Introduzione alla consultazione dei log tramite IceWarp Log Analyzer

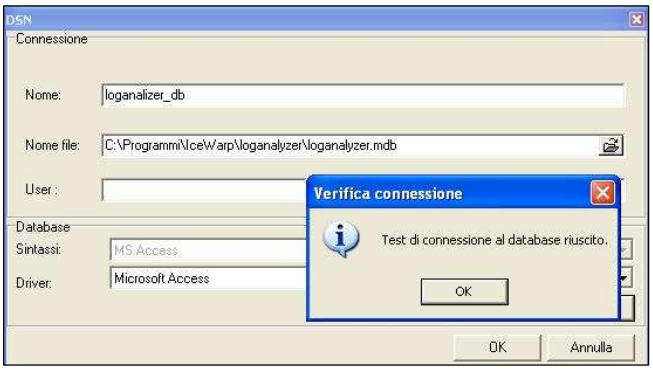
L'Analizzatore di Log è uno strumento che consente un'analisi statistica e logica dei file di log generati dal server.
Lo strumento permette principalmente due tipi di attività:

- analisi di log generati dal server previa importazione degli stessi
- analisi diretta di un file di log

La prima attività comporta l'esecuzione di una serie di analisi anche approfondite su molti elementi coinvolti nelle comunicazioni che passano dal server mentre la seconda permette di prendere in esame un file di log ed estrapolarne le sessioni fornendo pochi essenziali parametri di ricerca.

Database

La configurazione di default dello strumento prevede l'utilizzo di un database di appoggio Microsoft Access che è adeguato per installazioni con bassi volumi di traffico mentre per installazioni di elevate dimensioni è bene considerare la possibilità di usare soluzioni database più performanti come MySQL o MS SQL.
Nella definizione del Database Source Name è sempre bene indicare l'opportuno driver (nativo quando possibile) e la corretta sintassi.
E' poi bene verificare che la connessione sia corretta e funzionante e tentare un'importazione manuale verificandone l'esito nel log "Analizzatore di log".



