversa dispositivi di rete come router e switch; [7]
- **sFlow:** sviluppato da InMon Corp., è uno standard aperto per l'esportazione di pacchetti campionati al livello 2 del modello OSI. Questo protocollo utilizza il campionamento statistico dei pacchetti per fornire una visione in tempo reale del traffico di rete. Questo metodo consente di monitorare reti ad alta velocità con un impatto minimo sulle prestazioni del dispositivo; [8]

- **IPFIX (Internet Protocol Flow Information Export):** è stato standardizzato dall'IETF ed è basato su Netflow v9 e mira a fornire un protocollo universale per l'esportazione delle informazioni di flusso dai dispositivi di rete a un sistema di gestione. IPFIX permette infatti l'estensione dei dati di flusso con informazioni aggiuntive sul traffico di rete, come metadati del livello applicativo e statistiche sulle prestazioni della rete. Essendo uno standard aperto, IPFIX è supportato da diversi fornitori di dispositivi di rete, facilitando l'interoperabilità e l'integrazione in ambienti eterogenei. [9]

L'analisi del traffico basata sui flussi è un ottimo approccio monitorare il traffico di rete senza catturare pacchetti individuali. Ciò è significativo per rilevare anomalie e problemi di sicurezza (es. traffico sospetto, DDoS). Un'altro aspetto interessante è l'analisi dell'utilizzo della banda e identificazione delle applicazioni più esigenti.

2.3.4 Telemetria in Streaming

La **Telemetria in streaming** (o ***Streaming Telemetry***) è un approccio moderno al monitoraggio della rete che permette di raccogliere dati in tempo reale direttamente dai dispositivi di rete (router, switch, firewall, server). A differenza di protocolli tradizionali come SNMP o NetFlow, che usano un modello pull (polling a intervalli), lo streaming telemetry utilizza un modello ***push***, in cui:

- i dispositivi inviano continuamente e proattivamente i dati ai sistemi di monitoraggio;
- i dati vengono trasmessi in modo strutturato e scalabile, utilizzando formati come *JSON*, *GPB* (*Google Protocol Buffers*), *XML*;
- supporta protocolli moderni come *gRPC*, *Kafka*, *MQTT*, *RESTCONF* per l'invio e la raccolta dei dati

Con lo streaming telemetry possiamo quindi avere una misurazione di latenza, jitter, perdita di pacchetti e throughput senza ritardi: problemi di congestione e degrado delle prestazioni vengono rilevati nell'immediato. La scalabilità di questo approccio permette di gestire grandi volumi di dati senza sovraccaricare la rete e i formati leggibili e standardizzati facilitano l'integrazione con sistemi di analisi. I dati telemetrici possono essere integrati con sistemi di automazione, permettendo risposte automatiche a problemi di rete. Ad esempio, se un'interfaccia presenta un alto utilizzo di banda, un sistema può ridistribuire il traffico in automatico. [10]

Case produttrici come Cisco, Juniper, Arista, Nokia e molti altri hanno già cominciato ad implementare questo approccio nei loro dispositivi, quindi mancherà poco affinché anche quelli di altri fornitori attualmente distribuiti saranno abilitati allo streaming di telemetria. [11]

2.3.5 Differenze dalla cattura di pacchetti (Packet Capture)

Abbiamo presentato gli approcci al monitoraggio di rete, tuttavia bisogna che li distinguiamo dalla **cattura di pacchetti**. Conosciuta anche come *analisi dei pacchetti* o *sniffing PCAP*, questa tecnica cattura e archivia i pacchetti di dati dal livello 2 al livello 7 della rete. A differenza dagli altri quindi, il packet capture raccoglie i pacchetti completi (header + payload) utilizzando tecniche come i *network tap* o il *port mirroring*.

Come vantaggio abbiamo la possibilità di effettuare un'analisi dettagliata poiché l'ispezione approfondita del contenuto dei pacchetti permette un troubleshooting avanzato. D'altro canto però, la cattura di dati dettagliati sui pacchetti richiede molto spazio di archiviazione e necessità di risorse di calcolo per elaborare e analizzare i dati.

Di seguito mostriamo una tabella riassuntiva che mostra le caratterstiche salienti per ogni approccio che abbiamo approfondito finora.

	Monitoraggio SNMP	**RMON (Remote Monitoring)**	**Analisi del Traffico di Flusso**	**Streaming Telemetry**	**Packet Capture (PCAP)**
Dati Raccolti	Metriche sulle prestazioni dei dispositivi (CPU, memoria, traffico)	Statistiche dettagliate sul traffico di rete	Metadati sui flussi (IP sorgente/destinazione, protocolli, byte trasferiti)	Metriche di rete avanzate in tempo reale (latenza, throughput, errori, utilizzo banda)	Contenuto completo dei pacchetti (intestazioni + payload)
Livello di Dettaglio	Medio (monitoraggio dello stato dei dispositivi)	Alto (statistiche sui segmenti di rete)	Medio (dettagli sui flussi, ma senza payload)	Alto (monitoraggio continuo e dettagliato)	Alto (può vedere tutto il traffico)
Metodo di Raccolta	Interroga i dispositivi con richieste SNMP	Usa moduli passivi (probes) per il monitoraggio del traffico	I router e switch esportano i dati di flusso	Modello push: i dispositivi inviano continuamente dati ai sistemi di analisi	Cattura dei pacchetti tramite port mirroring o network tap
Efficienza	Media (richiede polling costante)	Medio-Alta (raccolta basata su eventi)	Alta (dati aggregati per efficienza)	Molto Alta (push continuo, meno overhead)	Bassa (grande quantità di dati non aggregati)
Supporto Multi-Vendor	Ampio (standardizzato, supportato da molti vendor)	Variabile (dipende dall'implementazione)	Ampio (NetFlow, sFlow, IPFIX sono standard)	In crescita (supportato da Cisco, Juniper, Arista, Nokia)	Limitato (dipende dagli strumenti di analisi)
Uso Tipico	Monitoraggio dello stato dei dispositivi, pianificazione della capacità di rete	Analisi del traffico a livello di segmento di rete	Monitoraggio della larghezza di banda, rilevamento anomalie, analisi delle tendenze	Monitoraggio in tempo reale, rilevamento anomalie, automazione delle risposte di rete	Monitoraggio della sicurezza, troubleshooting, analisi forense
Scalabilità	Alta (crescita in base ai dispositivi)	Media (richiede probes dedicati)	Alta (efficace per il monitoraggio su larga scala)	Molto alta (adatto a reti moderne e cloud)	Bassa (troppi dati in reti complesse)
Impatto sulle Prestazioni	Basso (se il polling è ottimizzato)	Medio-Alto (sovraccarico dovuto ai probes)	Medio (dipende dalla frequenza di raccolta dei flussi)	Medio (richiede capacità di calcolo per analisi in tempo reale)	Alto (richiede molta memoria e CPU)
Vantaggi	Standardizzato, ampio supporto tra i vendor	Statistiche dettagliate, riduzione del traffico di polling	Scalabile, basso impatto sulle risorse	Dati in tempo reale, maggiore efficienza rispetto a SNMP, scalabilità elevata	Massima visibilità sulla rete, analisi dettagliata
Svantaggi	Visibilità limitata sul traffico effettivo	Configurazione complessa, richiede probes dedicati	Nessuna ispezione del contenuto dei pacchetti, solo metadati	Richiede strumenti di analisi avanzati e supporto da parte dei vendor	Alto utilizzo di risorse, grande quantità di dati da archiviare

Tabella 2.1: Differenze tra PCAP, Streaming Telemetry, Monitoraggio SNMP, RMON e Analisi del Traffico di Flusso

2.4 Protocolli di discovery

Finora abbiamo introdotto gli approcci al monitoraggio della rete attraverso l'uso del protocollo SNMP, il Remote Monitoring, l'analisi del traffico di flusso di rete e la telemetria in streaming. Dopodiché li abbiamo confrontati con la cattura di pacchetti (PCAP) e mostrato le varie caratteristiche, usi tipici, vantaggi e svantaggi per ognuno. A complementare gli strumenti di monitoraggio delle performance della rete, gli amministratori e sistemisti di reti IT usano i cosiddetti protocolli di discovery come ICMP, CDP, LLDP, Syslog e WMI. Essi sono strumenti essenziali per raccogliere informazioni sulla rete e sui dispositivi connessi. Facciamo una distinzione tra gli approcci del monitoraggio della rete che abbiamo approfondito, poiché questi protocolli non forniscono metriche delle prestazioni in tempo reale. Tuttavia, hanno funzioni fondamentali, tra cui:

- identificare la presenza e la connettività dei dispositivi;
- raccogliere informazioni sulla topologia della rete;
- segnalare eventi o anomalie di sistema;
- facilitare la gestione e il troubleshooting;

2.4.1 ICMP

Internet Control Message Protocol (**ICMP**) [12] è un protocollo a livello di rete che viene utilizzato per la segnalazione di errori e la diagnostica operativa nelle reti IP. Il monitoraggio basato su ICMP sfrutta i messaggi ICMP (come `ping` e `traceroute`) per valutare le prestazioni, la connettività e lo stato di salute della rete. Particolari casi d'uso per questo tipo di approccio sono:

- controllo di connettività: quindi verificare se un dispositivo connesso nella rete è raggiungibile;
- misurazione della latenza: determinare il *round-trip time* (RTT) tra sorgente e destinazione;
- rilevamento di perdita di pacchetti: identifica i pacchetti persi che indicano congestione o instabilità della rete;
- problemi di tracciamento e routing: identificare il percorso seguito dai pacchetti e dove si verificano i ritardi;
- monitoraggio della disponibilità del servizio (*Automated Monitoring*): verificare costantemente se un servizio è online (es. con un bash script)

L'ICMP è limitato dalle informazioni che si possono ricavare, ciononostante, i messaggi ICMP rimangono strumenti fondamentali nella risoluzione dei problemi di rete.

2.4.2 Syslog

Syslog [13] è un protocollo standard ampiamente utilizzato da una vasta gamma di dispositivi di rete e IT, che consente loro di inviare messaggi di log in formato testo libero a un server centrale. Questi messaggi rappresentano eventi come modifiche nella configurazione del dispositivo, cambiamenti di stato delle porte o errori software, e vengono trasmessi al server centrale per scopi di gestione della rete. Analizzando attentamente i messaggi Syslog, i sistemi di monitoraggio possono identificare facilmente i guasti e associarli ad allarmi. Il protocollo Syslog non è real-time, poiché i log vengono elaborati solo dopo la loro generazione. Inoltre non vi è nessuna crittografia nativa, quindi i log possono essere intercettati se non vengono protetti con TLS (*Transport Layer Security*) o VPN. [14]

2.4.3 Cisco Discovery Protocol (CDP)

Il **Cisco Discovery Protocol** (**CDP**) [15] è un protocollo proprietario sviluppato da Cisco Systems, utilizzato principalmente per gestire reti composte da dispositivi Cisco. CDP consente ai dispositivi di rete di trasmettere messaggi ai dispositivi vicini, permettendo loro di scoprirsi e apprendere informazioni reciproche senza necessità di configurazioni manuali. Questi messaggi contengono dati utili, come ID del dispositivo, indirizzi IP e interfacce connesse, facilitando agli amministratori di rete la comprensione della topologia e del ruolo di ciascun dispositivo nella rete. Il CDP è solo un protocollo informativo, non fornisce metriche di performance quindi, inoltre, essendo proprietario, non viene supportato per altri vendor.

2.4.4 Link Layer Discovery Protocol (LLDP)

Link Layer Discovery Protocol, (**LLDP**) [16] è un protocollo standard (IEEE 802.1AB) utilizzato per consentire ai dispositivi di rete di scoprirsi reciprocamente e scambiarsi informazioni, indipendentemente dal produttore. Particolarmente, ogni dispositivo abilitato trasmette periodicamente pacchetti LLDP su tutte le sue interfacce di rete. Questi pacchetti contengono informazioni utili, come:

- Nome e modello del dispositivo
- Porte e interfacce connesse
- VLAN, ID del dispositivo e configurazioni
- Indirizzo IP e MAC

I dispositivi vicini ricevono questi pacchetti e possono utilizzarli per mappare automaticamente la topologia della rete. L'LLDP risulta utilissimo per esempio, per configurare in modo dinamico VoIP e telefoni IP con informazioni VLAN. Essendo uno standard aperto, può sostituire il protocollo proprietario CDP in ambienti misti con dispositivi di diversi vendor.

2.4.5 Windows Management Instrumentation (WMI)

Windows Management Instrumentation (**WMI**) [17] è una tecnologia di Microsoft che fornisce un'infrastruttura per la gestione e il monitoraggio dei sistemi operativi Windows. Implementando gli standard *Web-Based Enterprise Management* (*WBEM*) e *Common Information Model* (*CIM*), WMI consente l'accesso uniforme alle informazioni di gestione, facilitando il controllo e l'automazione delle operazioni sia su computer locali che remoti. Le principali funzionalità di WMI sono: [18]

- raccolta di informazioni di sistema: WMI permette di ottenere dati dettagliati su hardware, software, processi in esecuzione e configurazioni di rete, essenziali per il monitoraggio delle prestazioni e la risoluzione dei problemi;
- configurazione del sistema: attraverso WMI, è possibile modificare impostazioni di sistema, gestire account utente e configurare policy di sicurezza, assicurando coerenza e conformità alle best practice aziendali
- automazione delle attività: gli amministratori possono automatizzare compiti amministrativi utilizzando script o applicazioni che interagiscono con WMI;
- gestione remota: gli amministratori possono eseguire attività di manutenzione e configurazione da una posizione centralizzata, ottimizzando l'efficienza operativa

Essendo integrati nel sistema operativo a partire da Windows 2000, WMI non richiede l'installazione di software aggiuntivo: purtroppo ciò significa che la sua applicabilità in ambienti eterogenei è limitata. Offre un'interfaccia standardizzata per l'accesso alle informazioni di gestione, semplificando lo sviluppo di strumenti di monitoraggio e gestione. Oltretutto, da la possibilità di utilizzare linguaggi di scripting come PowerShell per interagire con WMI consente l'automazione di processi complessi, migliorando l'efficienza operativa. Tuttavia, se non configurato correttamente, WMI può rappresentare un vettore per attacchi, poiché consente l'esecuzione remota di comandi. È fondamentale implementare misure di sicurezza adeguate per limitare l'accesso non autorizzato. Infine, l'uso intensivo di WMI può comportare un aumento del consumo di risorse di sistema, influenzando le prestazioni, specialmente in ambienti con numerosi dispositivi monitorati.

Di seguito mostriamo una tabella riassuntiva che mostra le caratterstiche salienti dei protocolli di discovery che abbiamo appena approfondito.

	ICMP	**Syslog**	**CDP**	**LLDP**	**WMI**
Tipo	Protocollo di rete	Protocollo di logging	Protocollo di discovery (Cisco proprietario)	Protocollo di discovery (Standard IEEE 802.1AB)	Framework di gestione di Windows
Dati Raccolti	Stato di connettività, latenza, perdita di pacchetti	Messaggi di log su eventi di sistema, errori, avvisi	Informazioni sui dispositivi Cisco vicini, interfacce, VLAN	Informazioni sui dispositivi di rete multi-vendor, connessioni, ID interfacce	Dati su hardware, software, servizi e processi di sistemi Windows
Livello di Dettaglio	Basso (solo stato della connessione)	Medio (dettagli su eventi di sistema)	Alto (dettagli su dispositivi Cisco connessi)	Alto (dettagli su dispositivi di rete di qualsiasi vendor)	Alto (dati completi su configurazione e stato dei dispositivi Windows)
Metodo di Raccolta	Invia pacchetti ICMP echo request (ping, traceroute)	Dispositivi e server inviano log a un server centrale	I dispositivi Cisco inviano periodicamente messaggi CDP	I dispositivi inviano periodicamente pacchetti LLDP con informazioni di discovery	Query dirette o raccolta automatica di dati di sistema Windows
Scalabilità	Alta (monitoraggio leggero)	Alta (archiviazione centralizzata di log)	Media (solo dispositivi Cisco)	Alta (compatibile con più vendor)	Media (dipendente dal numero di dispositivi Windows monitorati)
Impatto sulle Prestazioni	Basso	Basso (log di eventi, poco impattante)	Basso (solo messaggi di discovery periodici)	Basso (messaggi periodici di discovery)	Medio (raccoglie molti dati, può impattare le prestazioni)
Caso d'Uso	Verifica della connettività di rete e diagnostica della latenza	Monitoraggio di eventi e problemi nei dispositivi e server	Scoperta e gestione della topologia in reti Cisco	Scoperta e gestione della topologia in reti multi-vendor	Monitoraggio avanzato di server e sistemi Windows
Vantaggi	Leggero, semplice da usare	Centralizza e organizza i log di rete e sicurezza	Fornisce dettagli completi su dispositivi Cisco connessi	Standard aperto, compatibile con più vendor	Accesso dettagliato a dati di sistema e supporto per automazione
Svantaggi	Informazioni limitate (solo connettività)	Non fornisce metriche di performance in tempo reale	Funziona solo con dispositivi Cisco	Può essere sfruttato in attacchi di rete se non protetto	Alto utilizzo di risorse, compatibile solo con Windows

Tabella 2.2: Confronto tra ICMP, Syslog, CDP, LLDP e WMI

3. Strumenti di monitoraggio

3.1 Cosa sono gli strumenti di monitoraggio della rete

Nel Capitolo 2 abbiamo introdotto il concetto di monitoraggio della rete ed esposto i vari approcci utilizzati, ora concentriamoci un po' sugli strumenti che permettono di fare tale attività. Inizialmente, il monitoraggio della rete era manuale e basata su semplici strumenti di diagnostica (es. `ping`, `traceroute`, `ifconfig`, `netstat`, `tcpdump`, consultazione dei log di sistema, etc.). Nel corso degli anni '90, con l'aumento delle reti e delle loro complessità, nacquero protocolli specifici come SNMP, che segnò un punto di svolta permettendo di standardizzare il monitoraggio attraverso vari dispositivi. [4]

Dagli anni 2000, gli strumenti di monitoraggio si sono evoluti significativamente, includendo analisi sempre più dettagliate, automazione, integrazioni con software di terze parti e avanzate capacità di alerting, consentendo così un monitoraggio proattivo e predittivo piuttosto che puramente reattivo.

