DigitalExpert di Carloalberto Sartor - **Part. IVA 03345470243**
Cod.Fisc: SRTCLL60C19C372T - CCIAA - n. REA: VI – 317948
Sede Legale : Via Astichelli, 14 - 36031 Dueville (VI) – ITALY
tel/fax: 0444592675 - cell: 3492517691
Email: **info@digitalexpert.it** - Web Site : **www.digitalexpert.it**

Dueville 02/01/2011

SERVIZIO di MONITORAGGIO LAN E CONNETTIVITA'

DESCRIZIONE DEL SERVIZIO

Il servizio permette di implementare un controllo generale e dettagliato delle problematiche comunicative interne ed intersede allo scopo di identificarle, gestirle, risolverle, prevenirle.

Queste fondamentali esigenze del cliente trovano una risposta precisa nel Phalanx NOC (Network Operation Center) il quale viene istruito a controllare costantemente il regolare stato di funzionamento degli apparati attivi aziendali (switches, router, access point, firewall, bridges) e delle principali tratte comunicative, siano esse interne o inter-sede.

Il sistema permette al cliente di avere costante evidenza dello stato della sua rete e, a fronte di condizioni anomale, puo' recepire rapidamente l'evento critico attraverso segnalazioni grafiche o tramite altri canali comunicativi (indicazioni acustiche, email, sms, etc).

Contestualmente al controllo di regolare funzionamento, vengono anche raccolte indicazioni diagnostiche specifiche da ogni singolo dispositivo da monitorare (traffico, errori, congestioni, etc), consentendo una completa visione non solo degli eventi critici ma anche il recepimento di condizioni anomale relative a problematiche fisiche dei cavi, a problematiche comunicative a carico di singoli server o clients, a problematiche di connettivita' intersede/internet.

Inoltre il NOC, nella sua costante attivita' di controllo di ogni singolo apparato, effettua anche una precisa rilevazione delle tempistiche comunicative, permettendo un chiaro recepimento delle prestazioni dell'infrastruttura di rete e delle tratte comunicative verso le sedi remote e l'infrastruttura pubblica.

Infine, all'interno del NOC sono presenti particolari strumenti software in grado di eseguire “on demand” una serie di sofisticate diagnosi aggiuntive ed approfondite, con cui rilevare qualunque problematica comunicativa interna o intersede. Tra gli altri, sono disponibili strumenti di misura della banda, generatori di carico, scanner di vario tipo, tools per la raccolta di statistiche di rete su singoli nodi, etc...

Va inoltre aggiunto che il NOC Phalanx, puo', a necessita', attivare tutti gli altri servizi caratteristici del framework Phalanx, permettendo quindi al cliente di affrontare con serenita' qualunque problematica aziendale sia sul fronte comunicativo che sistemistico.

Il servizio, tramite accesso remoto da parte del fornitore, permette “on demand” o tramite allarme automatico, un rapido intervento e una immediata comprensione dello stato della rete del cliente, consentendo quindi una tempestiva risposta consulenziale orientata all'identificazione e soluzione dei problemi esistenti.

Il presidio include un controllo della sicurezza interna (IDS) ed un inventario aggiornato delle interfaccie di rete presenti nell'infrastruttura aziendale, con archiviazione storica di tutti gli accessi identificati.

L'esperienza vasta ed eterogenea in questo tipo di implementazioni ci permette una rapida identificazione e soluzione delle problematiche del cliente.

DETTAGLI TECNICI

Il NOC Phalanx - E' realizzato tramite un pc (o un appliance) contenente il sistema operativo Linux ed il software apposito (Phalanx Framework).
L'accesso al servizio si effettua tramite un comune web browser senza necessita' di alcun software aggiuntivo.
L'accesso puo' essere effettuato anche da remoto, anche da cellulare.
L'implementazione standard permette di gestire reti di piccole e medie dimensioni (fino a 5.000 nodi).

OGGETTI MONITORATI - Tipicamente gli apparati su cui e' attivo il protocollo SNMP.
In subordine, anche se con minore dettaglio diagnostico, qualunque oggetto di rete, anche se non pingabile.
E' possibile attivare anche un monitoraggio "agent-based" per server o clients (windows, linux, etc) con cui rilevare condizioni sistemisiche ed applicative di particolare efficacia e profondita'.

RILEVAZIONI SNMP - Tramite il protocollo SNMP e' possibile effettuare una sofisticata serie di rilevazioni diagnostiche, di traffico e prestazionali, tra le quali sottolineiamo quelle standard, cioe':

- bytes/secondo in ingresso e in uscita, separatamente
- packtets/secondo in ingresso e in uscita, separatamente
- errori/secondo in ingresso e in uscita, separatamente
- accodamenti in uscita

MAPPER SNMP - Tramite il mapper e' possibile ottenere automaticamente l'esatta interconnessione logica/elettrica delle interfaccie di rete. Ad esempio e' possibile avere l'indicazione dello switch e della rispettiva porta a cui e' connesso ogni oggetto di rete. Cio' permette di evitare lunghe e difficoltose verifiche del percorso di un cavo per avere esatta indicazione della sua collocazione.

