

공개 S/W 기술지원
KOID(한국인포데이타)

한국소프트웨어진흥원
공개SW기술지원센터

<Revision 정보>

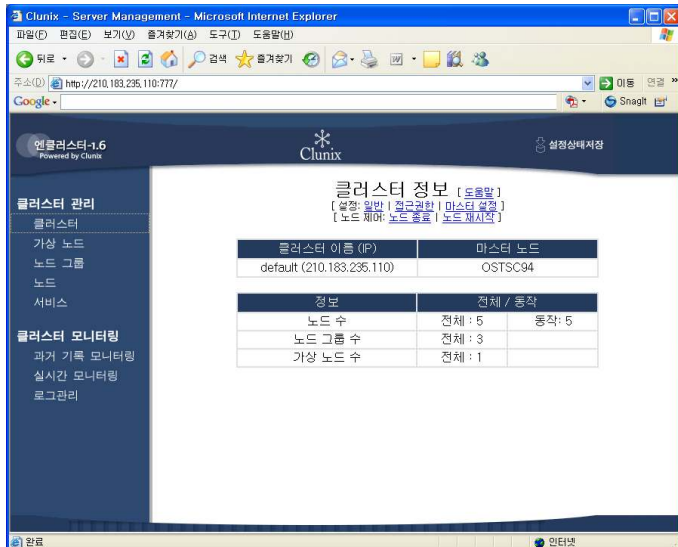
일자	VERSION	변경내역	작성자
2007. 2. 27	0.1	초기 작성	손명선

	공개SW 기술지원	
	구분 : 기술지원	단계:
	작성자: 손명선	작성일: 2007.2.27
	검토자:	검토일:
	승인자:	승인일:

1. 대상기업/기관 정보

구분	항목	내용	비고
기업/기관 정보	지역	대전시 중구 문화동 1-30	
	기업/기관 명칭	한국인포데이타(주)	
	부서	시스템운용부	
	직책		
	담당자 이름	박형국	
	전화번호 / 팩스번호	042-242-3114~5 / 042-226-3114	
	E-Mail	hkpark@koid.or.kr	

2. 대상기업/기관 지원사항

구분	항목	내용	비고
기업/기관 지원사항	접수내용	그룹웨어 리눅스 서버의 장애 조치	
	지원내역	1.1차 장애 점검 및 조치 (Spam필터 서버와 LB서버) - 증상 가. cluman 페이지가 정상적으로 뜨지 않는다. * 참고 : 정상동작 화면 	

		나. sshd 데몬이 죽는다. <pre>[root@lb1 ~]# ps aux grep sshd root 8362 0.0 0.0 3888 684 pts/2 S+ 15:28 0:00 grep sshd</pre> 다. 콘솔에서 명령어를 실행했을 경우 memory allocate error가 발생한다. - 원인 : /var 파티션이 full이 되어있어 발생한 것으로 예상. var가 full한 원인은 audit 데몬이 save.xxx 형식으로 로그를 발생시켜서 발생.audit는 보안, 감사 관련된 데몬임. - 해결 : var를 비우면서 해결이 되었다고 생각이 되나 내려간 김에 O/S부터 Encluster 까지 재설치 작업을 진행 2. 2차 장애 점검 및 조치 장애가 또 발생하여 다시 확인 작업을 진행함 이전까지는 장애가 발생하면 담당자가 바로 재부팅을 해서 장애 발생의 증상을 정확히 파악을 못했지만, 2차 장애 조치 작업에는 장애 발생 직후 바로 모니터링 및 분석을 통하여 원인을 찾아냄 장애원인 가. 문제 발생시 LB에서 외부로 네트워크 끊어짐. <pre>[root@lb1 ~]# ping 168.126.63.1 PING 168.126.63.1 (168.126.63.1) 56(84) bytes of data. From 211.48.62.187 icmp_seq=1 Destination Host Unreachable From 211.48.62.187 icmp_seq=2 Destination Host Unreachable From 211.48.62.187 icmp_seq=3 Destination Host Unreachable From 211.48.62.187 icmp_seq=4 Destination Host Unreachable</pre>	
--	--	--	--

	나. 방화벽의 root 프롬프트가 나오지 않음. 다. 방화벽 제거시 LB의 네트워크는 정상적으로 동작을 하지만, PING Loss 가 많이 생김. <pre>[root@lb1 ~]# ping 168.126.63.1 PING 168.126.63.1 (168.126.63.1) 56(84) bytes of data. 64 bytes from 168.126.63.1: icmp_seq=0 ttl=249 time=243.615 ms 64 bytes from 168.126.63.1: icmp_seq=1 ttl=249 time=236.441 ms 64 bytes from 168.126.63.1: icmp_seq=3 ttl=249 time=229.178 ms 64 bytes from 168.126.63.1: icmp_seq=4 ttl=249 time=230.197 ms 64 bytes from 168.126.63.1: icmp_seq=7 ttl=249 time=248.543 ms 64 bytes from 168.126.63.1: icmp_seq=8 ttl=249 time=231.518 ms 64 bytes from 168.126.63.1: icmp_seq=9 ttl=249 time=237.923 ms 64 bytes from 168.126.63.1: icmp_seq=12 ttl=249 time=235.860 ms ^C --- 168.126.63.1 ping statistics --- 32 packets transmitted, 20 packets received, 38% packet loss round-trip min/avg/max/stddev = 228.426/236.350/250.415/6.979 ms</pre> 근본원인 ; 아무래도 KOID 네트워크에 문제가 있음을 서로 발견하고 확인 결과 다른층의 Router단에 바이러스가 발생하여 전체 네트워크에 영향을 주고 있음을 규명하였음. 조치사항 가. 증상 파악 및 로그 분석에 따른 원인 규명 나. 문제 있는 해당 라우터 교체 및 모니터링을 통한 정상동작 확인	
--	--	--