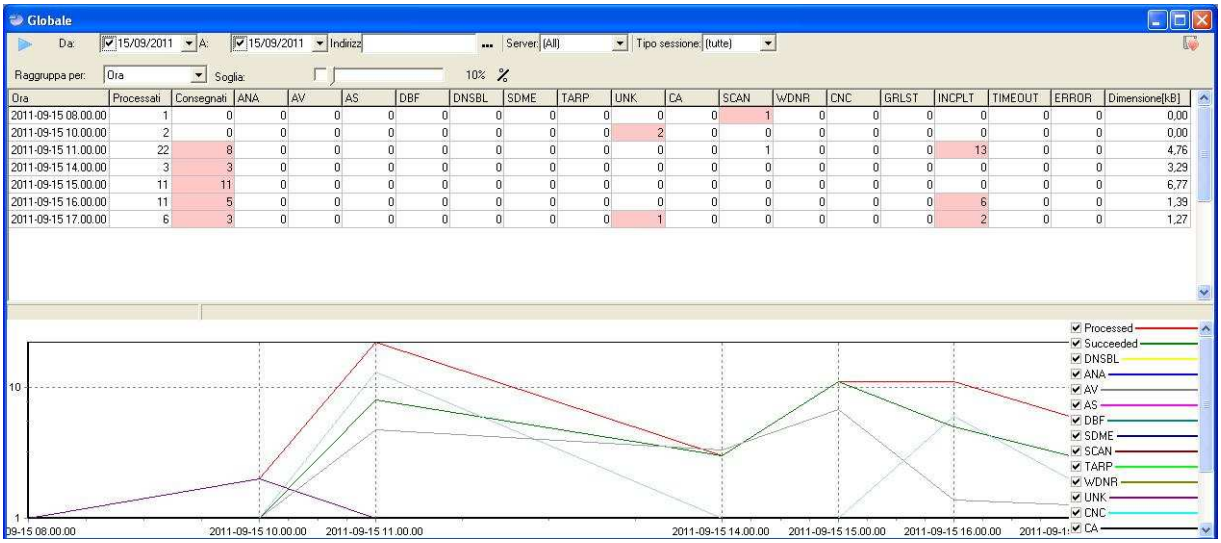
Importazione

Il processo di importazione dei log generati dal server è automatizzato e avviene ogni giorno alle ore 01:00. Sono quindi sempre disponibili i log fino al giorno precedente, ma si può comunque procedere ad un'importazione manuale per mezzo della funzione [Stato > Analizzatore di log > Importa adesso]. E' sufficiente fare doppio clic sul giorno desiderato per importare i log selezionati nell'apposito riquadro.

Dopo aver importato i log desiderati è possibile accedere all'interfaccia principale del Log Analyzer (il viewer) facendo clic sull'apposito pulsante.
L'interfaccia si presenta con una colonna sinistra (v. figura) nella quale viene mostrato l'albero di accesso alle varie sezioni del software.

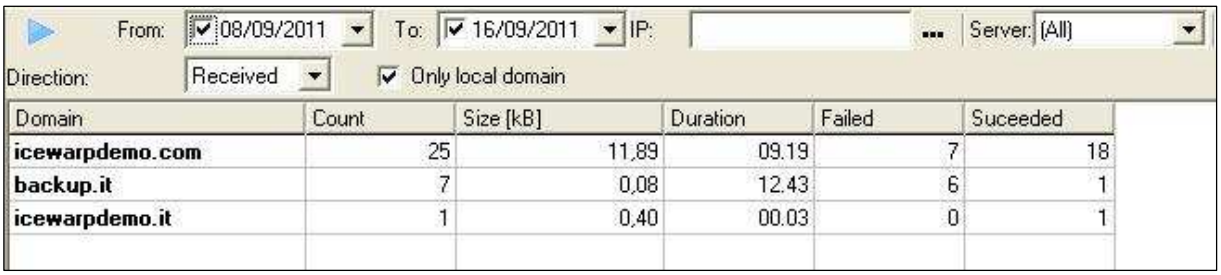
Statistiche

Questa sezione consente di produrre un'analisi statistica delle sessioni comprensiva di grafici temporali.



Per produrre il resoconto statistico è necessario definire un intervallo di tempo per cui siano stati importati almeno i log degli estremi temporali. Tra le impostazioni principali è da tenere in considerazione la possibilità di effettuare un filtraggio per IP, per tipologia di sessione (server/client) e la possibilità di raggruppare la statistica per differenti unità di tempo (ora, giorno, settimana, mese).

Oltre a produrre statistiche globali e filtrate per indirizzo IP è anche possibile raggrupparle per dominio e per account, così da avere un dettaglio dell'attività che tiene conto delle divisioni di appartenenza degli utenti che fanno uso del server.



Domain	Count	Size [kB]	Duration	Failed	Suceeded
icewarpdemo.com	25	11,89	09.19	7	18
backup.it	7	0,08	12.43	6	1
icewarpdemo.it	1	0,40	00.03	0	1

Account	Count	Size [kB]	Duration	Failed	Succeeded
N/A	3	0,92	00.05	2	1
user2	1	0,41	00.02	1	0
adminit	1	0,40	00.03	0	1
admin	1	0,42	00.01	1	0

E' altresì possibile avere una statistica delle durate delle varie tipologie di sessione (es: AS = Antispam, ERROR = Errore generico, INCPLT = Sessioni incomplete, etc.).

