WÜRTHPHOENIX NetEye

WÜRTHPHOENIX NetEye 2011 – 2012

State of direction paper

Agosto 2011

WÜRTHPHOENIX NetEye 2011

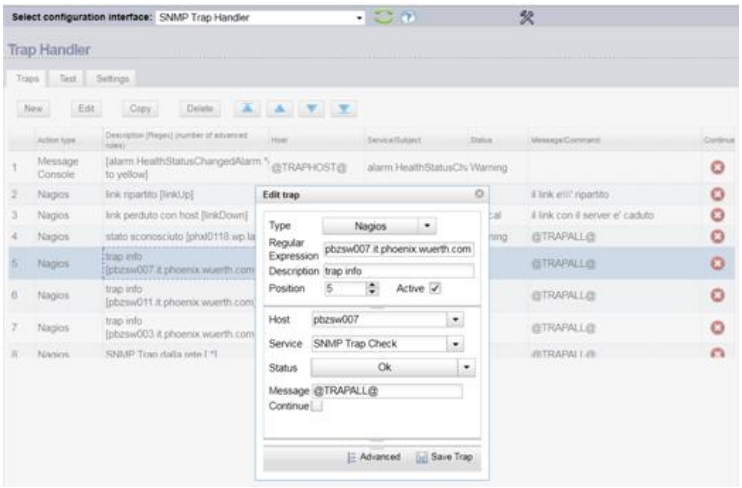
Monitoraggio dei processi aziendali orientato agli standard ITIL

NetEye si orienta sempre di più verso gli standard ITIL.

È stato introdotto un nuovo modulo per avere un maggior livello di astrazione per la definizione dei diversi servizi informatici.

È possibile strutturare le dipendenze dei servizi IT con i vari componenti dell'infrastruttura. In questo modo si simulano gli impatti che si possono riscontrare a livello business ad esempio a causa di un'anomalia di un server. È quindi possibile avere il risultato specifico sul livello di servizio erogato con delle statistiche accurate sulla disponibilità dei processi (spesso necessari per i Service Level Agreements).

Gestione degli SNMP Traps con un handler specifico



L'SNMP trap handler fornisce un modo semplice per configurare le azioni da intraprendere qualora vengano ricevuti degli SNMP traps.

È infatti possibile specificare dei matching-rules per identificare le SNMP Traps, per estrarle ed interpretare le informazioni in esse contenute. Questi dati possono poi essere utilizzati per notificare la message console host o il Nagios Service Check Acceptor (NSCA).

Monitoraggio dei client Windows con NSClient++ 0.3.8

La nuova versione 0.3.8 di NSClient++ è stata integrata in NetEye. Nell'Agent, utile per il monitoraggio delle attività in ambiente Microsoft, sono state introdotte nuove funzionalità quali una maggior semplificazione sul controllo degli event log, nuovi controlli del registro o miglioramenti sul controllo dei file. Vengono supportati, inoltre, performance counter multilingue e automatic volumes. Infine è stata svolta una semplificazione degli scripting con un nuovo VB Helper.

Una maggiore scalabilità con l'integrazione di Mod Gearman

La scalabilità dell'area di monitoraggio di NetEye è gestita in modo automatico per garantire un miglioramento lineare sul numero di possibili esecuzioni di controllo con delle risorse adeguate (ad esempio si possono ora svolgere oltre 100.000 checks).

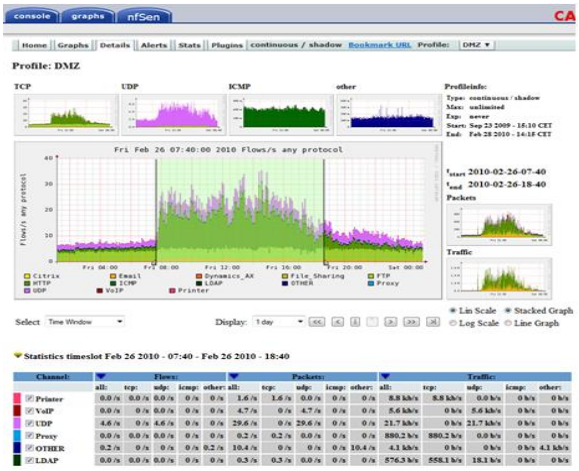
Per poter incrementare le prestazioni e il numero di possibili controlli processati in Nagios, NetEye ha introdotto l'utilizzo di Gearman e ModGearman, che riescono a programmare il controllo dei servizi e host in Nagios.

