Processi di monitoraggio e Nagios

Svilupparsi una rete complessa e distribuita

di apparati e servizi,

assicurare LdS decenti,

continuare a vivere senza frustrazioni

Inquadriamo la problematica

(e tanto per cominciare, fumate de meno che agli apparati fa male e al chiuso da fastidio!)

Gli obiettivi del monitoraggio

Il monitoraggio delle reti e dei sistemi consiste nella osservazione continua delle condizioni del traffico dati sulla infrastruttura, al fine di ***identificare colli di bottiglia*** *o di* ***risolvere criticità*** *dovute a problematiche hardware/software*

Non ci inventiamo l'acqua calda

- ✔ Codifica dei processi di monitoraggio, assistenza, supporto, documentazione e change management
- ✔ Adozione delle migliori pratiche (ITIL)
- ✔ Strumenti integrati
- ✔ Organizzazione + Process ownership
- ✔ Policy di esercibilità, promozione controllata
- ✔ Documentazione (knowledge base, configuration DB)
- ✔ Trouble ticketing parossistico di qualsiasi intervento
- ✔ Rigoroso governo dei change (di nuovo!)
- ✔ €, €, €, €, €, ...

Il Monitoraggio per la rete ninux

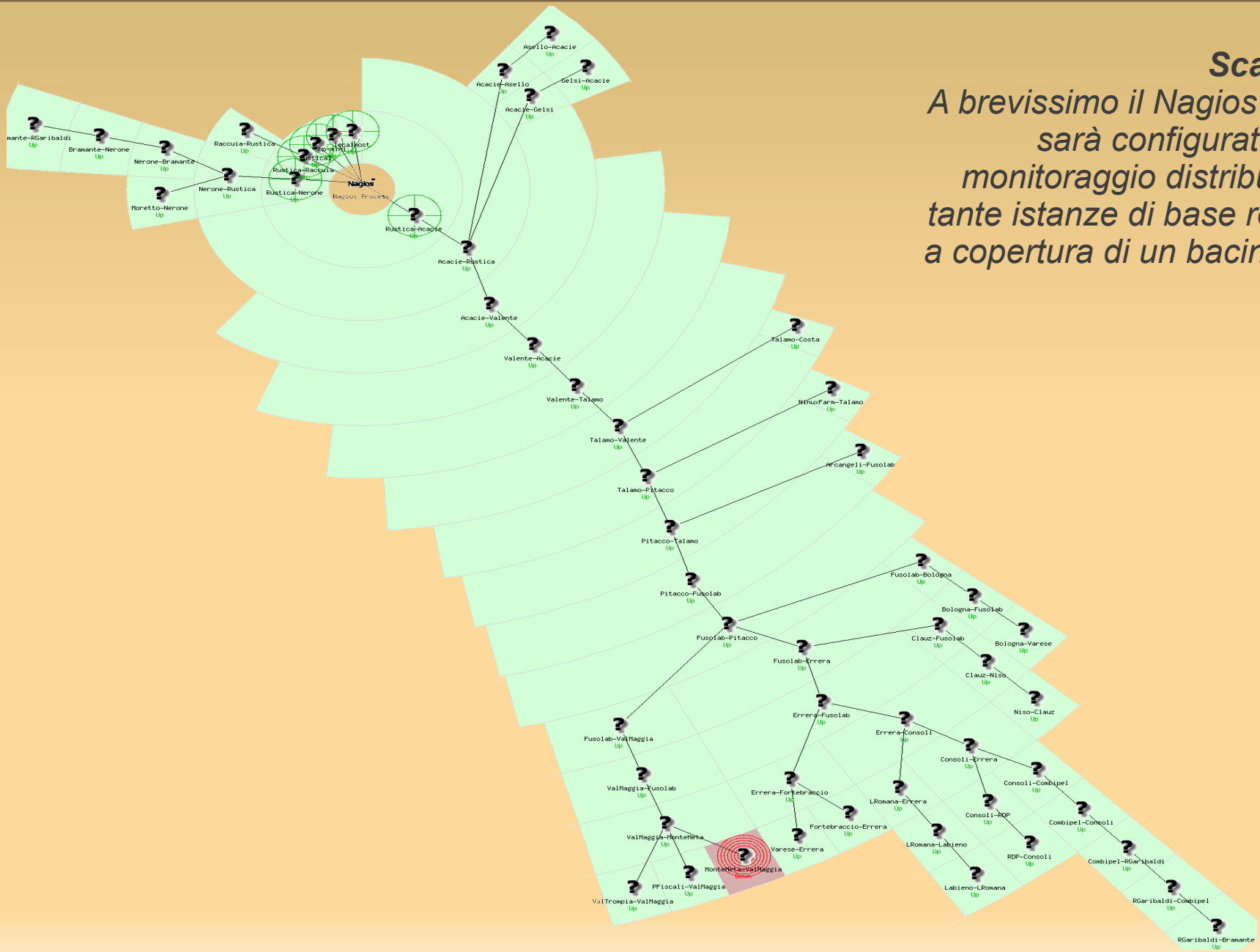
- ✔ VPN internazionali
- ✔ Streaming radio
- ✔ Hot spot WiFi
- ✔ Centralino VoIP (Asterisk)
- ✔ NAS
- ✔ Ping, web, ssh, mail, ...
- ✔ CPU load nei router
- ✔ Performance e altri aspetti legati alla modalità di trasmissione radio
- ✔ Intrusioni

