



로그 파일 관리

Linux 기본 사항

학습 내용

강의 핵심 내용

학습 내용:

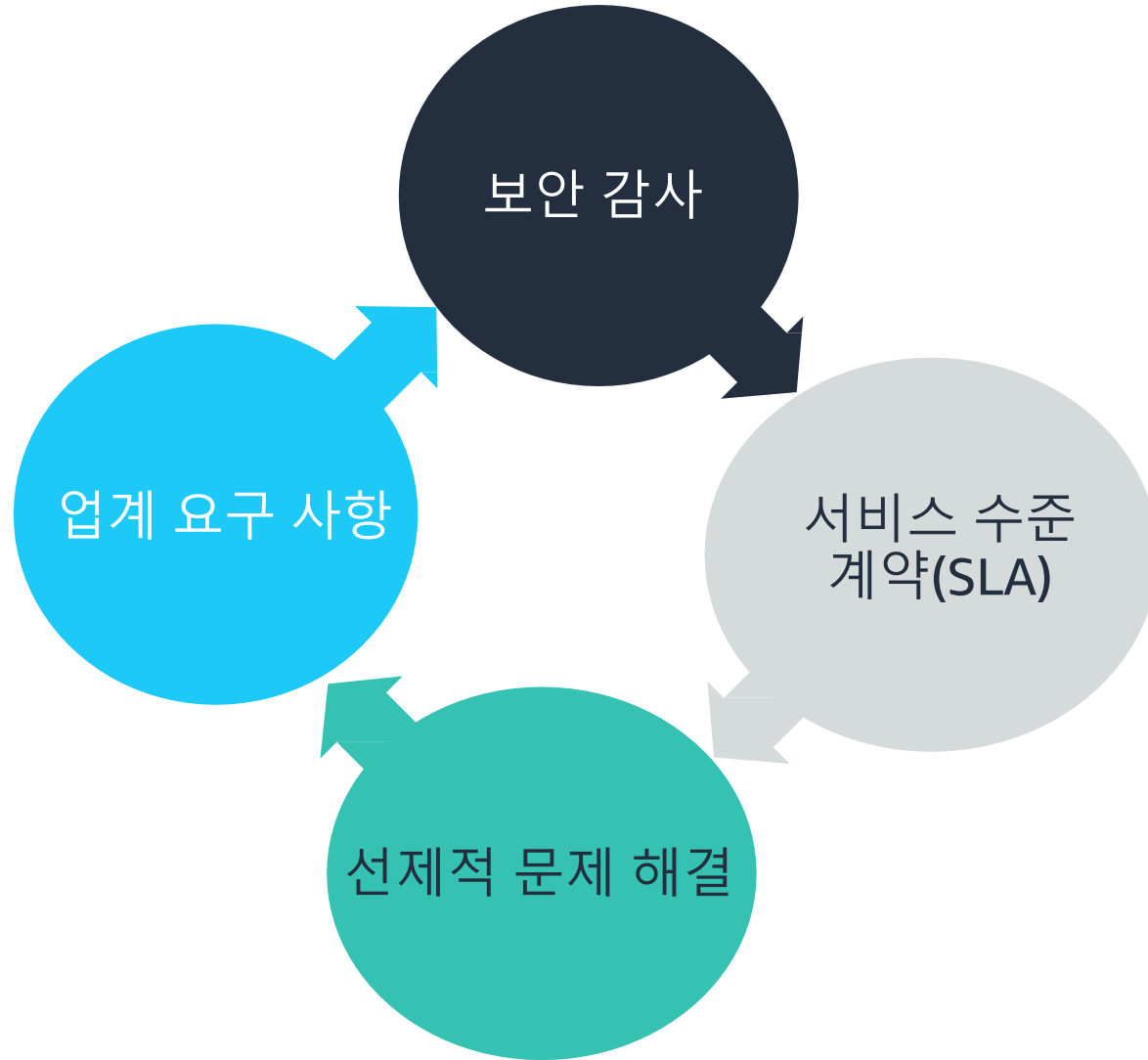
- 로그 파일을 정의합니다.
- 명령을 사용하여 로그 파일에서 다양한 유형의 메시지를 읽습니다.
- 로그 회전의 이점을 이해합니다.