ModGearman è un nuovo modo di gestire la distribuzione dei controlli della rete attivi in Nagios. Comprende il modulo NEB, che si trova nel core stesso di Nagios, e che aggiunge controlli sui servizi, sugli host e event handler alla coda Gearman.

Gearman fornisce un framework generico che reindirizza il carico di lavoro ad altre macchine o ad altri processi che si possono adattare in modo migliore alle singole attività. Permette perciò di avere attività in parallelo, di bilanciare i vari processi e invocare specifiche funzioni attraverso i vari linguaggi.

L'introduzione di questo nuovo motore eleverà quindi la qualità di monitoraggio di NetEye, portandolo ad un livello Enterprise, permettendo un controllo di molti più servizi e host attraverso l'utilizzo di un solo sistema.

ntop e nBox: un'analisi dettagliata sull'utilizzo del traffico di rete



Se state cercando uno strumento che oltre a monitorare la rete sia anche in grado di analizzarla in dettaglio, ntop è la soluzione per le vostre esigenze. Con il modulo di ntop integrato in NetEye infatti è possibile visualizzare dati e grafici su chi, per esempio, sta utilizzando la rete, chi sta visitando un sito web specifico o chi sta generando un traffico di dati maggiore.

nBox è un'appliance in grado di analizzare il traffico di rete ed esportare dati attraverso il protocollo di comunicazione Cisco NetFlow™.

La capacità di qualificare il traffico IP può portare degli aspetti critici in ambito di disponibilità e performance. A questo proposito nBox offre una soluzione scalabile, gestibile e affidabile per fornire i dati e le informazioni necessarie per l'ottimizzazione e risoluzione dei problemi a livello della rete. nBox include sia una sonda NetFlow™ (nProbe) sia un collettore (ntop) per flussi v5/v9/IPFIX NetFlow™.

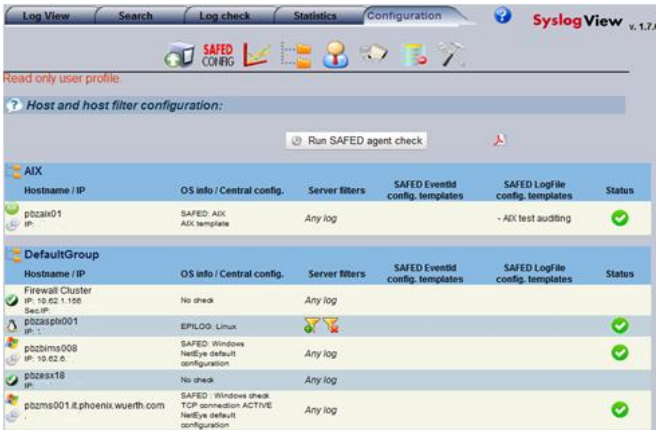
Ottimizzazione del modulo Syslog grazie al nuovo Safed Agent

In base alle richieste effettuate dagli utenti stessi, è stato deciso di effettuare dei significativi miglioramenti alle funzionalità del Syslog, modulo volto a soddisfare il provvedimento del Garante della Privacy. Würth Phoenix ha sviluppato internamente un agente Open Source denominato Safed (Security Auditing ForwardEr Daemon) utilizzato per l'archiviazione dei logs di accesso degli amministratori di sistema per il modulo Syslog.

Le principali caratteristiche sviluppate per il Safed Agent sono:

- Controllo della comunicazione tra l'Agent e il server syslog
- Ottimizzazione del motore di ricerca
- Configurazione del Safed Agent attraverso una semplice interfaccia web
- Rilevamento automatico dei ruoli degli amministratori Windows
- Configurazione centralizzata degli agenti sul server NetEye
- Identificazione con numerazione progressiva dei messaggi
- Possibilità di effettuare una ritrasmissione automatica dei messaggi in caso di errori
- Possibilità di ritrasmettere su richiesta messaggi mancanti
- Meccanismo di caching configurabile
- Trasmissione degli eventi attraverso comunicazione crittata TLS/HTTPS