3.2 Funzionalità chiave

Seguendo le pagine di documentazione delle aziende dei software in questione e diverse fonti online [19][20] [21][22], le funzionalità essenziali (o *must-have*) che uno strumento di monitoraggio della rete deve avere sono:

- **Device e Network Discovery:** processo automatizzato con cui si identificano e si catalogano dispositivi e servizi presenti in una rete (*autodiscovery*), costruendo così una mappa aggiornata della struttura della rete stessa. Questo aiuta a garantire visibilità, monitoraggio accurato e gestione efficace dell'infrastruttura;

- **Network Analysis:** implica l'analisi approfondita del traffico di rete per identificare eventuali anomalie, congestioni o uso improprio delle risorse, facilitando così decisioni informate per l'ottimizzazione della rete;

- **Monitoraggio delle prestazioni:** consiste nel monitorare metriche chiave come latenza, larghezza di banda, uptime, utilizzo CPU, memoria e interfacce per identificare rapidamente i problemi di performance dei dispositivi;

- **Alerting e notifiche:** gli alert indicano eventi che richiedono attenzione immediata quando specifiche metriche di rete superano soglie predefinite. È essenziale configurare attentamente i profili di alert per evitare notifiche eccessive e garantire che solo eventi significativi siano comunicati ai team responsabili;

- **Logging e Reporting:** un logging ben configurato consente di identificare tempestivamente modelli di problemi ricorrenti e facilita l'analisi delle cause principali.

Report accurati e periodici consentono invece di analizzare i trend storici delle performance di rete, migliorando così la capacità decisionale e la pianificazione delle risorse;

- **Security Monitoring:** individuazione e mitigazione di minacce come intrusioni, virus o attività sospette;
- **API Integration e Automazione:** integrazione con strumenti esistenti e automazione dei task ripetitivi per rendere più efficiente il lavoro amministrativo, riducendo errori e tempi operativi;

3.2.1 Caratteristiche secondarie

Considerando la varietà degli strumenti per il monitoraggio della rete disponibili sul mercato, le aziende puntano su caratteristiche opzionali che possono migliorare significativamente la qualità complessiva dell'esperienza d'uso e la gestione operativa *Quality of Life*. In particolare, si possono identificare le seguenti caratteristiche differenzianti:

- **Monitoraggio Agent-based vs agentless:** possibilità di monitorare dispositivi attraverso ***agent*** installati localmente (*agent-based*) o direttamente via rete senza installazioni aggiuntive (*agentless*);
- **Monitoraggio attivo vs passivo:** capacità di monitorare la rete inviando traffico specifico (active) o semplicemente ascoltando e analizzando il traffico esistente (passive);
- **Monitoraggio predittivo e basato sui trend:** possibilità di prevedere problemi futuri attraverso analisi predittive basate su trend storici e algoritmi di apprendimento automatico;
- **Monitoraggio open source vs proprietario:** differenza nel modello di licenza: strumenti open source (codice aperto, personalizzabili, gratuiti) o proprietari (licenza commerciale, supporto diretto, ma limitata personalizzazione);
- **Scalabilità & supporto multi-tenancy:** capacità dello strumento di adattarsi facilmente all'espansione della rete e supportare più utenti/clienti isolati all'interno di una sua singola istanza;
- **Role-based access control (RBAC) & sicurezza:** gestione avanzata degli accessi basata sui ruoli degli utenti, garantendo sicurezza e riservatezza delle informazioni;
- **Integrazione con ITSM & incident management:** integrazione diretta con strumenti di gestione dei servizi IT (IT Service Management), per gestire incidenti e richieste direttamente dal sistema di monitoraggio;
- **Monitoraggio di infrastrutture cloud e ibride:** capacità di monitorare in modo efficace non solo reti fisiche locali, ma anche ambienti cloud e infrastrutture ibride (combinazione tra cloud e on-premise);
- **User experience e facilità d'uso:** qualità dell'interfaccia utente, intuitività del prodotto, semplicità di configurazione e gestione ordinaria;

- **Licensing & cost model:** modello economico (subscription, perpetual licence, freemium, pay-per-use, ecc.) che influenza la scelta finale in base a budget e obiettivi aziendali;
- **Community e supporto tecnico:** disponibilità di una comunità attiva (per open source) o qualità e rapidità del supporto fornito dal produttore (per software proprietario);
- **Personalizzazione delle viste:** avere dashboard personalizzate a seconda dei propri bisogni aggiunge valore sul lavoro di analisi e comprensione dei problemi.

3.3 Gli strumenti

In questa sezione presentiamo i principali strumenti di monitoraggio della rete attualmente più diffusi e adottati dalle aziende a livello globale. Per ciascuno di essi verrà fornita una panoramica generale, accompagnata da un'analisi approfondita dei rispettivi punti di forza e delle eventuali criticità.

3.3.1 Zabbix

Zabbix [23] è una piattaforma open source di livello enterprise progettata per il monitoraggio in tempo reale di milioni di metriche raccolte da server, macchine virtuali e dispositivi di rete. La sua adozione è diffusa a livello globale, con una forte presenza in regioni come l'Asia-Pacifico (45,7%) e l'Europa orientale (21,4%). [24]

Zabbix offre funzionalità robuste per la scoperta automatica dei dispositivi, facilitando l'identificazione e il monitoraggio degli asset IT. Supporta sia il monitoraggio basato su agenti che quello senza agenti, garantendo una raccolta dati flessibile e completa. Consente la configurazione di avvisi personalizzati, assicurando notifiche tempestive in caso di anomalie o superamento di soglie critiche. La piattaforma offre strumenti avanzati per la visualizzazione e l'analisi dei dati, inclusi grafici dettagliati e report personalizzabili. La user experience è abbastanza friendly, tuttavia configurazione iniziale di Zabbix può risultare complessa.
Essendo una soluzione open source, Zabbix è altamente personalizzabile e priva di costi di licenza, rendendola accessibile a una vasta gamma di organizzazioni.

Zabbix fornisce API robuste che facilitano l'integrazione con altri sistemi e l'automazione dei processi di monitoraggio. In particolare Zabbix può essere integrato con altri strumenti e sistemi attraverso:

- API REST di Zabbix, per connettere Zabbix con strumenti di ITSM, DevOps, SIEM e altro;
- Webhook, utilizzati per inviare notifiche e azioni automatiche a servizi esterni (es.Slack e Microsoft Teams);
- Script personalizzati (Bash, Python, PowerShell) per interagire con altri strumenti e automatizzare attività;
- Database (MySQL, PostgreSQL, etc.)
- Agent personalizzati e plugin per raccogliere dati da applicazioni non supportate nativamente.

Non avendo integrazione nativa, l'aggiunta di sistemi di gestione dei servizi IT e di incident management nella piattaforma non è immediatamente disponibile e può richiedere personalizzazioni aggiuntive. Inoltre, le capacità di monitoraggio predittivo di Zabbix sono meno sviluppate rispetto ad alcune soluzioni commerciali, limitando le possibilità di analisi proattiva delle tendenze.

In sintesi, Zabbix rappresenta una soluzione potente e flessibile per il monitoraggio delle infrastrutture IT, con una solida base di utenti globali e partnership strategiche. [25] Tuttavia, le organizzazioni devono essere consapevoli delle sfide legate alla configurazione iniziale e alle funzionalità avanzate quando valutano l'adozione della piattaforma.

3.3.2 PRTG Network Monitor

PRTG (***Paessler Router Traffic Grapher***) **Network Monitor** [26], sviluppato da Paessler AG, è una soluzione proprietaria di monitoraggio della rete nota per la sua semplicità d'uso e la completezza funzionale, rivolta principalmente alle piccole e medie imprese (PMI). Questo strumento offre una panoramica completa dell'infrastruttura IT, monitorando sistemi, dispositivi, traffico e applicazioni. Le funzionalità di sicurezza, come il rilevamento di intrusioni o l'analisi delle vulnerabilità, sono invece meno sviluppate. PRTG offre un'installazione one-click e una rilevazione automatica della rete, facilitando l'avvio rapido del monitoraggio. Un altro punto di forza è che offre una visualizzazione chiara delle prestazioni della rete attraverso dashboard personalizzabili e mappe in tempo reale. La gestione delle notifiche avviene attraverso vari canali e la generazione dei report è abbastanza personalizzabile. Tuttavia potrebbe non offrire lo stesso livello di personalizzazione disponibile in soluzioni open source, limitando le possibilità di adattamento a esigenze specifiche. L'interfaccia utente è progettata per essere intuitiva, rendendo PRTG accessibile anche a utenti con competenze tecniche limitate. La piattaforma consente l'analisi storica dei dati, permettendo la previsione di potenziali problemi e la pianificazione proattiva delle risorse. Si tratta di uno strumento proprietario e offre una versione gratuita, limitata a 100 sensori. Questo ovviamente è un limite per reti medio-grandi, il che può risultare oneroso per organizzazioni con infrastrutture estese. Supporta efficacemente il monitoraggio di ambienti IT (*Information Technology*), OT (*Operation Technology*) e IoT (*Internet of Things*), inclusi sistemi on-premise, cloud e ibridi. PRTG offre un'ottima integrazione con API, che permettono di estendere le funzionalità del monitoraggio. Tuttavia, un altro limite importante da tenere a mente riguarda ambienti multi-tenant complessi, il che può rappresentare una sfida per i provider di servizi gestiti che necessitano di separare i dati dei clienti. [27]

In conclusione, PRTG Network Monitor rappresenta una soluzione completa e user-friendly per il monitoraggio delle infrastrutture IT, particolarmente adatta alle PMI. Tuttavia, le organizzazioni più grandi o con esigenze specifiche potrebbero trovare limitazioni in termini di costi, personalizzazione e funzionalità avanzate di sicurezza.

3.3.3 Nagios

Originariamente sviluppato da Ethan Galstad nel 1996 sotto il nome di NetSaint, **Nagios** [28] è progettato per monitorare l'infrastruttura IT, identificando e risolvendo problemi prima che possano influenzare i processi aziendali critici.

Essendo uno dei più longevi sistemi di monitoraggio open source, Nagios è ampiamente utilizzato per la sua flessibilità e per la vasta gamma di plugin ufficiali e non ufficiali. Ciò permette agli utenti di estendere le funzionalità del sistema per adattarsi alle esigenze specifiche dell'infrastruttura monitorata. Sempre grazie ai plugin aggiuntivi, la piattaforma fornisce notifiche tempestive attraverso vari canali, come email, cercapersone, SMS o altri sistemi definiti dall'utente. La piattaforma consente sia il monitoraggio attivo, in cui Nagios interroga direttamente i servizi, sia il monitoraggio passivo, dove i servizi inviano informazioni a Nagios senza una richiesta esplicita. Per ottenere funzionalità avanzate come l'analisi approfondita della rete o il monitoraggio della sicurezza, è spesso necessario integrare Nagios con plugin e componenti aggiuntivi, aumentando la complessità della configurazione e della manutenzione.[29] Si tratta comunque di uno strumento leggero e performate, in grado di operare efficacemente in ambienti di diverse dimensioni. L'interfaccia web di Nagios, sebbene funzionale, può apparire datata e meno user-friendly rispetto ad altre soluzioni moderne, richiedendo talvolta un maggiore sforzo di apprendimento da parte degli utenti. Le capacità native di reporting e logging sono piuttosto basilari (logging in file di testo, report di SLA, integrazione con email/sms), il che può limitare la capacità di analizzare storicamente le prestazioni e gli eventi senza l'ausilio di strumenti aggiuntivi. L'installazione e la configurazione iniziale di Nagios possono risultare complesse, specialmente per utenti meno esperti, a causa della necessità di configurare manualmente numerosi file e parametri. Esistono due principali versioni di Nagios: Nagios Core (gratuito e open-source sotto GPLv2) e Nagios XI (a pagamento, con interfaccia e funzionalità avanzate). Nagios Core è supportato da una vasta comunità di utenti e sviluppatori che contribuiscono attivamente al suo sviluppo e al supporto. Tuttavia, la versione gratuita, offre funzionalità API limitate, rendendo l'automazione e l'integrazione con altri sistemi meno immediate senza l'implementazione di plugin o script personalizzati.

In conclusione, Nagios rappresenta una soluzione robusta e flessibile per il monitoraggio delle infrastrutture IT, con una lunga storia nel settore e una vasta comunità di supporto. Tuttavia, le sue limitazioni in termini di interfaccia utente, funzionalità native e complessità di configurazione possono rappresentare delle sfide per alcune organizzazioni, richiedendo valutazioni attente in base alle specifiche esigenze e risorse disponibili.

3.3.4 Cacti

Cacti [30] è un'altra soluzione open source focalizzata sul monitoraggio grafico e l'analisi delle performance delle reti, che sfrutta strumenti come **RRDtool** (*Round-Robin Database Tool*), per la memorizzazione e la rappresentazione dei dati, e protocolli come SNMP, per raccogliere informazioni da dispositivi di rete e server. RRDTool è un database specializzato per la raccolta e la visualizzazione di dati di serie temporali, come metriche di rete, utilizzo della CPU, memoria, traffico di rete, ecc. Cacti invece agisce da interfaccia web basato RRDTool, che permette di visualizzare ed analizzare il monitoraggio di rete dai dati raccolti (*trend-based monitoring*). L'interfaccia web di Cacti è intuitiva e user-friendly, rendendo la configurazione e la gestione del moni-

toraggio accessibili anche a utenti con competenze tecniche limitate. La piattaforma ha comunque diversi limiti riguardanti le capacità di discovery automatica e l'alerting e sistema di notifiche di default. Non dispone infatti di funzionalità avanzate per la scoperta automatica dei dispositivi e delle reti, richiedendo spesso una configurazione manuale per l'aggiunta di nuovi elementi da monitorare. Le funzionalità di allerta e notifica native di Cacti sono basilari; per implementare sistemi di alerting più avanzati, è necessario ricorrere a plugin aggiuntivi. Inoltre non offre strumenti avanzati per il monitoraggio della sicurezza, limitando la sua efficacia in contesti dove la sicurezza è una priorità. Rispetto ad altri strumenti di monitoraggio, non fornisce API robuste per l'integrazione e l'automazione, rendendo complessa l'interoperabilità con altri sistemi o l'automazione di processi senza sviluppare soluzioni personalizzate. [31]
Infine, in ambienti aziendali di grandi dimensioni, Cacti può incontrare difficoltà di scalabilità, richiedendo risorse aggiuntive e configurazioni complesse per gestire efficacemente un numero elevato di dispositivi e metriche. Tuttavia, essendo open source, Cacti è disponibile gratuitamente, offrendo una soluzione efficace per esigenze di monitoraggio di base senza costi aggiuntivi.

Per concludere, Cacti rappresenta una soluzione valida per il monitoraggio grafico delle prestazioni di rete in contesti di piccole e medie dimensioni. Tuttavia, le sue limitazioni in termini di scoperta automatica dei dispositivi, funzionalità di alerting, monitoraggio della sicurezza, integrazione e scalabilità possono renderlo meno adatto per ambienti enterprise complessi che richiedono soluzioni più robuste e flessibili.

3.3.5 SolarWinds Network Performance Monitor

SolarWinds Network Performance Monitor (**NPM**) [32] è una soluzione commerciale di livello enterprise, nota per la sua robustezza e l'ampia gamma di funzionalità avanzate, parliamo di uno strumento utilizzato molto in grandi aziende per il monitoraggio e la gestione delle reti. Prima punto di forza riguarda sicuramente la scoperta automatica dei percorsi e nodi di rete. Utilizzando protocolli come ICMP, SNMP e WMI, esso offre una panoramica completa dei dispositivi e dei vendor presenti nella rete. Consente l'analisi dettagliata dei percorsi critici, facilitando la risoluzione dei problemi di rete attraverso una visualizzazione hop-by-hop. La configurazione iniziale di NPM può risultare complessa, richiedendo una curva di apprendimento significativa, soprattutto per gli utenti con meno esperienza nel settore del monitoraggio di rete. Secondo il datasheet [33], NPM offre oltre 100 modelli predefiniti per la generazione di report personalizzabili, permettendo una pianificazione e una generazione automatica dei report sulle prestazioni della rete. La piattaforma utilizza l'intelligenza artificiale per impostare avvisi avanzati (*predictive monitoring*), inclusi quelli basati su anomalie, garantendo una risposta rapida ai problemi di rete. Grazie a solide capacità di integrazione tramite API, NPM può essere collegato a strumenti ITSM e di gestione degli incidenti, migliorando l'efficienza operativa. Lo strumento è progettato per scalare in ambienti di grandi dimensioni, supportando la gestione multi-tenant attraverso l'applicazione di limitazioni basate su modelli, migliorando la sicurezza e la gestione degli accessi. Tuttavia la sua implementazione in ambienti di grandi dimensioni può necessitare di server con elevate prestazioni, inclusi dischi veloci e CPU potenti, per gestire efficacemente il carico di monitoraggio. La piattaforma fornisce API robuste che facilitano l'integrazione con altri sistemi e l'automazione dei processi di monitoraggio. Offre funzionalità avanzate di controllo degli accessi basate sui ruoli (RBAC) e strumenti per il monitoraggio della sicurezza, garantendo una gestione sicura e confor-

me dell'infrastruttura di rete. Essendo una soluzione commerciale di livello enterprise, NPM comporta costi di licenza significativi, che possono rappresentare una barriera per le organizzazioni con budget limitati. Sebbene NPM offra funzionalità per il monitoraggio di ambienti cloud e ibridi, queste possono essere meno complete rispetto a quelle offerte da strumenti specificamente progettati per il cloud monitoring.

Concludendo, SolarWinds Network Performance Monitor rappresenta una soluzione completa e potente per il monitoraggio delle reti in ambienti enterprise, offrendo una vasta gamma di funzionalità avanzate. Tuttavia, le organizzazioni devono considerare attentamente i costi associati, le risorse hardware necessarie e la complessità di configurazione quando valutano l'adozione di questa piattaforma.