로깅이란?

- 로그는 시스템 이벤트 레코드를 보관하므로 감사 작업에 도움이 됩니다.
- 로그의 유형은 다음과 같습니다.
 - 시스템 로그(시스템 스타트업 정보와 시스템 종료 횟수)
 - 이벤트 로그(사용자 로그인과 로그아웃 이벤트)
 - 애플리케이션 로그(스타트업 시간, 액션, 오류)
 - 서비스 로그

로깅의 중요성



로그 파일의 예

`sudo cat /var/log/yum.log`
파일은 설치되거나
업데이트된 프로그램을
나열합니다.

```
[ec2-user]$ sudo cat /var/log/yum.log
May 28 08:35:38 Updated: glibc-minimal-langpack-2.26-45.amzn2.x86_64
May 28 08:35:39 Updated: glibc-common-2.26-45.amzn2.x86_64
May 28 08:35:39 Updated: glibc-2.26-45.amzn2.x86_64
May 28 08:35:40 Updated: libcrypt-2.26-45.amzn2.x86_64
May 28 08:35:40 Updated: python3-pip-20.2.2-1.amzn2.0.2.noarch
May 28 08:35:41 Updated: python3-setuptools-49.1.3-1.amzn2.0.2.noarch
May 28 08:35:41 Updated: python3-3.7.9-1.amzn2.0.3.x86_64
May 28 08:35:43 Updated: python3-libs-3.7.9-1.amzn2.0.3.x86_64
May 28 08:35:43 Updated: 32:bind-license-9.11.4-26.P2.amzn2.5.noarch
May 28 08:35:43 Updated: 32:bind-libs-lite-9.11.4-26.P2.amzn2.5.x86_64
May 28 08:35:43 Updated: 32:bind-libs-9.11.4-26.P2.amzn2.5.x86_64
May 28 08:35:43 Updated: 32:bind-utils-9.11.4-26.P2.amzn2.5.x86_64
May 28 08:35:43 Updated: 32:bind-export-libs-9.11.4-26.P2.amzn2.5.x86_64
May 28 08:35:43 Updated: openssl-1.1.1j-5.amzn2.x86_64
```

```
[ec2-user]$ sudo cat /var/log/httpd/error_log-20210620
[Sun Jun 13 03:49:01.840870 2021] [lbmethod_heartbeat:notice] [pid 2901] AH02282: No slotmem from back
[Sun Jun 13 03:49:01.840916 2021] [http2:warn] [pid 2901] AH10034: The mpm module (prefork.c) is
http2. The mpm determines how things are processed in your server. HTTP/2 has more demands in th
ently selected mpm will just not do. This is an advisory warning. Your server will continue to v
otocol will be inactive.
[Sun Jun 13 03:49:01.840922 2021] [http2:warn] [pid 2901] AH02951: mod_ssl does not seem to be e
[Sun Jun 13 03:49:01.841367 2021] [mpm_prefork:notice] [pid 2901] AH00163: Apache/2.4.46 () conf
mal operations
[Sun Jun 13 03:49:01.841374 2021] [core:notice] [pid 2901] AH00094: Command line: '/usr/sbin/htt
[Tue Jun 15 12:23:06.907911 2021] [mpm_prefork:notice] [pid 2901] AH00170: caught SIGWINCH, shut
[Tue Jun 15 12:23:56.143046 2021] [suexec:notice] [pid 2899] AH01232: suEXEC mechanism enabled (
xec)
```

`sudo cat`
`/var/log/httpd/error_log`
파일은 웹 서버 서비스인
httpd의 로그 파일입니다.

