Przeglądanie i monitorowanie plików dziennika

1. Przegląd

System operacyjny Linux i wiele działających na nim aplikacji wykonuje dużo logowania. Te dzienniki są nieocenione do monitorowania i rozwiązywania problemów z systemem.

Czego się nauczysz

Przeglądanie dzienników za pomocą prostego narzędzia GUI

Podstawowe polecenia wiersza polecenia do pracy z plikami dziennika

Co będziesz potrzebował

Ubuntu Desktop lub Server

Bardzo podstawowa wiedza z linii poleceń (cd, lsetc.)

2. Lokalizacje plików dziennika

Istnieje wiele różnych plików dziennika, które służą różnym celom. Próbując znaleźć dziennik o czymś, powinieneś zacząć od zidentyfikowania najbardziej odpowiedniego pliku. Poniżej znajduje się lista typowych lokalizacji plików dziennika.

Dzienniki systemowe

Dzienniki systemowe zajmują się dokładnie tym - systemem Ubuntu - w przeciwieństwie do dodatkowych aplikacji dodawanych przez użytkownika. Dzienniki te mogą zawierać informacje o autoryzacjach, demonach systemowych i komunikatach systemowych.

Dziennik autoryzacji

Lokalizacja: /var/log/auth.log

Śledzi systemy autoryzacji, takie jak monity o hasło, sudopolecenia i zdalne logowanie.

Dziennik demona

Lokalizacja: /var/log/daemon.log

Demony to programy działające w tle, zwykle bez interakcji użytkownika. Na przykład serwer wyświetlania, sesje SSH, usługi drukowania, bluetooth i inne.

Dziennik debugowania

Lokalizacja: /var/log/debug

Dostarcza informacji o debugowaniu z systemu Ubuntu i aplikacji.

Dziennik jądra

Lokalizacja: /var/log/kern.log

Dzienniki z jądra Linux.

Dziennik systemu

Lokalizacja: /var/log/syslog

Zawiera więcej informacji o twoim systemie. Jeśli nie możesz znaleźć niczego w innych dziennikach, prawdopodobnie jest to tutaj.

Dzienniki aplikacji

Niektóre aplikacje również tworzą dzienniki /var/log. Poniżej kilka przykładów.

Dzienniki Apache

Lokalizacja: /var/log/apache2/(podkatalog)

Apache tworzy kilka plików dziennika w /var/log/apache2/podkatalogu. access.logPlik rejestruje wszystkie żądania do serwera plików dostępu. error.logrejestruje wszystkie błędy zgłoszone przez serwer.

Dzienniki serwera X11

Lokalizacja: /var/log/Xorg.0.log

Serwer X11 tworzy osobny plik dziennika dla każdego z wyświetlaczy. Wyświetlane liczby zaczynają się od zera, więc twój pierwszy wyświetlacz (wyświetlacz 0) zaloguje się do Xorg.0.log. Następny ekran (ekran 1) zaloguje się Xorg.1.logi tak dalej.

Dzienniki nieczytelne dla człowieka

Nie wszystkie pliki dziennika są przeznaczone do odczytu przez ludzi. Niektóre zostały stworzone do analizy przez aplikacje. Poniżej kilka przykładów.

Dziennik błędów logowania

Lokalizacja: /var/log/faillog

Zawiera informacje o błędach logowania. Możesz go wyświetlić za pomocą faillogpolecenia.

Ostatnie logowanie

Lokalizacja: /var/log/lastlog

Zawiera informacje o ostatnich logowaniach. Możesz go wyświetlić za pomocą lastlogpolecenia.

Zaloguj się

Lokalizacja: /var/log/wtmp

Zawiera dane logowania używane przez inne narzędzia do sprawdzania, kto jest zalogowany. Aby wyświetlić aktualnie zalogowanych użytkowników, użyj who polecenia.

Ta lista nie jest wyczerpująca!

Możesz przeszukiwać Internet, by znaleźć więcej lokalizacji związanych z tym, co próbujesz debugować. Jest też już lista tutaj .

https://help.ubuntu.com/community/LinuxLogFiles?&_ga=2.86536536.1753943578.1588076805-1109543190.1588076805#System_Logs

3. Przeglądanie dzienników za pomocą GNOME System Log Viewer

Przeglądarka dzienników systemu GNOME zapewnia prosty interfejs GUI do przeglądania i monitorowania plików dziennika. Jeśli korzystasz z systemu Ubuntu 17.10 lub nowszego, będzie się nazywał Dzienniki . W przeciwnym razie będzie to nazwa System Log .

Interfejs przeglądarki dziennika systemu

Interfejs przeglądarki dziennika systemu GNOME

Przeglądarka dziennika ma prosty interfejs. Pasek boczny po lewej stronie pokazuje listę otwartych plików dziennika, a zawartość aktualnie wybranego pliku jest wyświetlana po prawej stronie.

Przeglądarka dziennika nie tylko wyświetla, ale także monitoruje pliki dziennika pod kątem zmian. Pogrubiony tekst (jak pokazano na zrzucie ekranu powyżej) wskazuje nowe wiersze, które zostały zarejestrowane po otwarciu pliku. Gdy dziennik, który nie jest aktualnie wybrany, jest aktualizowany, jego nazwa na liście plików zmieni się na pogrubioną (jak pokazano auth.logna zrzucie ekranu powyżej).