3.3.6 Conclusioni di confronto

Zabbix è uno strumento open source robusto, personalizzabile, e scalabile. In tema di flessibilità, Nagios è preferibile per la vasta gamma di plugin personalizzati,ma accetta compromessi sull'usabilità. Cacti è una soluzione semplice e gratuita, adatta principalmente a monitoraggio di rete di base, meno completa per esigenze complesse. PRTG è ottimo per PMI o organizzazioni che cercano un prodotto completo, semplice, e immediatamente operativo, ma è proprietario e potenzialmente costoso. SolarWinds NPM è consigliato per ambienti enterprise che necessitano di monitoraggio approfondito, analisi predittiva e diagnostica avanzata, ma richiede investimenti significativi e competenze tecniche avanzate.

	Zabbix	**PRTG Network Monitor**	**Nagios**	**Cacti**	**SolarWinds NPM**
Device e Network Discovery	Ottimo, automatizzato	Eccellente, automatizzato	Efficace, ma dipendente da plugin	Limitato, richiede configurazione manuale	Eccellente, supporta più protocolli
Network Monitoring e Analysis	Completo, agent-based & agentless	Dettagliato, trend-based	Flessibile, ma dipende da plugin	Limitato a SNMP e grafici	Avanzato, con diagnostica approfondita
Alert e Notifiche	Avanzato, configurabile	Ottimo, personalizzabile	Solido, notifiche multiple	Limitato, necessita plugin	Eccellente, con AI-based alerts
Reporting & Logging	Dettagliato, con grafici	Personalizzabile, avanzato	Basilare, richiede add-on	Limitato, solo trend grafici	Avanzato, oltre 100 template
Integrità nativa	Molto completo nativamente	Ben integrato nativamente	Molto dipendente dai plugin	Funzionalità di base, molte dipendenti da plugin	Molto completo senza dipendenze
API e Integrazione esterna	API solide, buone integrazioni	Ottime API, integrazione fluida	API limitate senza plugin	Scarso supporto API	API avanzate per automazione completa
Scalabilità & Multi-Tenancy	Elevata scalabilità, supporto multi-tenant	Buona scalabilità, ma limitata multi-tenancy	Scalabile, con personalizzazione avanzata	Difficile scalabilità per grandi ambienti	Enterprise-level, multi-tenant avanzato
RBAC Support & Sicurezza	Presente, ma migliorabile	Presente, ma non avanzato	Limitato, gestione degli accessi basilare	Quasi assente	Avanzato, con policy di sicurezza definite
Costi	Open source, gratuito	Licenza proprietaria, costoso per grandi reti	Nagios Core open source, gratuito	Open source, gratuito	Costoso, licenza enterprise
Requisiti Hardware	Moderati, richiede ottimizzazione	Leggero e ben ottimizzato	Leggero e altamente efficiente	Leggero, ma limitato in grandi ambienti	Elevati, richiede server potenti
Complessità di Configurazione	Complesso da configurare inizialmente	Facile installazione e configurazione	Richiede configurazione avanzata	Facile da installare, ma con funzionalità limitate	Complesso, richiede competenze avanzate
UI & Personalizzazione	UI migliorabile, ma altamente personalizzabile	Ottima UI, facile da usare	UI datata, meno intuitiva	UI semplice, facile da usare	UI moderna, personalizzabile
Supporto Cloud & Hybrid	Supporto base per ambienti cloud	Ottimo supporto per cloud & hybrid	Limitato, necessita plugin	Quasi assente	Avanzato, con monitoraggio cloud dedicato

Tabella 3.1: Confronto tra Zabbix, PRTG Network Monitor, Nagios, Cacti e SolarWinds NPM

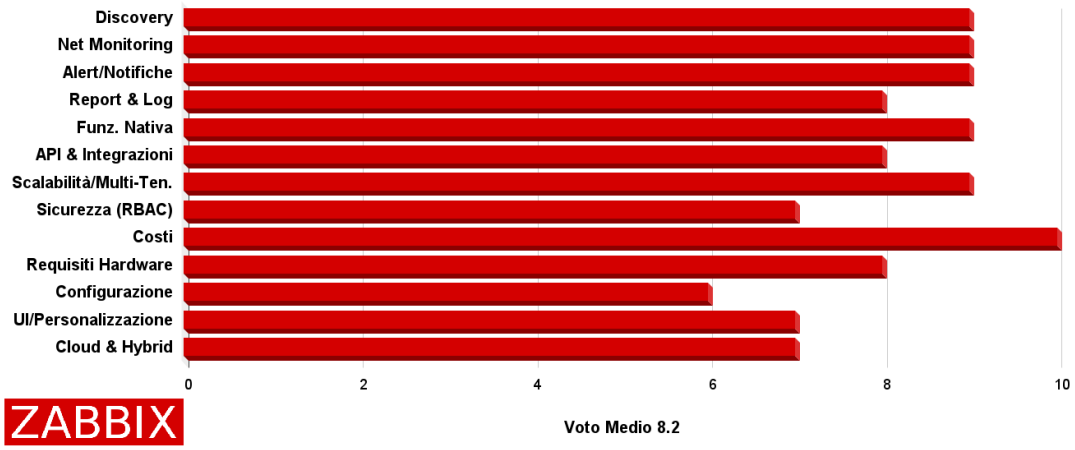

Figura 3.1: Grafico di valutazione di Zabbix

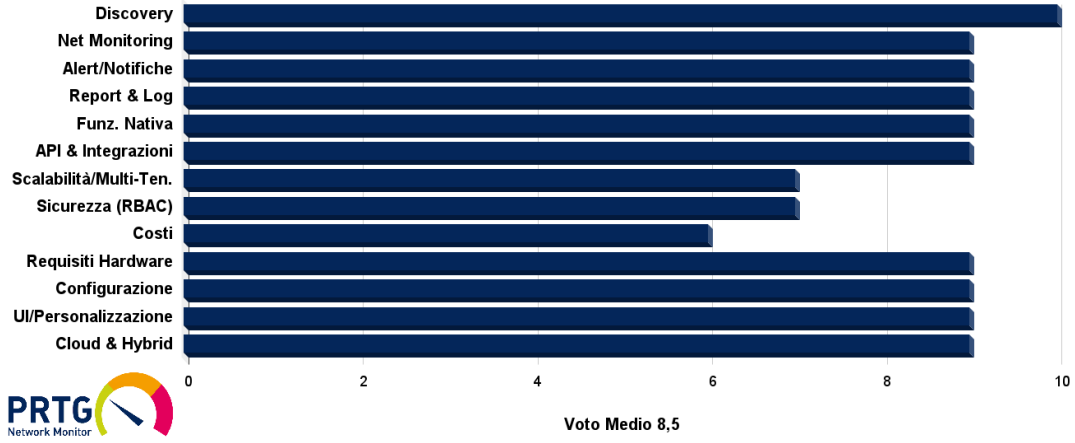

Figura 3.2: Grafico di valutazione di PRTG Network Monitor

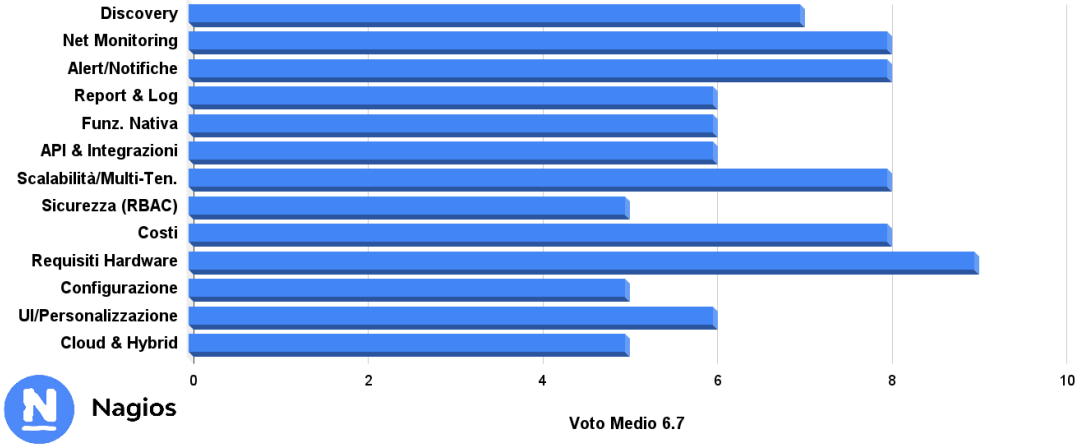

Figura 3.3: Grafico di valutazione di Nagios

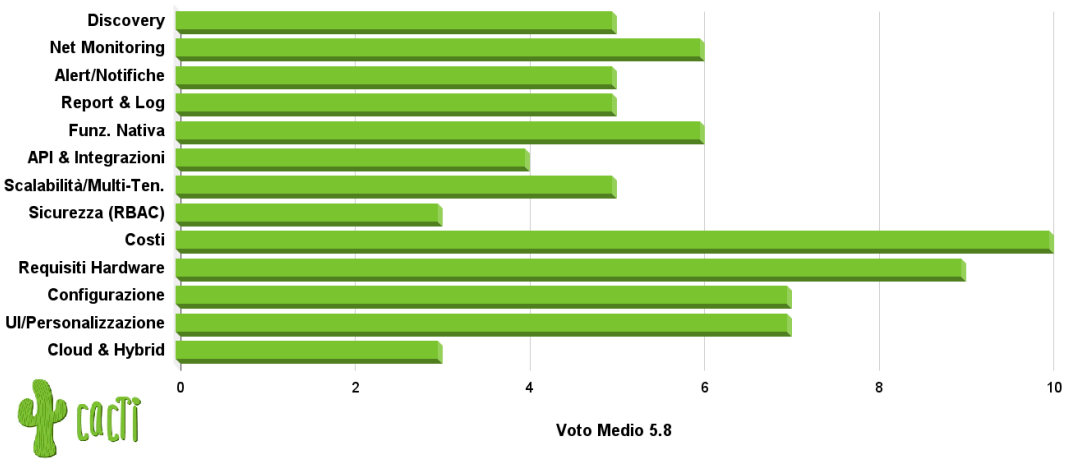

Figura 3.4: Grafico di valutazione di Cacti

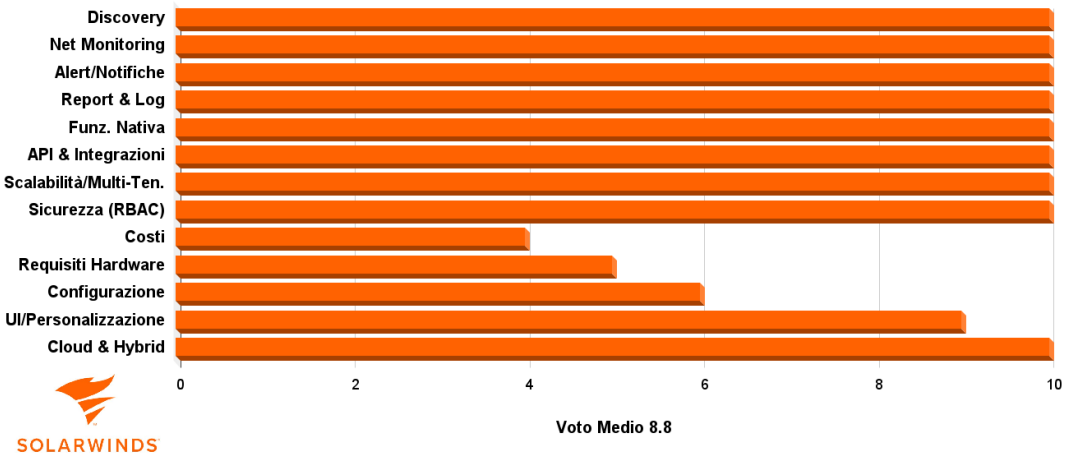

Figura 3.5: Grafico di valutazione di Solarwinds NPM

3.4 Considerazioni sulle attività da intraprendere

Abbiamo parlato approfonditamente del monitoraggio della rete, delle sue caratteristiche e delle tecniche più usate. Successivamente abbiamo introdotto gli strumenti di monitoraggio della rete più usati dalle aziende di tutto il mondo e messo a confronto i loro punti di forza e debolezza. In generale, come ogni nuovo strumento informatico, se non si ha molta conoscenza al riguardo, la decisione di meticolosamente pianificare ogni passo non è necessariamente la strada più giusta da prendere. Infatti, anche in questo caso è utile lasciarsi guidare dall'esplorazione pratica. Tuttavia, siccome parliamo di qualcosa che potrebbe aggiungere valore o diventare un collo di bottiglia al suo operato giornaliero, un amministratore di rete deve fare delle considerazioni.

3.4.1 Stabilire baseline e confronto storico

Con "stabilire una baseline" intendiamo misurare e registrare le metriche chiave della rete in condizioni di funzionamento normale per un periodo significativo (es. una settimana o un mese). Immaginiamo quindi di avere dati storici relativi a utilizzo di banda, latenza media, tempi di risposta, errori, stato dei dispositivi, etc. Questo storico ci permette di costruire un riferimento stabile da confrontare con i dati correnti. [34]

Grazie alla baseline, quindi, è possibile individuare facilmente anomalie, congestioni o malfunzionamenti prima che impattino gli utenti o i servizi aziendali. Inoltre, la conservazione dei dati storici supporta decisioni basate su evidenze oggettive e rende più efficace il capacity planning.

3.4.2 Sfruttare Tecniche di Monitoraggio Complete

Nella fase iniziale, sicuramente ci si può concentrare sulle metriche più importanti, tuttavia un sistema di monitoraggio efficace deve combinare diverse tecniche e tecnologie per offrire una visione completa dell'infrastruttura di rete. Dunque, implementare SNMP è utile per raccogliere dati sullo stato dei dispositivi (es. stato porte, utilizzo CPU/memoria). Usare eventualmente RMON diventa essenziale per analisi avanzate del traffico locale, catture pacchetti mirate e monitoraggio proattivo. Se invece vogliamo analizzare il traffico in dettaglio bisogna integrare sistemi di analisi dei flussi (NetFlow/sFlow/IPFIX). Infine, è importante tenere a mente che approcci più moderni come la telemetria streaming stanno sostituendo i modelli tradizionali, offrendo dati in tempo reale a bassa latenza e maggiore scalabilità.

L'utilizzo combinato di più tecniche offre una visione completa e granulare dello stato di salute della rete, consentendo di reagire tempestivamente ed efficacemente ai problemi emergenti.

3.4.3 Dare priorità agli avvisi e alle notifiche

Uno degli elementi centrali del monitoraggio è rappresentato dal sistema degli avvisi e delle notifiche. Una gestione efficace di questi alert è fondamentale per evitare sovraccarichi informativi e garantire tempi di risposta adeguati. Definire con precisione le soglie che attivano gli avvisi consente di ridurre al minimo i falsi positivi. Un esempio classico è quello del backup programmato: trattandosi di un'operazione ad alto consumo di banda, viene solitamente eseguito in orari notturni, quando la rete è meno trafficata. Tuttavia, se la soglia d'allarme è impostata al 90% dell'utilizzo di banda, il

sistema potrebbe erroneamente interpretare questo traffico legittimo come un attacco, generando un allarme inutile. Senza un'adeguata calibrazione, ciò può tradursi in una serie di segnalazioni infondate che rischiano di distrarre l'amministratore da problemi realmente critici, come ad esempio un effettivo attacco DDoS o il blocco di un servizio core.
Per rendere più efficace il processo decisionale in caso di alert, è opportuno organizzare le notifiche secondo livelli di criticità (es. critico, avvertimento, informativo) così da facilitare la gestione delle priorità.

Infine, stabilire procedure chiare per l'escalation e la gestione degli incidenti è altrettanto importante: definire chi interviene, con quale priorità e in che modo, riduce il rischio di incertezza e disorganizzazione nei momenti più delicati. Questo approccio strutturato consente di mantenere la rete stabile, reattiva e resiliente anche in situazioni di crisi.

3.4.4 Implementare automazione e integrazioni

L'attività di monitoraggio prevede diverse operazioni ripetitive (es. verifica status, raccolta dati, riavvio dei dispositivi, generazione report, etc.) che è il caso di automatizzare usando script (in Python o Bash) o richieste API specifiche. Similmente, l'integrazione dei sistemi di monitoraggio con piattaforme di gestione ticket (es. ServiceNow, Jira) e gestione incidenti è utile per automatizzare apertura e chiusura di ticket.

L'automazione è importante non solo per l'efficienza operativa, ma anche perché riduce errori umani, velocizza il rilevamento e la risoluzione dei problemi e permette al personale di dedicarsi a compiti strategici.

3.4.5 Monitoraggio con focus sulla sicurezza

Allineare il monitoraggio della rete con le pratiche di cybersecurity sostiene il miglioramento della visibilità e il rilevamento avanzato delle minacce. Soluzioni di sicurezza come IDS/IPS e SIEM, garantiscono infatti la conformità alle normative di sicurezza poiché consentono di rilevare e rispondere in modo efficace a minacce sia interne che esterne. Altre attività correlate riguardano la configurazione degli avvisi specifici per eventi di sicurezza rilevanti (tentativi di accesso falliti, attività insolite, traffico sospetto) e la messa in atto di analisi periodiche per identificare vulnerabilità e tentativi di intrusione.

Reti monitorate con attenzione alla sicurezza permettono una risposta rapida agli incidenti informatici, riducendo il rischio di violazioni dati e danni alla reputazione aziendale.