Duration

From: 08/09/2011 To: 16/09/2011 IP: ... Server: (All

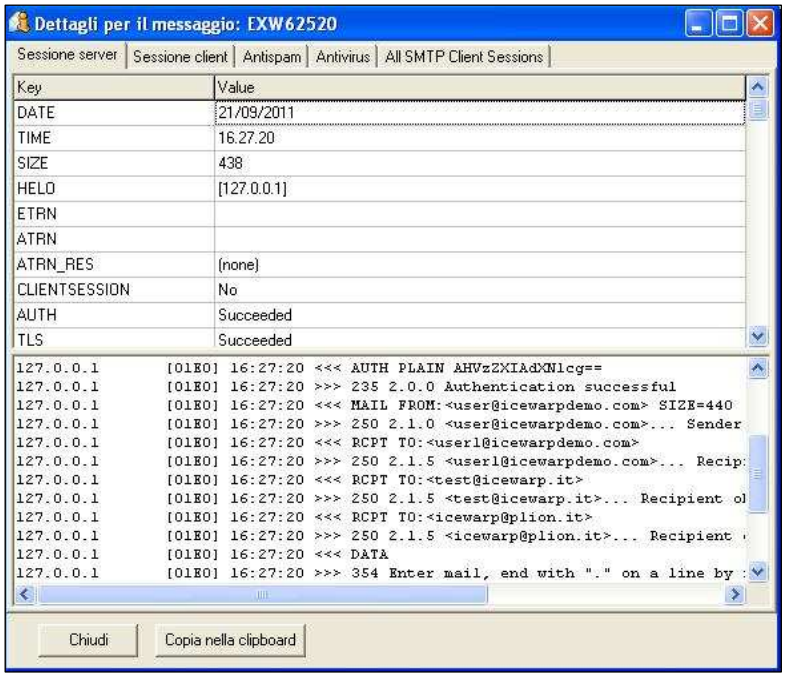
Result	Count	Min duration	Max duration	Average durat...	Total duration	Size [kB]
AS	3	00.01	00.03	00.02	00.06	0,00
ERROR	1	00.04	00.04	00.04	00.04	0,00
INCPLT	27	00.01	02.57	00.27	12.08	0,00
OK	43	00.01	03.35	00.18	12.47	0,02
SCAN	15	00.01	06.24.16	25.38	06.24.37	0,00
TIMEOUT	1	05.19	05.19	05.19	05.19	0,00
UNK	6	00.01	00.47	00.10	00.58	0,00
WDNR	2	01.46	01.46	01.46	03.32	0,00

Ricerca

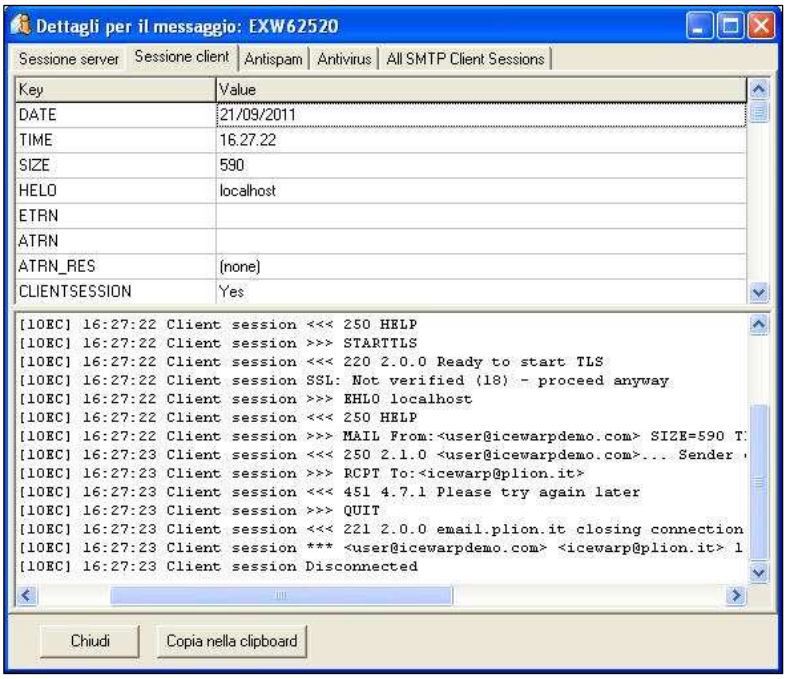
Questa sezione consente di effettuare una ricerca nei log dei tre principali servizi (SMTP, POP, IMAP) con varie opzioni di filtraggio e andando di fatto a produrre un elenco di singole sessioni isolate. Tra le varie opzioni di filtraggio vi è anche la possibilità di ottenere l'elenco di tutte le sessioni originate da uno specifico mittente o indirizzate ad un determinato destinatario.
L'elenco appare come segue (sessioni relative a un unico invio verso destinatari multipli):