INVENTARIO DI RETE - Durante l'utilizzo del NOC, viene contemporaneamente effettuata una accurata registrazione di tutti gli accessi fisici e logici alla rete, tramite catalogazione di ogni MAC Address connesso alla rete locale e relativa tipologia di accesso (protocollo, ultima frame transitante, etc).
In questo modo si crea automaticamente un inventario di rete, comprensivo di:

- mac address
- vendor (costruttore della scheda di rete)
- eventuale indirizzo IP, se assegnato/definito
- data e ora dell'ultimo accesso
- ultimo protocollo IP utilizzato
- ultima frame transitante da/per il nodo

INVENTARIO PROTOCOLLI - Il sistema effettua anche una contemporanea registrazione di tutti i protocolli attivi in rete, con indicazione precisa e puntuale dell'ultima attivita' effettuata per ognuno dei protocolli identificati. Cio' permette di effettuare una accurata valutazione della tipologia di traffico circolante, rendendo agevole l'identificazione di problematiche legate al traffico o alla non corretta configurazione di apparati e servizi di rete.

IDS – Intrusion Detection
Nel NOC e' attivo un particolare controllo di sicurezza che registra tutte le connessioni in essere all'interno della rete aziendale. Cio' permette di identificare anche eventuali connessioni anomale.

BENCHMARK DI RETE
Sono presenti strumenti per effettuare accurate misure di portata delle tratte comunicative locali/intersede.
Cio' permette di verificare l'esatta modalita' di risposta comunicativa, permettendo di identificare l'esistenza di condizioni di congestione, microinterruzione, degrado.

ALCUNE OPZIONI AGGIUNTIVE *nota 1)

TACHIMETRO CONNETTIVITA'
E' possibile visualizzare in tempo reale un indicatore di performance della connettivita' espressa in Mbit/secondo e pacchetti/secondo (download/upload) come pure riportare in un grafico apposito l'andamento nel tempo di questo importantissimo parametro.

TACHIMETRO LAN *nota 2)
Tramite una accurata definizione dei sensori Phalanx, e' possibile generare un pannello con indicazioni prestazionali relative alla LAN nel suo complesso o di specifiche aree. Anche in questo caso e' possibile riportare Mbit/secondo e/o Pacchetti/secondo.

TACHIMETRO SERVER *nota 3)
Questo servizio riporta in sintesi o in dettaglio il traffico emesso o ricevuto da ogni singolo server, oltre all'esistenza di errori, ritrasmissioni, intasamenti.
Indispensabile strumento per avere un quadro accurato del peso di ogni server e di eventuali anomalie comunicative relative agli stessi.

TACHIMETRO CLIENTS *nota 3)
Questo servizio riporta in sintesi o in dettaglio il traffico emesso o ricevuto da ogni singolo client, permettendo una accurata valutazione delle dimensioni e problematiche di connessione e di sistema esistenti all'interno di ogni singolo client.

ANALISI DEL TRAFFICO REALTIME
E' possibile visualizzare in dettaglio la composizione del traffico transitante in rete.
In particolare possiamo visualizzare tabelle riportanti percentuali di traffico suddivise per:

- tipologia di protocollo
- porte (IPV4/IPV6)
- sorgente e destinazione
- dimensione frames
- congestione

DIAGNOSI MPLS
Questo particolare ed esclusivo strumento effettua una sofisticata analisi della composizione strutturale e prestazionale della MPLS, registrando ed evidenziando in tempo reale eventuali variazioni strutturali o prestazionali di questa connettivita', spesso causa (ad insaputa della stessa Telecom) di anomalie subdole di difficile identificazione e correlazione.
Lo strumento nasce dall'esperienza diagnostica specifica e ci ha permesso in molte occasioni di risolvere gravi e ripetuti problemi legati a questa connettivita' o, al contrario, di escludere l'elemento “connettivita'” dalle cause di specifiche anomalie lamentate dal cliente.

CATALOGO UTENTI WINDOWS/SMB
Questo interessante tool permette di catalogare gli utenti windows esistenti in rete, anche nel caso essi operino da clients non gestiti dal Domain Controller aziendale o nel caso in cui utilizzino utenze non gestite o non conosciute. Lo strumento raccoglie queste indicazioni anche nel caso in cui il cliente non utilizzi un domain controller aziendale. Questo strumento si integra con l'analisi del traffico realtime e con l'inventario di rete.

NOTE:
Nota 1) a seconda delle attivita' in carico al NOC, questa opzione potrebbe richiedere un pc client dedicato separato o un client di maggiori capacita'
Nota 2) questo strumento puo' operare in sinergia con Tachimetro Server
Nota 3) servizio “agent-based” che richiede il servizio di Monitoring e l'installazione dell'agente Phalanx su ognuno dei server fisici/virtuali