3.4.6 Pianificazione per scalabilità e infrastrutture moderne

In un contesto in cui le architetture IT diventano sempre più ibride, composte da ambienti on-premises, cloud e virtualizzati, è fondamentale che il sistema di monitoraggio sia in grado di adattarsi a questa complessità crescente.
Uno dei primi aspetti da considerare è l'integrazione con ambienti cloud pubblici e privati. Strumenti nativi come AWS CloudWatch, Azure Monitor e Google Cloud Operations Suite offrono metriche dettagliate, log centralizzati e notifiche in tempo reale, consentendo ai team IT di monitorare le risorse distribuite su larga scala. [35]
Un altro pilastro per l'adeguamento delle reti moderne è l'adozione di Software-Defined

Networking (SDN). Separando il piano di controllo da quello dei dati, l'SDN permette una gestione centralizzata, dinamica e programmabile della rete. Questo approccio offre flessibilità operativa e semplifica la configurazione di policy, migliorando la sicurezza e la resilienza dell'infrastruttura. [36]

In definitiva, pianificare per la scalabilità significa non solo predisporre risorse adeguate, ma anche dotarsi degli strumenti e delle architetture in grado di adattarsi al cambiamento. Il monitoraggio della rete va inteso quindi come un componente attivo e strategico nella gestione dell'infrastruttura e della sua modernizzazione: senza un monitoraggio adatto, la scalabilità diventa cieca, lenta e rischiosa. L'adozione di monitoraggio cloud-native e SDN non è solo una questione di performance, ma una garanzia di resilienza e preparazione al futuro in un ecosistema IT in continua trasformazione.

3.4.7 Considerare la conformità e la governance

La conformità alle normative (come GDPR, ISO 27001, NIS2, HIPAA) richiede la registrazione, il controllo e l'auditing delle attività di rete e di sicurezza. È quindi indispensabile che il monitoraggio supporti anche queste esigenze. Condurre audit regolari della strategia di monitoraggio, assicura che gli strumenti e le configurazioni siano allineati con le esigenze aziendali in evoluzione e con i requisiti normativi in vigore.

La conformità normativa protegge l'azienda da sanzioni e da rischi legali, garantendo anche la fiducia di clienti e partner commerciali. Salvare i log, impostare una politica di conservazione dei dati (*retention policy*), documentare gli incidenti e rendere tracciabili le modifiche sono elementi fondamentali per una governance IT trasparente ed efficace.

3.4.8 Utilizzare analisi avanzata e intelligenza artificiale

Le tecnologie basate su intelligenza artificiale, in particolare il machine learning, stanno rivoluzionando il modo in cui si analizzano e interpretano i dati di rete. Gli strumenti di monitoraggio avanzati sono oggi in grado di apprendere i comportamenti normali della rete e generare alert solo in caso di reali anomalie, riducendo drasticamente i falsi positivi. L'adozione dell'analisi comportamentale e dell'apprendimento automatico consente di individuare minacce che sfuggono ai controlli tradizionali, migliorando significativamente la sicurezza e l'efficienza delle reti moderne. [37]

Questa tipologia di intelligenza può anche essere utilizzata per prevedere guasti o congestioni imminenti, supportando una manutenzione predittiva e decisioni più intelligenti.

4. Caso d'uso: Monitoraggio della rete con GNS3

4.1 Panoramica del caso d'uso

Ora che abbiamo una visione più larga della teoria che c'è dietro il monitoraggio della rete, parliamo di come è stata messa alla prova. Il caso d'uso pratico si basa sulla simulazione del monitoraggio della rete, virtualizzando in GNS3 le componenti interconnesse.

4.1.1 GNS3

GNS3 (**Graphical Network Simulator-3**) [38] è un software open source multipiattaforma che permette di creare e simulare reti virtuali complesse. Ci sono due componenti distinte che dobbiamo chiarire brevemente:

- **GNS3 VM:** è una macchina virtuale preconfigurata (basata tipicamente su VMware o VirtualBox) che ospita direttamente i dispositivi virtuali (router, switch, firewall, ecc.).

- **GNS3 App:** è il software installato direttamente sul computer host (Windows, Linux o Mac) che può gestire autonomamente topologie semplici con limitate risorse virtuali.

Il vantaggio di questa separazione è che abbiamo la parte che necessita di molte risorse per l'esecuzione dei dispositivi virtualizzati divisa dalla gestione dell'interfaccia della topologia della rete. Quando usato senza la VM, l'app sfrutta esclusivamente le risorse locali del PC, limitando la scalabilità e la complessità della simulazione. È possibile usare solo l'app senza la VM, ma la divisione garantisce una maggiore stabilità e performance nelle simulazioni poiché abbiamo un ambiente isolato e ottimizzato per l'esecuzione di apparati virtualizzati. L'app GNS3 permette anche di collegarsi alla VM in esecuzione in un server fisico o su cloud. Questa soluzione permette di avere un maggiore controllo delle risorse nella macchina host da parte dell'interfaccia GNS3 e gestire le risorse della VM completamente in maniera separata.

Usare GNS3 nel caso d'uso è vantaggioso anche per i seguenti motivi:

- supporta immagini reali di dispositivi (es. Cisco IOS, firewall, appliance Linux), permettendo simulazioni molto vicine a scenari reali;

- l'interfaccia drag-and-drop rende semplice creare e visualizzare topologie di rete;

- integra facilmente macchine virtuali e container Docker per espandere le funzionalità (server, client, tool di monitoraggio, ecc.);
- è possibile combinare diversi sistemi operativi, software e apparati in una rete completamente personalizzata;

4.1.2 Scelte e considerazioni iniziali

Per il caso d'uso è stata scelta l'esecuzione della macchina virtuale di GNS3 su VMware, nella stessa macchina host in cui viene eseguita l'app GNS3. Questa scelta è stata presa per la pura semplicità della configurazione. Lo scopo di questo caso d'uso non era quello di poter raggiungere i limiti degli strumenti di monitoraggio o della piattaforma di simulazione, ma solo avere una panoramica generale di come possono essere configurati e usati gli strumenti di monitoraggio candidati in un ambiente di laboratorio.

L'host in cui GNS3 (sia app che VM) e le macchine virtuali in VMware vengono eseguiti presenta le seguenti caratteristiche tecniche:

- **Processore:** i7-8700K 3.70 GHz
- **Memoria RAM:** 32GB
- **Storage:** SSD 1TB
- **OS:** Windows 11 Pro

Alla macchina virtuale di GNS3 sono state assegnate le seguenti caratteristiche:

- 8GB di RAM;
- 4 core (2 processori con 2 core ciascuno);
- 20GB di hard disk;

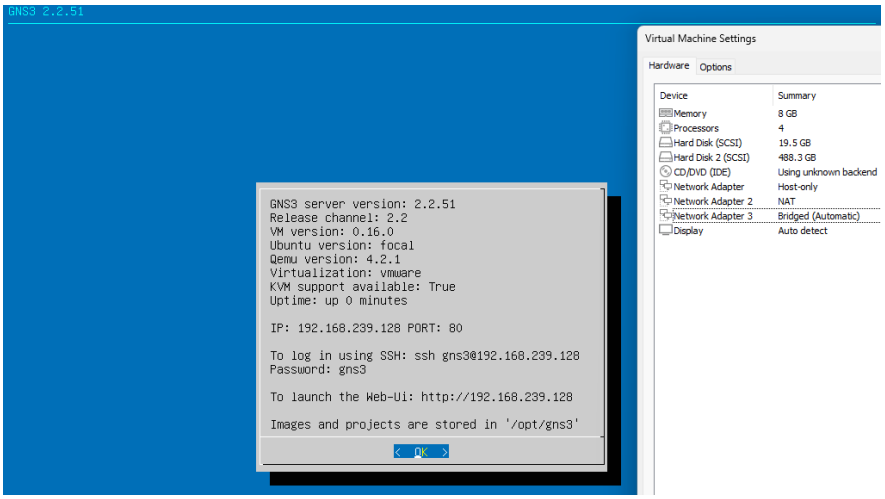

Figura 4.1: Configurazione di GNS3 VM in VMware

Inoltre, come si può vedere nella Figura 4.1 è stato aggiunto un adattatore bridged per configurare la porta WAN dal firewall della rete simulata e poterlo raggiungere dalla macchina host.

Inizialmente, per familiarità e facilità di gestione, era stato deciso di installare e configurare switch Cisco e un firewall ASA nella rete simulata. Tuttavia, dopo aver configurato l'emulatore dell'ASA in GNS3, esso presentava problemi di perdita di pacchetti con alcuni dispositivi mentre con altri no. In un ambiente di simulazione è normale che alcuni elementi presentino malfunzionamenti, dato che la virtualizzazione dei componenti non sempre è un rapporto 1:1 con quelli fisici. Tuttavia, le problematiche che stava presentando l'ASA sembravano troppo aleatorie, quindi si è optato invece per un emulatore di Fortigate come firewall. Rispetto all'ASA, Fortigate ha un interfaccia grafica più *user-friendly*. Ovviamente i comandi CLI sono differenti da quelli Cisco, ma per la configurazione della rete simulata non parliamo di tanta complessità. Infine, essendo una versione di testing, l'immagine del Fortigate ha una scadenza di 15 giorni, dopodiché il firewall non funziona più. Per questo motivo è più semplice salvarsi i comandi CLI della configurazione per poi fare un reset e riconfigurare il firewall daccapo.

Gli switch utilizzati sono quelli Cisco, dato che non presentavano grossi problemi. L'unico aspetto ingombrante riguarda frammentazione della memoria che appare dopo un po' di tempo, probabilmente, come con l'emulatore dell'ASA, dovuti all'immagine del dispositivo (anche perché si tratta di una versione da laboratorio). Una volta che appare questo problema, la soluzione è spegnere e riaccendere gli switch e tutto ritorna a funzionare: quindi non si perde la configurazione dello switch.

La macchina Windows Server 2016 invece, che viene usata per il servizio DHCP e DNS nella rete simulata, è stata anch'essa scelta per familiarità e semplicità di configurazione.

Mentre, per uniformare l'installazione degli strumenti di monitoraggio, sono stati scelti due server Ubuntu. Di nuovo, essendo ben documentati le configurazioni e installazioni dei due strumenti candidati per server linux, allora si è optato per questo sistema operativo.

Passiamo ai due strumenti di monitoraggio: Zabbix e Cacti. La direzione della tesi è stata quella di volgersi principalmente verso il mondo open-source e gratuito. Strumenti come PRTG e SolarWinds sono commerciali e nella versione gratuita offrono funzionalità limitate (es. PRTG limita a 100 sensori). Questo rende Zabbix e Cacti ideali per un uso accademico e sperimentale, dove si predilige l'accessibilità completa e senza costi. Sia Zabbix che Cacti godono di una vasta comunità di utenti e sviluppatori, con forum, guide, manuali e tutorial facilmente reperibili. Ciò facilita l'apprendimento e la risoluzione di problemi durante le fasi di laboratorio. SolarWinds e PRTG, invece, hanno una documentazione molto orientata all'ambiente enterprise che richiede un supporto a pagamento. Nagios Core è la versione open e gratuita di Nagios, tuttavia, essendo basato su un sistema di plugin e riguardo la sua implementazione potrebbe richiedere configurazioni meno immediate, si è scelto di lasciarlo per futuri sviluppi di testing. Cacti e Zabbix invece funzionano molto bene in ambienti virtualizzati come GNS3, perché supportano nativamente SNMP e possono essere configurati con sistemi Linux lightweight.

4.1.3 Topologia della rete

La figura seguente mostra la topologia della rete simulata che è stata creata in GNS3. Il dispositivo in alto, denominato `Internet`, è identificato di default in GNS3 come Cloud. Non è altro che un ponte tra la topologia simulata e la rete fisica in cui è collegato la macchina host.

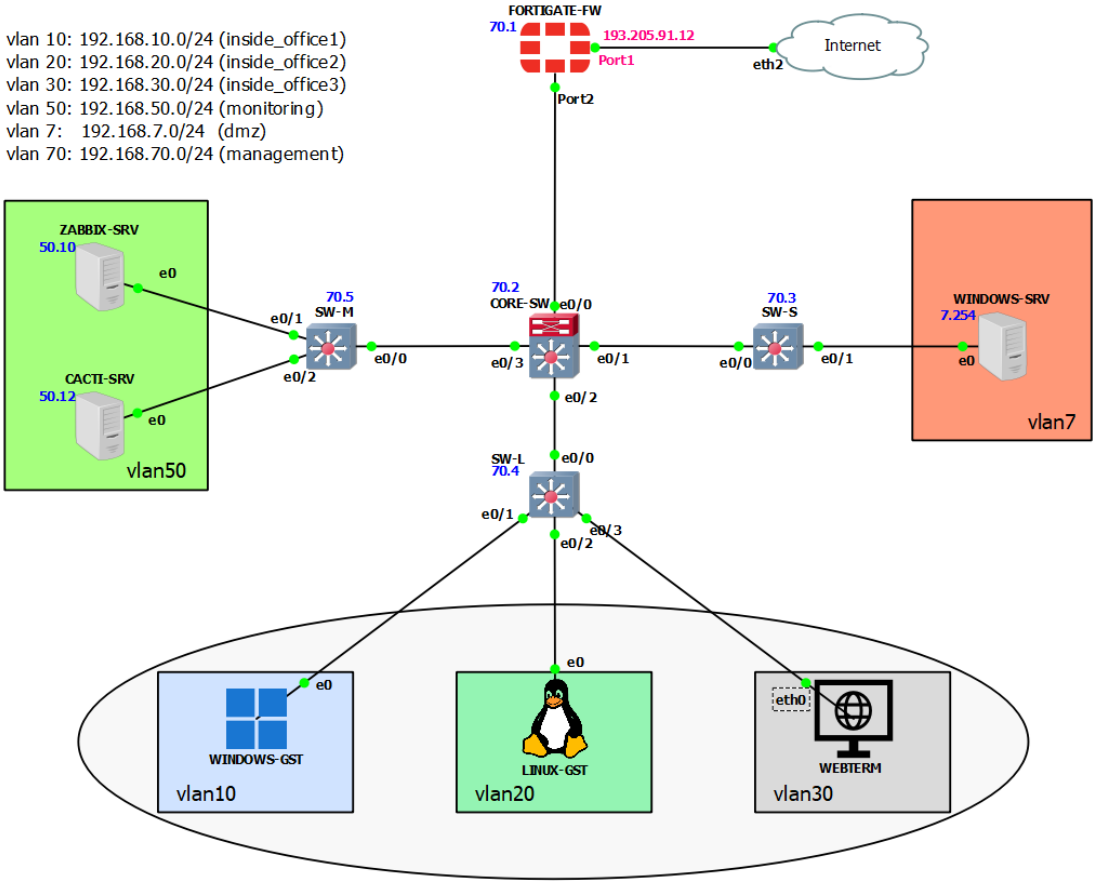

Figura 4.2: Topologia della rete di simulazione in GNS3

Nome Dispositivo	**Versione**	**Note**
FORTIGATE-FW	FortiGate-VM64-KVM v7.0.9	Versione virtuale del firewall FortiGate
CORE-SW, SW-S, SW-L, SW-M	Cisco IOS L2 Switch (I86BI_LINUXL2-IPBASEK9-M), 15.1	Immagini base IOU (IOS on Unix) di switch Cisco di livello 2, versione da laboratorio
WINDOWS-SRV	Windows Server 2016	Macchina virtuale in VMware, Server DHCP e DNS
ZABBIX-SRV	Ubuntu Server 24.04	Macchina virtuale in VMware, Server per Zabbix
CACTI-SRV	Ubuntu Server 24.04	Macchina virtuale in VMware, Server per Cacti
WINDOWS-GST	Windows 11 Pro	Macchina virtuale in VMware, guest
LINUX-GST	Linux Mint	Macchina virtuale in VMware, guest
WEBTERM	Docker Container	Terminale web-based

Tabella 4.1: Tabella dei dispositivi virtuali nella rete di GNS3

Come si può vedere dalla Figura 4.2, sono state definite sei VLAN:

- **VLAN 10 - 192.168.10.0/24** (inside_office1): VLAN per guests
- **VLAN 20 - 192.168.20.0/24** (inside_office2): VLAN per guests
- **VLAN 30 - 192.168.30.0/24** (inside_office3): VLAN per guests
- **VLAN 50 - 192.168.50.0/24** (monitoring): VLAN per i server degli strumenti di monitoraggio
- **VLAN 70 - 192.168.70.0/24** (management): VLAN per management degli apparati (switches e firewall)
- **VLAN 7 - 192.168.7.0/24** (dmz): VLAN per server farm

Il server Windows ha un indirizzo IP fisso 192.168.7.254. Stesso discorso per i server Ubuntu: Zabbix 192.168.50.10 e Cacti 192.168.50.12. Questi ultimi due sono indirizzi cui è stata impostata la prenotazione nel DHCP sul server Windows.
Mentre gli indirizzi vicino al firewall e agli switch indicano le interfacce virtuali nella VLAN 70, quella di management, che viene usata dai server Zabbix e Cacti per monitorare gli apparati.
I client nelle VLAN 10, 20 e 30 invece sono impostati per prendere l'IP in automatico dal server DHCP.

4.2 Configurazioni dei dispositivi

In questa sezione ci concentriamo sulla particolare configurazione dei dispositivi connessi.

4.2.1 Fortigate Firewall

Il firewall Fortigate ha la porta `Port1` cui è impostato l'indirizzo IP fisso 193.205.91.12/24. Mentre la porta `Port2` non è stato impostato un IP, però sono state definite tutte le sottointerfacce per le VLAN.

Name	Type	IP/Netmask	Administrative Access	DHCP Ranges
Physical Interface 16				
LAN (port2)	Physic...	0.0.0.0/0.0.0.0		
dmz (vlan7)	VLAN	192.168.7.1/255.255.255.0	PING	
management (vlan70)	VLAN	192.168.70.1/255.255.255.0	PING SNMP	
monitoring (vlan50)	VLAN	192.168.50.1/255.255.255.0	PING SNMP	Relay: 192.168.7.254
office1 (vlan10)	VLAN	192.168.10.1/255.255.255.0	PING	Relay: 192.168.7.254
office2 (vlan20)	VLAN	192.168.20.1/255.255.255.0	PING	Relay: 192.168.7.254
office3 (vlan30)	VLAN	192.168.30.1/255.255.255.0	PING	Relay: 192.168.7.254

Figura 4.3: Configurazione delle VLAN nel Fortigate

Come si può notare dalla Figura 4.3, per le VLAN 10, 20, 30 e 50 è stato impostato il DHCP Relay all'indirizzo del server Windows (192.168.7.254). Nelle VLAN 50 e 70 è stato autorizzato il protocollo `SNMP` oltre al `PING` per poter monitorare gli apparati da Zabbix e Cacti.

