Nmail PHP 로그분석

http://passkorea.net

2007-04-17

1. 로그 구분

- SMTP 로그

: 웹메일에서 메일을 보낼때 외부에서 메일을 받을때 SMTP 서버레벨에서의 응답이기록됩니다. RBL에 의한 IP차단, 존재하지 않는 사용자 등도 여기에 기록됩니다.

: 로그 위치.(날짜별로 생성) - /var/MailRoot/logs/smtp-200604170000

- SMAIL 로그

: SMTP 서버레벨에서 전달받은 메일을 실제 외부, 내부로 전송시도 한 후의 결과가기록됩니다.

: 로그 위치.(날짜별로 생성) - /var/MailRoot/logs/smail-200604170000

- 웹메일 로그

: 사용자들이 웹메일 사용중 발생했던 에러를 남겨두어 사용자의 리포팅 없이도 관리자가 에러를 파악할 수 있도록 해두었습니다.

: 가능한 서버관리자가 이해할 수 있도록 에러를 남기고 있습니다. 이해하기 어려운 부분은 패스코리아넷으로 문의주시기 바랍니다.

: 로그 위치.(날짜별로 생성) - /home/nmail2/weblogs/error-20060417.txt

2. SMTP 로그 분석방법

- 로그 필드 안내

메일서버FQDN | 메일서버도메인 | IP | 날짜 | 보낸도메인 | 받는도메인 | 보낸주소 | 받는주소 | 메세지ID | 상태 | SMTP인증여부 | 크기 | 클라이언트FQDN

- 메일을 받았을때의 분석 예제

"to.com" "to.com" "211.1.1.1" "2006-04-10 16:14:09" "from.com" "to.com" "id@from.com" "admin@to.com" "S293D9" "RCPT=OK" "" "0" ""

=> id@from.com 에서 admin@to.com 으로 보낸 메일입니다.

=> 'RCPT=OK'는 admin@to.com 사용자가 존재하거나 외부로의 릴레이권한이 있어서 메일전송을 시작한다는 의미입니다.

"to.com" "to.com" "211.1.1.1" "2006-04-10 16:14:10" "from.com" "to.com" "id@from.com" "admin@to.com" "S293D9" "RECV=OK" "" "1795" ""

=> 'RECV=OK'는 1795byte 크기의 메일을 성공적으로 수신/송신했다는 의미입니다.

- 메일을 보냈을때의 분석 예제

"from.com" "from.com" "127.0.0.1" "2006-04-10 16:27:45" "localhost" "to.com" "admin@from.com" "id@to.com" "S293DE" "RCPT=OK" "" "0" ""

"from.com" "from.com" "127.0.0.1" "2006-04-10 16:27:45" "localhost" "to.com" "admin@from.com" "id@to.com" "S293DE" "RECV=OK" "" "898" ""

=> 웹메일(127.0.0.1)에서 admin@from.com 이 id@to.com 으로 보낸 메일입니다.

=> 메일을 받았을 때의 로그와 '받는사람, 보낸사람'만 다르고 의미는 동일합니다.

3. SMAIL 로그 분석방법

- 로그 필드 안내

메일서버FQDN | 파일명 | 메세지ID | 보낸주소 | 받는주소 | 종류 | 받는주소(알리아스 사용시 실제 사용자명) | 날짜

- 메일을 내부 사용자가 받았을때의 분석 예제

"to.com" "1176750679692.2799696816.3f99e.eml" "SAFF9E" "id@from.com" "admin@to.com" "LOCAL" "admin@to.com" "2007-04-17 04:11:22"

=> id@from.com 사용자가 보낸 메일이 메일서버내부에 존재하는 admin@to.com 사용자에게 도착했다는 의미입니다.

=> 메세지ID(SAFF9E)는 SMTP 로그와 연계해서 분석할때 사용되는 특정 메세지의 고유 ID입니다.

- 메일을 외부 메일서버로 보냈을때의 분석 예제

"to.com" "1176750682029.2971507632.3f99f.eml" "SAFF9E" "id@from.com" "admin@to.com" "SMTP" "admin@to.com" "2007-04-17 04:11:23"

=> id@from.com 사용자가 보낸 메일의 외부 메일서버에 존재하는 admin@to.com 사용자에게 메일을 정상적으로 발송했다는 의미입니다.

- 메일 포워딩에 의해 다른 사용자에게 재전송을 시도할때의 분석 예제

"to.com" "1176750679692.2799696816.3f99e.eml" "SAFF9E" "id@from.com" "admin@to.com" "REDIR" "admin@forward.com" "2007-04-17 04:11:22"

=> id@from.com 사용자가 보낸 메일이 메일서버내부에 존재하는 admin@to.com 사용자의 '포워딩 설정'에 의해 admin@forward.com 사용자에게 전달(포워딩)을 시도했다는 의미입니다. '전달'시도 후 최종 성공 결과는 'LOCAL/SMTP' 형태로 다시 남게 됩니다.