Semplicità di gestione: configurazione centralizzata per il Safed Agent



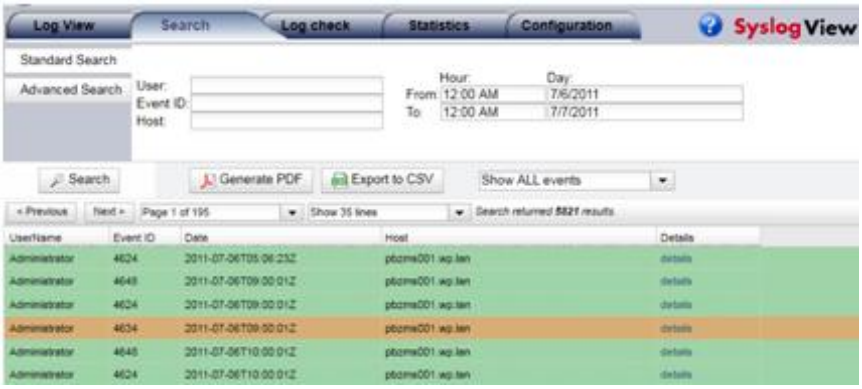
Per riuscire a facilitare il più possibile la gestione del modulo syslog, è ora possibile configurare e aggiornare automaticamente e in modo centralizzato tutti i Safed Agent installati nell'infrastruttura.

L'installazione viene semplificata grazie ad un unico file MSI eseguibile che non necessita di alcuna interazione da parte dell'utente.

Maggior sicurezza per il modulo Syslog: controllo di integrità dei Logfile

Per essere certi di adempiere pienamente al provvedimento del garante della privacy bisogna poter disporre di un controllo sicuro sull'integrità dei files archiviati nel modulo Syslog di NetEye. A questo proposito è stata definita una strategia efficiente che controlla l'integrità basandosi sul numero sequenziale dei file di log. Infatti nel caso in cui questa sequenza non è continua le linee mancanti vengono recuperate dal Safed Agent e un controllo finale assicura il corretto completamento dell'attività.

Prestazioni più performanti con il nuovo motore di ricerca per il Syslogview



Con la finalità di ottenere prestazioni più elevate dal motore di ricerca del Syslogview è stata introdotta una nuova tecnologia che si basa sul progetto Open Source Apache Lucene™.

Invece di compiere ricerche su ogni file basandosi su schemi specifici con Apache Lucene™ è possibile utilizzare un'indicizzazione altamente performante e di utilizzare algoritmi di ricerca accurati ed efficienti.

Sarà possibile con questa versione compiere ricerche utilizzando parametri come il nome utente, il nome dell'host, il tipo di evento (login, logout, login failure), data e ora, ed esportare i risultati in formato pdf o CSV per eventuali analisi.

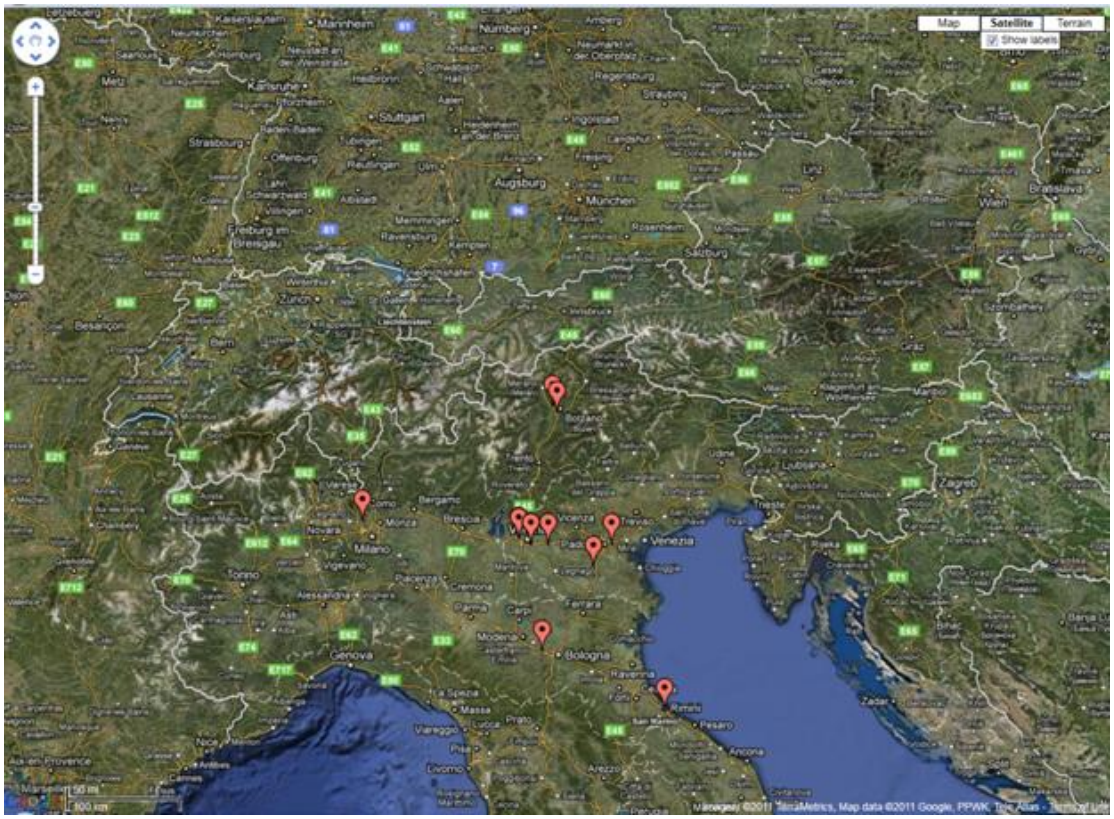
Nuova reportistica per gli eventi Syslog