Tutte le VLAN sono state inserite dentro una zona cui è stata abilitato il traffico interno. Inoltre, per semplicità, il traffico proveniente da questa zona verso l'interfaccia WAN (o `Port1`, quindi che esce fuori dalla rete) è stato abilitato per ogni servizio attraverso le policy di accesso del firewall. Di conseguenza, dato che la porta WAN deve poter uscire fuori dalla rete simulata, è stata impostata la rotta di default (0.0.0.0/0) con gateway quello della macchina host. Infine, è stato configurato l'agent SNMP e creata la comunity `public` per i server Zabbix e Cacti.
Per ulteriori informazioni sulla configurazione, fare riferimento all'Appendice A.1

SNMP Agent

Description	SNMP Monitoring Agent
Location	Camerino
Contact Info	besjan.veizi@unicam.it

SNMP v1/v2c

+Create New | Edit | Delete | Status

Name	Queries	Traps	Hosts	Events	Status
public	v1 Enable v2 Enable	v1 Enable v2 Enable	192.168.50.10/32 192.168.50.12/32	37	Enable

Figura 4.4: Configurazione del SNMP nel Fortigate

4.2.2 Core Switch

Il Core Switch è collegato con il firewall dall'interfaccia `e0/0`, con lo switch verso la server farm (SW-S) dall'interfaccia `e0/1`, con lo switch verso le vlan delle macchine guest (SW-L) dall'interfaccia `e0/2` e con lo switch verso la vlan degli strumenti di monitoraggio (SW-M) dall'interfaccia `e0/3`. Tutte le interfacce sono state impostate come porte trunk 802.1Q.

Inoltre è stata definita l'interfaccia virtuale VLAN 70 con indirizzo ip 192.168.70.2/24 e l'ip del default gateway è stato impostato 192.168.70.1. Per permettere il monitoraggio SNMP è stata impostata la community `public`.

Sono state definite le altre VLAN e infine è stato impostato il dominio VTP e impostato come server. In questo modo, gli altri switch, registrandosi con le stesse credenziali del dominio VTP e impostati come client partecipano allo scambio di informazioni: in particolare delle altre VLAN senza doverle definire manualmente nella configurazione. Per ulteriori informazioni sulla configurazione, fare riferimento all'Appendice A.2

4.2.3 Access Switches

Gli switch access invece hanno tutti la prima interfaccia (`e0/0`) che è collegata al core switch: questa è stata impostata come trunk 802.1Q. Mentre tutte le altre porte collegate sono in access. In particolare:

- SW-S ha in access la porta `e0/1` verso la VLAN 7;
- SW-L ha in access le tre porte `e0/1`, `e0/2` ed `e0/3` rispettivamente verso la VLAN 10, 20 e 30;
- SW-M ha in access le porte `e0/1` ed `e0/2` verso la VLAN 50;

A ciascuno dei tre switch è stata definita l'interfaccia virtuale VLAN 70 con un indirizzo ip differente: 192.168.70.3/24 per SW-S, 192.168.70.4/24 per SW-L e 192.168.70.5/24 per SW-M.

Infine, come per il core switch, per ognuno è stato impostato il gateway di default con l'ip della sotto-interfaccia del firewall 192.168.70.1/24 e impostata la community `public` per il monitoraggio SNMP. Per ulteriori informazioni sulla configurazione degli access switch SW-S, SW-L e SW-M, fare riferimento rispettivamente all'Appendice A.3, A.4 e A.5

4.2.4 Windows Server 2016

La macchina virtuale di Windows Server 2016 è stata configurata con 4 GB di RAM e 2 core. In essa sono state installate le funzionalità DHCP e DNS dal server manager. Seguendo la Figura 4.3, sono stati definiti i 4 ambiti per ciascuna VLAN interessata. Inoltre, nella VLAN 50, sono state definiete le prenotazioni per i server di Zabbix (ubuntuserver) e Cacti (cactisrv). Per quanto riguarda il DNS, sono stati scelti i server DNS pubblici di Google (8.8.8.8 e 8.8.4.4).

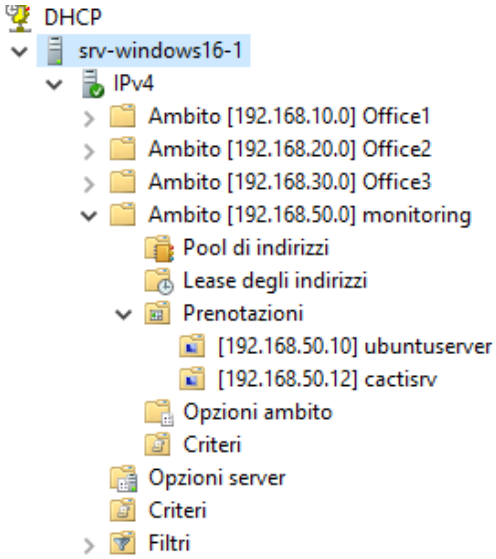

Figura 4.5: Configurazione ambiti e prenotazioni DHCP su Windows Server

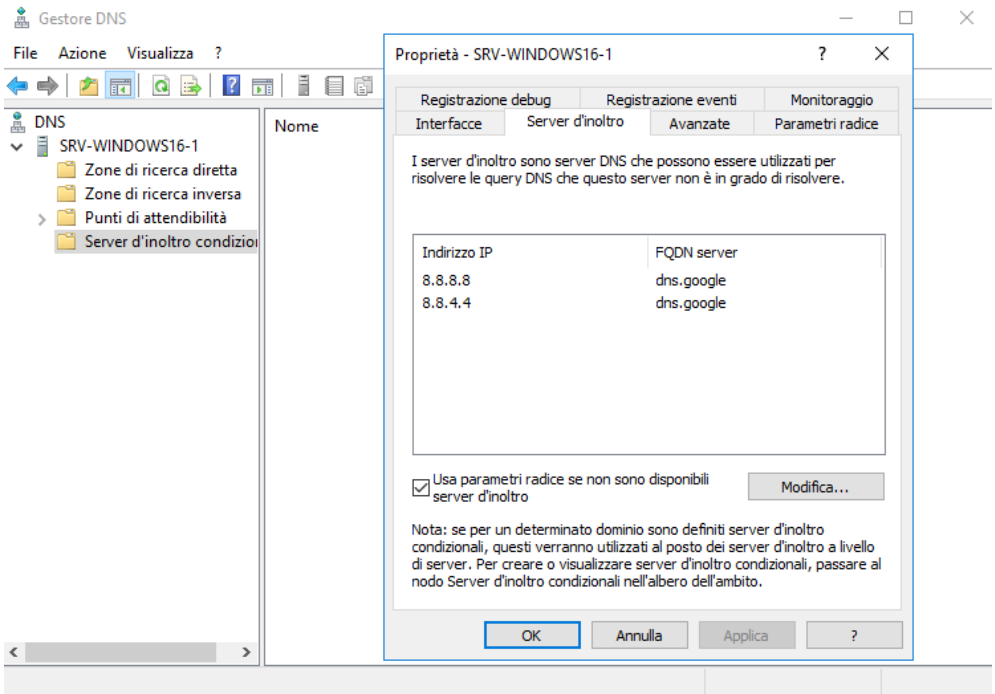

Figura 4.6: Configurazione DNS su Windows Server

4.2.5 Zabbix - Server Ubuntu

Per configurare Zabbix abbiamo detto che è stato scelto il server Ubuntu come macchina virtuale. A quest'ultima sono state assegnate 2 core, 4GB di RAM e 40 di disco. Una volta creata la macchina virtuale con VMware, è stato installato e configurato Zabbix come segue.

```
sudo -s
wget https://repo.zabbix.com/zabbix/7.2/release/ubuntu/pool/main/z/zabbix
    -release/zabbix-release_latest_7.2+ubuntu22.04_all.deb
dpkg -i zabbix-release_latest_7.2+ubuntu22.04_all.deb
apt update
```

Codice 4.1: Installazione della repository di Zabbix

```
apt install zabbix-server-mysql zabbix-frontend-php zabbix-apache-conf
    zabbix-sql-scripts zabbix-agent
```

Codice 4.2: Installazione del server Zabbix, del frontend e dell'agent

Ora accediamo a MySQL e configuriamo il database per Zabbix. Il database si chiama `zabbixdb`, l'utente è `zabbix` e la password è `zabbix`.

```
mysql -uroot -p
# <root-password>
create database zabbixdb character set utf8mb4 collate utf8mb4_bin;
create user zabbix@localhost identified by 'zabbix';
grant all privileges on zabbixdb.* to zabbix@localhost;
set global log_bin_trust_function_creators = 1;
quit;
```

Codice 4.3: Configurazione del database di Zabbix

Carichiamo lo schema iniziale (tabelle, indici, dati iniziali) nel database e utente MySQL appena creati

```
> zcat /usr/share/zabbix/sql-scripts/mysql/server.sql.gz | mysql --
    default-character-set=utf8mb4 -uzabbix -p zabbixdb
```

Codice 4.4: Caricamento dello schema del database di Zabbix

Dopo aver importato lo schema del database, disabilitiamo l'opzione `log_bin_trust_function_creators`

```
mysql -uroot -p
# <password>
set global log_bin_trust_function_creators = 0;
quit;
```

Codice 4.5: Disabilitazione dell'opzione log_bin_trust_function_creators

Modifichiamo il file di configurazione del server Zabbix per aggiungere la password del database

```
sudo vim /etc/zabbix/zabbix_server.conf
# aggiungi le seguenti righe nel file
DBName=zabbixdb
DBPassword=zabbix
DBHost=localhost
```

Codice 4.6: Modifica del file di configurazione del server Zabbix

Rieseguiamo i processi del server e dell'agent e li abilitiamo all'avvio del boot.

```
systemctl restart zabbix-server zabbix-agent apache2
systemctl enable zabbix-server zabbix-agent apache2
```

Codice 4.7: Restart e abilitazione del server e agent Zabbix

Con una delle guest machine, accediamo dal browser a 192.168.50.10/zabbix, accediamo con username `Admin` e password `zabbix` e saremo all'interno della piattaforma web dello strumento di monitoraggio.

4.2.6 Cacti - Server Ubuntu

Per configurare Cacti abbiamo scelto le stesse caratteristiche del server Ubuntu di Zabbix: 2 core, 4GB di RAM e 40GB di disco. Una volta creata la macchina virtuale con VMware, è stato installato e configurato Cacti come segue.

Prima installiamo le dipendenze e poi Cacti.

```
sudo apt install -y apache2 mariadb-server php php-mysql php-gd php-xml
    php-mbstring php-snmp rrdtool snmp snmpd libapache2-mod-php unzip
sudo apt install -y cacti
```

Codice 4.8: Installazione delle dipendenze e del package di Cacti

Configuriamo il database MariaDB per Cacti

```
sudo mysql_secure_installation
sudo mysql -u root -p
# <password>
ALTER DATABASE cactidb CHARACTER SET utf8mb4 COLLATE utf8mb4_unicode_ci;
GRANT ALL PRIVILEGES ON cactidb.* TO 'cacti'@'localhost' IDENTIFIED BY '
    cacti';
FLUSH PRIVILEGES;
EXIT;
```

Codice 4.9: Configurazione del database per Cacti

Configuriamo l'SNMP per il server.

```
sudo systemctl enable snmpd
sudo systemctl start snmpd
sudo vim /etc/snmp/snmpd.conf
# modifica le seguenti righe
agentAddress udp:161,udp6:[::1]:161
rocommunity public
sysLocation "Camerino"
sysContact besjan.veizi@unicam.it
# salva ed esci
sudo systemctl restart snmpd
```

Codice 4.10: Configurazione dell'SNMP per Cacti

Configuriamo il web server Apache per Cacti

```
sudo nano /etc/apache2/sites-available/cacti.conf
Alias /cacti /usr/share/cacti
# aggiungi le seguenti righe
<Directory /usr/share/cacti/>
   Options +FollowSymLinks
   AllowOverride None
   <IfModule mod_authz_core.c>
      Require all granted
   </IfModule>
</Directory>
# salva ed esci
sudo a2enmod rewrite
sudo systemctl restart apache2
```

Codice 4.11: Configurazione di Apache per Cacti

Configuriamo il poller per raccogliere dati dai dispositivi monitorati da Cacti a intervalli di tempo definiti (ogni 5 minuti) attraverso un cron job.

```
sudo nano /etc/cron.d/cacti
# assicurati che ci sta la seguente riga
*/5 * * * * www-data php /usr/share/cacti/poller.php > /dev/null 2>&1
# salva ed esci
sudo systemctl restart cron
```

Codice 4.12: Configurazione del poller per Cacti

Con una delle guest machine, accediamo dal browser a 192.168.50.12/cacti, accediamo con username `admin` e password `admin` e saremo all'interno della piattaforma web dello strumento di monitoraggio.

4.2.7 Clients nelle VLAN 10, 20 e 30

Per i client nelle VLAN 10 (inside_office1), 20 (inside_office2) e 30 (inside_office3) abbiamo scelto Windows 11 Pro, Linux Mint 22.1 e un semplice webterminal. Le prime due sono macchine virtuali che sono eseguite con VMware e poi collegate in GNS3, mentre il webterminal è un container Docker preconfigurato che fornisce un terminale web-based direttamente all'interno della topologia di rete GNS3.

4.3 Integrazione e scoperta dei dispositivi

In questa sezione ci concentreremo sui passi per integrare e fare la scoperta (*discovery*) dei dispositivi su Zabbix e Cacti.

4.3.1 Integrazione e scoperta su Zabbix

Per integrare correttamente il firewall e gli switch nel sistema di monitoraggio, è fondamentale verificare che il protocollo SNMP sia abilitato. Zabbix supporta sia il monitoraggio agentless che quello basato su agent. Siccome con Cacti abbiamo scelto un approccio senza agent, con Zabbix abbiamo deciso di testare l'uso dell'agent, installandolo sul server Windows nella nostra rete. L'agent si può scaricare dalla pagina ufficiale di Zabbix[1].

[1] https://www.zabbix.com/download_agents

Una volta scaricato l'installer lo eseguiamo, accettiamo i termini della licenza e alla configurazione impostiamo l'indirizzo IP del server Zabbix 192.168.50.10. La porta che l'agent di default utilizza è la 10050.

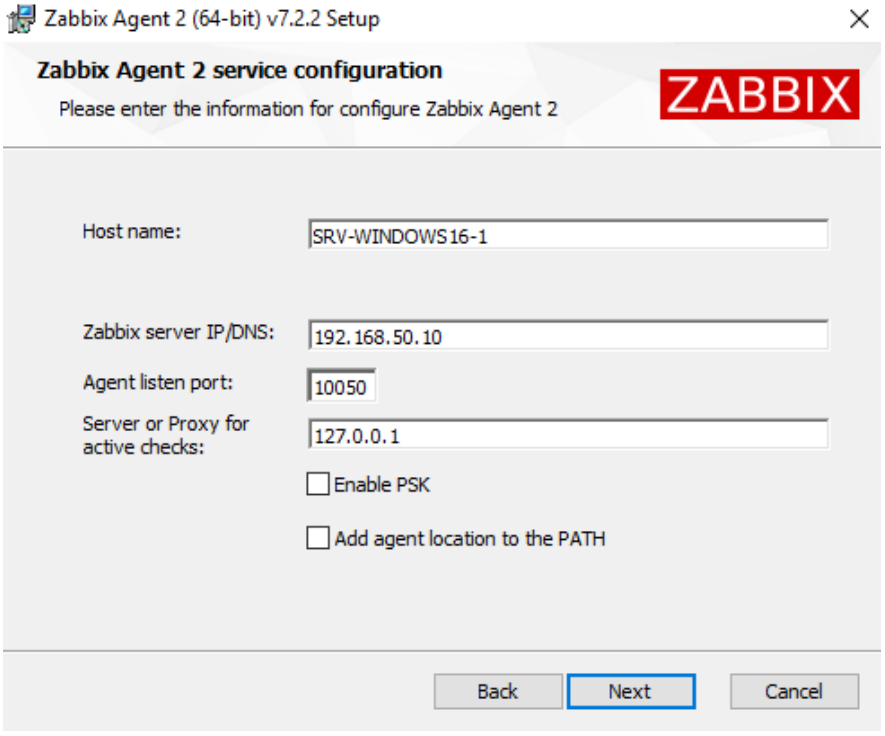

Figura 4.7: Configurazione IP del server Zabbix nell'agent

Dopodiché assicuriamoci che il servizio dell'agent è attivo e si esegue in automatico all'avvio del server.

