Przeglądanie i monitorowanie plików dziennika

Cel ogólny lekcji: Nauczyć się przeglądać i monitorować pliki dziennika w systemie operacyjnym Linux za pomocą narzędzi GUI i wiersza poleceń oraz zrozumieć, jakie informacje można uzyskać z różnych lokalizacji plików dziennika.

Cele szczegółowe lekcji:

1. Nauczyć się przeglądać dzienniki za pomocą prostego narzędzia GUI oraz podstawowych poleceń wiersza poleceń do pracy z plikami dziennika.
2. Zidentyfikować różne lokalizacje plików dziennika i zrozumieć, jakie informacje można z nich uzyskać.
3. Nauczyć się korzystać z różnych poleceń wiersza poleceń do przeglądania i monitorowania plików dziennika.
4. Zrozumieć, jakie rodzaje informacji są rejestrowane w plikach dziennika systemu Ubuntu i aplikacji.
5. Nauczyć się rozwiązywać problemy związane z systemem Ubuntu, korzystając z informacji uzyskanych z plików dziennika.

Elementy:

1. Przegląd

System operacyjny Linux i wiele aplikacji, które na nim działają, wykonują wiele operacji rejestrowania. Te dzienniki są nieocenione przy monitorowaniu i rozwiązywaniu 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

Komputer stacjonarny lub serwer Ubuntu

Bardzo podstawowa znajomość wiersza poleceń (cd, ls, itp.)

2. Lokalizacje plików dziennika

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

Logi systemowe

Logi systemowe dotyczą właśnie tego - systemu Ubuntu - w przeciwieństwie do dodatkowych aplikacji dodawanych przez użytkownika. Logi te mogą zawierać informacje o uprawnieniach, demonach systemowych oraz komunikatach systemowych.

Dziennik autoryzacji

Lokalizacja:/var/log/auth.log

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

Dziennik demonów

Lokalizacja:/var/log/daemon.log

Demony to programy działające w tle, zazwyczaj bez udziału użytkownika. Na przykład serwer wyświetlania, sesje SSH, usługi drukowania, Bluetooth i inne.

Dziennik debugowania

Lokalizacja:/var/log/debug

Zawiera informacje debugowania z systemu Ubuntu i aplikacji.

Dziennik jądra

Lokalizacja:/var/log/kern.log

Logi z jądra Linuksa.

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 tworzą również dzienniki w formacie /var/log. Poniżej znajduje się kilka przykładów.

Logi Apache'a

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

Apache tworzy kilka plików dziennika w /var/log/apache2/podkatalogu. Plik access.logrejestruje wszystkie żądania dostępu do plików kierowane do serwera. error.logrejestruje wszystkie błędy zgłaszane przez serwer.

Logi serwera X11

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

Serwer X11 tworzy osobny plik dziennika dla każdego z Twoich wyświetlaczy. Wyświetlane numery zaczynają się od zera, więc pierwszy wyświetlacz (wyświetlacz 0) zostanie zalogowany do Xorg.0.log. Następny ekran (ekran 1) logowałby się do Xorg.1.log, i tak dalej.