Per ottenere una panoramica sui dati di log come il numero di linee archiviate giornalmente per ogni host registrato o i valori delle medie settimanali, mensili e annuali con la loro rappresentazione grafica è stata introdotta la sezione "Statistics".

Questa reportistica infatti fornisce una visualizzazione più generale rispetto al FileLog View che mostra solamente il contenuto dei singoli files di log. È infine anche possibile generare le statistiche in formato pdf per poterle inviare automaticamente via email ad un elenco di destinatari predefinito.

Nagmap: integrazione di Google Map in NetEye

Per visualizzare la topologia della rete in base alle informazioni del config e status file di Nagios, è stato integrato in NetEye Nagmap, un'applicazione Nagios che usa l'API di Google Maps.



Integrazione di OTRS in NetEye: Sistema di Service Desk e Ticketing basato sugli standard ITIL

Per una gestione più strutturata e trasparente di tutte le messaggistiche di errore e richieste di supporto da parte degli utenti è stato introdotto OTRS. OTRS è un software Open Source che gestisce una vasta gamma di processi aziendali, dall'Help Desk al supporto alla gestione dei servizi IT.

Basandosi su un set di funzionalità sviluppate intorno al concetto di "trouble ticket", OTRS è stato progettato per consentire ai dipartimenti di supporto, vendita, pre-vendita, fatturazione, IT e support desk di reagire tempestivamente e responsabilmente ad ogni richiesta in entrata.

NUOVI SVILUPPI NEL 2012

Sicurezza della rete con PacketFence

Per una maggior sicurezza delle reti - dalle più semplici alle più complesse - è stato integrato PacketFence, un sistema Open Source per i controlli degli accessi in rete.

PacketFence è dotato di una serie impressionante di funzionalità tra cui un captive portal per la registrazione e remediation, una gestione centralizzata delle reti wired e wireless, supporto 802.1X, isolamento layer-2 delle problematiche sui vari dispositivi, integrazione con Snort IDS e Nessus per la scansione della vulnerabilità.

Controllo del sistema di monitoraggio con SMS Watchdog

Anche un sistema di monitoraggio necessita di essere controllato per garantirne la disponibilità. A questo proposito è stata definita una nuova strategia per monitorare costantemente lo status di NetEye.

In caso l'applicazione riscontra alcune anomalie, un SMS automatico viene inviato come notifica. Per essere veramente efficiente questo meccanismo ovviamente non può trovarsi sull'appliance di NetEye stesso, viene perciò installato sull'SMS Gateway box, che lavora in modo totalmente indipendente.

Inoltre, NetEye compie continuamente dei ping verso l'SMS Gateway attraverso una porta seriale per garantirne la disponibilità.

Nuove funzionalità per il modulo Syslog

Il modulo Syslog verrà ulteriormente sviluppato per aumentarne le funzionalità, come l'amministrazione SSL, LogFiles/Directories SizeView, Statistiche sulle dimensioni, monitoraggio automatico di Nagios (Server, Agent) e integrazione Unix Audit + Rulebase.