Lo strumento Nagios

Introduzione a Nagios

- ✔ Monitoraggio sulla disponibilità dei servizi di rete: POP3, HTTP, FTP, SSH, ….
- ✔ Monitoraggio sistemistico: CPU, disco, RAM, processi, …
- ✔ Monitoraggio applicativo
- ✔ Gestione della topologia della rete e della gerarchia dei servizi
- ✔ Possibilità di definire script da attivare automaticamente per particolari eventi
- ✔ Nessun problema nel distribuire il monitoraggio su sedi diverse
- ✔ Definizione di raggruppamenti arbitrari dei monitoraggi: per servizio, tipologia di host, tipo di misura, collocazione geografica, ...
- ✔ Gestione dei fermi pianificati, per evitare allarmi durante le indisponibilità previste
- ✔ Visualizzazione e reportistica multidimensionale delle misure effettuate
- ✔ Gestione delle autorizzazioni e dei profili utente
- ✔ Integrabilità con altri strumenti e protocolli: MRTG, SNMP, portscan, cacti, ...

Screenshot della topologia (ninux Roma)



Scalabilità:
A brevissimo il Nagios di ninux sarà configurato per un monitoraggio distribuito, con tante istanze di base replicate, a copertura di un bacino locale

Alcune situazioni riconosciute

- ✔ FLAPPING
  - Questa situazione viene riconosciuta quando Nagios rileva una frequenza di cambio stato superiore a una data soglia massima (parametrica per servizio) sulle ultime 21 misurazioni effettuate
  - Il flapping viene segnalato in console con un messaggio e una icona specifici
  - Un servizio esce dal flapping quando la frequenza dei cambiamenti di stato torna inferiore a una soglia minima (parametrica per servizio)
- ✔ GESTIONE EVENTI
  - Nagios può essere esteso per gestire le transizioni di stati e conservarne traccia in un EventDB (è un modulo separato)
- ✔ MANUTENZIONE PROGRAMMATA
  - L'interfaccia Web di Nagios consente di specificare, per ogni host e ogni servizio definito, un calendario di manutenzioni programmate
  - Gli allarmi provenienti da un host/servizio in manutenzione non vengono considerati ne notificati
  - Il calendario interventi può anche essere prodotto con uno strumento esterno e importato in Nagios da file

Meccanismo di notifica degli alert

- ✔ Ogni oggetto host/service possiede un riferimento (nome) esplicito
- ✔ Uno o più riferimenti possono appartenere a un gruppo di contatto
- ✔ Quando si produce un allarme su un oggetto, Nagios provvede a inviare una notifica (mail, sms) a tutti i referenti previsti per il gruppo di contatto
- ✔ IMPORTANTE: in caso di **flapping** di un oggetto, Nagios smette di inviare notifiche fino alla normalizzazione della situazione.