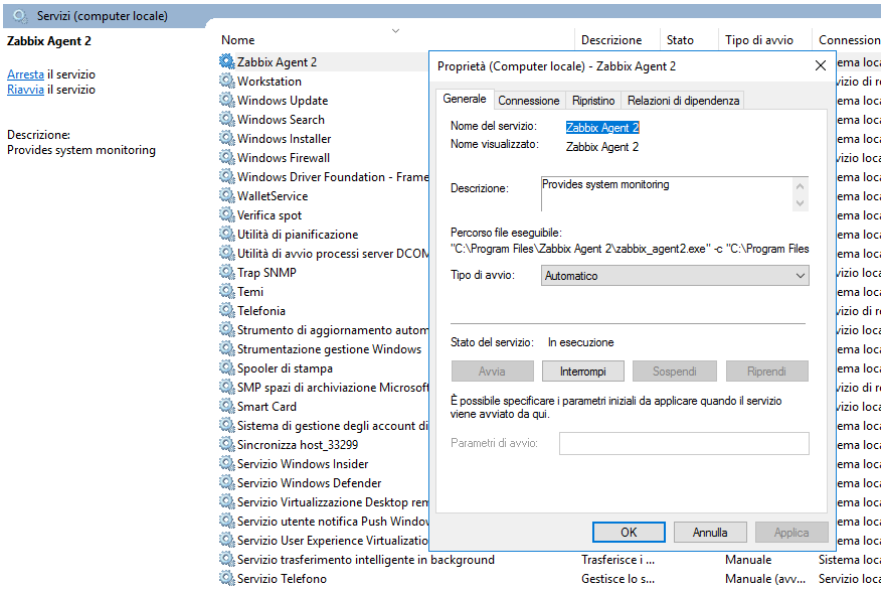

Figura 4.8: Servizio dell'agent di Zabbix abilitato in automatico

Tutti i dispositivi critici sono stati configurati per poter comunicare con lo strumento: ora dobbiamo integrarli su Zabbix.
Prima di tutto creiamo dei gruppi per aggregare i nostri dispositivi. Dal menù a destra andiamo su **Data collection → Host groups** e clicchiamo sul pulsante **Create host group** in alto a destra. Creiamo quindi i gruppi ***Core Network*** per gli switch e il firewall e il gruppo ***Server Farm*** dove ci andrà il server Windows.
Per aggiungere i dispositivi invece, dal menù a sinistra andiamo su **Data collection → Hosts** e poi clicchiamo sul pulsante **Create Host** in alto a destra. A questo punto scegliamo il nome dell'host, il template adatto all'host che vogliamo monitorare e l'interfaccia.
I template che Zabbix offre sono diversi, nel nostro caso il template usato per il Fortigate firewall è stato **Fortigate by SNMP**, per i switches **Cisco IOS by SNMP** e per il server Windows è stato scelto **Windows by Zabbix agent** dato che abbiamo installato l'agent.
Riguardo all'interfaccia invece, per il server scegliamo l'opzione `Agent` e mettiamo il suo indirizzo IP 192.168.7.254. Mentre per gli switch e il firewall scegliamo SNMP e scegliamo l'indirizzo IP dell'interfacca della VLAN 70 (management) assegnatogli in configurazione. Copiamo la stringa {`$SNMP_COMMUNITY`} nella voce ***SNMP community***, ci rechiamo nella tab ***Macro*** e la incolliamo nella prima casella, mentre come valore mettiamo `public` poiché è quello il nome della comunity che abbiamo scelto per tutti i dispositivi.

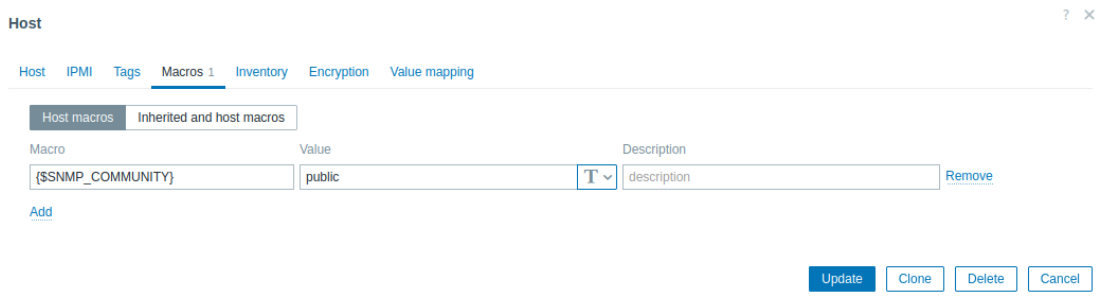

Figura 4.9: Configurazione community 'public' per firewall e switches su Zabbix

Di seguito mostriamo le configurazioni per il firewall, il core switch e Windows Server. Gli access switches sono impostati come il core switch: l'unica cosa che cambia è l'indirizzo IP che è stato assegnato alla loro SVI della VLAN 70 nella loro configurazione.

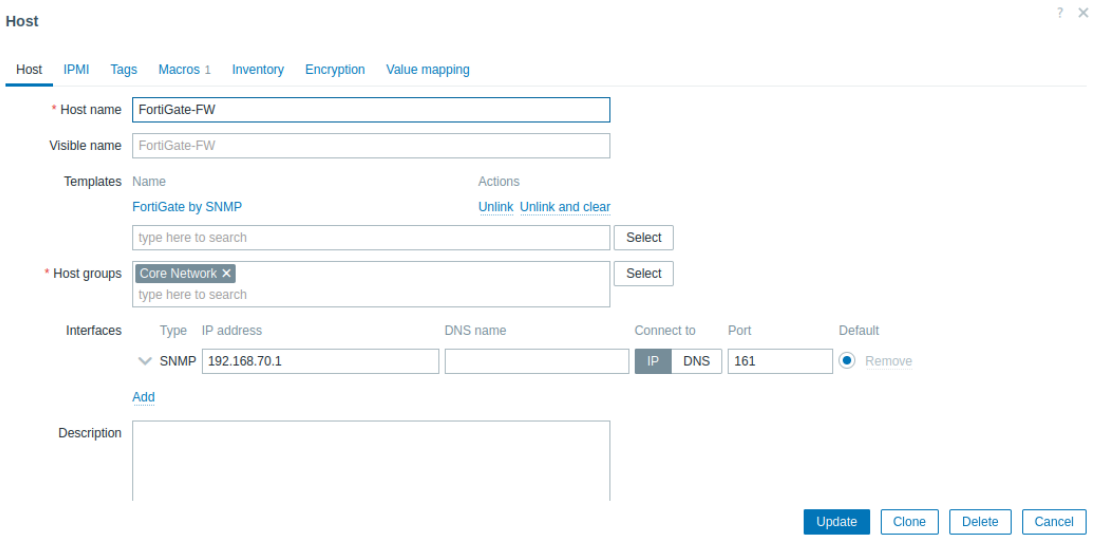

Figura 4.10: Configurazione del firewall su Zabbix

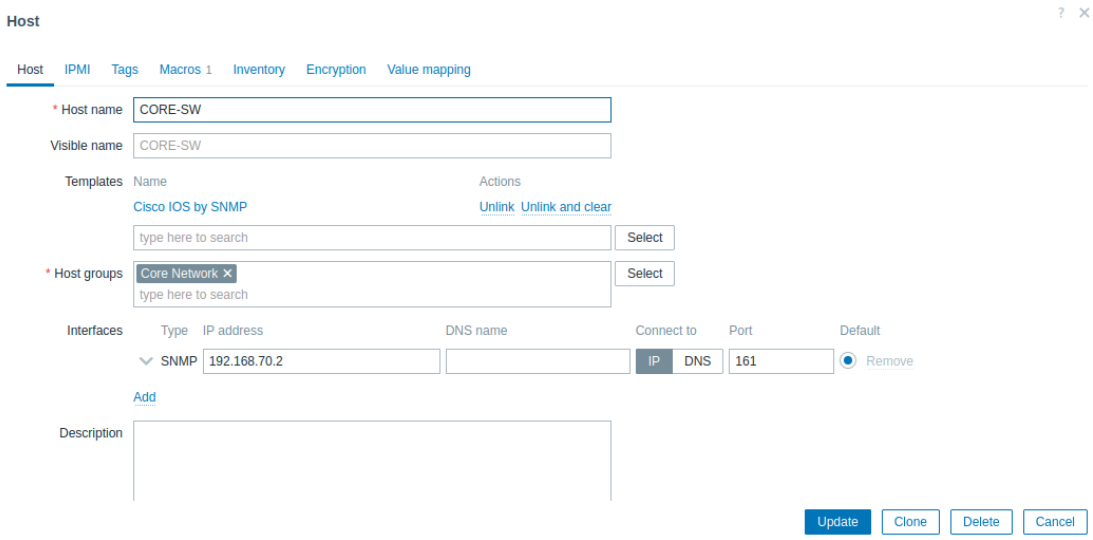

Figura 4.11: Configurazione del core switch su Zabbix

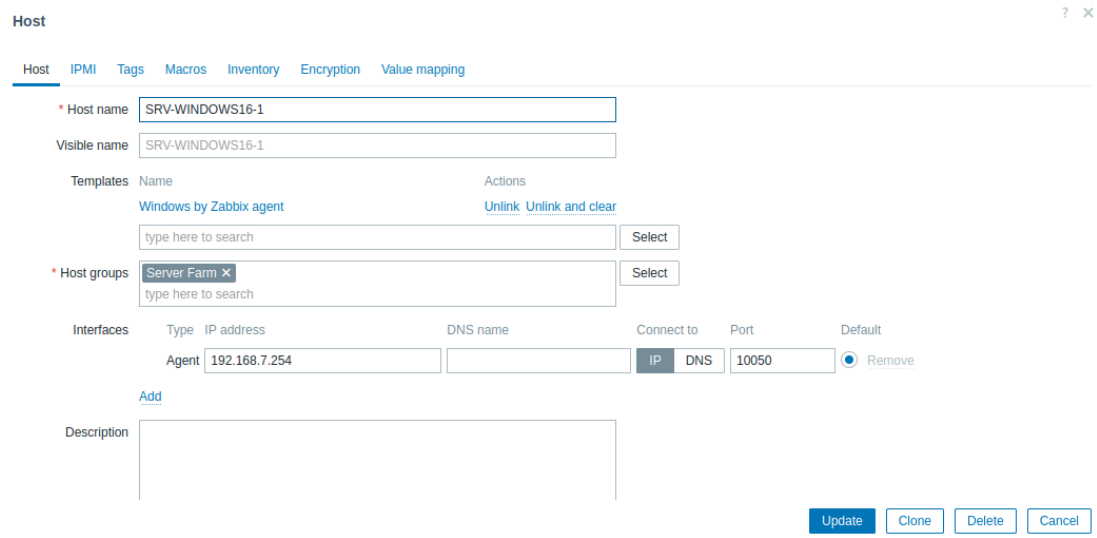

Figura 4.12: Configurazione del windows server su Zabbix

A questo punto i dispositivi saranno visualizzati come segue nella Figura 4.13 sottostante.

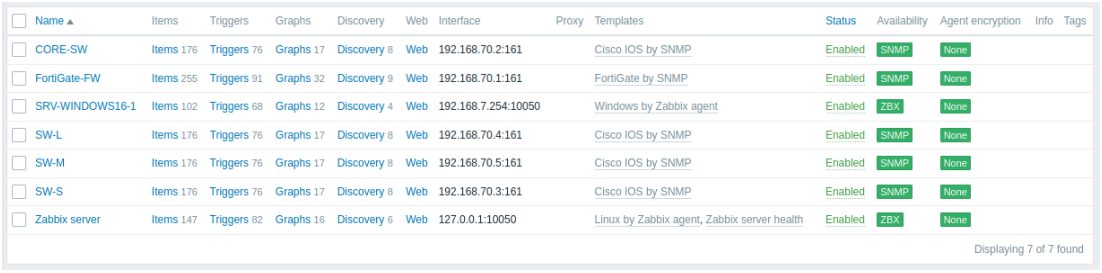

Figura 4.13: Integrazione degli dispositivi su Zabbix

4.3.2 Integrazione e scoperta su Cacti

A differenza di Zabbix, di default Cacti è considerato uno strumento di monitoraggio agentless poiché la raccolta dei dati avviene tramite SNMP polling. Può essere configurato per usare script custom o plugin che eseguono comandi direttamente su un sistema tramite SSH o cron job locali nel server. Tuttavia, siccome non esiste un "Cacti Agent" ufficiale da installare come nel caso di Zabbix, configuriamo i dispositivi per essere monitorati con l'SNMP.
Gli switch e il firewall sono già a posto, mentre nel server Windows avevamo usato l'agent di Zabbix ma non abbiamo attivato e configurato il servizio SNMP. Rechiamoci quindi nei Servizi e cerchiamo "Servizio SNMP" tra le voci, abilitiamo l'esecuzione automatica del servizio e nella voce ***Sicurezza*** configuriamo la comunity `public` in sola lettura e aggiungiamo l'host di Cacti, 192.168.50.12.

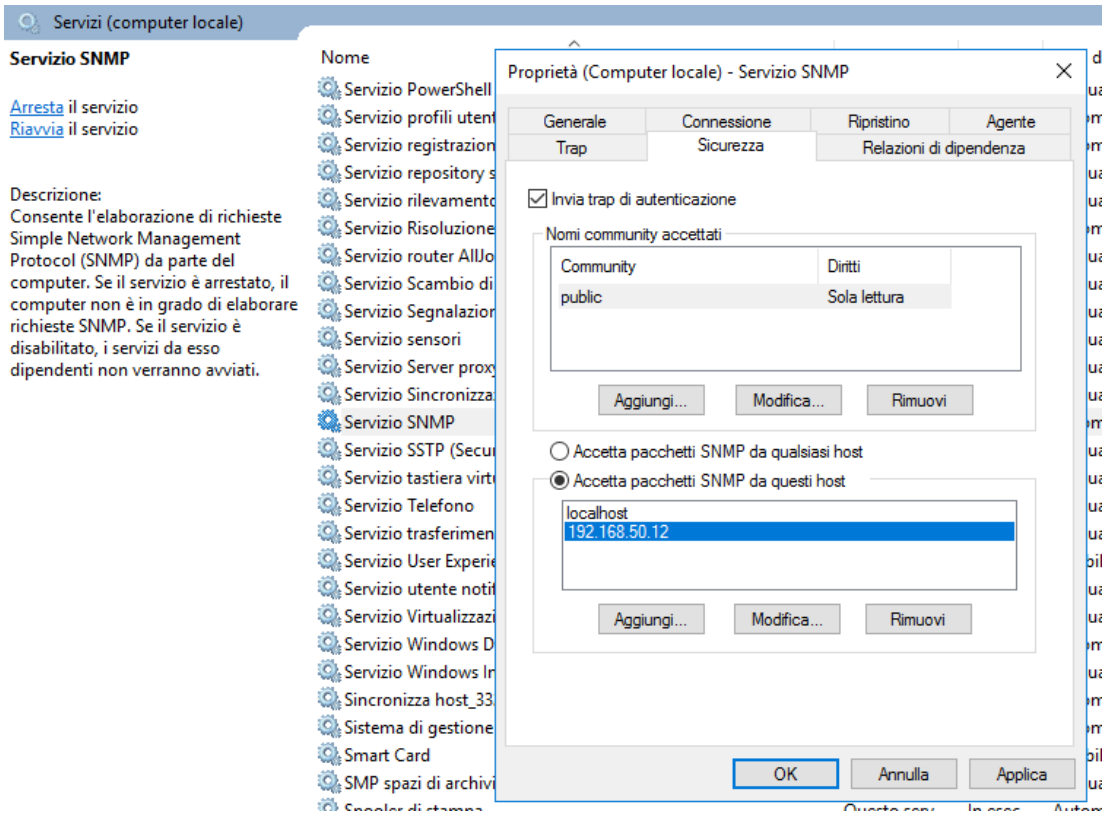

Figura 4.14: Configurazione Servizio SNMP in Windows Server

Fatto ciò possiamo recarci sulla piattaforma di Cacti e integrare i vari dispositivi. Andiamo quindi su **Console → Gestione → Dispositivi** e poi facciamo click sul + in alto a destra per aggiungere un dispositivo. Aggiungiamo per esempio il core switch. Come si può vedere dalla Figura 4.15, mettiamo i soliti dati come su Zabbix. L'unica cosa che cambia sono i template. Purtroppo, di default, Cacti non ha un template per gli switch Cisco (soltanto per i router ci sta uno). Quindi abbiamo optato per la voce `Generic SNMP Device`. Fatto ciò, clicciamo nella voce **Create Graphs for this Device** e selezioniamo le interfacce interessate che vogliamo monitorare. Nel caso del nostro Core Switch, siamo interessati alle 4 interfacce in trunk e l'interfaccia virtuale del management.

Figura 4.15: Configurazione del dispositivo Core Switch in Cacti

Data Query [SNMP - Interface Statistics]

All 19 Elementi

Index	Status	AdminStatus	Description	Name (IF-MIB)	Alias (IF-MIB)	Type	Speed	High Speed	Hardware Address	IP Address	
1	Up	Up	Ethernet0/0	Et0/0	Link to Firewall	6	10000000	10	AA BB CC 00 01 00		☑
2	Up	Up	Ethernet0/1	Et0/1	Link to SW-S	6	10000000	10	AA BB CC 00 01 10		☑
3	Up	Up	Ethernet0/2	Et0/2	Link to SW-L	6	10000000	10	AA BB CC 00 01 20		☑
4	Up	Up	Ethernet0/3	Et0/3	Link to SW-M	6	10000000	10	AA BB CC 00 01 30		☑
5	Up	Up	Ethernet1/0	Et1/0		6	10000000	10	AA BB CC 00 01 01		☐
6	Up	Up	Ethernet1/1	Et1/1		6	10000000	10	AA BB CC 00 01 11		☐
7	Up	Up	Ethernet1/2	Et1/2		6	10000000	10	AA BB CC 00 01 21		☐
8	Up	Up	Ethernet1/3	Et1/3		6	10000000	10	AA BB CC 00 01 31		☐
9	Up	Up	Ethernet2/0	Et2/0		6	10000000	10	AA BB CC 00 01 02		☐
10	Up	Up	Ethernet2/1	Et2/1		6	10000000	10	AA BB CC 00 01 12		☐
11	Up	Up	Ethernet2/2	Et2/2		6	10000000	10	AA BB CC 00 01 22		☐
12	Up	Up	Ethernet2/3	Et2/3		6	10000000	10	AA BB CC 00 01 32		☐
13	Up	Up	Ethernet3/0	Et3/0		6	10000000	10	AA BB CC 00 01 03		☐
14	Up	Up	Ethernet3/1	Et3/1		6	10000000	10	AA BB CC 00 01 13		☐
15	Up	Up	Ethernet3/2	Et3/2		6	10000000	10	AA BB CC 00 01 23		☐
16	Up	Up	Ethernet3/3	Et3/3		6	10000000	10	AA BB CC 00 01 33		☐
17	Up	Up	Null0	Nu0		1	4294967295	10000			☐
18	Down	Down	Vlan1	Vl1		53	1000000000	1000	AA BB CC 80 01 00		☐
19	Up	Up	Vlan70	Vl70		53	1000000000	1000	AA BB CC 80 01 00	192.168.70.2	☑

Figura 4.16: Creazione dei grafi per il Core Switch in Cacti

Aggiungiamo anche gli altri dispositivi e poi andiamo su **Console → Gestione → Alberi** e, cliccando sul simbolino di aggiunta in alto a destra, creiamo 3 alberi: Servers, Access Layer e Centro Stella. Li selezioniamo tutti e tre e scegliamo l'azione **Pubblica** per poterli usare.
Andiamo quindi sui dispositivi e inseriamo il firewall e il core switch sul Centro Stella: azione "Place on a Tree (Centro Stella). Gli access switches li inseriamo nell'Access Layer e il server Windows in Servers.
Ora se ci rechiamo in **Grafici** possiamo vedere la suddisione degli alberi e in ciascuno vedremo i dispositivi che abbiamo pubblicato.

