



Università degli Studi di Camerino

Scuola di Scienze e Tecnologie

Corso di Laurea in Informatica Classe L-31

Monitoraggio di Reti “Zabbix”

Studenti	Matricola	Relatore
Pallotta Fabio		Prof. Marcantoni Fausto

Anno Accademico 2018 – 2019

INDICE

INDICE	2
1 INTRODUZIONE	4
2 PROTOCOLLO SNMP	6
2.1 STORIA E FUNZIONAMENTO	6
2.2 SNMP VERSIONI	9
2.2.1 SNMPv1.....	9
2.2.2 SNMPv2.....	9
2.2.3 SNMPv3.....	10
3 APPLICATIVI SISTEMA DI MONITORAGGIO	11
3.1 INTRODUZIONE	11
3.2 ManageEngine OpManager	13
3.3 Solaris Winds	13
3.4 Nagios	14
3.5 Zabbix	14
4 ZABBIX: SISTEMA DI MONITORAGGIO	15
4.1 ZABBIX	15
4.2 FUNZIONALITA'	16
4.2.1 RACCOLTA DATI.....	16
4.2.2 ANALISI DEI PROBLEMI.....	17
4.2.3 NOTTIFICHE.....	17
4.2.4 VISUALIZZAZIONE.....	19
4.2.5 AUTO-DISCOVERY.....	19
4.2.6 IT INVENTORY.....	21
5 INSTALLAZIONE	22
5.1 PREREQUISITI	22
5.1.1 INSTALLAZIONE SSH.....	23
5.1.2 INSTALLAZIONE APACHE.....	23
5.1.3 DISABILITAZIONE FIREWALL.....	23
5.1.4 INSTALLAZIONE MySQL.....	23
5.1.5 INSTALLAZIONE PHP.....	24
5.2 INSTALLAZIONE ZABBIX 4.2	24
5.2.1 CREAZIONE DATABASE ZABBIX.....	24
5.2.2 CREAZIONE SCHEMA ZABBIX.....	24
5.2.3 SETTAGGIO CONFIGURAZIONE ZABBIX.....	24
5.2.4 APACHE CONFIGURAZIONE.....	25
5.2.5 MODIFICA SELINUX.....	25
5.2.6 AVVIO ZABBIX.....	26
5.3 WEBMIN	29
5.3.1 INSTALLAZIONE.....	29
5.4 POSTFIX	30
5.4.1 INSTALLAZIONE.....	30

5.4.2 CONFIGURAZIONE..... 31

6 ZABBIX AVVIO34

6.1 ZABBIX MACCHINE WINDOWS35

6.1.1 CONFIGURAZIONE AGENT SU WINDOWS 35

6.1.2 INSERIMENTO MACCHINA WINDOWS SU ZABBIX 37

6.2 INSERIMENTO ROUTER MIKROTIK SU ZABBIX.....38

7 CONCLUSIONI.....40

8 BIBLIOGRAFIA41

RINGRAZIAMENTI43

1 INTRODUZIONE

Le reti negli ultimi decenni sono diventate un elemento di fondamentale e di vitale importanza per un qualsiasi Ente o Azienda; basti pensare che si è passati dal collegamento di qualche host all'interno di uno stabile al collegamento di moltissimi host anche su aree geografiche distanti migliaia di chilometri fra loro.

Questo ha fatto sì che realizzare una semplice infrastruttura di rete non è più sufficiente, da essa ci si aspetta Affidabilità, Sicurezza e Performance, al fine di offrire pieno supporto ad applicazioni innovative quali Multimedia, e-Learning, Telemedicina, Fonia ecc.

Ad esempio, un sito internet momentaneamente non raggiungibile può causare dei disservizi e quindi provocare danni, sia a livello di immagine aziendale che a livello economico.

L'amministratore di rete ha il compito di mantenere in funzione la rete, gestire e prevenire i problemi ed infine disporre degli strumenti adatti per risolvere criticità come:

- Funzionamento;
- Configurazione;
- Degradi prestazionali;
- Danneggiamenti o rotture

Da qui nasce il bisogno di uno strumento di gestione in grado di operare in ambiente multivendor e quindi la necessità di fissare tecniche per rappresentare e scambiare dati relativi al Network Management, questi strumenti o sistemi vengono chiamati più comunemente "SISTEMI DI MONITORAGGIO".

Inoltre un sistema di monitoraggio oltre a controllare i servizi erogati deve anche monitorare le risorse interne della rete, perché un disservizio che colpisce una pagina internet potrebbe essere causato anche da un crash della macchina che ospita il web-server.

In definitiva il compito di un buon sistema di monitoraggio è di dare una visione globale della rete in tempo reale, controllando lo stato dei servizi e delle risorse interne ed in caso di anomalie inviare delle notifiche di allarme agli amministratori della rete.

Nel 1989 nasce il protocollo SNMP che viene pensato come punto di partenza su cui sviluppare dei sistemi che siano in grado di risolvere e prevedere tutti i problemi che nascono dalla gestione di una rete. La versatilità di questo protocollo gli ha permesso di trovare da subito un riscontro positivo dal mondo degli sviluppatori e dalle aziende del settore, infatti dopo la prima versione ne sono state implementate altre due. Oggi lo standard SNMP è supportato da una grandissima quantità di dispositivi alcuni dei quali esulano dalla categoria dei componenti di rete come ad esempio alcune stampanti.

L'obiettivo di questa tesi è l'utilizzo di un software open source che dia la possibilità all'amministratore di rete di controllare e visionare lo stato dei vari nodi all'interno della rete in modo che si possano risolvere in modo veloce ed efficace eventuali anomalie.

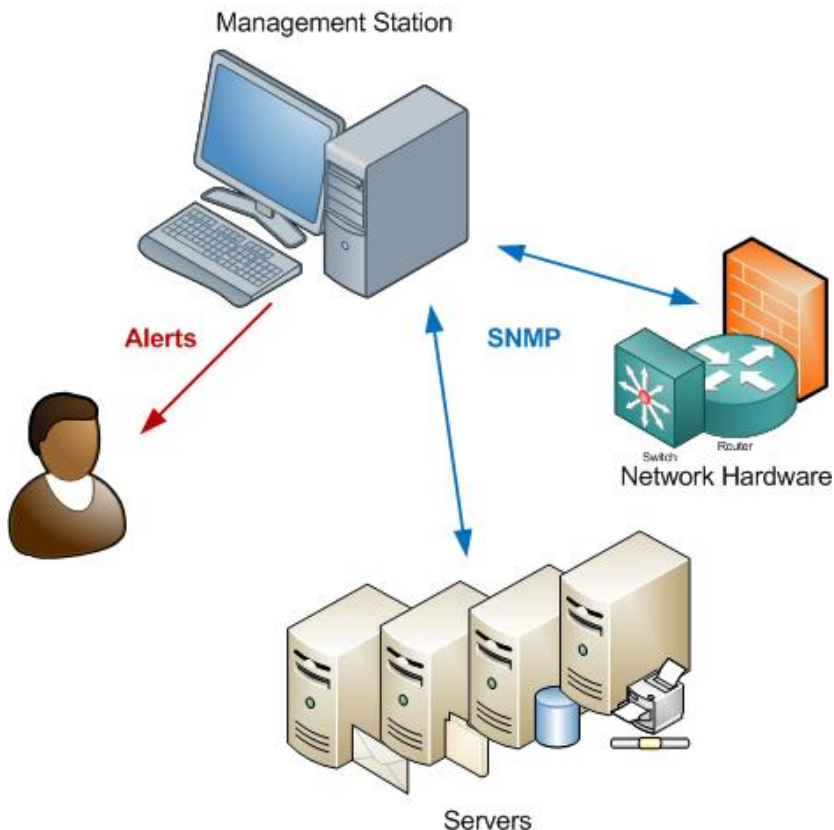
2 PROTOCOLLO SNMP

2.1 STORIA E FUNZIONAMENTO

Il protocollo SNMP (Simple Network Management Protocol) ufficialmente nasce nel 1989 e viene definito dalla Internet Engineering Task Force (IETF). Da quel momento SNMP diventa uno standard industriale per controllare gli apparati di rete tramite un'unica applicazione di controllo. SNMP rappresenta una serie di funzioni e protocolli per la gestione di rete che comunicano tra di loro attraverso l'Internet Protocol (IP), infatti la prima implementazione avviene su protocollo TCP/IP, ma in seguito verrà sviluppato anche su reti IPX e AppleTalk. Questo protocollo permette agli amministratori di rete di individuare ed in seguito isolare i componenti difettosi che si possono trovare su una rete, configurare i vari componenti in remoto e monitorare lo stato e le performance della rete. SNMP opera allo strato applicativo del livello OSI (livello 7 - APPLICATION) e utilizza un'architettura di comunicazione di tipo client-server con il protocollo UDP (User Datagram Protocol) sfruttando di default le porte 161 e 162.

I tre componenti logici fondamentali del framework SNMP per il suo funzionamento sono:

- sistema gestito (managed object);
- agente di gestione (management agent o master agent) e vari subagente (su sistema gestito);
- sistema di gestione (manager) da remoto;



Ogni sistema gestito (per esempio un semplice nodo, un router, una stampante o qualsiasi altro dispositivo che fornisca un'interfaccia di gestione SNMP) ospita un agente di gestione (master agent) e solitamente un certo numero di subagent. Il master agent ha almeno il ruolo di intermediario fra il manager (che è l'applicazione remota che prende le decisioni di gestione, per esempio sotto il controllo diretto dell'operatore umano) e i subagent (che sono gli esecutori di tali decisioni). Ciascun subagent è incaricato di attuare le decisioni di gestione da parte del manager nel contesto di un particolare sottosistema o relativamente a un particolare aspetto del sistema gestito. In sistemi che forniscono meccanismi di gestione particolarmente semplici, master agent e subagent possono confluire in un unico componente software capace sia di dialogare con il manager che di attuarne le decisioni; in questo caso si parlerà semplicemente di agent.

SNMP utilizza quindi una chiara separazione fra il protocollo di gestione e la struttura dell'oggetto gestito. Nell'architettura SNMP, per ogni sottosistema è definita una base di dati detta MIB (Management Information Base), gestita dal corrispondente subagent, la quale rappresenta lo stato del sottosistema gestito, o meglio, una proiezione di tale stato limitata agli aspetti di cui si vuole consentire la gestione. Si tratta di una base dati che si potrebbe definire, mutuando un termine dalla riflessione, "causalmente connessa": in altre parole, ogni modifica alla MIB causa un corrispondente mutamento nello stato del sottosistema rappresentato, e viceversa. Garantire questa proprietà della MIB è la funzione principale del subagent che la gestisce.

L'accesso alla MIB (in lettura e scrittura) rappresenta l'interfaccia fornita al manager per gestire il sistema. Ogni MIB, pur variando nei contenuti specifici, ha la medesima struttura generale e i medesimi meccanismi generali di accesso da parte del manager (lettura e scrittura dei dati). Grazie alla connessione causale della MIB, è quindi possibile al manager agire sullo stato del sottosistema in un modo che è largamente indipendente dalle procedure concrete che devono poi essere messe in atto (dal subagent) per estrarre le informazioni di stato rappresentate nella MIB, o attuare le modifiche di stato a seguito di cambiamenti dei contenuti della MIB. Così, per esempio, si potrebbe avere un dato di MIB che rappresenta l'indirizzo IP del sistema gestito; per modificare tale indirizzo, al manager è sufficiente accedere alla MIB sovrascrivendo il dato corrispondente, prescindendo dei dettagli di come una tale modifica venga poi concretamente "attuata" sul sistema gestito attraverso l'agent o il subagent.

<i>Categoria della MIB</i>	<i>Specifica informazione su....</i>
system	sistema operativo del dispositivo (router, server, ecc)
interfaccia	singola interfaccia di rete
al	traduzione degli indirizzi (es. traduzione di ARP)
ip	software IP
icmp	software ICMP

<i>Categoria della MIB</i>	<i>Specifica informazione su....</i>
tcp	software TCP
udp	software UDP
ospf	software OSPF
bgp	software BGP
rip-2	software RIP
dns	software DNS

Più in dettaglio, il manager dialoga con i sistemi gestiti essenzialmente in due modi: invia richieste SNMP e riceve notifiche SNMP.

