

CYBERDET
DETECTION ENGINEERING TEAM
GÖREV YÖNERGESİ

Görev Veriliş Tarihi: 13.09.2024

Görev Teslim Tarihi: 20.09.2024

Görev Açıklaması

Takım üyelerinin **Debian tabanlı Linux dağıtımlarını** kullanarak sistem yöneticiliği yetkinlikleri kazanmalarını sağlamak amacıyla, aşağıdaki görevleri tamamlamaları beklenmektedir:

1. 60 saniyede bir **google.com**'a ping atılarak sonucunu **/var/log/google_ping.log** dosyasına yazan bir **crontab** süreci oluşturulması. (**crontab süreci root kullanıcısı yetkileri ile çalışmalıdır.**)
2. 60 saniyede bir sistemin **cpu (kullanım yüzdesi), ram (GB cinsinden kullanım miktarı) ,disk (doluluk yüzdesi)** metriklerini **/var/log/system_monitoring.log** dosyasına yazan bir **systemd** servisi oluşturulması.

Her bir görev için izlenen adımların detaylı bir şekilde açıklanarak bir rapor halinde sunulması gerekmektedir.

Bu görevin tamamlanmasıyla takım üyeleri aşağıdaki kazanımları kavranması beklenmektedir:

1. **crontab kullanımı ve zamanlanmış görev yönetimi:** Google'a düzenli aralıklarla ping atarak sonuçları bir log dosyasına yazan bir crontab süreci oluşturarak, takım üyeleri crontab kullanımını öğrenmiş olacak ve zamanlanmış görevlerin yönetimi konusunda deneyim kazanacaklardır. Bu yetkinlik, belirli aralıklarla çalışan görevlerin otomasyonunda ve yönetiminde kritik öneme sahiptir.
2. **systemd servis yönetimi:** Sistem kaynaklarının (CPU, RAM, disk) düzenli izlenmesi ve sonuçların bir log dosyasına kaydedilmesi için bir **systemd** servisi oluşturulması, takım üyelerine **systemd** ile servis yönetimi konusunda uygulamalı deneyim sağlayacaktır. Bu görev, temel servis oluşturma, başlatma, durdurma ve sistemle bütünleşik bir hizmetin nasıl yapılandırılacağı konusunda önemli bir bilgi kazandıracaktır.
3. **Log dosyası yönetimi:** Her iki görevde de log dosyalarının kullanımı öne çıkmaktadır. Bu süreçte takım üyeleri log dosyası oluşturma, logların yönetimi ve takibi konusunda bilgi sahibi olacaklardır. Log dosyalarının izlenmesi ve analiz edilmesi, sistem yöneticiliğinde hayati bir öneme sahiptir.
4. **Sistem kaynaklarının izlenmesi:** CPU, RAM ve disk gibi temel sistem kaynaklarının izlenmesi, sistem performansının anlaşılması ve sorunların tespiti için kritik bir beceridir. Bu görev, takım üyelerine sistem kaynaklarını izleme ve bu bilgileri raporlama yeteneği kazandıracaktır.
5. **Zaman ve kaynak yönetimi becerisi:** Sürekli çalışan sistem süreçlerinin nasıl yapılandırılacağını öğrenerek, sistem kaynaklarının en verimli şekilde kullanılmasını sağlayacak süreçlerin nasıl oluşturulacağı konusunda tecrübe edinilecek.

Teslim

Takım üyeleri oluşturdukları raporları **zip** dosya formatında sıkıştırıp paylaşılan Google formu atmalıdır.

Kaynaklar

- <https://www.youtube.com/watch?v=N1vgvhiyq0E&list=PLtK75qxsQaMKPbuVpGuqUQYRiTWTAmqeI>
- <https://www.youtube.com/watch?v=7cbP7fzn0D8>
- <https://www.youtube.com/watch?v=PN211ARk84M&list=PLeKWVPCoT9e0jHStZlH-z8Gsoo1SBZJlG>
- <https://www.youtube.com/watch?v=HrlZAE9Hn8o>
- <https://medium.com/@benmorel/creating-a-linux-service-with-systemd-611b5c8b91d6>
- <https://linuxhandbook.com/create-systemd-services/>
- <https://www.shubhamdipt.com/blog/how-to-create-a-systemd-service-in-linux/>
- <https://help.dreamhost.com/hc/en-us/articles/215767047-Creating-a-custom-Cron-Job>
- <https://phoenixnap.com/kb/set-up-cron-job-linux>
- https://medium.com/@The_Anshuman/linux-commands-to-check-cpu-utilization-memory-and-disk-c9daf8a53be8
- <https://phoenixnap.com/kb/linux-ping-command-examples>
- <https://www.javatpoint.com/ping-command-in-linux>
- <https://phoenixnap.com/kb/check-cpu-usage-load-linux>
- <https://www.uptimia.com/learn/linux-cpu-utilization>

