born2beroot Evaluations Cevapları

>> Bir sanal makine nasıl çalışır?

Sanal makineler, sanallaştırma teknolojisi ile mümkün kılınmaktadır. Sanallaştırma, birden çok VM'nin tek bir makinede çalışmasına izin veren sanal donanımı simüle etmek için yazılım kullanır. Fiziksel makine ana bilgisayar olarak bilinirken, üzerinde çalışan VM'lere misafir denir.

>> Sanal makinenin amacı nedir?

VM'ler, farklı seviyelerde işlem gücü ihtiyaçlarını karşılamak, farklı bir işlem gücü gerektiren yazılımı çalıştırmak için dağıtılabilir. İşletim sistemi veya güvenli, korumalı bir ortamda uygulamaları test etmek için cm'ler tercih edilir.

>> Neden Debain işletim sistemi tercih edildi?

Subject'te toy olanlar için tavsiye olarak verildiğinden dolayı.

>> CentOS ve Debian arasındaki temel farklar nelerdir?

CentOS, Debian'ın yaptığı kadar çok mimariyi desteklemez.

CentOS, destek sağalayan daha büyük bir topluluğa sahiptir ve dolayısıyla Red Hat Limited tarafından sağlanan ek destek sayesinde Debian'dan daha kararlıdır.

Hem Debian hem de CentOS düzenli olarak daha yeni sürümlere yükseltilir, ancak fark yaşam döngülerindedir. CentOS, düzenli büyük güncellemeleri desteklemez, ancak zaman zaman bazı küçük ince ayarlar ve hata düzeltmeleri olabilir. CentOS sürümleri yaklaşık on yıl sürer ve daha yeni sürüme geçiş sorunsuz değildir. Buna karşılık Debian, her 2 ila 3 yılda bir düzenli sürüm güncellemelerini destekler ve Debian'ın geçiş süreci de çok sorunsuz ve çoğunlukla hatasızdır.

Destek açısından, hem Debian hem de CentOS ve her ikisi de açık kaynaklı Linux çekirdeğine dayandığından topluluk tarafından desteklenir. Ancak CentOS kullanıcıları, kilitlenme ve hata raporlarını, bunları küçük bir yukarı akış sürümünde değiştirmek için Red Hat'e gönderebilir.

Paket yönetimi için, paket formatı olarak RPM(Red Hat Package Manager) ve paket yöneticisi olarak YUM/DNF, CentOS tarafından desteklenirken, Debian, paket formatı olarak DEB(Debian Software Package file)'ye ve paket yöneticisi olarak dpkg/APT'ye sahiptir.

>> aptitude ve apt arasındaki fark nedir?

Aptitude APT'ın kullanıcı arabirimidir. Yazılım paketlerini listelemeye, onları seçip kurmaya ve kaldırmaya yarar. APT debian tabanlı sistemlerin paket

yöneticisidir APT ile yazılım kurma, yazılım kaldırma, sistemi güncelleme, çekirdeği derleme gibi işlemleri terminal üzerinden gerçekleştirebilirsiniz.

APT'nin alt düzey bir paket yöneticisi ve Aptitude'un üst düzey bir paket yöneticisi olmasıdır. Bu, APT'nin diğer üst düzey paket yöneticilerinde kullanılabileceği anlamına gelir.

Diğer bir büyük fark, her iki aracın da sunduğu işlevselliktir. Aptitude, apt-get'e kıyasla daha iyi işlevsellik sunar. Aslında, apt-get, apt-mark ve apt-cache işlevlerini içerir.

Örneğin, apt-get paket yükseltme, yükleme, bağımlılıkları çözme, sistem yükseltme yükseltme vb. için etkin bir şekilde kullanılabilir. Ancak Aptitude, apt-cache ve apt-mark işlevlerinin dahil edilmesi sayesinde daha fazla özellik sunar. Bu, Aptitude'un paket arama, paket kurulumunu otomasyon veya manuel olarak ayarlama ve paketler üzerinde daha iyileştirilmiş eylemler dahil olmak üzere daha fazla işlevsellik için kullanılabileceği anlamına gelir.