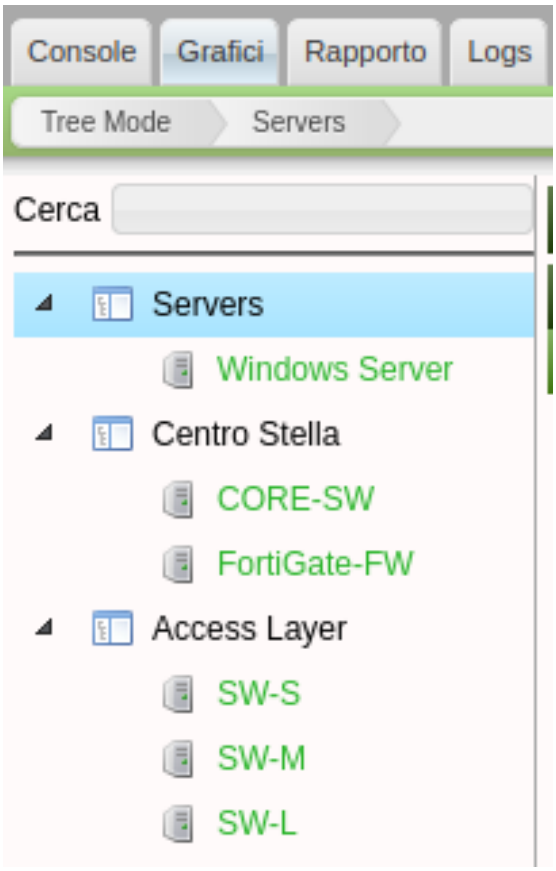

Figura 4.17: Suddivisione degli alberi nei grafi in Cacti

4.3.3 Autodiscovery

Nel nostro caso, possiamo aggiungere i dispositivi manualmente poiché sono pochi. Tuttavia, un aspetto molto importante del monitoraggio della rete è la possibilità di automatizzare le operazioni che sono ripetitive: una tra queste è la scoperta, configurazione e abilitazione al monitoraggio dei vari dispositivi nella rete.

Vediamo come Zabbix consente di effettuare questa operazione in modo nativo sia tramite agent che tramite SNMP. Come abbiamo visto nella sezione 4.3.1, nel nostro server Windows è stato installato l'agent di Zabbix. Quindi per effettuare l'autodiscovery rechiamoci nella piattaforma web di Zabbix, andiamo su **Data Collection → Discovery** e clicchiamo il bottone in alto a destra **Create Discovery Rule**. Diamo un nome alla regola e come range ip diamo quello della VLAN 7 (192.168.7.1-254). Come con-

trollo invece usiamo `Zabbix agent` la porta `10050` e la chiave `system.hostname`.

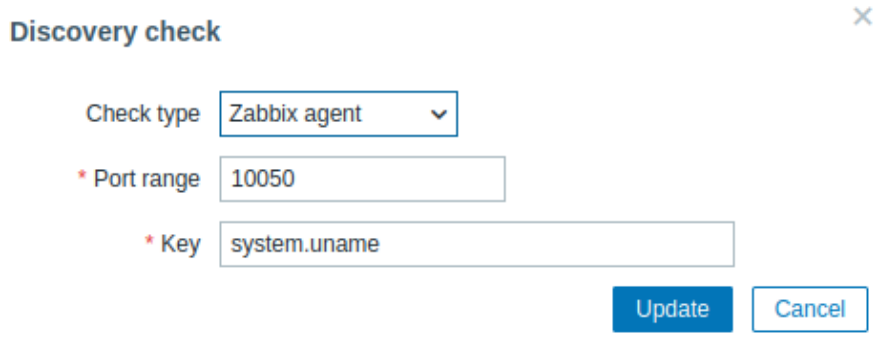

Figura 4.18: Controllo di discovery su Zabbix

Ora che abbiamo la regola della scoperta, creamo un'azione per registrare i dispositivi che vengono scoperti (nel nostro caso sarà solo il server Windows). Andiamo su **Alerts → Actions → Discovery Actions** e clicciamo sul bottone **Create Action** in alto a destra. Diamo un nome e come condizione mettiamo la regola di discovery appena creata e nella tab **Operations** configuriamo l'aggiunta del dispositivo, il gruppo degli host di appartenenza, il template da usare e infine lo abilitiamo al monitoraggio (vedi Figura 4.19).

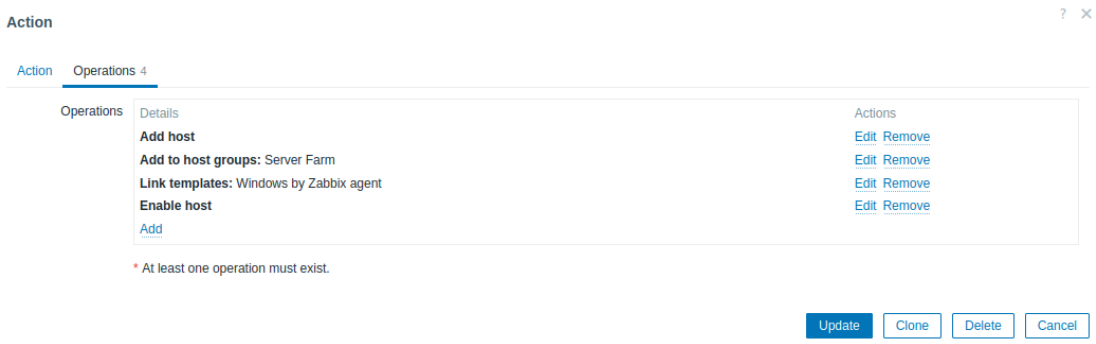

Figura 4.19: Operazioni delle azioni per Windows Server su Zabbix

Se ora ci rechiamo su **Monitoring → Discovery** vedremo il nostro Server Windows che è stato scoperto. Fatto ciò, scatta l'azione di registrazione e possiamo verificare che il server si trova tra gli host monitorati.
Proviamo a fare l'autodiscovery con SNMP invece per gli switch Cisco. Dato che SNMP funziona con gli OID per monitorare i vari dati da un dispositivo, dobbiamo sapere quale identificativo usare per i nostri dispositivi. Nel caso di Cisco possiamo usare l'OID `1.3.6.1.2.1.1.1.0` che ci restituisce la descrizione del sistema (parametro `sysDescr`). Eseguendo infatti il comando `snmpwalk` nel server Zabbix possiamo avere una risposta dal dispositivo in questione.

```
snmpwalk -v2c -c public 192.168.70.2 1.3.6.1.2.1.1.1.0
iso.3.6.1.2.1.1.1.0 = STRING: "Cisco IOS Software, Solaris Software (
    I86BI_LINUXL2-IPBASEK9-M), Experimental Version 15.1(20130726:213425)
     [dstivers-july26-2013-team-track 105] Copyright (c) 1986-2013 by
    Cisco Systems, Inc. Compiled Fri 26-Jul-13 16:12 by dstivers"
```

Codice 4.13: Richiamo della variabile `sysDescr` per MIB di switch Cisco

Quindi, riandiamo sulla piattaforma web di Zabbix e questa volta creiamo una nuova regola per i switch Cisco. Questa volta sul controllo scegliamo `SNMPv2 agent`, la porta `161`, nome della community `public` e OID `1.3.6.1.2.1.1.1.0`. Creiamo anche un'azione per registrare i dispositivi, impostanto la regola di scoperta creata come condizione e nelle operazioni.

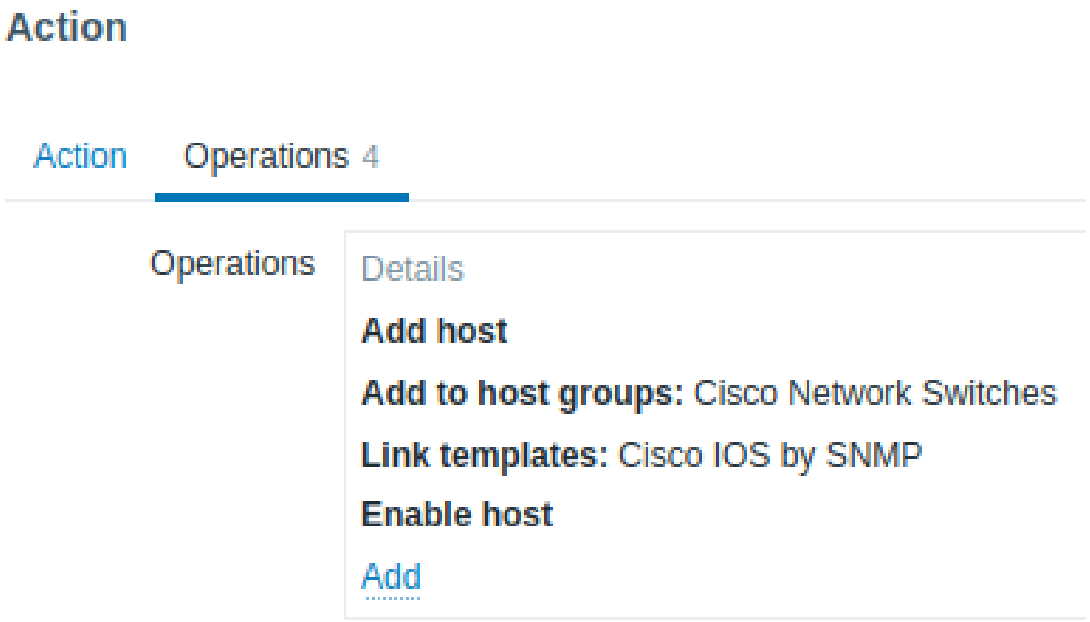

Figura 4.20: Operazioni delle azioni per switch Cisco su Zabbix

A differenza di Zabbix, Cacti non permette nativamente di effettuare l'autodiscovery ma ha bisogno di ulteriori configurazioni con plugin.

5. Conclusioni e Sviluppi Futuri

Nel Capitolo 4 abbiamo documentato come è analizzato e testato il funzionamento di due strumenti open-source per il monitoraggio della rete: Zabbix e Cacti. Entrambi sono risultati simili nella complessità di configuraizone ed installazione. Essendo strumenti open-source, è stato relativamente facile trovare guide e risoluzioni a problematiche di piccolo ordine. Zabbix ha ovviamente il vantaggio di avere una community più vasta, il che ha reso molto fluido questo primo aspetto.
Focalizzandoci sulle attività specifiche del caso d'uso, Zabbix è molto più intuitivo ed eccelle nella configurazione dell'autodiscovery, sia con agent che senza. Cacti invece non offre in maniera predefinita la possibilità di poter fare autodiscovery ma ha bisogno di usare plugin che devono essere installati e configurati. Tuttavia, un grande punto di forza di Cacti è che si basa su RRDTool, che permette di memorizzare i dati storici in un database a dimensione fissa. Questo lo rende perfetto per il graphing a lungo termine (mesi o anni) senza che il database cresca troppo. Inoltre, i grafici di Cacti sono altamente personalizzabili e facilmente esportabili o pianificabili in report: quindi perfetti per l'analisi di capacità o l'uso storico.
Zabbix crea grafici di dati SNMP, ma è più focalizzato su allarmi e automazione e meno sulle visualizzazioni di trend a lungo termine. Bisogna tenere a mente che, di default, Zabbix usa database SQL che può crescere nel tempo. Zabbix può essere configurato per supportare RDD, ma ciò implica tempo e risorse che deve essere dedicato per il *fine-tuning* dello strumento.
Nell'aspetto dell'analisi del monitoraggio, Cacti possiede alcuni template per poter usare, tuttavia, nativamente non ha un template per switch Cisco: infatti per il use case è stato usato un template generico per dispositivi SNMP che ha rilevato le interfacce (virtuali e fisiche) e permetteva di effettuare i grafici sul polling SNMP, l'uptime del dispositivo e la latenza del ping.
Zabbix invece possedeva già tutti i template per i dispositivi che sono stati usati nel caso d'uso e tanti altri. Inoltre, i template erano raggruppati per ambito, quindi era anche semplice ritrovarsi il template adatto.
Rimanendo sull'aspetto organizzativo, il raggruppamento degli host in "alberi" (o `tree`) in Cacti, rappresenta solo una struttura di visualizzazione. Servono infatti per facilitare la navigazione e trovare il grafico che vogliamo visualizzare. Su Zabbix invece gli "host groups" sono più funzionali rispetto agli alberi di Cacti poiché servono a:

- organizzare gli host logicamente, ad esempio per tipologia (servers, switches), per dipartimento (HR, IT), o per ambiente (production, testing);
- controllare i permessi di accesso, quindi decidere quali utenti hanno accesso a quale gruppo di host;
- applicare template in modo massivo (es. tutti switch Cisco);

- determinare le codizioni delle azioni (es. per autodiscovery);

Le limitazioni di questo studio riguardano principalmente l'ampiezza della simulazione e la tipologia di test effettuati. L'ambiente simulato con GNS3 e VMware, pur realistico, non è stato sottoposto a carichi elevati né a scenari estremi di traffico, limitando così la valutazione della scalabilità e delle performance effettive degli strumenti.

Inoltre, l'analisi è stata concentrata soprattutto sulle funzionalità base di monitoraggio SNMP, tuttavia ci sono altri aspetti interessanti che possono essere verificati e confrontati. In particolare, si suggeriscono i seguenti punti per approfondimenti e sviluppi futuri:

- **Implementare scenari avanzati di monitoraggio:** lo scopo è quello di arrivare a scenari reali (es. interruzioni parziali di servizio o guasti) per verificare il comportamento dello strumento;
- **Simulare ambienti complessi:** GNS3 può rimanere il candidato per la simulazione della rete, ma la VM deve essere eseguita da remoto e allocare molte più risorse per avere un numero maggiore di dispositivi per testare la scalabilità dello strumento in condizioni più vicine possibili alla realtà operativa aziendale;
- **Esplorare l'integrazione con altri sistemi:** in particolare con piattaforme SIEM e struemnti di gestione incidenti per creare ecosistemi valutare la loro robustezza;
- **Monitorare ambienti cloud e ibrid:** con lo scopo di verificare le capacità e i limiti degli strumenti nel gestire scenari più moderni, dinamici e distribuiti.

La scelta del giusto strumento di monitoraggio dipende fortemente dalle esigenze specifiche dell'ambiente in cui verrà utilizzato. Il lavoro ha evidenziato come Zabbix e Cacti siano entrambi validi, ciascuno con i propri punti di forza che vanno valutati con attenzione prima dell'implementazione. Molto più importante però, il semplice caso d'uso ha permesso già di vedere come gli strumenti di monitoraggio puntano a focalizzarsi in diverse funzionalità. Per questo motivo vanno quindi usati in combinazione per avere una resa migliore. Infine, bisogna tenere a mente che nella pratica operativa, è preferibile optare per soluzioni semplici e intuitive rispetto a quelle più complete ma complesse da gestire. Il monitoraggio della rete deve aggiungere valore all'organizzazione, facilitando il lavoro dell'amministratore di rete anziché appesantirlo con una gestione eccessivamente onerosa. Indipendentemente dallo strumento scelto, resta fondamentale la consapevolezza che un monitoraggio della rete IT ben gestita rappresenta un tassello essenziale nella sicurezza e nell'efficienza della gestione della rete aziendale.

A. Comandi di configurazione

Qui riportiamo le configurazioni complete degli apparati.