main	21/09/2011	16.27.20	127.0.0.1	00.03	user@icewarpdemo.com	user1@icewarpdemo.com	0,43	OK	N	EXW62520
main	21/09/2011	16.27.20	127.0.0.1	00.03	user@icewarpdemo.com	test@icewarp.it	0,43	OK	N	EXW62520
main	21/09/2011	16.27.20	127.0.0.1	00.03	user@icewarpdemo.com	icewarp@plion.it	0,43	OK	N	EXW62520
main	21/09/2011	16.27.22	89.186.73.168	00.01	user@icewarpdemo.com	test@icewarp.it	0,58	OK	Y	EXW62520
main	21/09/2011	16.27.22	151.1.24.25	00.01	user@icewarpdemo.com	icewarp@plion.it	0,58	GRLST	Y	EXW62520

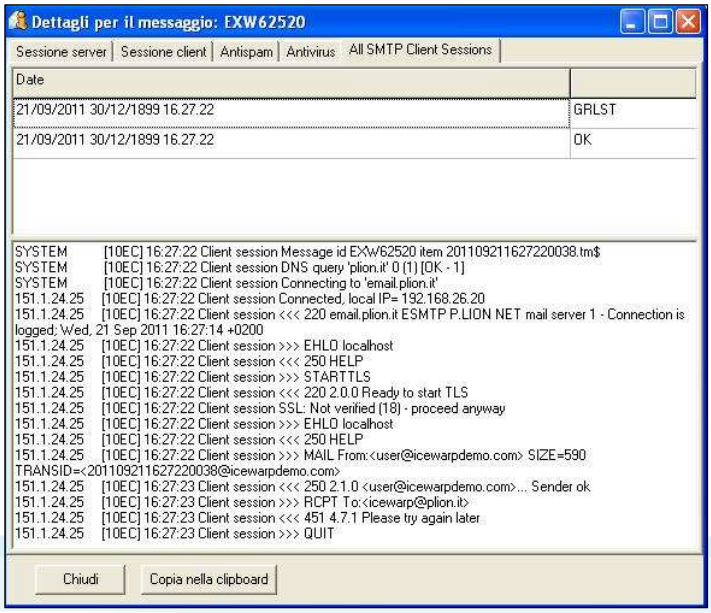
Come si può notare le sessioni vengono mostrate in ordine cronologico e tutti i dettagli più importanti vengono messi in risalto. Cliccando sul *Message ID* viene mostrata un'interfaccia dove le sessioni corrispondenti ad uno stesso messaggio (di cui appunto il *Message ID* è identificatore univoco) vengono automaticamente correlate.