Yüklü paketleri ve kullanılmayan paketleri kaldırmak istiyorsanız, Aptitude kullanmanız gerekir. apt-get durumunda, “-auto-remove” seçeneğini kullanarak kullanılmayan paketlerden kurtulmak istediğinizi açıkça belirtmeniz gerekir.

aptitude kurulu olarak bulunmamaktadır, kurulması gerekmektedir. “apt-get install aptitude”

>> APPArmor nedir?

AppArmor ("Uygulama Zırhı"), sistem yöneticisinin programların özelliklerini program başına profillerle kısıtlamasına izin veren bir Linux çekirdeği güvenlik modülüdür. Profiller, ağ erişimi, ham soket erişimi ve eşleşen yollardaki dosyaları okuma, yazma veya yürütme izni gibi yeteneklere izin verebilir.

AppArmor, savunmasız süreçleri kilitler, bu süreçlerdeki güvenlik açıklarının neden olabileceği hasarı sınırlar.

AppArmor'un sloganı, her şeye izin vermek ve ardından yavaş yavaş sıkılaştırmaktır.

>> APPArmor Yüklü mü kontrol etmek için?

sudo aa-status

>> Sunucuya bağlantı kurma;

ssh root@127.0.0.1 -p 4242
ssh akaraca@127.0.0.1 -p 4242

>> UFW hizmeti başlatıldı mı?

sudo ufw status

>> SSH hizmeti başlatıldı mı?

sudo systemctl status ssh

 # systemctl nedir?

> Systemctl, systemd ve hizmetleri kontrol etmek ve yönetmek için kullanılan bir Linux komut satırı yardımcı programıdır. Systemctl'yi Systemd init hizmeti için bir kontrol arayüzü olarak düşünebilirsiniz, systemd ile iletişim kurmanıza ve işlemleri gerçekleştirmenize izin verir. Systemctl, Init'in halefidir.

 # sudo systemctl status ssh nedir?

> Yönetici izni sistem hizmet bilgilerini kullanarak güvenli kabuk hakkında bilgileri çekmeyi amaçlar.

>> İşletim sisteminin kontrolü;

hostnamectl

—> hostnamectl komutu nedir? (Hostname-control)

“hostnamectl komutu, Linux sistemi ana bilgisayar adını kontrol etmek ve ilgili ayarlarını değiştirmek için kullanılan uygun bir API sağlar. Komut, belirli bir sistemde /etc/hostname dosyasını gerçekten bulup düzenlemeden ana bilgisayar adını değiştirmeye de yardımcı olur.

>> Kullanıcı sudo ve user42 grupları altında mı kontrol;

groups

>> Kullanıcı(root ve akaraca) şifre politiklarına uymuş mu?

chage -l akaraca && sudo chage -l root

>> Yeni bir kullanıcı oluşturun;

adduser deneme1

>> Şifreleme politikları nelerdir? Açıklayınız.

vim /etc/pam.d/common-password

minlen=10, en az 10 karakter uzunluğu istenmektedir.
ucredit=-1, en az 1 büyük karakter istenmektedir. (Pozitif durumda Max içeriği belirler.)
lcredit=-1, en az 1 küçük karakter istenmektedir. (Pozitif durumda Max içeriği belirler.)

maxrepeat=3, 3’ten fazla art arda karakter içermemelidir.
user_check=0, şifre, kullanıcı adını içermemlidir.
difok=7, eski şifre kullanılmak isteniyorsa, eski şifreden farklı olarak en az 7 karakter içermelidir.
enforce_for_root, belirtilen kuralları root yani kök kullanıcı şifresi içinde uygula anlamına geliyor.
retry=3, standart kuraldır. Art arda 3 defa şifre giriş işlemi gerçekleştirilebilir.