Dzienniki nieczytelne dla człowieka

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

Dziennik błędów logowania

Lokalizacja:/var/log/faillog

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

Dziennik ostatnich logowań

Lokalizacja:/var/log/lastlog

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

Dziennik rekordów logowania

Lokalizacja:/var/log/wtmp

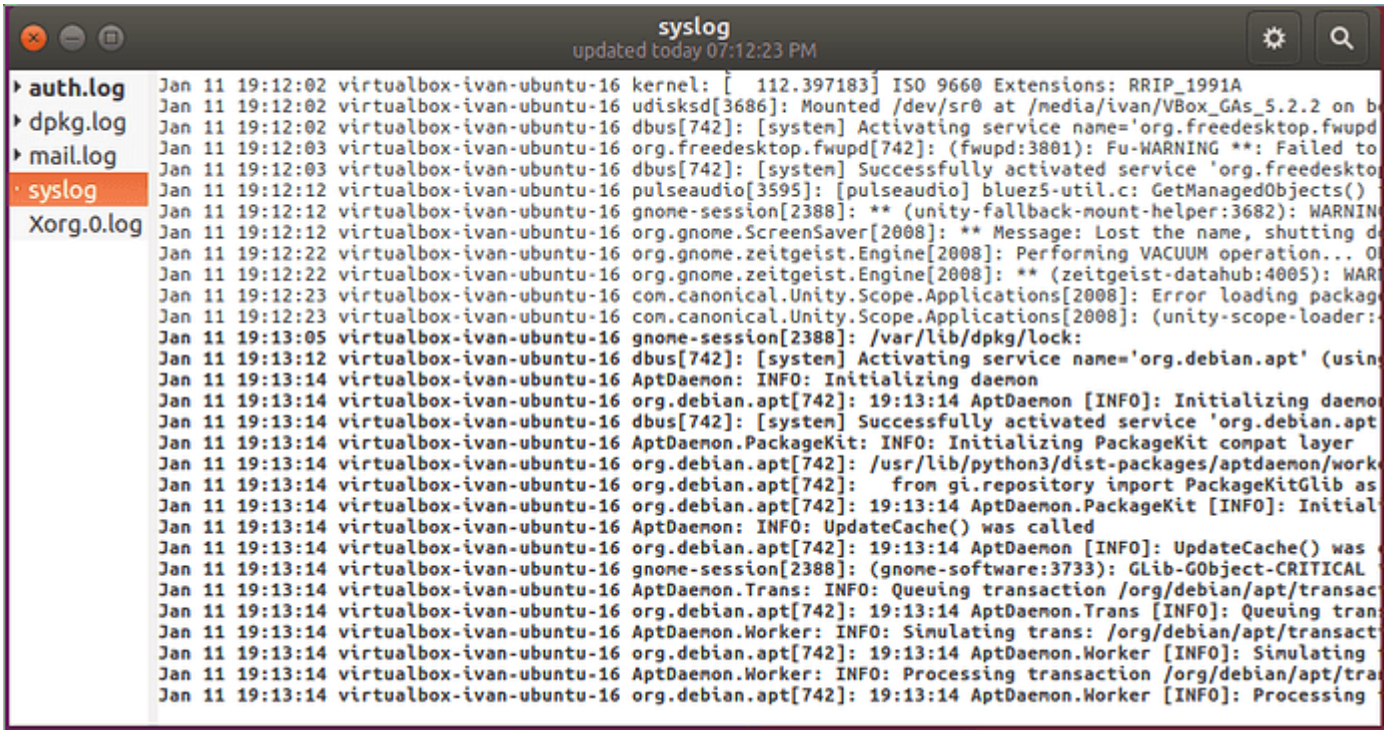
Zawiera dane logowania używane przez inne narzędzia do sprawdzania, kto jest zalogowany. Aby wyświetlić aktualnie zalogowanych użytkowników, użyj who polecenia.

3. Przeglądanie dzienników za pomocą Przeglądarki dzienników systemu GNOME

Przeglądarka dzienników systemu GNOME zapewnia prosty graficzny interfejs użytkownika do przeglądania i monitorowania plików dziennika. Jeśli korzystasz z systemu Ubuntu 17.10 lub nowszego, będzie się on nazywał Logs . W przeciwnym razie będzie pod nazwą Dziennik systemowy .

Interfejs przeglądarki dziennika systemu

Interfejs przeglądarki dziennika systemu GNOME



Przeglądarka logów ma prosty interfejs. Pasek boczny po lewej stronie pokazuje listę otwartych plików dziennika, z zawartością aktualnie wybranego pliku wyświetlaną po prawej stronie.

Przeglądarka dzienników nie tylko wyświetla, ale także monitoruje pliki dziennika pod kątem zmian. Pogrubiony tekst (jak widać na powyższym zrzucie ekranu) wskazuje nowe linie, które zostały zarejestrowane po otwarciu pliku. Gdy dziennik, który nie jest aktualnie wybrany, zostanie zaktualizowany, jego nazwa na liście plików zmieni kolor na pogrubiony (jak pokazano auth.logna powyższym zrzucie ekranu).

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.