Un maggior controllo per il Security Management con NAC – NetMon

Il modulo di Security Management viene rafforzato grazie ad una capacità di monitoraggio degli accessi in rete più estesa. Infatti è stato integrato PacketFence (SNORT, Netflow plugin policy editor), è stato fatto il port di NetMon alla nuova GUI e il demonize di NetMon check.

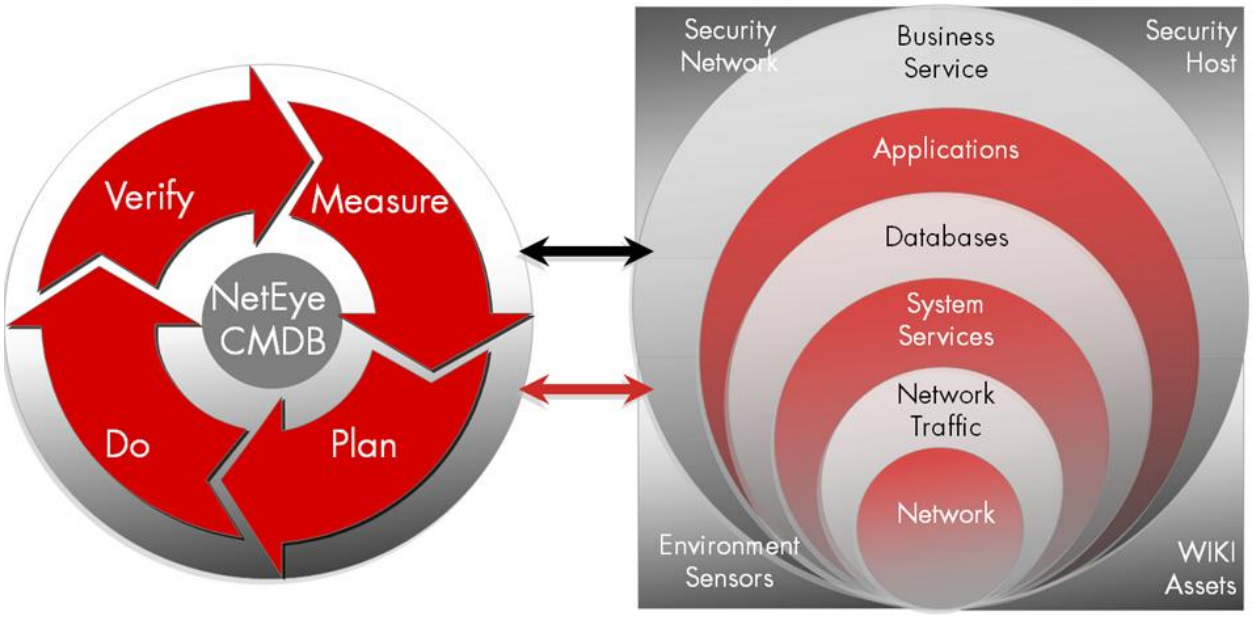
Integrazione della nuova versione di OTRS

In NetEye verrà integrata la nuova versione di OTRS - 3.0.7 e OTRS ITSM - 3.0.4, che includerà un aggiornamento automatico attraverso RPM, l'installazione dei moduli OTRS attraverso RPM, una CMDB per asset loading da GLPI e monitoring config generation.

IT Service Management con CMBD centrale

La visione a medio termine per NetEye è quella di creare uno strumento di IT Service Management con un CMBD centrale per supportare i processi ITIL dalle seguenti diverse prospettive:

- Monitoraggio della rete
- Monitoraggio del traffico della rete
- Monitoraggio dei sistemi e servizi
- Monitoraggio database
- Monitoraggio delle applicazioni e prestazioni
- Monitoraggio dei servizi aziendali
- Monitoraggio della sicurezza di rete e host
- Monitoraggio ambientale
- Documentazione



Aggiornamenti automatici del sistema con Centos

Vi sarà la possibilità di compiere aggiornamenti automatici del sistema operativo con l'utilizzo di Centos 5 + php update e Centos 6 per i moduli:

- RRD tools / RRD cache
- PNP
- NagVis
- GLPI
- OCS Inventory
- Dokuwiki
- Cacti

NfSen per il Network Traffic monitoring

NfSen è un'interfaccia grafica web-based nata per la gestione dei flussi di dati attraverso apparati di rete, mediante l'analisi delle informazioni prodotte tramite il protocollo NetFlow.