로깅 수준

심각도 수준	식별	설명
0	EMERGENCY	시스템이 불안정해지면 메시지 로그
1	ALERT	즉각적인 작업이 필요하면 로그
2	CRITICAL	심각한 오류에 대한 메시지만 로그: 시스템을 사용하지 못하게 될 수 있음
3	ERROR	심각하지 않은 오류 상태를 나타내는 메시지 또는 좀 더 심각한 메시지만 로그
4	WARN	경고 메시지 또는 좀 더 심각한 메시지만 로그(일반적으로 Linux 디스트리뷰션의 기본 로그 수준)
5	NOTICE	정상적인 이벤트이지만 매우 중요한 메시지 로그
6	INFO	모든 정보 메시지와 좀 더 심각한 메시지 로그
7	DEBUG	모든 디버그 수준 및 INFO 메시지 로그

시스템 로그

tail, head, less 명령은 로그 파일 항목을 보는 데 사용됩니다. grep을 사용하여 패턴을 찾습니다.

```
[ec2-user]$ sudo tail /var/log/yum.log | grep httpd
Jun 10 13:55:49 Installed: httpd-tools-2.4.46-1.amzn2.x86_64
Jun 10 13:55:49 Installed: generic-logos-httpd-18.0.0-4.amzn2.noarch
Jun 10 13:55:49 Installed: httpd-filesystem-2.4.46-1.amzn2.noarch
Jun 10 13:55:50 Installed: httpd-2.4.46-1.amzn2.x86_64
[ec2-user]$
```

```
[ec2-user]$ sudo head -n 5 /var/log/yum.log
May 28 08:35:38 Updated: glibc-minimal-langpack-2.26-45.amzn2.x86_64
May 28 08:35:39 Updated: glibc-common-2.26-45.amzn2.x86_64
May 28 08:35:39 Updated: glibc-2.26-45.amzn2.x86_64
May 28 08:35:40 Updated: libcrypt-2.26-45.amzn2.x86_64
May 28 08:35:40 Updated: python3-pip-20.2.2-1.amzn2.0.2.noarch
[ec2-user]$
```

```
[ec2-user]$ sudo tail -n 5 /var/log/yum.log
Jun 10 13:55:49 Installed: generic-logos-httpd-18.0.0-4.amzn2.noarch
Jun 10 13:55:49 Installed: mailcap-2.1.41-2.amzn2.noarch
Jun 10 13:55:49 Installed: httpd-filesystem-2.4.46-1.amzn2.noarch
Jun 10 13:55:50 Installed: mod_http2-1.15.14-2.amzn2.x86_64
Jun 10 13:55:50 Installed: httpd-2.4.46-1.amzn2.x86_64
[ec2-user]$
```

grep을 사용한 로그 파일 검색

- grep 명령은 지정된 파일에서 지정된 문자열 또는 단어와 일치하는 행을 검색합니다.
- 로그 파일에서 텍스트의 특정 문자열 찾을 때 grep 명령을 추가합니다.
- grep은 Linux에서 매우 유용한 명령 중 하나입니다.
- 예를 들면 다음과 같습니다.
 - `cat yourlog.log | grep ERROR`
 - `tail -f yourlog.log | grep error`
 - `sudo cat /tmp/log/secure | grep LOGIN > SharedFolders/logins.csv`

```
[ec2-user]$ sudo tail /var/log/secure | grep "invalid user"
Jun 22 14:45:45 ip-172-31-27-186 sshd[1131]: input_userauth_request: invalid user ec3-user [preauth]
Jun 22 14:45:59 ip-172-31-27-186 sshd[1137]: input_userauth_request: invalid user ec4-user [preauth]
[ec2-user]$
```