4. Przeglądanie i monitorowanie dzienników z wiersza poleceń

Ważne jest również, aby wiedzieć, jak przeglądać dzienniki w wierszu poleceń. Jest to szczególnie przydatne, gdy jesteś zdalnie połączony z serwerem i nie masz GUI.

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

Przeglądanie plików

Najbardziej podstawowym sposobem przeglądania plików z wiersza poleceń jest użycie catpolecenia. Po prostu przekazujesz nazwę pliku, a wyświetla całą zawartość pliku: cat file.txt.

Może to być niewygodne w przypadku dużych plików (co nie jest rzadkością w przypadku dzienników!). Moglibyśmy użyć edytora, chociaż może to być przesada, aby zobaczyć plik. W tym miejscu lesspojawia 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, użyć /do wyszukiwania i nacisnąć, qaby wyjść. Dostępnych jest jeszcze kilka funkcji, z których wszystkie opisano, naciskając przycisk , haby otworzyć pomoc.

Wyświetlanie początku lub końca pliku

Możemy również chcieć szybko wyświetlić pierwszą lub ostatnią nliczbę wierszy pliku. Tutaj z pomocą przychodzą polecenia headi . tailTe polecenia działają podobnie jak cat, chociaż możesz określić, ile linii od początku/końca pliku chcesz wyświetlić. Aby wyświetlić pierwsze 15 wierszy pliku, uruchamiamy head -n 15 file.txt, a aby wyświetlić ostatnie 15, uruchamiamy tail -n 15 file.txt. Ze względu na charakter plików dziennika dołączanych na dole, tailpolecenie będzie generalnie bardziej przydatne.

Pliki monitorowania

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

Wyszukiwanie plików

Jednym ze sposobów wyszukiwania plików, na który patrzyliśmy, jest otwarcie pliku lessi naciśnięcie /. Szybszym sposobem na to jest użycie greppolecenia. Określamy, co chcemy wyszukać, w podwójnych cudzysłowach, wraz z nazwą pliku, i grepwypiszemy wszystkie wiersze zawierające wyszukiwane hasło w pliku. Na przykład, aby wyszukać wiersze zawierające „test” w file.txt, należy uruchomić grep "test" file.txt.

Jeśli wynik grepwyszukiwania jest zbyt długi, możesz go potokować do less, umożliwiając przewijanie i przeszukiwanie go: grep "test" file.txt | less.

Edycja plików

Najprostszym sposobem edycji plików z wiersza poleceń jest użycie nano. nanoto prosty edytor wiersza poleceń, który ma wszystkie najbardziej przydatne skróty klawiszowe drukowane bezpośrednio na ekranie. Aby go uruchomić, po prostu nadaj mu nazwę pliku (nano file.txt). Aby zamknąć lub zapisać plik, naciśnij Ctrl + X. Edytor zapyta, czy chcesz zapisać zmiany. Naciśnij yna tak lub nna nie. Jeśli wybierzesz tak, poprosi Cię o podanie nazwy pliku, w którym ma zostać zapisany plik. Jeśli edytujesz istniejący plik, nazwa pliku już tam będzie. Po prostu zostaw to tak, jak jest, a zostanie zapisane we właściwym pliku.

5. Wniosek

Gratulacje, masz teraz wystarczającą wiedzę na temat lokalizacji plików dziennika, korzystania z przeglądarki dziennika systemu GNOME i podstawowych poleceń wiersza poleceń, aby właściwie monitorować i rozwiązywać problemy pojawiające się w systemie.

6. Wykonaj czynności zawarte w pliku: Jak używać Journalctl do przeglądania i manipulowania dziennikami systemowymi.

Po wykonaniu wszystkich czynności z powyższej instrukcji przeczytaj ponownie z zrozumieniem cel ogólny i cele szczegółowe, które znajdują się na pierwszej stronie instrukcji. Jeżeli one zostały niezrealizowane to powtarzaj wykonie tej instrukcji w szkole lub/i w domu do momentu zrealizowania.

Dalsza lektura

Ubuntu Wiki zawiera artykuł, który bardziej szczegółowo opisuje pliki dziennika Ubuntu.

To ćwiczenie zostało utworzone w oparciu o artykuł społeczności DigitalOcean dotyczy przeglądania dzienników Systemd