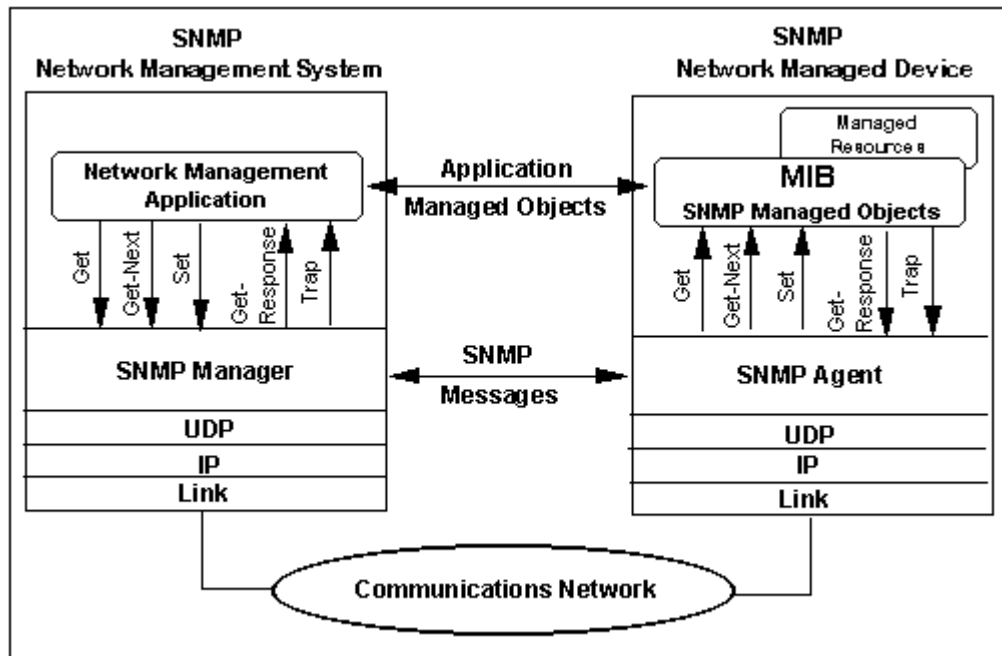
Alcuni esempi di richieste sono:

- GET, usata per leggere uno o più dati di MIB;
- GETNEXT, usata per leggere iterativamente una sequenza di dati di MIB;
- GETBULK, usata per leggere con una sola richiesta grandi porzioni di MIB;
- SET, usata per scrivere (modificare) uno o più dati di MIB.

Le notifiche sono messaggi asincroni inviati dall'agent per segnalare eventi occorsi nel sistema gestito (p.es. allarmi in caso di guasti). Le notifiche SNMP senza acknowledgement vengono comunemente chiamate trap, anche se la terminologia esatta varia a seconda della versione di SNMP in questione. Le notifiche SNMP con acknowledgement vengono invece chiamate inform.

Per motivi di sicurezza, i sistemi facenti parte di una rete SNMP vengono raggruppati in una cosiddetta comunità. La comunità è identificata da una stringa di 32 byte e ciascun sistema può appartenere a più di una di queste comunità. L'agent SNMP accetta richieste solo da un manager della stessa comunità che si identifica e autentica con la suddetta stringa ottenendo l'autorizzazione o meno a procedere nel controllo remoto di gestione. L'autorizzazione dei membri di una comunità ad operare su un oggetto può essere di tre tipi:

- read: il manager può interrogare l'agent solo per conoscere lo stato del sistema (solo GET o modalità di sola lettura);
- write: dove il manager può anche variarne l'impostazione (GET e SET, o modalità lettura/scrittura);
- trap: l'agent può inviare trap al manager.



La figura mostra il modello di comunicazione usato tra manager e agent.

2.2 SNMP VERSIONI

2.2.1 SNMPv1

L'SNMPv1, la prima versione del protocollo di gestione di rete, si basa sul modello manager-agent e rappresenta la base per la comunicazione tra la manager station e i singoli agent. Il Simple Network Management Protocol è un protocollo semplice che agisce sul livello di applicazione e su UDP (User Datagram Protocol) e Internet Protocol (IP), ma può poggiarsi anche su protocolli di rete simili come AppleTalks DDP (Datagram Delivery Protocol) o Internet Packet Exchange (IPX). L'unico meccanismo di sicurezza integrato è lo scambio di una cosiddetta "stringa di comunità" che viene inviata tramite la relativa request.

2.2.2 SNMPv2

Un grosso limite della prima versione del protocollo SNMP è che la stringa di comunità veniva trasmessa solo in testo semplice. Ciò non era abbastanza in termini di sicurezza, così gli sviluppatori si misero al lavoro per ottenere una nuova variante dal nome Secure SNMP, in cui le stringhe venivano trasmesse in forma cifrata. Tale versione, tuttavia, non è mai stata pubblicata in quanto venne rimpiazzata direttamente dall'SNMPv2. Vennero effettuati ulteriori miglioramenti alla versione originale del protocollo, tra cui un'ottimizzazione della gestione degli errori, la possibilità di una comunicazione manager-manager e comandi

SET più funzionali. Tuttavia il grosso vantaggio in confronto all'SNMPv1 è rappresentato dall'implementazione di nuove tipologie di messaggi GETBULK (per la richiesta di più dati in un'unica request) e INFORM (per le conferme di ricezione alle risposte degli agent).

2.2.3 SNMPv3

Dopo i primi piccoli miglioramenti della seconda versione del protocollo, lo IETF si è focalizzato sull'aspetto della sicurezza e ha sostituito le stringhe di comunità con username e password. La terza versione del protocollo, a differenza delle precedenti, contiene delle funzioni che permettono di crittografare la trasmissione di pacchetti SNMP. SNMPv3 offre tre diverse modalità di autenticazione e cifratura:

	Autenticazione	Cifratura	Username	Password
noAuthNoPriv	No	No	Si	No
authNoPriv	Si	No	Si	Si
authPriv	Si	Si	Si	Si

3 APPLICATIVI SISTEMA DI MONITORAGGIO

3.1 INTRODUZIONE

Esistono moltissimi software o applicativi che, permettono, il monitoraggio e la scansioni della rete o di apparati ad essa collegati come router, switch, server, sonde, ecc.

Essi possono essere più o meno complessi, si parte da chi utilizza solo il protocollo ICMP a quelli più complessi che permettono di utilizzare protocolli più evoluti come SNMP e che, quindi permettono di ricevere molte più informazioni che possono essere utilizzate per la visualizzate sotto forma di grafici o più semplicemente di valori numeri; altri software danno anche la possibilità di ricevere notifiche tramite SMS o Email di eventuali guasti o anomalie.

Così come posso essere differenti le piattaforme su cui lavorano Linux o Windows o il loro utilizzo da quelli a pagamento a quelli open-source.

Inoltrarsi in questa giungla non è stato facile e quindi si è decisi di fare alcune ricerche su internet cercando però software di monitoraggio più evoluti; da quindi si è scovato un elenco per il 2019 dei software di monitoraggio più utilizzati come riportato sotto:

- ManageEngine OpManager
- NetCrunch
- PRTG Network Monitor
- SolarWinds Network Performance Monitor
- Nagios
- Zabbix
- LogicMonitor
- Icinga
- Spiceworks
- Datadog
- WhatsUp Gold

Il passo successive è stato quello di creare una tabella dove nelle righe venivano riportati i vari software sopra descritti e nelle colonne venivano inseriti dei campi per noi basilari nella scelta come:

- Sistema Operativo
- Prezzo
- Informazioni come la soddisfazione degli utilizzatori su prodotto, la facilità di utilizzo, le caratteristiche generali ed in fine il rapporto qualità Prezzo.

TABELLA RIASSUNTIVA

<i>Software</i>	<i>S.O.</i>	<i>Prezzo Base in \$</i>	<i>Soddisfazione Da 1 a 5</i>	<i>Facilità Da 1 a 5</i>	<i>Caratteristiche Da 1 a 5</i>	<i>Rapp. Prezzo Da 1 a 5</i>
ManageEngine OpManager	Windows Linux	245,00	4,6	4,2	4,4	4,5
NetCrunch	Windows	1.200,00	4,7	4,5	4,6	4,7
PRTG	Windows	1.600,00	4,6	4,4	4,4	4,4
Solari Winds	Windows Linux	2.995,00	4,6	4,6	4,4	4,5
Nagios	Windows Linux Mac Unix	1.995,00	4,7	4,4	4,4	4,3
Zabbix	Windows Linux	Free	4,5	3,8	4,3	4,6
LogicMonitor	Windows	Quote	4,7	4,5	4,5	4,5
Icinga	Linux	Quote	4,6	3,8	4	5
Spiceworks	Windows	Free	4,4	4,3	4,2	4,6
Datadog	Cloud	Quote	4,6	4,2	4,4	4,2
WhatsUp	Windows	2.656,00	4,2	3,8	4	4
			4,5	4,2	4,3	4,5

Successivamente si è andati a filtrare solo quelli che sono multi piattaforma e quindi si sono studiate le caratteristiche dei prodotti selezionati sotto brevemente descritti.

3.2 ManageEngine OpManager

ManageEngine OpManager è una soluzione di gestione della rete integrata che facilita una gestione della rete efficiente e senza problemi.

Consente agli amministratori di rete / IT di eseguire contemporaneamente più operazioni come il monitoraggio delle prestazioni di rete, l'analisi della larghezza di banda, la gestione della configurazione, la gestione del firewall, il monitoraggio dell'archiviazione, la gestione degli indirizzi IP (IPAM) e la gestione delle porte switch (SPM).

L'intera infrastruttura di rete di un'organizzazione può essere visualizzata da una dashboard altamente personalizzabile su OpManager.

L'interfaccia grafica intuitiva offre una panoramica pronta all'uso che consente all'utente di monitorare metriche importanti senza la necessità di navigare attraverso più opzioni di menu, fornendo quindi visibilità approfondita e controllo completo per eliminare tutti i problemi relativi alla rete facilmente.

3.3 Solari Winds

Fornisce il monitor delle prestazioni di rete in grado di ridurre le interruzioni di rete e migliorare le prestazioni. È una soluzione scalabile con una scalabilità più intelligente per ambienti di grandi dimensioni.

Caratteristiche:

- Ha funzionalità per il monitoraggio e la gestione della rete wireless.
- Ti consentirà di visualizzare le metriche delle prestazioni per punti di accesso autonomi.
- Dispone di funzionalità per avvisi avanzati e generazione automatica di mappe intelligenti.
- Per i firewall di rete critici, gli switch e i bilanciatori del carico, SolarWinds fornirà una rappresentazione visiva delle prestazioni.

SolarWinds Network Performance Monitor ha funzionalità per il monitoraggio della rete multi-vendor e il monitoraggio SDN con il supporto Cisco ACI. Fornisce una scalabilità più intelligente per reti robuste.

3.4 Nagios

Offre soluzioni come software di monitoraggio della rete, monitoraggio del traffico di rete e analizzatore di rete. Nagios Network Analyzer include funzionalità come un dashboard completo, visualizzazioni avanzate, monitoraggio personalizzato delle applicazioni, avvisi automatici, viste specializzate e gestione avanzata degli utenti.

Caratteristiche:

- Può monitorare la disponibilità dei nodi e il loro tempo di attività.
- Può anche controllare il tempo di risposta di ogni nodo.
- Fornisce report e rappresentazioni visive.
- Esegue il monitoraggio della rete per problemi come server bloccati, ecc.
- Il software di monitoraggio della rete supporta Microsoft, VMWare e Linux.

Nagios fornisce strumenti di monitoraggio della rete open source. Esegue il monitoraggio della rete per sovraccarico da collegamenti dati, connessioni di rete, monitoraggio router, switch, ecc.

3.5 Zabbix

Zabbix fornisce servizi di monitoraggio della rete open source per rete, server, cloud, applicazioni e servizi. Ha funzionalità di rilevamento avanzato dei problemi e avvisi e soluzioni intelligenti. Offre le sue soluzioni per vari settori come quello aerospaziale, commerciale, governativo, ecc.

Caratteristiche:

- La raccolta dei dati sarà flessibile ed estendibile.
- Può rilevare automaticamente i dispositivi di rete e le modifiche alla configurazione dei dispositivi.
- Fornisce una varietà di opzioni per le notifiche.
- Ti consentirà di creare scenari di escalation flessibili.