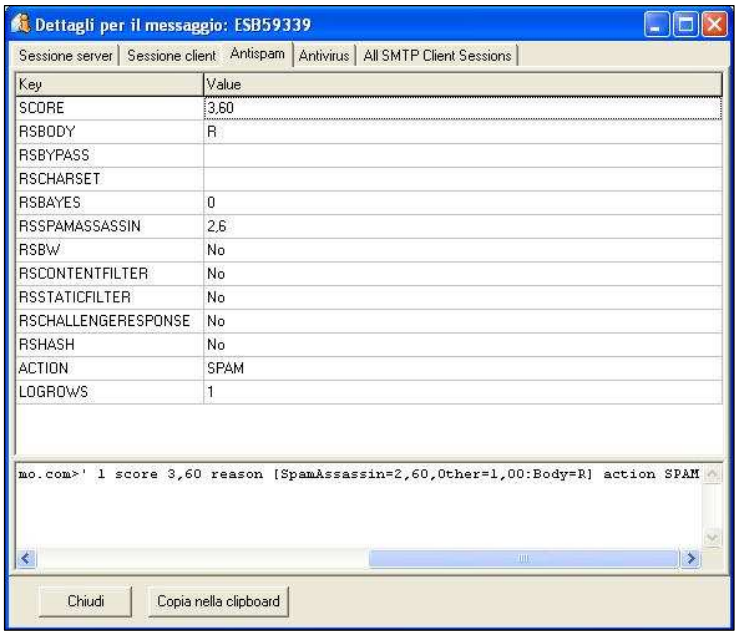
Questa funzionalità è estremamente utile in quanto consente di analizzare il percorso del messaggio nelle sue varie fasi, permettendo così di identificare più facilmente eventuali impedimenti (impossibilità di connessione al server remoto, azioni Antispam, ecc.).
Ad esempio nell'immagine sopra è mostrata la sessione Server relativa all'invio verso destinatari multipli dei quali abbiamo riportato l'elenco.
La seguente immagine mostra invece una delle corrispondenti sessioni Client (sulla sezione "*Sessione client*"):



Mentre nelle situazioni di invio ad un solo destinatario la consultazione della *Sessione client* da un'indicazione immediata riguardo all'esito dell'invio, in un invio a destinatari multipli la sessione mostrata è l'ultima avvenuta in ordine cronologico ed è quindi necessario tenere conto della potenziale presenza di più sessioni client alcune delle quali andate a buon fine mentre altre no. Per questo motivo è presente un elenco di tutte le sessioni Client con dettaglio dell'esito di ciascuna.



L'estratto del log Antispam relativo al medesimo invio è invece il seguente:



E' bene tenere conto che l'estratto visualizzato sarà sempre relativo alla valutazione effettuata in corrispondenza di uno solo degli invii. Trattandosi dello stesso messaggio inviato più volte la classificazione fatta è comunque la medesima in ogni caso.

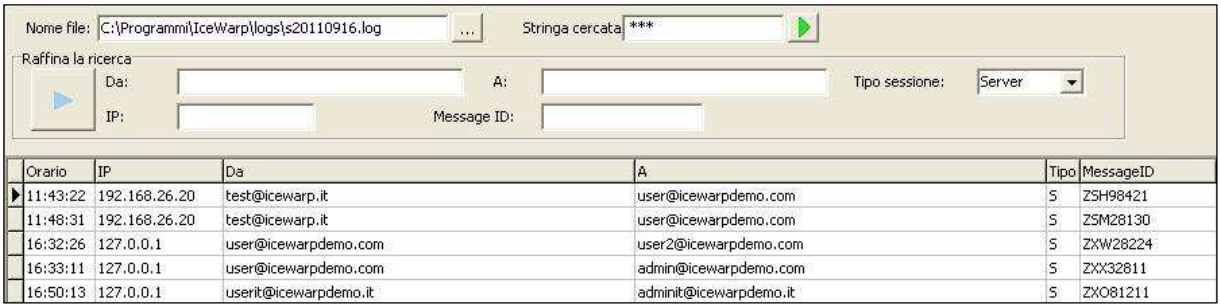
Interrogazioni personalizzate

In questa sezione è possibile affidarsi a query predefinite per ottenere informazioni utili riguardo all'attività del server e che sarebbe laborioso ottenere in altri modi.
Tra queste query ve ne sono ad esempio alcune che consentono di ottenere dati quantitativi sul traffico in ingresso e in uscita per singolo dominio o il totale degli errori per ogni IP di provenienza o ancora gli IP o gli account più attivi per quanto riguarda il servizio POP.
Accanto a queste query predefinite vi è ovviamente la possibilità di definirne di nuove e poterle poi eseguire sulla totalità dei log importati.