>> Grup oluşturun.
addgroup evaluating

>> Yeni kullanıcıyı gruba dahil edin.
adduser deneme1 evaluating

>> Atanan kullanıcı grupta mı kontrol edin.
getent group evaluating

getent nedir?; getent, kullanıcının veritabanları adı verilen bir dizi önemli metin dosyasına girdi almasına yardımcı olan bir Unix komutudur. Bu, kullanıcı bilgilerini depolayan passwd ve grup veritabanlarını içerir - bu nedenle getent, Unix'te kullanıcı ayrıntılarını aramanın yaygın bir yoludur.

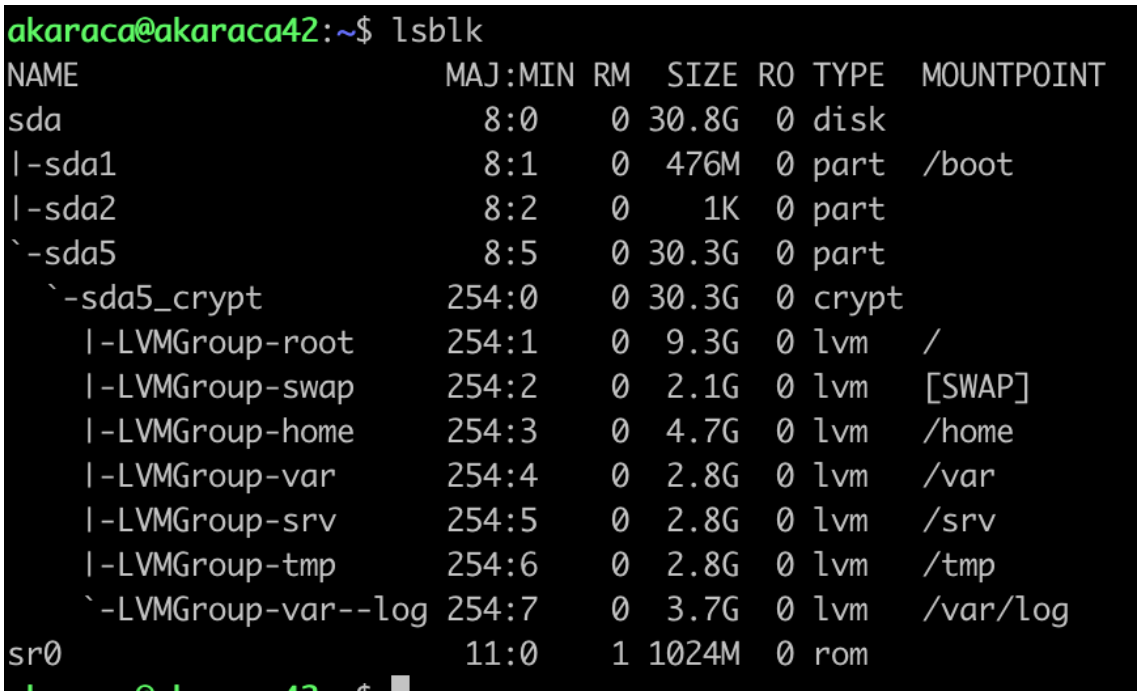
>> Şifreleme politikasının avantaj ve dezavantajları nelerdir?
Daha güvenilir bir sistem oluşturulmuş oluyor ve var olan kullanıcıların parolarının kırılmasını zorlaştırmaya yarıyor. Kısa sürede parolanın yenilenmesi ise şifreyi kıracak kişi için iyice işi zorlaştırıyor sebebi ise var olan şifreyi belirli bir zaman zarfında kırması gerektiği oluşumu ortaya çıkmasındandır. Dezavantajı ise parola unutulunca ortaca çıkan durumdur.