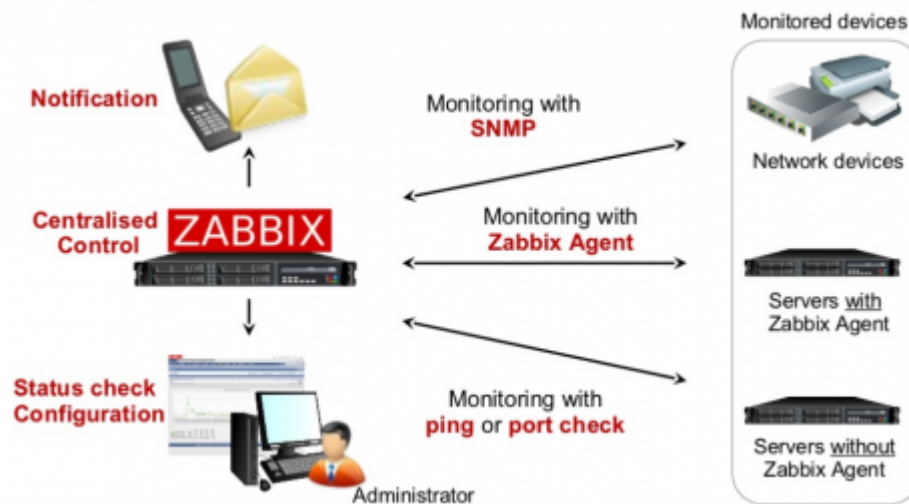
Zabbix ha funzionalità per la raccolta delle metriche, il rilevamento dei problemi, le notifiche, le API e il monitoraggio distribuito. Utilizza vari metodi e protocolli di raccolta metrica come SNMP, IPMI, ecc.

4 ZABBIX: SISTEMA DI MONITORAGGIO

4.1 ZABBIX

Zabbix è un software di monitoring che consente di controllare la disponibilità e le performance di una infrastruttura. Zabbix è open source e gratuito per qualsiasi utilizzo.

Con Zabbix è possibile raccogliere dati da qualsiasi tipo di dispositivo (server, apparato di rete, virtual machine). Oltre ad alimentare un prezioso storico di informazioni, Zabbix ha potenti funzioni di visualizzazione (mappe, overview, grafici e dashboard) e metodi altamente flessibili di analizzare i dati per generare alert o azioni automatiche. E' progettato per scalare fino a reti grandi e complesse grazie alle funzionalità di Distributed Monitoring.



Supporta il monitoraggio tramite polling dei dati o tramite pushing / trapping, può sfruttare gli agent software disponibili per tutti i principali sistemi operativi o basarsi interamente su metodi agent-less (SNMP, SSH, WMI, IPMI) per coprire virtualmente qualsiasi tipo di dispositivo. Le sue funzioni base includono sia il monitoraggio di applicazioni Web così come il monitoraggio di ambienti virtuali VMware.

Con l'auto-discovery Zabbix può eseguire scansioni della rete per rilevare nuovi dispositivi ed assegnare in modo automatico controlli di performance agli elementi trovati.

L'interfaccia web consente sia la configurazione del sistema, sia la visualizzazione dei dati in forma sicura, attraverso un sistema di controllo degli accessi granulare e personalizzabile.

Tutte le informazioni (sia le configurazioni sia i dati raccolti dalla rete) sono memorizzate in un database relazionale per una elaborazione semplice ed accessibile.

Zabbix consente di monitorare con facilità server, apparati di rete, ambienti VMware e applicazioni di qualsiasi tipo, raccogliendo statistiche e performance dettagliate.

4.2 FUNZIONALITA'

4.2.1 RACCOLTA DATI

Zabbix dispone di numerosi metodi per acquisire informazioni:

- **Zabbix Agent:** installato su un host consente di recuperare informazioni in tempo reale sull'utilizzo delle risorse (CPU, memoria, dischi, interfacce di rete) sullo stato dei servizi (processi, porte aperte, ecc.) sul contenuto di file, sulla presenza di errori nei file di log e molto altro ancora;
- **SNMP e IPMI:** Zabbix supporta il protocollo SNMP per accedere alle metriche di apparati di rete, stampanti, NAS, UPS e molti altri dispositivi. Grazie allo standard IPMI è inoltre possibile monitorare le informazioni hardware dai dispositivi HP iLO o Dell DRAC (temperatura, alimentazione, velocità delle ventole, stato dei dischi fisici e delle periferiche hardware);
- **Simple check:** Zabbix può monitorare la disponibilità e le performance di un servizio dall'esterno sfruttando i protocolli di rete ICMP (Ping) verificando la risposta di servizi TCP (FTP, IMAP, LDAP, NNTP, POP3) o eseguendo comandi via SSH o Telnet;
- **Custom monitoring:** oltre che dai check predefiniti Zabbix è in grado di acquisire dati richiamando un qualsiasi script esterno, sviluppato in un linguaggio a piacere (bash, Perl, PHP, Python, Ruby, ecc.) o integrando una libreria modulare sviluppata ad hoc;
- **VMware:** Zabbix rileva automaticamente gli host e le VM, così come le installazioni di vCenter e vSphere presenti in rete. E' in grado di acquisire le statistiche, le performance e le impostazioni di tutti i sistemi rilevati;
- **Web Scenario:** consentono di controllare in modo approfondito il corretto funzionamento delle applicazioni Web simulando una reale sessione utente (incluso il login e i metodi GET, POST) e monitorando i tempi di risposta, la velocità di download e l'output di ogni richiesta;
- **Applicazioni Java:** Zabbix supporta in modo nativo il monitoraggio con lo standard JMX (Java Management Extension) in grado di acquisire dati dai più diffusi application server (JBoss, Tomcat, WebSphere, ActiveMQ, GlassFish, ecc.);
- **Database monitoring:** attraverso la tecnologia ODBC, Zabbix può interrogare direttamente qualsiasi RDBMS come MySQL, PostgreSQL, Oracle e Microsoft SQL Server, generando grafici, allarmi o notifiche in caso di problemi o degrado delle performance;
- **Valori calcolati e aggregati:** in Zabbix è possibile creare sorgenti di dati virtuali applicando espressioni aritmetiche a piacimento (ad esempio è possibile calcolare la somma del traffico di due interfacce di rete e usare questo valore per tracciare un grafico o generare un allarme);
- **Performance interne:** Zabbix monitora se stesso per consentire di rilevare eventuali problemi di performance nel monitoraggio, soprattutto in reti molto grandi.

4.2.2 ANALISI DEI PROBLEMI

Non appena i dati vengono acquisiti dalla rete, inizia il processo di valutazione dei dati, che sfrutta differenti metodi disponibili in Zabbix. Le regole di valutazione o trigger expressions, in terms of Zabbix, forniscono una definizione formale di una condizione di errore, a partire dai dati ricevuti dalle macchine monitorate. Quando l'espressione descritta dal trigger si attiva, il trigger cambia il suo stato da OK a PROBLEM, evento cui può essere abbinata una o più risposte.

Zabbix fornisce dei metodi per far scattare i trigger in modo mirato ed intelligente. Un trigger può definire una soglia semplice come "maggiore di x", ma può anche combinare espressioni matematiche a piacere come divisioni, moltiplicazioni, medie o funzioni logiche come AND e OR.

Non solo, Zabbix permette di creare un trigger expression che tiene conto dei valori ottenuti da più host contemporaneamente. Questo consente di costruire soglie estremamente flessibili e particolareggiate che minimizzano i falsi positivi, permettendo agli amministratori di concentrarsi solo sui problemi reali.

Tra le funzioni avanza c'è la possibilità di confrontare il dato attualmente acquisito con uno ottenuto nel passato. In questo modo risulta semplice correlare periodi di tempo simili tra loro (ad esempio le performance di questo Lunedì con quelle di Lunedì scorso, oppure quelle di oggi pomeriggio con quelle di due settimane fa). Tutto ciò è estremamente utile quando il carico sulla rete non è uniforme e il confronto dei dati di Lunedì mattina con quelli di Martedì pomeriggio non offrirebbero alcuna informazione utile.

4.2.3 NOTTIFICHE

Zabbix non solo consente di acquisire, memorizzare ed analizzare informazioni sull'ambiente monitorato, ma anche di informare il personale addetto del verificarsi di eventi importanti, usando diversi canali e opzioni. Zabbix fornisce un workflow completo per inviare notifiche, raccogliere gli acknowledge degli amministratori, scalare il problem ad altri operatori e addirittura ad eseguire azioni in automatico sui sistemi coinvolti.

4.2.3.1 AVVISI

Zabbix dispone di diversi metodi predefiniti per l'invio delle notifiche. Gli amministratori possono ricevere notifiche:

- via e-mail;
- via SMS;
- via Jabber (messaging protocol);

- attraverso uno script personalizzato;

4.2.3.2 AZIONI AUTOMATICHE

Quando un trigger si attiva dei comandi di shell possono essere eseguiti automaticamente sui sistemi remoti, ad esempio per rimediare a situazioni in cui un sistema è sovraccarica o dei servizi hanno smesso di funzionare. L'utilizzo tipico di questa funzione è per riavviare un servizio o eseguire il reboot di un server. I comandi possono essere eseguiti :

- su Zabbix server
- su Zabbix agent
- utilizzando il protocollo IPMI
- utilizzando il protocollo telnet oppure SSH

4.2.3.3 ESCALATION

L'escalation descrive uno scenario in cui viene inviata una notifica, inizialmente ad un destinatario, quindi, se il problema persiste e nessuno acknowledge viene ricevuto, ad altri destinatari ed in assenza di ulteriori riscontri esegue un comando automatico. Zabbix fornisce regole estremamente efficaci e flessibili per definire uno scenario di escalation. Funzioni supportate:

- Notifica immediata dei nuovi problemi agli utenti.
- Monitoraggio proattivo: Zabbix esegue script predefiniti (comandi remoti)
- Ripetizioni della notifica finché il problema non viene risolto
- Notifiche ritardate
- Scalabilità del problema ad altri gruppi di utenti
- Possibilità di scalare diversamente i problemi con acknowledge e quelli senza acknowledge.
- Invio dei messaggi recovery a tutte le parti coinvolte
- Numero illimitato di escalation

Nelle notifiche può essere inserita l'intera cronologia di escalation in modo che il destinatario possa vedere cosa sta succedendo e perché ha ricevuto il messaggio.

4.2.4 VISUALIZZAZIONE

Il frontend web di Zabbix ha numerose funzionalità legate alla visualizzazione dei dati:

- **Dashboard:** un cruscotto sintetico per avere a colpo d'occhio lo stato della vostra infrastruttura.
- **Graph:** per tracciare i dati monitorati attraverso vari metodi (istogrammi, diagrammi a linea, diagrammi a torta,)
- **Map:** per collocare i dati monitorati e i trigger attivi direttamente su una mappa geografica, una planimetria, un diagramma rack, un diagramma di flusso, ecc.
- **Screen:** aggrega in un'unica pagina gli elementi più importanti di un dato sottosistema, permettendo di confrontare ad esempio, più diagrammi tra loro
- **Slide shows:** scorri automaticamente un insieme di screens ad intervalli prefissati, utile per i monitor delle sale operative.
- **Access to raw data:** visualizza all'occorrenza il dato grezzo ricevuto dal dispositivo.
- **Event and notification details:** visualizza gli eventi e i trigger attivi, nonché lo stato delle notifiche inviate
- **Security and Authentication:** crea utenti e gruppi di utenti, definendo in modo granulare a quali informazioni possono accedere. Centralizza l'autenticazione su un sistema di autenticazione esterno.

4.2.5 AUTO-DISCOVERY

Il monitoraggio di ambienti molto grandi e complessi può diventare un incubo senza automazione. Zabbix fornisce diversi metodi per automatizzare la gestione di tali ambienti. Con Zabbix i dispositivi e gli oggetti all'interno dei dispositivi (come filesystems e interfacce di rete) possono essere aggiunti o rimossi dal monitoraggio non appena entrano o escono dalla vostra rete. Automaticamente.

Le funzionalità principali per il rilevamento e la gestione automatica dei dispositivi sono tre:

- Network discovery;
- Low-level discovery;
- Agent auto registration.

4.2.5.1 NETWORK DISCOVERY

Questa funzione permette di condurre periodiche scansioni della rete alla ricerca di host, servizi o agent in funzione, e di eseguire azioni predefinite in caso di rilevamento.