Con NfSen è possibile visualizzare i dati del flusso di rete: flussi, pacchetti e bytes utilizzando RRD (Round Robin Database); navigare con facilità attraverso i dati dei flussi di rete; processare i dati dei flussi di rete all'interno di un lasso di tempo specifico; creare profili storicizzati; configurare alerts in base a diverse condizioni e scrivere plugins propri per processare i dati del flusso di rete in intervalli regolari.

Nella nuova versione verrà aggiornato il PortTracker plugin, l'AS plugin (sistema autonomo) e gli alerts con SNMP traps.

Nuovi templates per velocizzare la configurazione di monitoraggio

Saranno inseriti nuovi templates per facilitare e velocizzare la configurazione del monitoraggio in NetEye per i seguenti sistemi:

- Microsoft Exchange
- Microsoft Sharepoint
- MSSQL
- Oracle
- OS (Windows, Linux, AIX, HPUX, Sun Solaris, AS400)
- Hardware (IBM, HP, Dell, Fujitsu)

Action Handler per gli operatori del Service Desk

Per permettere l'invio automatico di comandi agli operatori del Service Desk verrà realizzato un Action handler.

Attraverso una semplice interfaccia grafica sarà possibile inviare comandi multipli predefiniti con utente amministrativo o estemporanei con utente non amministrativo sui server controllati, predefiniti o selezionati al momento.

Inoltre vi sarà la possibilità di utilizzare uno schedulatore (cron) di comandi o batch, con invio automatico sull'esito dell'azione.

Test automatici con Selenium

Selenium è un software Open Source che permette di svolgere test automatici per applicazioni web.

Fornisce la possibilità di svolgere dei test registrando ed eseguendo azioni su pagine web. Selenium offre un DSL (domain specific language) per scrivere test cases in diversi linguaggi di programmazione come C #, Java, Groovy, Perl, PHP, Python e Ruby. I test di Selenium possono essere eseguiti sui più comuni web browser su piattaforme Windows, Linux e Macintosh.

L'ultima novità è Selenium Grid che consente di eseguire simultaneamente diversi test in diversi sistemi locali o remoti, minimizzando il tempo di esecuzione.

Nuova interfaccia grafica Web frontend

In NetEye viene implementata una nuova interfaccia grafica web per i moduli di:

- Monitoraggio dei processi aziendali
- Configurazione di base dell'appliance (Sendmail, Configurazione della rete, servizi NetEye status/stop/start/restart, KVM/IPMI Ip config, Filesystem status/enlarge, Gearman/Modgerman, NSCA Config, NRPE config)
- SSO (Multiple LDAP, Kerberos, OpenLDAP)
- Autorizzazioni (Accessi di base solo per la homepage di NetEye, nuovi accessi di monitoraggio (Nagios), definizione del profile utente per applicazioni di default)
- Sidebar menu
- Nuova GUI Nagios (Trunk)

NetEye diventa mobile

Per poter accedere in ogni momento ed in ogni luogo a NetEye è stato sviluppato un web client con un'interfaccia grafica per i più comuni smart phones (iPhone, Android).

WÜRTHPHOENIX NetEye 2011: SUCCESSO NEL MERCATO ITALIANO

WÜRTHPHOENIX NetEye nel corso del 2011 ha ulteriormente sviluppato la propria presenza sul mercato italiano. Interamente sviluppato in Italia, da Würth Phoenix, unico Nagios Enterprises partner su suolo nazionale, il sistema si è dimostrato una valida alternativa Open Source ai pacchetti offerti da note case informatiche che operano a livello internazionale. Infatti oltre 150 aziende hanno scelto NetEye tra cui marchi rinomati quali Diesel, Ferrari Spumanti, Tecnica, Lotto, Subaru Italy, Technogym.

Rimaniamo a vostra disposizione per qualsiasi ulteriore informazione.

I nostri contatti:

Würth Phoenix S.r.l.
Via Kravogl, 4
39100 Bolzano

Telefono: +39 0471 56 41 11
Fax: +39 0471 56 41 22

E-mail: info@wuerth-phoenix.com
Website: http://www.wuerth-phoenix.com/neteye
Blog: http://www.neteye-blog.it/