Kliknięcie koła zębatego w prawym górnym rogu okna otworzy menu umożliwiające zmianę niektórych ustawień wyświetlania, a także otwieranie i zamykanie plików dziennika.

Po prawej stronie koła zębatego znajduje się również ikona szkła powiększającego, która umożliwia wyszukiwanie w aktualnie wybranym pliku dziennika.

Więcej informacji

Jeśli chcesz dowiedzieć się więcej o Przeglądarce dzienników systemu GNOME, możesz odwiedzić oficjalną dokumentację.

https://help.gnome.org/users/gnome-system-log/

4. Przeglądanie i monitorowanie dzienników z wiersza poleceń

Ważne jest również, aby wiedzieć, jak przeglądać dzienniki w wierszu polecenia. Jest to szczególnie przydatne, gdy jesteś zdalnie podłączony do serwera i nie masz GUI.

Poniższe polecenia będą przydatne podczas pracy z plikami dziennika z wiersza poleceń.

Przeglądanie plików

Najbardziej podstawowym sposobem przeglądania plików z wiersza poleceń jest użycie cat polecenia. Wystarczy przejść w nazwie pliku, i wyprowadza całą zawartość pliku: cat file.txt.

Może to być niewygodne w przypadku dużych plików (co nie jest rzadkością w logach!). Przydałby się nam edytor, choć może to być przesada, aby wyświetlić plik. W tym miejscu less pojawia się polecenie. Przekazujemy mu nazwę pliku (less file.txt), a plik zostanie otwarty w prostym interfejsie. Stąd możemy użyć klawiszy strzałek (lub j / k, jeśli znasz Vima), aby poruszać się po pliku, używać /do wyszukiwania i nacisnąć, q aby wyjść. Jest jeszcze kilka funkcji, z których wszystkie są opisane poprzez naciśnięcie, h aby otworzyć pomoc.

Wyświetlanie początku lub końca pliku

Możemy również chcieć szybko wyświetlić pierwszą lub ostatnią n liczbę wierszy pliku. Tutaj przydają się polecenia head i tail. Te polecenia działają podobnie cat, chociaż można określić, ile wierszy z początku / końca pliku chcesz wyświetlić. Aby wyświetlić pierwsze 15 wierszy pliku, uruchamiamy head -n 15 file.txt, a aby wyświetlić ostatnie 15 wierszy , uruchamiamy tail -n 15 file.txt. Ze względu na charakter plików dziennika dołączanych na dole, tail polecenie będzie ogólnie bardziej przydatne.

Pliki monitorowania

Aby monitorować plik dziennika, możesz przekazać -f flagę do tail. Będzie działał, drukując nowe dodatki do pliku, dopóki go nie zatrzymasz (Ctrl + C). Na przykład: tail -f file.txt.

Wyszukiwanie plików

Jednym ze sposobów, w jaki szukaliśmy plików, jest otwarcie pliku less i naciśnięcie /. Szybszym sposobem na to jest użycie grep polecenia. Określamy, co chcemy wyszukać w podwójnych cudzysłowach, wraz z nazwą pliku i grep wypiszemy wszystkie wiersze

zawierające to wyszukiwane hasło w pliku. Na przykład, aby wyszukać wiersze zawierające „test” w file.txt, uruchomisz grep "test" file.txt.

Jeżeli wynik grep wyszukiwania jest zbyt długi, to może ona do rury less, dzięki czemu można przewijać i przeglądać go: grep "test" file.txt | less.

Edycja plików

Najprostszym sposobem edycji plików z wiersza poleceń jest użycie nano. Nano to prosty edytor wiersza poleceń, w którym wszystkie najbardziej przydatne skróty klawiszowe są drukowane bezpośrednio na ekranie. Aby go uruchomić, po prostu podaj mu nazwę pliku (nano file.txt). Aby zamknąć lub zapisać plik, naciśnij Ctrl + X. Edytor zapyta, czy chcesz zapisać zmiany. Naciśnij, y aby potwierdzić lub n - nie. Jeśli wybierzesz opcję tak, poprosi Cię o nazwę pliku, aby zapisać plik jako. Jeśli edytujesz istniejący plik, nazwa pliku już tam będzie. Po prostu zostaw go takim, jakim jest, a zapisze się w odpowiednim pliku.

Gratulacje, teraz masz wystarczającą wiedzę na temat lokalizacji plików dziennika, korzystania z GNOME System Log Viewer i podstawowych poleceń wiersza poleceń, aby właściwie monitorować i rozwiązywać problemy, które pojawiają się w twoim systemie.

Dalsza lektura

Na Ubuntu Wiki znajduje się artykuł, który bardziej szczegółowo omawia pliki dziennika Ubuntu.

https://help.ubuntu.com/community/LinuxLogFiles?_ga=2.82361686.1753943578.1588076805-1109543190.1588076805

Ten DigitalOcean portalu artykuł okładki Wyświetlanie dzienników Systemd

https://www.digitalocean.com/community/tutorials/how-to-use-journalctl-to-view-and-manipulate-systemd-logs