Per ogni elemento rilevato viene generato un discovery event, che può essere la base per eseguire una specifica azione, come:

- Inviare una notifica;
- Aggiungere automaticamente il dispositivo in Zabbix (o rimuoverlo);
- Inserire il dispositivo in un gruppo di host;
- Applicare automaticamente un template al dispositivo, in modo da iniziare a monitorarlo;
- Eseguire uno script remoto.

4.2.5.2 LOW-LEVEL DISCOVERY

Questa funzione fornisce un sistema per creare automaticamente item, trigger e grafici per ciascun elemento rilevato all'interno di un dispositivo. Ad esempio Zabbix può iniziare in automatico a monitorare i file system o le interfacce di rete presenti su una macchina, senza la necessità di creare manualmente gli item per ciascun file system o interfaccia di rete.

Se in un secondo momento all'host vengono aggiunte interfacce di rete o filesystem Zabbix le rileva e inizia a monitorarle senza intervento dell'utente.

Zabbix supporta tre tipi di item discovery:

- Discovery dei file systems;
- Discovery delle interfacce di rete (anche interfacce virtuali e in teaming/bonding);
- Discovery degli oggetti SNMP (OID).

4.2.5.3 AUTO-REGISTRATION

Questa funzione permette ad un server Zabbix di iniziare a monitorare automaticamente nuovi dispositivi se questi dispositivi hanno uno Zabbix agent installato. In tal modo non è necessaria alcuna operazione manuale per inserire un nuovo host sul server Zabbix: è sufficiente installare lo Zabbix agent e farlo puntare all'indirizzo del Zabbix server.

4.2.6 IT INVENTORY

Un inventory di rete sempre aggiornato

Zabbix in grado di mantenere le informazioni di inventario host (ad esempio, il numero di serie, l'indirizzo MAC, OS, software). Può essere utile per la gestione patrimoniale delle infrastrutture. Queste informazioni possono anche essere incluse in un messaggio di notifica quando si segnalano problemi con un dispositivo, rendendo il compito di un amministratore di sistema di capire la causa del problema e trovare una soluzione più facile.

Campi di inventario Host possono essere compilati automaticamente. Gli articoli speciali possono raccogliere informazioni di inventario e riempire un campo inventario nella definizione di host.

Gestisci i Dispositivi di script personalizzati con Script definiti dall'utente possono essere eseguiti nel web frontend Zabbix. Sul cruscotto, nella mappa e eventi schermi un amministratore può eseguire script facendo clic su un'icona hostname o una mappa, e selezionando uno script dall'elenco a discesa.

Questa funzione è utile per la prima reazione a problemi nel sistema. Comandi ping e traceroute sono disponibili per impostazione predefinita.

5 INSTALLAZIONE

Si andrà ora ad analizzare i procedimenti necessari per l'installazione del Server Zabbix e degli Agent nelle macchine da monitorare.

Si utilizzerà la distribuzione Linux CentOS 7.

5.1 PREREQUISITI

Al fine di installare Zabbix, occorre analizzare i prerequisiti:

- My SQL;
- Apache;
- PHP.

Iniziamo con entrare come “root” ed aprire il terminale linux.

Da riga comando digitare il comando inserito sotto per vedere la versione di Linux installata:

```
#cat /etc/redhat-release
```

Il risultato di ritorno sarà:

```
CentOS Linux release 7.7.1908 (Core)
```

Successivamente andiamo a vedere la versione del Kernel inserendo il comando:

```
# uname -r
```

Il risultato di ritorno sarà:

```
3.10.0-1062.1.2.el7.x86_64
```

Andiamo a controllare eventuali aggiornamenti del S.O. e successivamente a dare un nome host alla macchina:

```
# yum update
```

```
# hostname zabbix-server
```

Aggiungiamo a file host il nome della macchina precedentemente inserito:

```
# vi /etc/hosts
```

```
127.0.0.1    localhost zabbix-server
```

5.1.1 INSTALLAZIONE SSH

```
# service sshd start
# sudo systemctl enable sshd
# nano /etc/ssh/sshd_config
    mettere PermitRootLogin yes
# chkconfig httpd --level 345 on
# service sshd restart
```

5.1.2 INSTALLAZIONE APACHE

```
# yum install httpd
# chkconfig httpd --level 345 on
# firewall-cmd --add-service=http
# firewall-cmd --reload
# systemctl start httpd.service
# systemctl enable httpd.service
```

5.1.3 DISABILITAZIONE FIREWALL

```
# systemctl status firewalld
# systemctl stop firewalld
# systemctl disable firewalld
```

5.1.4 INSTALLAZIONE MySQL

```
# yum install mysql mysql-server -y
# chkconfig mysqld --level 345 on
# service mysqld start
# mysql_secure_installation
```

5.1.5 INSTALLAZIONE PHP

```
# yum install php php-cli php-common php-devel php-pear php-gd php-mbstring
```

5.2 INSTALLAZIONE ZABBIX 4.2

```
# rpm -Uvh Uvh https://repo.zabbix.com/zabbix/4.2/rhel/7/x86_64/zabbix-release-4.2-1.el7.noarch.rpm
```

```
# yum install zabbix-server-mysql zabbix-web-mysql
```

```
# yum install zabbix-agent
```

5.2.1 CREAZIONE DATABASE ZABBIX

```
# mysql -u root -p
```

```
mysql> create database zabbix character set utf8 collate utf8_bin;
```

```
mysql> grant all privileges on zabbix.* to zabbix@localhost identified by 'zabbix';
```

```
mysql> exit
```

5.2.2 CREAZIONE SCHEMA ZABBIX

```
# zcat /usr/share/doc/zabbix-server-mysql*/create.sql.gz | mysql -uzabbix -p zabbix
```

5.2.3 SETTAGGIO CONFIGURAZIONE ZABBIX

```
# vi /etc/zabbix/zabbix_server.conf
```

```
DBHost=localhost
```

```
DBName=zabbix
```

```
DBUser=zabbix
```

```
DBPassword=Zabbix
```


5.2.4 APACHE CONFIGURAZIONE

```
# vi /etc/httpd/conf.d/zabbix.conf
    php_value max_execution_time 600
    php_value memory_limit 256M
    php_value post_max_size 32M
    php_value upload_max_filesize 2M
    php_value max_input_time 600
    php_value date.timezone Europe/Rome
# systemctl restart zabbix-server zabbix-agent httpd
# systemctl enable zabbix-server zabbix-agent httpd
```

5.2.5 MODIFICA SELINUX

```
#getenforce
#vi /etc/selinux/config

# This file controls the state of SELinux on the system.
# SELINUX= can take one of these three values:
# enforcing - SELinux security policy is enforced.
# permissive - SELinux prints warnings instead of enforcing.
# disabled - SELinux is fully disabled.

SELINUX=enforcing

# SELINUXTYPE= type of policy in use. Possible values are:
#     targeted - Only targeted network daemons are protected.
#     strict - Full SELinux protection.
```

```
SELINUXTYPE=targeted
```

L'unica modifica che dovete fare, in sostanza, è modificare la voce **SELINUX=enforcing** a **SELINUX=permissive**.

```
# systemctl restart zabbix-server zabbix-agent httpd
```

5.2.6 AVVIO ZABBIX

Aprire il browser e scrivere :

http://<youripaddress>/zabbix oppure http://localhost/zabbix

Esempio:

Se l'indirizzo ip del mio server Zabbix è 192.168.56.101

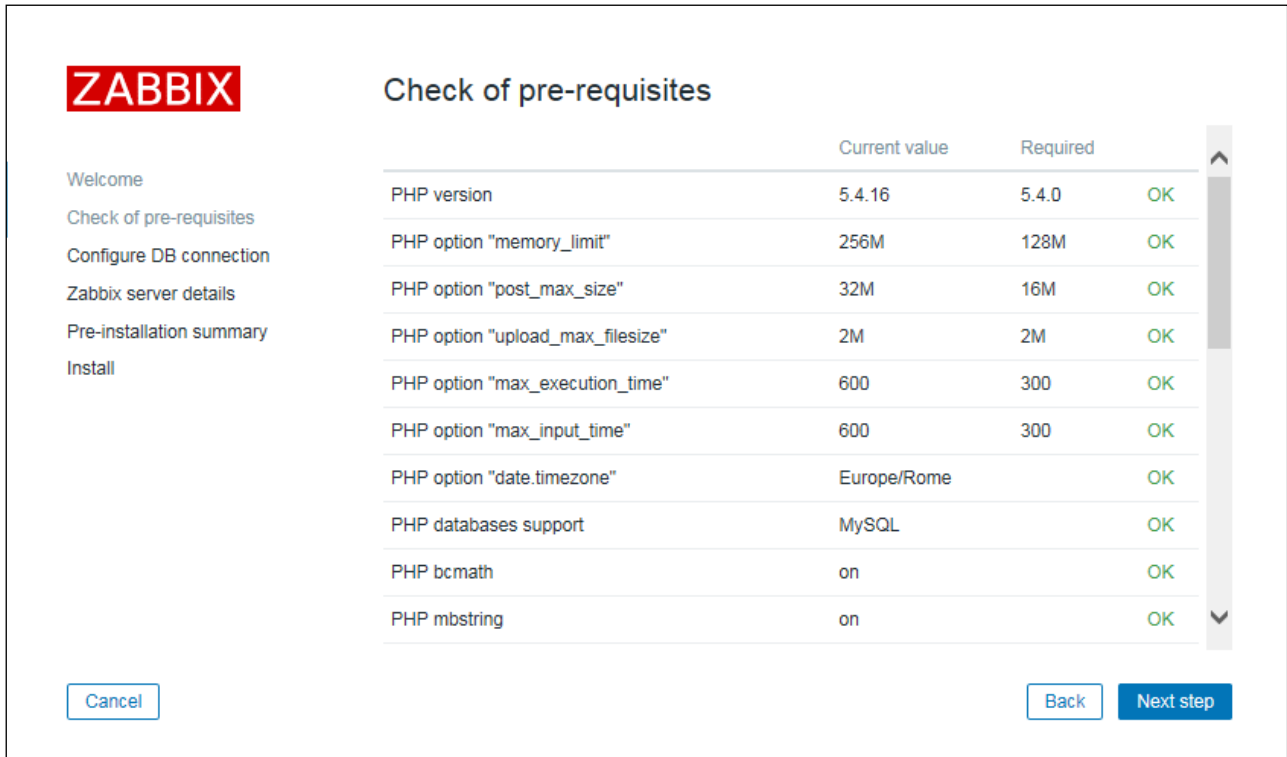
Dovrò scrivere http://192.168.56.101/zabbix/setup.php

Si aprirà una schermata di benvenuto ed inizieremo la configurazione



Cliccare Next step

Punto 2: Verranno visualizzati tutti i prerequisiti installati:



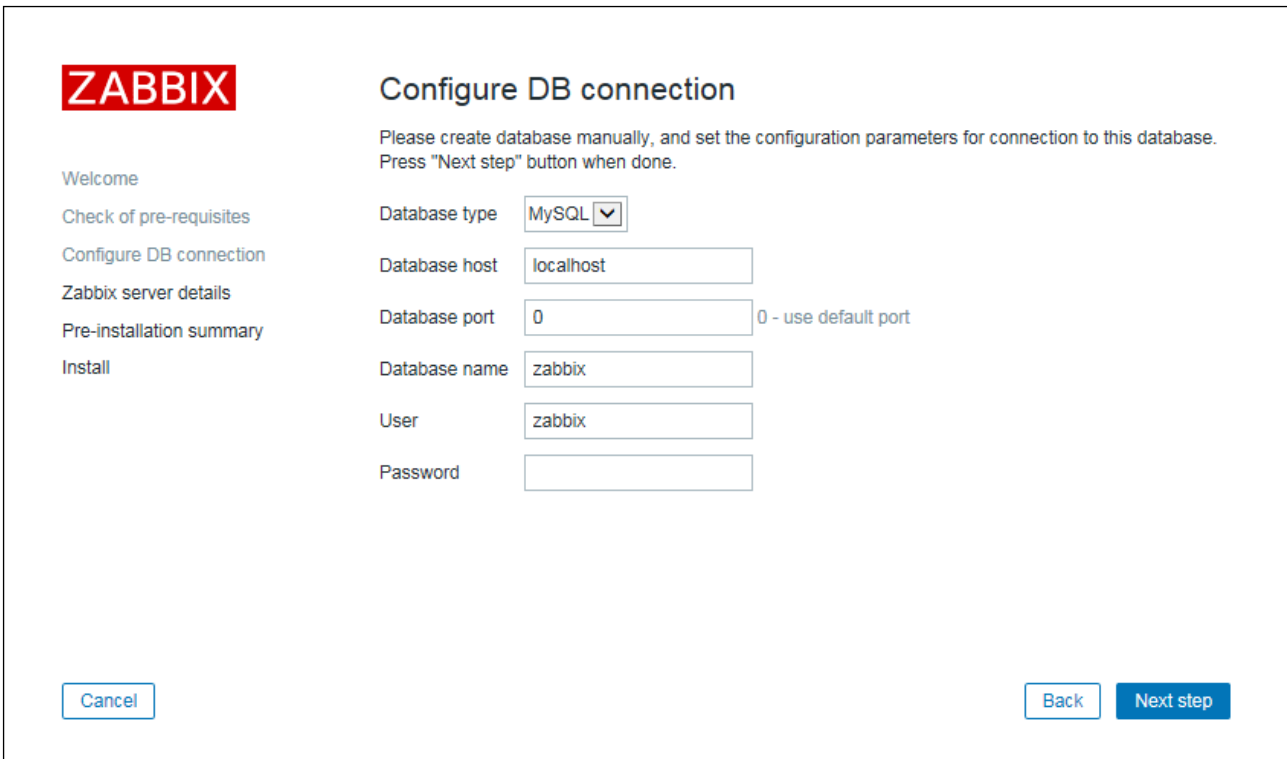
The screenshot shows the Zabbix installation wizard's 'Check of pre-requisites' screen. On the left is a navigation menu with the following items: Welcome, Check of pre-requisites (highlighted), Configure DB connection, Zabbix server details, Pre-installation summary, and Install. The main area contains a table with the following data:

	Current value	Required	
PHP version	5.4.16	5.4.0	OK
PHP option "memory_limit"	256M	128M	OK
PHP option "post_max_size"	32M	16M	OK
PHP option "upload_max_filesize"	2M	2M	OK
PHP option "max_execution_time"	600	300	OK
PHP option "max_input_time"	600	300	OK
PHP option "date.timezone"	Europe/Rome		OK
PHP databases support	MySQL		OK
PHP bcmath	on		OK
PHP mbstring	on		OK

At the bottom of the screen are three buttons: 'Cancel', 'Back', and 'Next step'.

Tutti devono essere OK, dopo di che cliccare su Next step.

Punto 3: Configurazione del DB MySQL



The screenshot shows the Zabbix installation wizard's 'Configure DB connection' screen. On the left is a navigation menu with the following items: Welcome, Check of pre-requisites, Configure DB connection (highlighted), Zabbix server details, Pre-installation summary, and Install. The main area contains the following configuration fields:

- Database type: MySQL (dropdown menu)
- Database host: localhost
- Database port: 0 (with note "0 - use default port")
- Database name: zabbix
- User: zabbix
- Password: (empty text box)

At the bottom of the screen are three buttons: 'Cancel', 'Back', and 'Next step'.

Inserirei i parametri metti in zabbix_server.conf e poi continuiamo cliccando su Next step.

Punto 4 : Dettaglio del server

ZABBIX

Zabbix server details

Please enter the host name or host IP address and port number of the Zabbix server, as well as the name of the installation (optional).

Host:

Port:

Name:

Cancel Back Next step

Inserire il nome del Server e poi Cliccare su Next step.

Punto 5: Sommario dei parametri di pre-installazione.

ZABBIX

Pre-installation summary

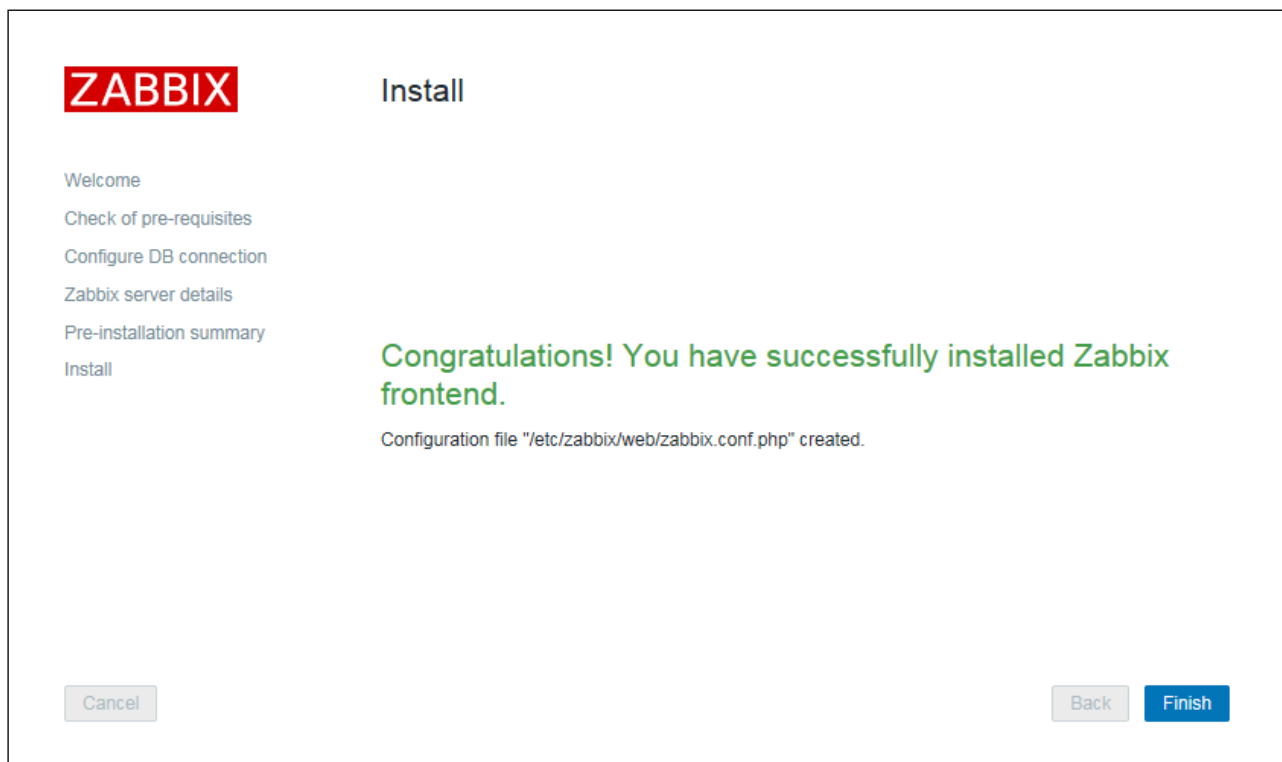
Please check configuration parameters. If all is correct, press "Next step" button, or "Back" button to change configuration parameters.

Database type	MySQL
Database server	localhost
Database port	default
Database name	zabbix
Database user	zabbix
Database password	*****
Zabbix server	localhost
Zabbix server port	10051
Zabbix server name	zabbix

Cancel Back Next step

Se tutto ok successivamente Cliccare su Next step.

Punto 6 : Installazione



Installazione completata , per finire premere Finish.

5.3 WEBMIN

5.3.1 INSTALLAZIONE

Loggarsi come root ed aprire una sessione terminale.

```
# wget http://prdownloads.sourceforge.net/webadmin/webmin-1.740-1.noarch.rpm
```

Una volta scaricato il pacchetto, scaricare eventuali dipendenze

```
# yum -y install perl perl-Net-SSLeay openssl perl-IO-Tty
```

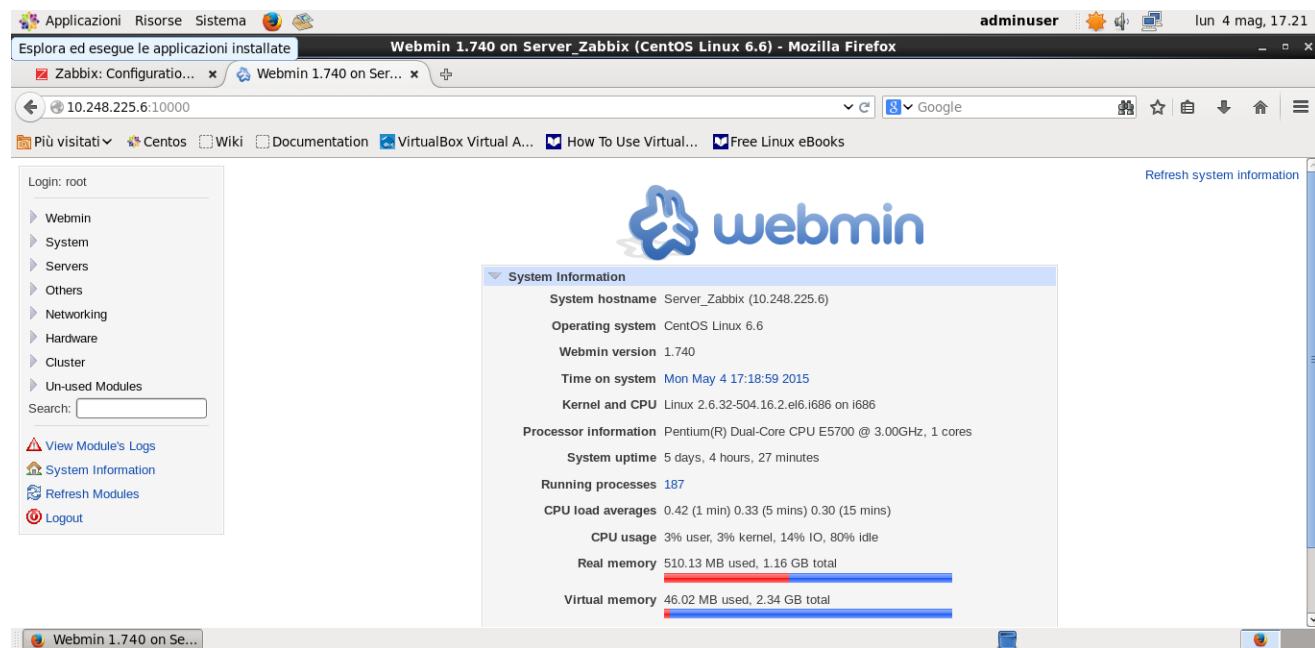
Concluso, lanciare l'installazione di Webmin vera e propria

```
# rpm -U webmin-1.740-1.noarch.rpm
```

Il resto della installazione sarà fatto automaticamente nella directory /usr/libexec/webmin.

Per accedere al Webmin aprime un browser e digitare sull'URL `http://localhost:10000`, a questo punto basta mettere root e relativa password.

Verrà aperta la finestra come in figura sottostante.



5.4 POSTFIX

5.4.1 INSTALLAZIONE

Se non si ha Postfix configurato, loggarsi come root ed aprire una sessione terminale.

```
# yum install postfix
```

Configurare Postfix come MTA di default

```
# alternatives --set mta /usr/sbin/postfix
```

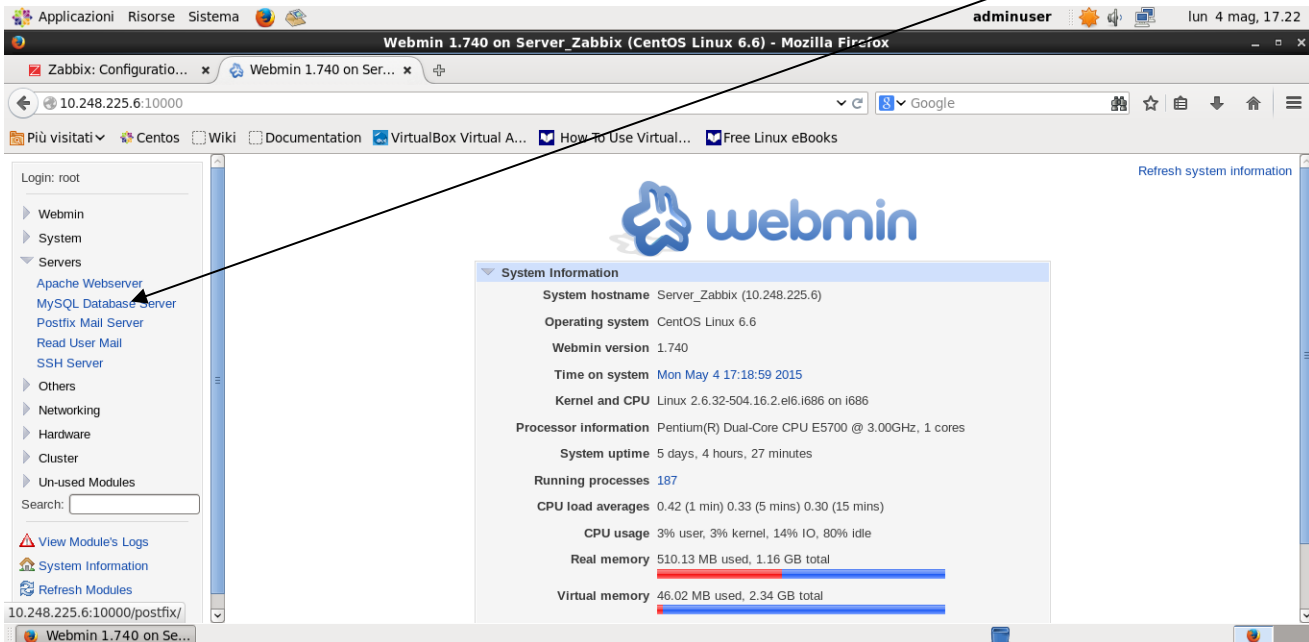
Se il comando sopra non funziona e si ottiene il seguente messaggio `"/usr/sbin/postfix non è stato configurato come alternativa per MTA"`, utilizzare il comando seguente per fare la stessa cosa

```
# alternatives --set mta /usr/sbin/sendmail.postfix
```