Linux의 로그 파일 저장 위치

- Linux와 애플리케이션은 일반적으로 /var/log 디렉터리에 로그 파일을 저장합니다.
- 대규모로 예측하기 어렵고 빠르게 변경되는 파일을 저장할 때 /var 디렉터리를 사용합니다.

```
[ec2-user]$ ls /var/log
amazon          btmp-20210601      grubby            messages-20210530  spooler-20210530
audit           chrony             grubby_prune_debug messages-20210606  spooler-20210606
boot.log        cloud-init.log     httpd            messages-20210613  spooler-20210613
boot.log-20210616 cloud-init-output.log journal          messages-20210620  spooler-20210620
boot.log-20210617 cron              lastlog          sa                tallylog
boot.log-20210618 cron-20210530      maillog          secure            wtmp
boot.log-20210619 cron-20210606      maillog-20210530 secure-20210530   yum.log
boot.log-20210620 cron-20210613      maillog-20210606 secure-20210606
boot.log-20210621 cron-20210620      maillog-20210613 secure-20210613
boot.log-20210622 dmesg             maillog-20210620 secure-20210620
btmp            dmesg.old         messages         spooler
[ec2-user]$
```

중요한 로그 파일

로그 파일	설명
/var/log/syslog	시스템 정보 저장
/var/log/secure	Red-Hat에서 파생된 디스트리뷰션에 대한 인증 정보 저장
/var/log/kern	Linux 커널 정보 저장
/var/log/boot.log	스타트업 메시지 저장
/var/log/maillog	메일 메시지 저장
/var/log/daemon.log	백그라운드 서비스 실행에 관한 정보 저장
/var/log/auth.log	Debian에서 파생된 디스트리뷰션에 대한 인증 정보 저장
/var/log/cron.log	예약된 태스크에 대한 cron 메시지 저장
/var/log/httpd	Red-Hat에서 파생된 디스트리뷰션에 대한 Apache 정보 저장

lastlog 명령

시스템에 대한 최근 로그인 정보 보고

특정 사용자에게 대한 모든 로그인 또는 로그인 정보 보고 가능



모든 사용자

Username	Port	From	Latest
ec2-user	pts/0	72-21-198-64.ama	Wed Jun 23 08:10:16 +0000 2021
mmajor	pts/0		Tue Jun 22 09:31:07 +0000 2021
jdoe	pts/0		Mon Jun 21 08:25:22 +0000 2021



특정 사용자

Username	Port	From	Latest
ec2-user	pts/0	72-21-198-64.ama	Wed Jun 23 08:10:16 +0000 2021


로그 회전

- 서버는 일반적으로 대규모 애플리케이션을 실행합니다.
 - 서버는 모든 요청을 로그하는 경우가 많습니다.
 - 이러한 로깅은 많은 로그 파일을 만들어 냅니다.
- 로그 회전은 대용량 로그와 관련하여 다음과 같은 도움을 줄 수 있습니다.
 - 유지되는 로그의 전체 크기를 제한하는 방법입니다.
 - 최근 이벤트를 분석하는 데에도 도움이 됩니다.
- 로그 회전은 자동화된 프로세스로, 날짜가 지정된 로그 파일을 보관하는 시스템 관리에서 사용됩니다.

확인 질문



사용자 로그인 시도 문제를 해결하려면 어떤 로그 파일을 사용해야 합니까?



시스템 관리자에게 로그 파일이 중요한 이유는 무엇입니까?

요점



- 로깅을 사용하여 시스템에서 발생하는 이벤트를 기록합니다.
- 로그 파일은 커질 수 있습니다. 관리할 수 있는 상태로 로그를 유지하려면 로그 회전을 사용하여 파일을 정기적으로 저장해야 합니다.
- 로깅 수준으로 로그 세부 정보의 양을 조절할 수 있습니다.



감사합니다.

© 2021 Amazon Web Services, Inc. 또는 자회사. All rights reserved. 본 내용은 Amazon Web Services, Inc.의 사전 서면 허가 없이 전체 또는 일부를 복제하거나 재배포할 수 없습니다. 상업적인 복제, 임대 또는 판매는 금지됩니다. 수정해야 할 사항, 피드백 또는 기타 질문이 있다면 <https://support.aws.amazon.com/#/contacts/aws-training>에서 문의해 주십시오. 모든 상표는 해당 소유자의 자산입니다.