>> Makine adını değiştir.
hostnamectl set-hostname <new_hostname>

>> Sanal makine bölümleri nasıl görüntülenir?
lsblk

—>lsbk(list block devices) nedir?
lsblk komutunun, /sys/dev/block kullanılarak yapılan her bir blok aygıtına

bakmaktadır. Blok aygıtlarla ilgili ayrıntıları görüntülemek için kullanılır ve bu blok aygıtlar(ram disk hariç, bu bir hata değil özelliktir) temelde bilgisayara bağlı aygıtları temsil eden dosyalardır. Çıktıyı temel olarak ağaç benzeri bir yapıda vermektedir, “lsblk -T” (tree)komutu ile aynı işlevdedir.



---> var (/var) (variable, değişken) nedir?
/var, Linux ve diğer Unix benzeri işletim sistemlerinde, sistemin çalışması sırasında veri yazdığı dosyaları içeren kök dizinin standart bir alt dizinidir.

var local ne için kullanılır? "/var" genellikle günlük dosyaları, 'geçici' dosyalar (posta biriktirme, yazıcı biriktirme vb.), veritabanları ve belirli bir kullanıcıya bağlı olmayan diğer tüm veriler için kullanılır.

#Bu dizin, biriktirme(spool, daha sonra işlenmeyi bekleyen veriler) ve günlük dosyaları gibi boyutu değişebilen dosyaları içerir.

/var/tmp, /tmp gibi, bu dizin de belirsiz bir süre boyunca saklanan geçici dosyaları tutar.

---> srv (/srv) (service, hizmetler) nedir?
Web sunucuları için veriler ve komut dosyaları, FTP sunucuları tarafından sunulan veriler ve sürüm kontrol sistemleri için depolar gibi bu sistem tarafından sunulan siteye özgü veriler. srv, hizmet anlamına gelir. Sunucuya özel hizmetlerle ilgili verileri içerir. Örnek, /srv/cvs, CVS ile ilgili verileri içerir.

Bu, sistem tarafından sağlanan hizmetler için veri olan sunucu verileridir.

Bu dizin, bu sistem tarafından sunulan siteye özel verileri içerir.

>> LVM nasıl çalışıyor?

LVM, fiziksel disklerimizi sanal bir grup oluştururak tek bir diskmiş bir biçimde göstermek için kullanılıyor, bu kullanımın farklı versiyonlarıda bulunmaktadır.

>> LVM neyle ilgilidir?

lvm yani logical volume manager, mantıksal birim yönetimi ile mantıksal diskler üzerinde birim adı verilen kısımların oluşturulmasında rol oynarak bilgisayarın dosya dizinlerinin tanımlanmasında yer almaktadır.

>> Sudo kurulumu kontrol et?

sudo yaz entere bas.

>> Yeni kullanıcı sudo grubuna dahil mi kontrol et.

getent group sudo

>> Sudo için uygulanan politikalar nelerdir? Açıklayınız.

#sudo visudo

env_reset : Tüm potansiyel olarak tehlikeli ortam değişkenlerini kara listeye almak mümkün olmadığından, varsayılan env_reset davranışının kullanılması teşvik edilir. İşletim sisteminin kurulumunda standart olarak bulunan bir ayardır.

mail_badpass: Standart bir flag'dir.

Secure_path=" ": Secure_path değeri ayarlandıysa, sudo kullanarak çalıştırdığınız komutlar için PATH ortam değişkeni olarak kullanılacaktır. Bunun anlamı, örneğin çalıştırdığınızda sudo apt update , sistem apt komutunu Secure_path içinde belirtilen dizinlerde belirtilen sırayla aramaya çalışacaktır.

badpass_message=" ": Sudo komutu dahilinde girilen şifrenin yanlış olması durumunda ekrana çıktısı olacak olan mesajdır.

passwd_tries=3: Sudo komutu dahilinde girilen şifrenin 3 kerelik hatalı girme durumunun olduğunu belirtmektedir. Çıplak hali ile herhangi bir işlevi yoktur.

logfile=" "; log_input ve log_output olarak verilen çıktıların ~/sudo/sudo.log dosyası içerisine kaydedileceğini belirtir.

requiretty: TTY gereksinimi, SSH'nin, parola isterken diğer birçok Unix programının yaptığı gibi, standart girdi yoluyla parola istemine yanıt olarak yönlendirme girişimlerini reddetmesine olanak tanır.