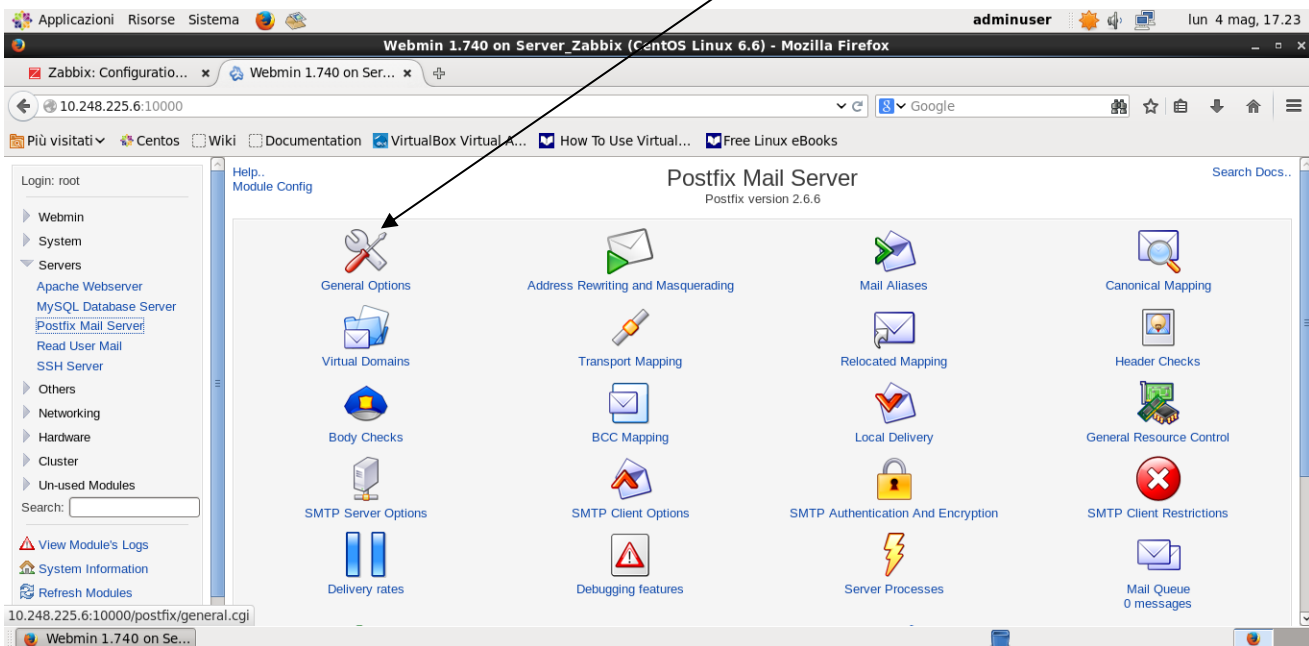
5.4.2 CONFIGURAZIONE

Aprire Webmin <http://localhost:10000> con utente e password root.

Alla finestra cliccare su Servers e successivamente su “POSTFIX MAIL SERVER”



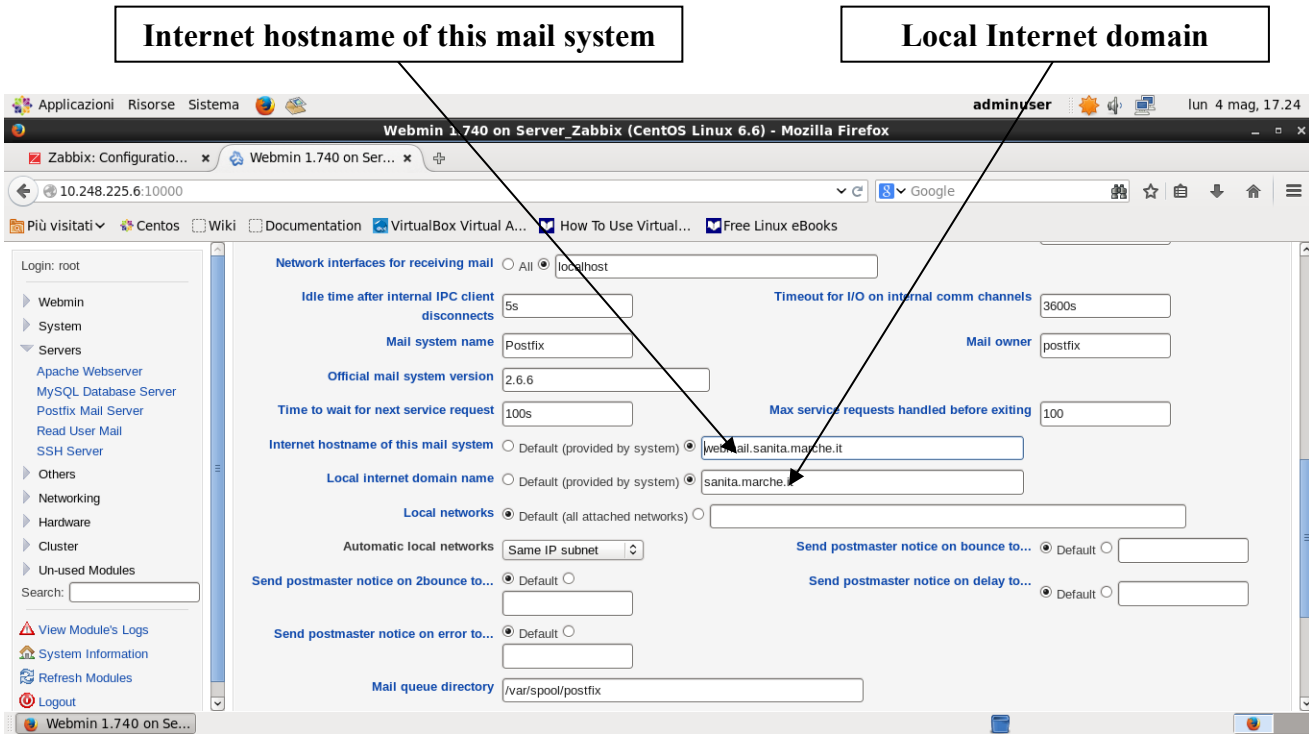
Alla finestra successiva cliccare su “GENERAL OPTIONS”



Riempire i campi:

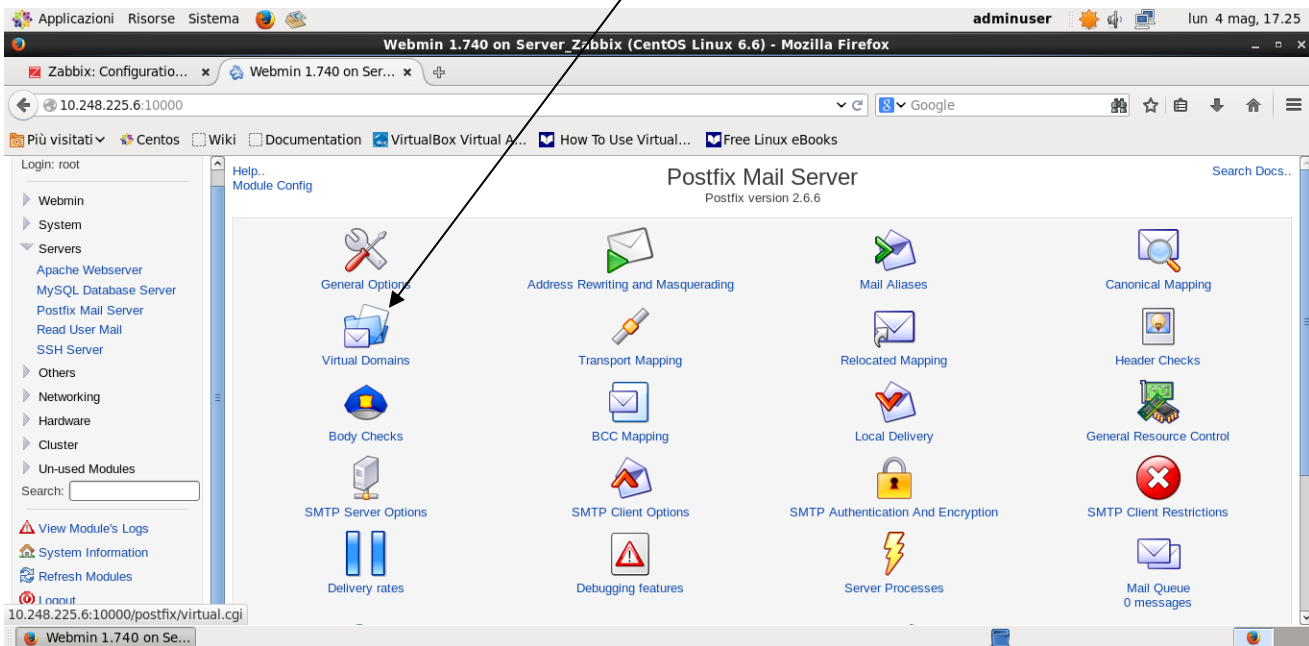
Internet hostname of this mail system : Nome Server Mail del dominio.

Local Internet domain name : Nome del dominio.

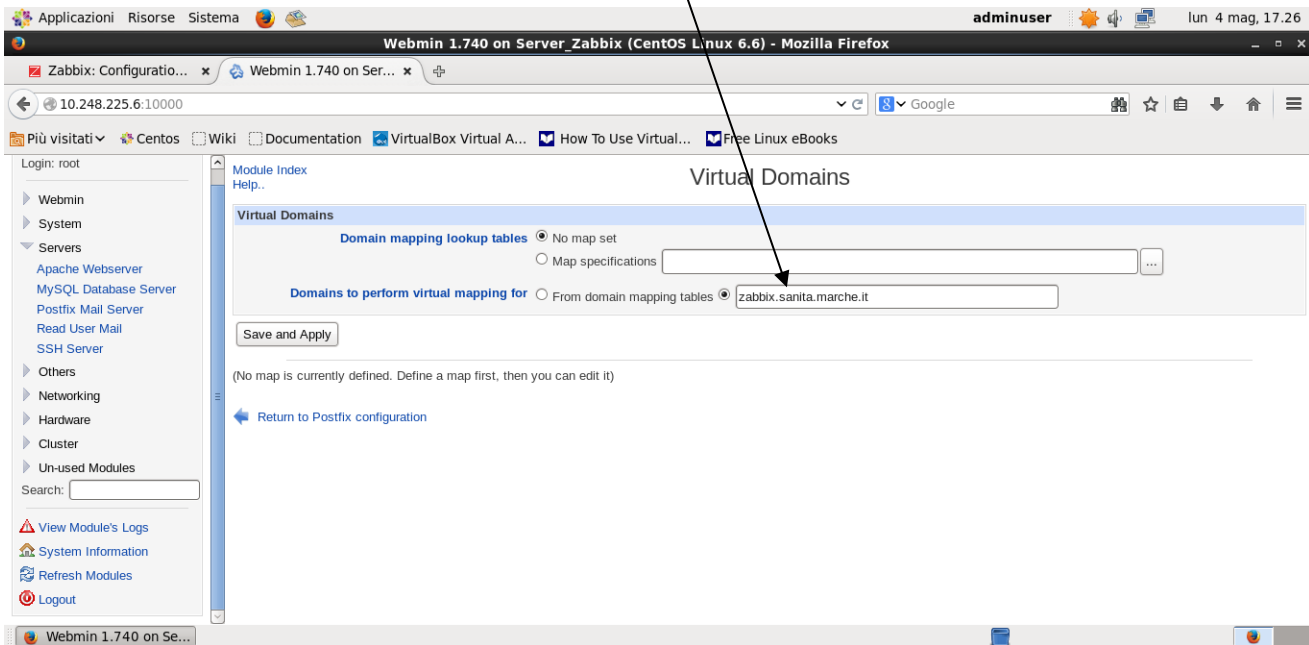


Finito Cliccare su Salvataggio e ritornate al Menù Precedente.