A.1 Configurazione del Fortigate Firewall

```
# CAMBIAMO L'HOSTNAME DEL FIREWALL
config system global
    set hostname FortiGate-FW
end

# CONFIGURA LE INTERFACCE E LE SOTTE INTERFACCE
config system interface
    edit "port1"
        set vdom "root"
    set mode static
        set ip 193.205.91.12 255.255.255.0
        set allowaccess ping https http
        set type physical
        set alias "WAN"
        set lldp-reception enable
        set role wan
        set snmp-index 1
    next

    edit "port2"
        set alias "LAN"
        set device-identification enable
        set lldp-transmission enable
        set role lan
    next
    edit "vlan10"
        set vdom "root"
        set dhcp-relay-service enable
        set ip 192.168.10.1 255.255.255.0
        set allowaccess ping
        set alias "office1"
        set device-identification enable
        set role lan
        set snmp-index 15
        set dhcp-relay-ip "192.168.7.254"
        set interface "port2"
        set vlanid 10
    next
    edit "vlan20"
        set vdom "root"
        set dhcp-relay-service enable
        set ip 192.168.20.1 255.255.255.0
```

```
            set allowaccess ping
            set alias "office2"
            set device-identification enable
            set role lan
            set snmp-index 16
            set dhcp-relay-ip "192.168.7.254"
            set interface "port2"
            set vlanid 20
        next
        edit "vlan30"
            set vdom "root"
            set dhcp-relay-service enable
            set ip 192.168.30.1 255.255.255.0
            set allowaccess ping
            set alias "office3"
            set device-identification enable
            set role lan
            set snmp-index 17
            set dhcp-relay-ip "192.168.7.254"
            set interface "port2"
            set vlanid 30
        next
        edit "vlan50"
            set vdom "root"
            set dhcp-relay-service enable
            set ip 192.168.50.1 255.255.255.0
            set allowaccess ping snmp
            set alias "monitoring"
            set device-identification enable
            set role lan
            set snmp-index 18
            set dhcp-relay-ip "192.168.7.254"
            set interface "port2"
            set vlanid 50
        next
        edit "vlan7"
            set vdom "root"
            set ip 192.168.7.1 255.255.255.0
            set allowaccess ping
            set alias "dmz"
            set device-identification enable
            set role lan
            set snmp-index 19
            set interface "port2"
            set vlanid 7
        next
        edit "vlan70"
            set vdom "root"
            set ip 192.168.70.1 255.255.255.0
            set allowaccess ping snmp
            set alias "management"
            set device-identification enable
            set role lan
            set snmp-index 20
            set interface "port2"
            set vlanid 70
        next
    end

    # CONFIGURA LA ZONA "Inter-Vlan"
    config system zone
```

```
    edit "Inter-Vlan"
        set intrazone allow
        set interface "vlan7" "vlan10" "vlan20" "vlan30" "vlan50" "
vlan70"
    next
end

# CONFIGURA LA ROTTA DI DEFAULT
config router static
edit 1
    set dst 0.0.0.0 0.0.0.0
    set gateway 193.205.91.2
    set device port1
next
end


CONFIGURA LA POLICY DI ACCESSO
config firewall policy
    edit 1
        set name "ALLOW-LAN"
        set srcintf "Inter-Vlan"
        set dstintf "port1"
        set action accept
        set srcaddr "all"
        set dstaddr "all"
        set schedule "always"
        set service "ALL"
        set nat enable
    next
end

# CONFIGURA L'SNMP
config system snmp sysinfo
    set status enable
    set description "SNMP Monitoring Agent"
    set contact-info "besjan.veizi@unicam.it"
    set location "Camerino"
end

# CONFIGURA LA COMUNITY "public" PER I DUE STRUMENTI DI MONITORAGGIO
config system snmp community
    edit 1
        set name "public"
        config hosts
            edit 1
                set ip 192.168.50.10 255.255.255.255
            next
            edit 2
                set ip 192.168.50.12 255.255.255.255
            next
        end
    next
end
```

A.2 Configurazione del Core Switch

```
configure terminal

# CONFIGURIAMO L'HOSTNAME DELLO SWITCH
hostname CORE-SW

# CONFIGURIAMO LE PORTE TRUNK
interface Ethernet0/0
description "Link to Firewall"
switchport trunk encapsulation dot1q
switchport mode trunk
no shutdown

interface Ethernet0/1
description "Link to SW-S"
switchport trunk encapsulation dot1q
switchport mode trunk
no shutdown

interface Ethernet0/2
description "Link to SW-L"
switchport trunk encapsulation dot1q
switchport mode trunk
no shutdown

interface Ethernet0/3
description "Link to SW-M"
switchport trunk encapsulation dot1q
switchport mode trunk
no shutdown
exit

# DISABILITIAMO IL ROUTING A LIVELLO 3
no ip routing

# CREIAMO LE ALTRE VLAN
vlan 10
name office1
vlan 20
name office2
vlan 30
name office3
vlan 50
name monitoring
vlan 7
name server-side
vlan 70
name management

# CREIAMO LA SVI DELLA VLAN 70 E ASSEGNAMO L'IP 192.168.70.2/24
interface vlan70
ip address 192.168.70.2 255.255.255.0
no shutdown
exit

# IMPOSTIAMO L'IP DEL GATEWAY 192.168.70.1 (IP FORTIGATE SUB-INT)
ip default-gateway 192.168.70.1

# CONFIGURA VTP
```

```
vtp domain unicam.it
vtp version 2
vtp password unicam
vtp mode server

# IMPOSTIAMO SNMP
snmp-server community public RO
snmp-server contact besjan.veizi@unicam.it
snmp-server location Camerino

end
copy running-config startup-config
```

A.3 Configurazione Switch SW-S

Questa è la configurazione dello switch che si trova tra il Core-Switch e la server farm.

```
configure terminal

# CONFIGURIAMO L'HOSTNAME DELLO SWITCH
hostname SW-S

# CONFIGURIAMO LA PORTA TRUNK VERSO CORE-SWITCH
interface Ethernet0/0
description "Link to CORE-SW"
switchport trunk encapsulation dot1q
switchport mode TRUNK

# CONFIGURIAMO LA PORTA ACCESS VERSO LA VLAN 7
interface Ethernet0/1
description "Link to DMZ"
switchport access vlan 7
switchport mode access
exit

# DISABILITIAMO IL ROUTING A LIVELLO 3
no ip routing

# IMPOSTIAMO IL VTP CLIENT
vtp domain unicam.it
vtp version 2
vtp password unicam
vtp mode client

# CREIAMO LA SVI DELLA VLAN 70 E ASSEGNAMO L'IP 192.168.70.3/24
interface vlan70
ip address 192.168.70.3 255.255.255.0
no shutdown
exit

# IMPOSTIAMO L'IP DEL GATEWAY 192.168.70.1 (IP FORTIGATE SUB-INT)
ip default-gateway 192.168.70.1

# IMPOSTIAMO SNMP
snmp-server community public RO
snmp-server contact besjan.veizi@unicam.it
snmp-server location Camerino
```

```
end
copy running-config startup-config
```

A.4 Configurazione Switch SW-L

Questa è la configurazione dello switch che si trova tra il Core-Switch e le VLAN dei client.

```
configure terminal

# CONFIGURIAMO L'HOSTNAME DELLO SWITCH
hostname SW-L

# CONFIGURIAMO LA PORTA TRUNK VERSO CORE-SWITCH
interface Ethernet0/0
description "Link to CORE-SW"
switchport trunk encapsulation dot1q
switchport mode TRUNK

# CONFIGURIAMO LE PORTE ACCESS VERSO LE VLAN 10, 20 e 30
interface Ethernet0/1
description "Link to Office 1"
switchport access vlan 10
switchport mode access

interface Ethernet0/2
description "Link to Office 2"
switchport access vlan 20
switchport mode access

interface Ethernet0/3
description "Link to Office 3"
switchport access vlan 30
switchport mode access
exit

# DISABILITIAMO IL ROUTING A LIVELLO 3
no ip routing

# IMPOSTIAMO IL VTP CLIENT
vtp domain unicam.it
vtp version 2
vtp password unicam
vtp mode client

# CREIAMO LA SVI DELLA VLAN 70 E ASSEGNAMO L'IP 192.168.70.4/24
interface vlan70
ip address 192.168.70.4 255.255.255.0
no shutdown
exit

# IMPOSTIAMO L'IP DEL GATEWAY 192.168.70.1 (IP FORTIGATE SUB-INT)
ip default-gateway 192.168.70.1

# IMPOSTIAMO SNMP
snmp-server community public RO
snmp-server contact besjan.veizi@unicam.it
snmp-server location Camerino
```

```
end
copy running-config startup-config
```

A.5 Configurazione Switch SW-M

Questa è la configurazione dello switch che si trova tra il Core-Switch e la VLAN 50.

```
configure terminal

# CONFIGURIAMO L'HOSTNAME DELLO SWITCH
hostname SW-M

# CONFIGURIAMO LA PORTA TRUNK VERSO CORE-SWITCH
interface Ethernet0/0
description "Link to CORE-SW"
switchport trunk encapsulation dot1q
switchport mode TRUNK

# CONFIGURIAMO LE PORTE ACCESS VERSO LA VLAN 50
interface Ethernet0/1
description "Link to Monitoring"
switchport access vlan 50
switchport mode access

interface Ethernet0/2
description "Link to Monitoring"
switchport access vlan 50
switchport mode access

# DISABILITIAMO IL ROUTING A LIVELLO 3
no ip routing

# IMPOSTIAMO IL VTP CLIENT
vtp domain unicam.it
vtp version 2
vtp password unicam
vtp mode client

# CREIAMO LA SVI DELLA VLAN 70 E ASSEGNAMO L'IP 192.168.70.5/24
interface vlan70
ip address 192.168.70.5 255.255.255.0
no shutdown
exit

# IMPOSTIAMO L'IP DEL GATEWAY 192.168.70.1 (IP FORTIGATE SUB-INT)
ip default-gateway 192.168.70.1

# IMPOSTIAMO SNMP
snmp-server community public RO
snmp-server contact besjan.veizi@unicam.it
snmp-server location Camerino

end
copy running-config startup-config
```

Bibliografia

[1] European Parliament and Council of the European Union. *Regolamento Generale sulla Protezione dei Dati (GDPR) - Articolo 32*. Accesso il: 15 Marzo 2025. 2016. URL: https://www.privacy-regulation.eu/it/32.htm.

[2] International Organization for Standardization (ISO). *ISO/IEC 27001:2022 - Information security, cybersecurity and privacy protection — Information security management systems — Requirements*. Accesso il: 15 Marzo 2025. 2022. URL: https://www.iso.org/standard/88435.html.

[3] Cybersecurity360. *NIS 2 e i requisiti e controlli della ISO/IEC 27001: analisi puntuale e confronto tra le norme*. Accesso il: 15 Marzo 2025. 2024. URL: https://www.cybersecurity360.it/legal/privacy-dati-personali/nis-2-e-i-requisiti-e-controlli-della-iso-iec-27001-analisi-puntuale-e-confronto-tra-le-norme/.

[4] J. Case, M. Fedor, J. Davin e M. Schoffstall. *Simple Network Management Protocol - SNMP*. Rapp. tecn. RFC 1157. IETF, 1990. URL: https://www.rfc-editor.org/rfc/rfc1157 (visitato il giorno 15/03/2025).

[5] S. Waldbusser. *Remote Network Monitoring Management Information Base Version 2 using SMIv2*. Rapp. tecn. RFC 2021. IETF, 1997. URL: https://www.rfc-editor.org/rfc/rfc2021 (visitato il giorno 15/03/2025).

[6] Robert Grimmick. *Network Flow Monitoring Explained: NetFlow vs sFlow vs IPFIX*. 2023. URL: https://www.varonis.com/blog/flow-monitoring (visitato il giorno 15/03/2025).

[7] B. Claise. *Cisco Systems NetFlow Services Export Version 9*. Rapp. tecn. RFC 3954. IETF, 2004. URL: https://www.rfc-editor.org/rfc/rfc3954 (visitato il giorno 15/03/2025).

[8] P. Phaal, S. Panchen e N. McKee. *InMon Corporation's sFlow: A Method for Monitoring Traffic in Switched and Routed Networks*. Rapp. tecn. RFC 3176. IETF, 2001. URL: https://www.rfc-editor.org/rfc/rfc3176 (visitato il giorno 15/03/2025).

[9] Ed. B. Claise, Inc Cisco Systems, Ed. B. Trammell e P. Aitken. *Specification of the IP Flow Information Export (IPFIX) Protocol for the Exchange of Flow Information*. Rapp. tecn. RFC 7011. IETF, 2013. URL: https://www.rfc-editor.org/rfc/rfc7011 (visitato il giorno 15/03/2025).

[10] Proofpoint. *What is Telemetry? Definition and Importance in Cybersecurity*. 2025. URL: https://www.proofpoint.com/us/threat-reference/telemetry (visitato il giorno 15/03/2025).

[11] Network Computing. *Streaming Telemetry Has Arrived: Why You Should Care*. 2025. URL: https://www.networkcomputing.com/network-infrastructure/streaming-telemetry-has-arrived-why-you-should-care- (visitato il giorno 15/03/2025).

[12] J. Postel. *Internet Control Message Protocol - ICMP*. Rapp. tecn. RFC 792. IETF, 1981. URL: https://www.rfc-editor.org/rfc/rfc792 (visitato il giorno 15/03/2025).

[13] IETF - Internet Engineering Task Force. *SYSLOG Working Group Charter*. 2025. URL: https://datatracker.ietf.org/wg/syslog/charter/ (visitato il giorno 26/03/2025).

[14] UMBOSS. *Network Monitoring Protocols: Essential Tools for Network Management*. 2025. URL: https://umboss.com/blog/network-monitoring-protocols/ (visitato il giorno 15/03/2025).

[15] Cisco Systems. *NetFlow Services and Applications: A Technology Overview*. White paper Cisco. 2025. URL: https://www.cisco.com/en/US/technologies/tk652/tk701/technologies_white_paper0900aecd804cd46d.html (visitato il giorno 26/03/2025).

[16] Blatherwick, A. *Ethernet Frame Study: A Presentation to IEEE 802.3 Working Group*. Rapp. tecn. IEEE 802.3 Working Group, 2009. URL: https://www.ieee802.org/3/frame_study/0409/blatherwick_1_0409.pdf (visitato il giorno 15/03/2025).

[17] Microsoft Docs. *WMI - Windows Management Instrumentation Start Page*. Microsoft Developer Network. 2025. URL: https://learn.microsoft.com/en-us/windows/win32/wmisdk/wmi-start-page (visitato il giorno 26/03/2025).

[18] Lansweeper. *What is WMI? Benefits, Usage, and Security*. 2025. URL: https://www.lansweeper.com/blog/itam/what-is-wmi-benefits-usage-and-security/ (visitato il giorno 15/03/2025).

[19] ManageEngine. *Network Monitoring Essentials Whitepaper*. 2025. URL: https://www.manageengine.com/network-monitoring/whitepaper-network-monitoring-essentials.html (visitato il giorno 15/03/2025).

[20] IR. *Guide to Network Monitoring Tools*. 2025. URL: https://www.ir.com/guides/network-monitoring-tools (visitato il giorno 15/03/2025).

[21] SolarWinds. *Network Monitoring: Definition and Importance*. 2025. URL: https://www.solarwinds.com/resources/it-glossary/network-monitoring (visitato il giorno 15/03/2025).

[22] Zabbix. *Zabbix Network Monitoring Overview*. 2025. URL: https://www.zabbix.com/network_monitoring (visitato il giorno 15/03/2025).

[23] Zabbix LLC. *Zabbix - Enterprise-Class Monitoring Platform*. 2025. URL: https://www.zabbix.com/ (visitato il giorno 26/03/2025).

[24] Verdict. *Zabbix Partner Ecosystem Profile*. 2025. URL: https://www.verdict.co.uk/zabbix-partner-ecosystem-profile/?cf-view (visitato il giorno 15/03/2025).

[25] Zabbix. *Zabbix Partner Network*. 2025. URL: https://www.zabbix.com/partners#map_of_partners (visitato il giorno 15/03/2025).

[26] Paessler AG. *PRTG Network Monitor – All-in-One Monitoring Solution*. 2025. URL: https://www.paessler.com/prtg (visitato il giorno 26/03/2025).

[27] Paessler AG. *PRTG Manual: Basic Procedures*. 2025. URL: https://www.paessler.com/it/manuals/prtg/basic_procedures (visitato il giorno 15/03/2025).

[28] Nagios. *Nagios: The Industry Standard in IT Infrastructure Monitoring*. 2025. URL: https://www.nagios.org/ (visitato il giorno 15/03/2025).

[29] Nagios. *Nagios Plugins Downloads*. 2025. URL: https://www.nagios.org/downloads/nagios-plugins/ (visitato il giorno 15/03/2025).

[30] Cacti Team. *Cacti - The Complete Network Graphing Solution*. 2025. URL: https://www.cacti.net/ (visitato il giorno 26/03/2025).

[31] DBSnoop. *What is Cacti? Monitoring and Visualization Explained*. 2025. URL: https://dbsnoop.com/what-is-cacti-monitoring-visualization/ (visitato il giorno 15/03/2025).

[32] SolarWinds. *SolarWinds NPM: Your Complete Network Monitoring Solution (Video)*. 2025. URL: https://www.solarwinds.com/resources/video/solarwinds-npm-your-complete-network-monitoring-solution (visitato il giorno 15/03/2025).

[33] SolarWinds. *SolarWinds Network Performance Monitor Datasheet*. Rapp. tecn. SolarWinds, 2025. URL: https://www.solarwinds.com/assets/solarwinds/swdcv2/licensed-products/network-performance-monitor/resources/datasheets/npm-datasheet.pdf (visitato il giorno 15/03/2025).

[34] LiveAction. *What is Network Performance Baselining?* 2025. URL: https://www.liveaction.com/resources/blog-post/what-is-network-performance-baselining/ (visitato il giorno 15/03/2025).

[35] DigitalOcean. *What is Cloud Monitoring? Definition, Benefits, and Tools*. 2025. URL: https://www.digitalocean.com/resources/articles/cloud-monitoring (visitato il giorno 15/03/2025).

[36] Ascendant Technologies. *Software Defined Networking (SDN): How It Works and Why It Matters*. 2025. URL: https://ascendantusa.com/2025/01/08/software-defined-networking-sdn/ (visitato il giorno 15/03/2025).

[37] DT Asia Group. *The Future of Network Monitoring: How AI and Machine Learning Are Changing the Game*. 2025. URL: https://dtasiagroup.com/the-future-of-network-monitoring-how-ai-and-machine-learning-are-changing-the-game/ (visitato il giorno 15/03/2025).

[38] GNS3. *GNS3 - Graphical Network Simulator*. 2025. URL: https://www.gns3.com/ (visitato il giorno 15/03/2025).

Ringraziamenti

Giunto al termine di questa tesi, desidero esprimere i miei più sinceri ringraziamenti a tutte le persone che mi hanno sostenuto e guidato nella sua realizzazione.
In primo luogo, ringrazio calorosamente il mio relatore, il Dott. Fausto Marcantoni, per la sua guida, i suoi consigli significativi e la sua costante disponibilità.
Sono anche grato ai membri della commissione per il tempo dedicato alla valutazione di questo lavoro.
Estendo i ringraziamenti anche a tutti i professori del dipartimento di Informatica dell'Università di Camerino per i loro insegnamenti e la loro dedizione.
Ci tengo a ringraziare l'Area Infrastrutture e Servizi Informatici, in particolare il direttore Dott. Francesco De Angelis, il responsabile del settore reti e mio correlatore, il Dott. Marco Maccari e il collega Emanuele Fattinanzi per il supporto e i consigli che sono stati molto d'aiuto per concludere questo lavoro.

Desidero ringraziare la mia famiglia per avermi supportato ed incoraggiato da sempre. A papà Habib e a mamma Selvie, apprezzo il sostegno che mi avete dato da sempre e la creanza che ha fatto di me l'uomo che sono oggi. Sono grato ai miei fratelli Hasan e Jeims: avete definito la mia adolescenza e siete fonte di ricordi bellissimi.
Desidero inoltre ringraziare i miei amici più cari, Vlad, Riccardo e Simone per avermi accompagnato e incoraggiato, condividendo esperienze e stimoli costanti.
Infine, un ringraziamento di cuore va a te Angela, il cui sostegno, comprensione e affetto sono stati fondamentali dal primo giorno che ti ho incontrata.