Script di monitoraggio dei flussi SMTP

IceWarp Server tiene traccia di numerose statistiche relative alle operazioni svolte dai servizi. Tra le tante informazioni che risultano accessibili ad un amministratore di sistema possono risultare di non trascurabile utilità le statistiche del servizio SMTP. Verificando il quantitativo di messaggi inviati o ricevuti dal server in diversi periodi e confrontandoli fra di loro è possibile avere utilissime indicazioni sull'andamento del traffico e, soprattutto, avvisaglie di potenziali situazioni di criticità.
Con questa guida desideriamo presentare uno **script** creato proprio allo scopo di sfruttare le statistiche del servizio SMTP, estraendone le informazioni più significative, aggregandole e producendo un rapporto da inviare ad un destinatario che si occupi della loro interpretazione e che sia eventualmente pronto ad intraprendere azioni di contenimento dei casi di criticità evidenziati.
Ipotizziamo che il traffico possa essere descritto da un modello di distribuzione normale.

Specifiche di funzionamento

Lo script si occupa di segnalare situazioni anomale di uno dei seguenti indicatori:

SMTP_RECVD_MSGS: messaggi ricevuti;
SMTP_SENT_MSGS: messaggi inviati;
SMTP_RELAY_MSGS: messaggi inviati all'esterno;

SMTP_RECVD_MSGS_W,
SMTP_SENT_MSGS_W,
SMTP_RELAY_MSGS_W: stessi dati ma riferiti ai soli giorni feriali (lunedì - venerdì).

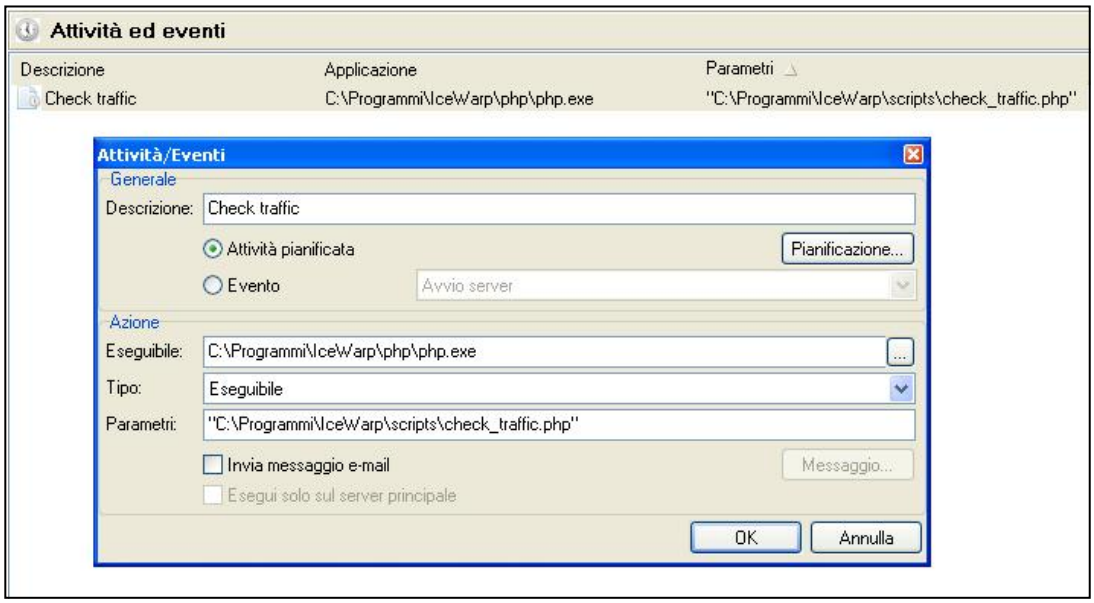
Nello specifico le situazioni “sospette” che vengono segnalate sono:

- quando il valore attuale si discosta di più del doppio dello scarto quadratico medio dalla media
- quando un account in un giorno ha inviato all'esterno più messaggi di un limite stabilito

FAST*flow* S.r.l. – IceWarp Italia
Via A. Manzoni, 25 – 22040 Lurago d’Erba (CO)
Tel. 031-697457, Fax: 031-2280459
e-mail: info@icewarp.it - web: www.icewarp.it

Installazione dello script

Lo script può essere inserito in una posizione qualsiasi sulla macchina che ospita IceWarp Server ma è necessario che la sua esecuzione sia schedulata per mezzo della apposita funzionalità integrata nel Server, disponibile al percorso [Sistema > Strumenti > Attività ed eventi].



Lo script può essere eseguito più volte al giorno. In occasione della prima esecuzione vengono aggiornati i valori statistici e verificati i limiti mentre successivamente vengono verificati i soli limiti di invio e la corrispondenza delle previsioni.

Nel file *check_traffic.php* sono definiti i due valori che vengono presi come riferimento per generare le notifiche e che possono essere modificati secondo preferenze.

La configurazione di default è:

```
define("MAX_RELAY", 100 );
define("DAYS_OF_DATA", 15 );
```

Nella prima riga si definisce il limite di messaggi inviati all'esterno in un giorno per singolo account, superato il quale viene generata una segnalazione.

Nella seconda riga è invece definito l'intervallo di giorni per i quali le statistiche vengono raccolte e analizzate. Per questo valore è consigliato non scendere al di sotto dei 15 giorni per avere un insieme consistente di valori campione.
E' inoltre necessario definire i dettagli per l'invio del messaggio di rapporto

```
$com->RemoteHost = "localhost";     //quale SMTP utilizzare per l'invio
$com->Helo = "localhost";           //con che nome presentarsi in sessione

$com->FromName = "Statistics";      //nome mittente negli header del
messaggio
$com->FromAddress = "admin@demo.com";     //indirizzo mittente negli header

// Mittente e Destinatario dichiarati in sessione
$com->MailFrom = "admin@demo.com";
$com->AddRecipient("user@demo.com", "Monitoraggio");

$com->Subject = "Loganalyzer Statistics Alert"; //Oggetto del messaggio
```

I messaggi generati avranno la seguente forma:

```
SMTP_RECVD_MSGS_W scostamento oltre il limite V:2387 M:3335.42857143 S:319.289101932
Account user@domain.com inviati: 445 messaggi
```

Legenda:

V = Valore attuale;
M = Media nel periodo definito;
S = Scarto quadratico medio.