A questo punto cliccate su “VIRTUAL DOMAINS”



Riempire il campo **Domains to perform virtual mapping for** con un nome scelto a piacere



Anche in questo caso appena finito cliccare su Salvataggio.

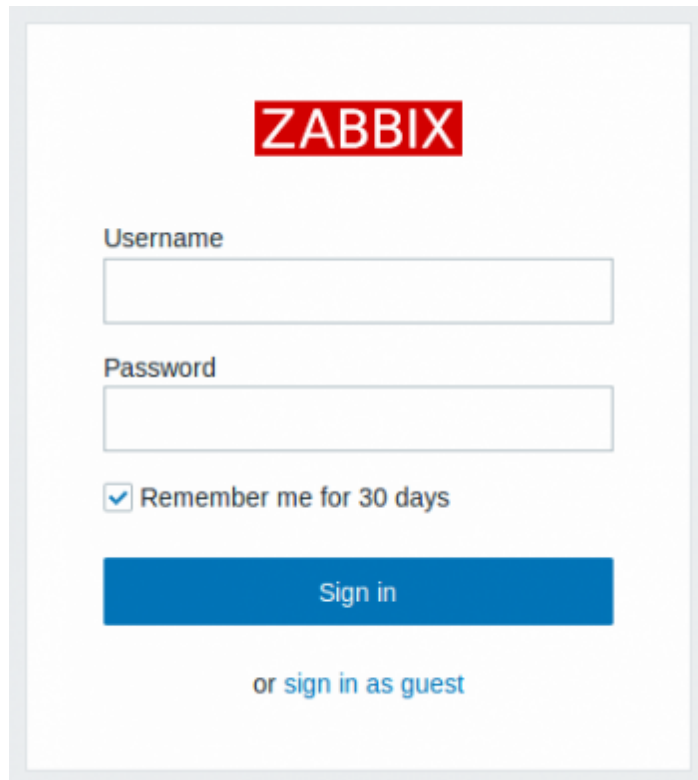
A questo punto Postfix è installato e funzionante per girare i messaggi di “Alert” provenienti da Zabbix.

6 ZABBIX AVVIO

Completata la procedura di installazione del frontend saremo indirizzati alla maschera di login dove dobbiamo inserire le credenziali iniziali:

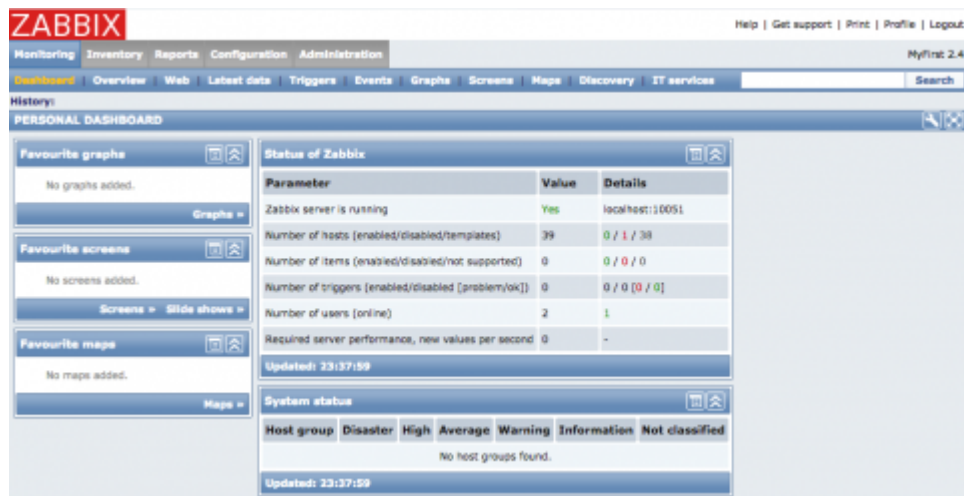
user: Admin

password: zabbix



The image shows the Zabbix login interface. At the top center is the ZABBIX logo in a red box. Below it are two input fields: 'Username' and 'Password'. Under the password field is a checkbox labeled 'Remember me for 30 days' which is checked. At the bottom is a blue 'Sign in' button and a link 'or sign in as guest'.

Inserite le credenziali Username e Password entreremo nella Dashboard principale



The image shows the Zabbix main dashboard. At the top left is the ZABBIX logo. The top navigation bar includes 'Monitoring', 'Inventory', 'Reports', 'Configuration', and 'Administration'. The main content area is titled 'PERSONAL DASHBOARD' and contains several widgets:

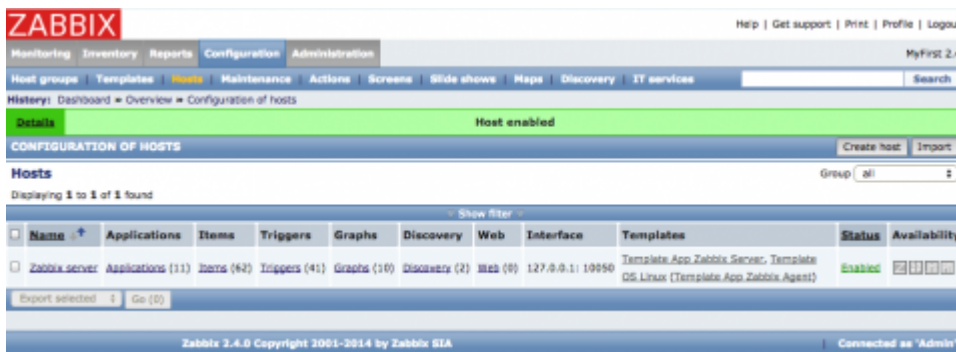
- Favourite graphs:** No graphs added.
- Favourite screens:** No screens added.
- Favourite maps:** No maps added.
- Status of Zabbix:** A table showing system parameters.
- System status:** A table showing host group status.

Parameter	Value	Details
Zabbix server is running	Yes	local host: 10051
Number of hosts [enabled/disabled/templates]	39	0 / 1 / 38
Number of items [enabled/disabled/not supported]	0	0 / 0 / 0
Number of triggers [enabled/disabled [problem/ok]]	0	0 / 0 [0 / 0]
Number of users [online]	2	1
Required server performance, new values per second	0	-

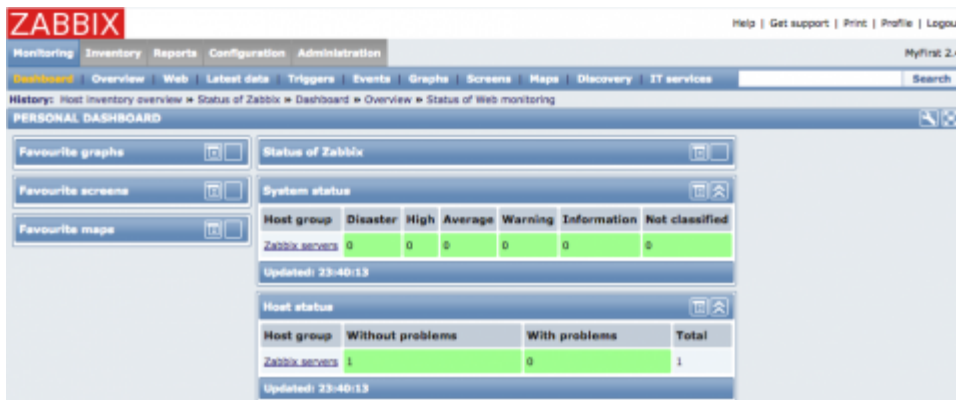
Host group	Disaster	High	Average	Warning	Information	Not classified
No host groups found.						

Andiamo ad abilitare l'unico host presente al momento nella nostra installazione, ovvero il server di monitoraggio stesso.

Configuration > Hosts > Zabbix Server > Disabled->Enable



Torniamo alla Dashboard per notare che Zabbix ha iniziato a monitorare l'host, tramite il suo Zabbix agent.



6.1 ZABBIX MACCHINE WINDOWS

6.1.1 CONFIGURAZIONE AGENT SU WINDOWS

Scaricare l'ultimo "Zabbix-Agent" per Windows dal sito ufficiale e scompattarlo sul desktop.

1. Creare una cartella sotto c: con il nome di zabbix
2. Copiare dalla cartella scompattata sul desktop sotto "bin" e poi relativo S.O 32/64bit i file sotto elencati nella cartella c:\zabbix:
 - zabbix_agentd.exe
 - zabbix_get.exe

- zabbix_sender.exe
3. Copiare dalla cartella scompattata sul desktop sotto “conf” il file nella cartella c:\zabbix:
 - zabbix_agentd.win.conf;
 4. Entrare nella cartella c:\zabbix e rinominare il file zabbix_agentd.win.conf in zabbix_agentd.conf;
 5. Aprire il file zabbix_agentd.conf con un editor e posizionarsi alla riga successiva #Server=[zabbix server ip] e scrivere:
 - Server=”Ip Server Zabbix”;
 6. Aprire una riga di comando DOS e scrivere:
 - cd c:\zabbix;
 - c:\zabbix > zabbix_agentd.exe --config c:\zabbix_agentd.conf --install
zabbix_agentd.exe [xxxx]: service [Zabbix Agent] installed successfully
zabbix_agentd.exe [xxxx]: event source [Zabbix Agent] installed successfully
 - C:\zabbix> zabbix_agentd.exe --stop
zabbix_agentd.exe [xxxx]: service [Zabbix Agent] stopped successfully
 - C:\zabbix> zabbix_agentd.exe --start
zabbix_agentd.exe [xxxx]: service [Zabbix Agent] started successfully

Se eseguite il comando “services.msc”, tra i servizi attivi ne troverete uno con il nome di **Zabbix Agent** in esecuzione.

A questo punto non ci resta che configurare L’host all’interno di Zabbix.

6.1.2 INSERIMENTO MACCHINA WINDOWS SU ZABBIX

Entrare su Zabbix – Configuration – Hosts e cliccare su Create Host

The screenshot shows the 'Configuration of hosts' page in Zabbix. The 'Host name' field is filled with '10.248.224.228'. The 'Groups' section shows 'Windows' selected in the 'In groups' list. The 'New group' field is empty. The 'Agent interfaces' section has '10.248.224.228' entered in the 'IP address' field. Annotations with arrows point to these fields and the 'Other groups' list.

- 1 Inserire Host
- 2 Inserire il **Group** di appartenenza cliccando su quelli presenti
- 3 Se si desidera creare un nuovo gruppo riempire il campo **New Group**;
- 5 Inserire **Indirizzo IP** della macchina da monitorare.

Premere successivamente su **TEMPLATETES**

The screenshot shows the 'Configuration of hosts - Templates' page. The 'Linked templates' table shows 'Template OS Windows' with 'Unlink' and 'Unlink and clear' actions. The 'Link new templates' section has a search box and a 'Select' button. The 'Update' button is highlighted. Annotations with arrows point to the 'Select' button and the 'Update' button.

- 5 Cliccare su **Select** e selezionare **Template OS Windows** ;
- 6 Cliccare su **ADD** in modo da aggiungere il template;
- 7 Finito cliccare su

Se tutto è andato a buon fine tra gli host avremmo anche quest'ultimo nel giro di qualche minuto comparirà sulla colonna Avviabilità la "Z" di colore Verde.