Ricerca diretta

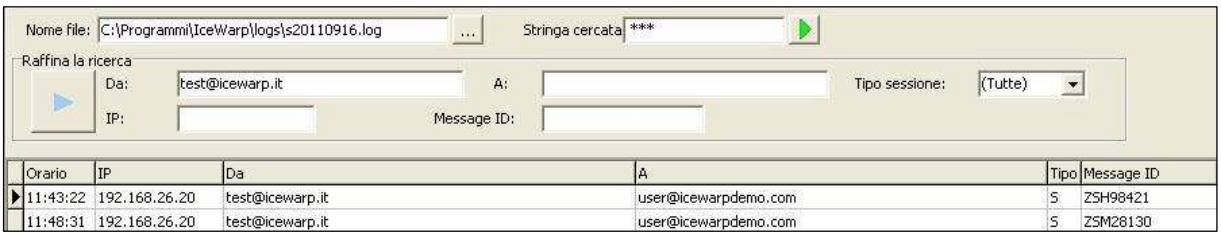
E' quindi possibile eseguire una ricerca su un file di log indicandone direttamente il percorso, senza doverlo prima importare nel database del software.
Con questo mezzo si possono eseguire ricerche filtrate da vari parametri.

Per ottenere un elenco di tutte le sessioni si può ricercare la stringa “ *** ”.



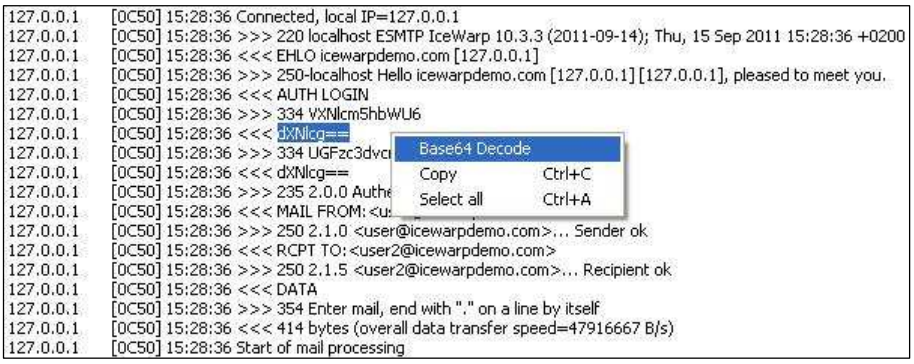
Orario	IP	Da	A	Tipo	MessageID
11:43:22	192.168.26.20	test@icewarp.it	user@icewarpdemo.com	S	ZSH98421
11:48:31	192.168.26.20	test@icewarp.it	user@icewarpdemo.com	S	ZSM28130
16:32:26	127.0.0.1	user@icewarpdemo.com	user2@icewarpdemo.com	S	ZXW28224
16:33:11	127.0.0.1	user@icewarpdemo.com	admin@icewarpdemo.com	S	ZXX32811
16:50:13	127.0.0.1	userit@icewarpdemo.it	adminit@icewarpdemo.it	S	ZXO81211

Dopo aver effettuato questa prima ricerca si può procedere ad un affinamento dei risultati ottenuti aggiungendo ulteriori parametri come in questo esempio:



Orario	IP	Da	A	Tipo	Message ID
11:43:22	192.168.26.20	test@icewarp.it	user@icewarpdemo.com	S	ZSH98421
11:48:31	192.168.26.20	test@icewarp.it	user@icewarpdemo.com	S	ZSM28130

Ricercando invece la stringa “*AUTH*” è possibile avere un elenco di tutte le sessioni in cui è stata effettuata autenticazione SMTP.
Un'utile strumento nella consultazione delle sessioni autenticate è il decodificatore Base64 integrato che permette di verificare le credenziali con le quali l'account si è autenticato (o ha tentato di farlo).



Calendario

Vi è infine una sezione Calendario che permette di avere una panoramica immediata sui log importati nel database del Log Analyzer.
Per mezzo di un codice a colori è possibile capire a quali log si può avere accesso per ciascun giorno di modo da sapere se si hanno i dati necessari ad ottenere le statistiche o ad effettuare le ricerche desiderate.