6.2 INSERIMENTO ROUTER MIKROTIK SU ZABBIX

Entrare su Zabbix – Configuration – Hosts e cliccare su Create Host

The screenshot shows the Zabbix Configuration Hosts page. Four numbered callouts are present:

- 1 Inserire Host**: Points to the 'Host name' field containing '10.248.224.001'.
- 2 Inserire il Group di appartenenza cliccando su quelli presenti:**: Points to the 'In groups' list, which includes 'Router MikroTik'.
- 3 Se si desidera creare un nuovo gruppo riempire il campo New Group:**: Points to the 'New group' input field.
- 4 Inserire Indirizzo IP della macchina da monitorare.**: Points to the 'SNMP interfaces' table, where the 'IP address' field contains '10.248.224.1'.

Cliccare su Update per inserire l'host.

Se tutto è andato a buon fine tra gli host avremmo anche quest'ultimo nel giro di qualche minuto comparirà sulla colonna Avviability la "Z" di colore Verde.

Inseriti tutti i nostri vari host ritornando alla Dashboard principale potremmo controllare in modo veloce ed in tempo reale tutti i nostri apparati, andando a consultare i vari riquadri contenuti:

The screenshot shows the Zabbix Global view dashboard. It contains several sections:

- System information**: A table with parameters like 'Zabbix server is running', 'Number of hosts', 'Number of items', 'Number of triggers', 'Number of users', and 'Required server performance'.
- Problems by severity**: A table showing the number of problems for different host groups, categorized by severity (Disaster, High, Average, Warning, Information, Not classified).
- Problems**: A table showing a list of problems with columns for Time, Info, Host, Problem + Severity, Duration, Ack, Actions, and Tags.

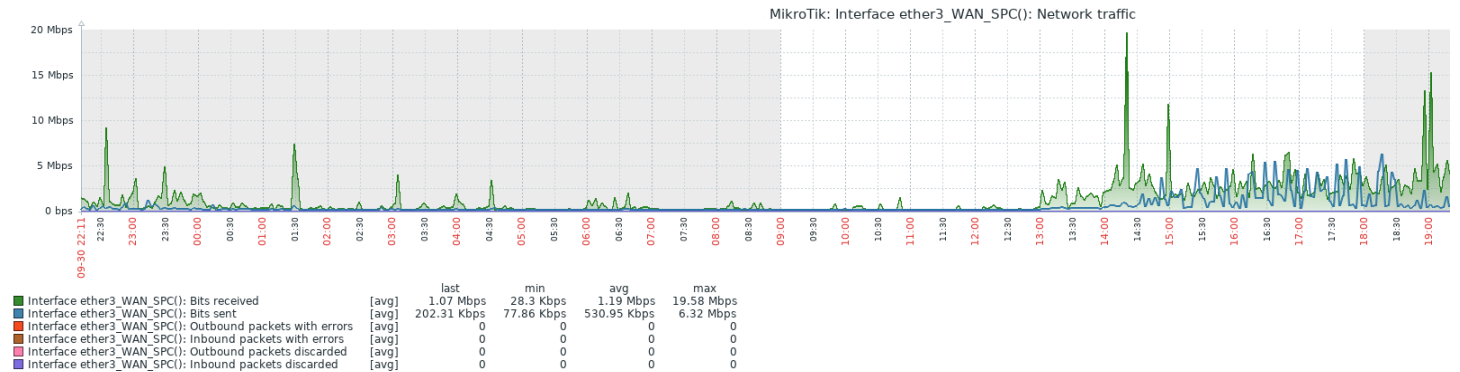
System information: informazioni generali relative al numero di host/items/triggers/users;

Problems by severity: Tutti i problemi a secondo della severità dei gruppi inseriti con differenti colori;

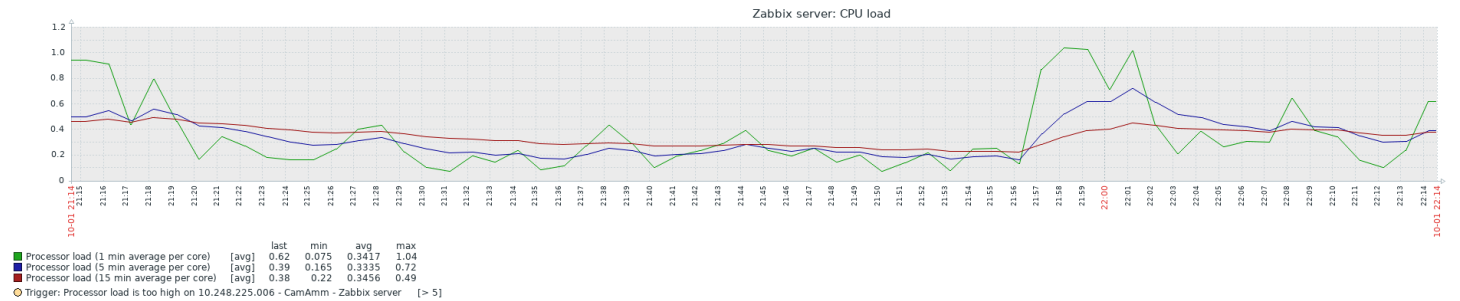
Problems: Dettaglio dei problemi di tutti gli host ordinati per giorno e ora evento, e distinti per colore e gravità dell'evento.

Inoltre la Dashboard può essere personalizzata per utente aggiungendo riquadri che non ci sono e togliere quelli che per noi non sono importanti.

Altro punto di forza del prodotto sono i grafici per controllare per esempio la banda utilizzata del nostro router, potendo scegliere di visualizzare ogni singola porta e il lasso di tempo da monitorare.



Oppure l'utilizzo della CPU Load di un determinato Server



In caso di eventuali problemi se attivato l'allert ad esempio tramite mail ci arriverà il seguente messaggio:

Problem started at 09:32:58 on 2019.10.04 Problem name: Unavailable by ICMP ping

Host: 10.248.225.001 - CamAmm Server DHCP

Severity: High

Original problem ID: 1452888

Mentre alla risoluzione del problema avremmo il seguente avviso:

Problem has been resolved at 09:41:58 on 2019.10.04 Problem name: Unavailable by ICMP ping

Host: 10.248.225.001 - CamAmm Server DHCP

Severity: High

Original problem ID: 1452888

7 CONCLUSIONI

In questo lavoro di tesi sono state descritte alcune delle molteplici possibilità che un sistema di monitoraggio di rete come ZABBIX possa aiutare nel lavoro quotidiano un Amministratore di Rete.

Si è partiti introducendo il significato di rete e la presentazione di uno dei protocolli più utilizzati in essa ossia il protocollo SNMP, per poi passare prima una panoramica descrittiva di vari software che eseguono il monitoraggio di reti sia open source che a pagamento ed il perché è stato scelto ZABBIX.

Quindi successivamente, si è entrati nel dettaglio dall'installazione e configurazione dello stesso e di altri prodotti come POSTIFIX e WBEMIN che posso essere ad esse correlati.

Si è concluso facendo vedere le possibilità che tale strumento come il monitoraggio degli errori e relativi messaggi di alert, la visualizzazione grafica dei flussi e la semplicità con cui possono essere aggiunti differenti dispositivi come Pc con S.O. Windows, Router e Switch di brand differenti fra loro.

Allo stato attuale tale prodotto è installato e funzionante all'interno AV3 – Camerino ex ZT10 per il monitoraggio di differenti supporti (Router, Switch, Server.....) delle varie sedi del territorio e presidi ospedalieri.

Nonostante i risultati ottenuti nel suo utilizzo abbiano portato allo stato attuale un netto miglioramento nella governance della networking all'interno della struttura; si è già pensato ai successivi passi da intraprendere in un futuro prossimo ossia (grazie alla grande gamma di Template presenti per Zabbix) la rilevazione di apparati UPS associati ad elettromedicali come TAC, Risonanze Magnetiche o associati a machine di Laboratorio o ad altri macchinari di vitali importanza; questo perché permetterebbe di monitorare in tempo reale il livello di carica delle batterie in essi ed il loro corretto funzionamento. Si è anche pensato poi di andare a studiare eventuali sonde che permettano la rilevazione di temperatura di frigoriferi che contengano ad esempio medicinali o sacche per trasfusioni.

8 BIBLIOGRAFIA

1. NETWORK MONITORING (Wikipedia https://en.wikipedia.org/wiki/Network_monitoring)
2. DEFINIZIONE NETWORK (Dizionario Treccani <http://www.treccani.it/vocabolario/network/>)
3. SNMP CONFIGURATION GUIDE (Cisco <https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/snmp/configuration/12-4t/snmp-12-4t-book/nm-snmp-cfg-snmp-support.html>)
4. MIKROTIK MANUALI (Mikrotik <https://wiki.mikrotik.com/wiki/Manual:TOC>)
5. ZABBIX MANUALI E SOFTWARE (Zabbix <https://www.zabbix.com/>)
6. ZABBIX ITALIA FORUM (Zabbix <https://www.zabbix.com/forum/forum/zabbix-in-your-language/in-lingua-italiana/29473-uso-di-zabbix-in-italia>)
7. CENTOS MANUALI E SOFTWARE (Centos <https://www.centos.org/>?)
8. APACHE MANUALI E SOFTWARE (Apache <http://httpd.apache.org/>)
9. PHP MANUALI E SOFTWARE (Php <https://www.php.net/index.php>)
10. MYSQL MANUALI E SOFTWARE (MySql <https://www.mysql.com/it/>)
11. POSTFIX MANUALI E SOFTWARE (Postfix <http://www.postfix.org/>)
12. WEBMIN MANUALI E SOFTWARE (Webmin <http://www.webmin.com/>)
13. CONFIGURE SNMP ON VMWARE (VMware <https://pubs.vmware.com/vsphere-51/index.jsp?topic=%2Fcom.vmware.vsphere.monitoring.doc%2FGUID-8EF36D7D-59B6-4C74-B1AA-4A9D18AB6250.html>)
14. HUAWEI ROUTER CONFIGURE SNMP (Huawei <https://support.huawei.com/enterprise/en/doc/EDOC1000142088/5ea92ab7/snmp-configuration>)
15. UDP PROTOCOL (Wikipedia https://it.wikipedia.org/wiki/User_Datagram_Protocol)
16. SNMP PROTOCOL (Wikipedia https://it.wikipedia.org/wiki/Simple_Network_Management_Protocol)
17. MD5 CRITTOGRAFIA (Wikipedia <https://it.wikipedia.org/wiki/MD5>)
18. SHA CRITTOGRAFIA (Wikipedia https://it.wikipedia.org/wiki/Secure_Hash_Algorithm)

19. IPMI PROTOCOL (Wikipedia
https://en.wikipedia.org/wiki/Intelligent_Platform_Management_Interface)
20. ZABBIX TEMPLATE (Zabbix <https://share.zabbix.com/>)
21. SINMPLE NETWORK MANAGMENT PROTOCOL (Blogspot
<http://quotezg.blogspot.com/2014/07/simple-network-management-protocol.html>)
22.) SINMPLE NETWORK MANAGMENT PROTOCOL (P. Op de Beeck - De Nayer Instituut
http://telescript.denayer.wenk.be/~hcr/cn/idoceo/udp_snmp.html)

RINGRAZIAMENTI

Finalmente il giorno è arrivato: scrivere queste frasi di ringraziamento è il tocco finale della mia tesi. È stato un periodo di profondo apprendimento, non solo a livello scientifico, ma anche personale. Vorrei spendere due parole di ringraziamento nei confronti di tutte le persone che mi hanno sostenuto e aiutato durante questo periodo.

Prima di tutto, un ringraziamento particolare va al mio relatore, professor Fausto Marcantoni per i suoi preziosi consigli. Mi ha fornito tutti gli strumenti di cui avevo bisogno per intraprendere la strada giusta e portare a compimento la mia tesi.

A Paolo Gaspari per avermi aiutato a muovere i primi passi in questo fantastico mondo delle reti.

A tutto il personale del Cinfo di UNICAM dal Responsabile Maurizio Mauri ai suoi diretti collaboratori, per la loro fantastica collaborazione. Mi avete sostenuto e siete sempre stati pronti ad aiutarmi.

Al precedente responsabile dott. Luigi Tartabini ed al nuovo responsabile dott. Antonio Agostini dei Sistemi Informativi di ASUR MARCHE Area Vasta 3 che mi hanno dato la possibilità condurre la mia ricerca per la tesi di laurea.

Alla mia famiglia che mi ha spronato dopo anni dal conseguimento del Diploma Universitario di riiniziare questa avventura.

Alla mia fidanzata che mi è stata vicina in questo percorso fatto di molti sacrifici e rinunce.

Per ultimi ma non meno importanti, i miei colleghi di lavoro ed i miei amici.

Un sentito grazie a tutti!