-> Neden sadece visudo komutu kullanılır? /etc/sudoers klasörü düzenlenmesi tavsiye edilmez.

Sadece visudo kullanmak daha güvenlidir. /etc/sudoers'ı doğrudan düzenleyebilirsiniz, ancak orada bir yazım hatası yaparsanız, artık sudo kullanamazsınız. Ve hatanızı düzeltemeyeceksiniz. visudo, sudoers dosyasını birden çok eşzamanlı düzenlemeye karşı kilitler, temel akıl kontrolleri sağlar ve ayrıştırma hatalarını kontrol eder.

—> sudo (super user do), nedir?

Yönetici izinlerine sahip olmayan bir kullanıcıyı, root(kök) kullanıcısı gibi sınırlı yetkiler içerisinde özgür bırakmak için sudo argümanı kullanılır. Bu argümanın erişilebilir olması için öncelikle root ile kullanıcıya bu komutu kullanma izni verilmelidir.

Sudo komutunun diğer bir işlevi ise terminal üzerinde kullandığımız komut satırlarının komut olduğunu belirtmek için kullanılır. Örn: “sudo visudo” komutunu girdiğim zaman visudo’yu bir komut olarak algılar. Lakin sadece “visudo” şeklinde komut girersem bunu komut olarak algılamıyor.

 # UFW sanal makineye kurulumu kontrol edilir?

> **sudo ufw status verbose**

verbose : ayrıntılı demek.

 # UFW düzgün çalışıyor mu kontorl edilir?

> sudo ufw status

 # UFW nedir?

—> UFW (Uncomplicated Firewall) yani Karmaşık olmayan Güvenlik Duvarı nedir?

Kullanımı kolay olacak şekilde tasarlanmış bir netfilter(internet filitresi) güvenlik duvarını yönetmek için kullanılan bir programdır. Az sayıda basit komuttan oluşan bir komut satırı arabirimi kullanır ve yapılandırma için iptables kullanır.

iptables, Linux için bir güvenlik duvarı programıdır. Tabloları kullanarak sunucunuza gelen ve sunucunuza gelen trafiği izleyecektir. Bu tablolar, gelen ve giden veri paketlerini filtreleyecek, zincir adı verilen kural kümelerini içerir.

8080 numaralı portu açmak için:
> sudo ufw allow 8080

 # 8080 portunu silmek için;
> sudo ufw status numbered
> sudo ufw delete 2 - 3

 # SSH kurulumu kontrol etmek için;
> ssh
 # Düzgün çalışıyor mu kontrol etmek için;
> systemctl status ssh

SSH veya Secure Shell, iki bilgisayarın iletişim kurmasını (http veya web sayfaları gibi köprü metni aktarmak için kullanılan protokol olan köprü metni aktarım protokolü) ve verileri paylaşmasını sağlayan bir ağ iletişim protokolüdür.
-> sunucumuzda henüz ssh kurulu olmadığından dolayı kurmak için; “apt-get Install openssh-server” komutu kullanılır.

 # 4242 portu üzerinde kullanıldığını doğrula;
> sudo systemctl status ssh

 # yeni kullanıcı ssh üzerinden oturum açabilmelidir.
> ssh deneme1@127.0.0.1 -p 4242

Script kodunu gösterin ve anlatın.
> vim /usr/local/bin/monitoring.sh

```
#!/bin/bash
arc=$(uname -a)
pcpu=$(grep "physical id" /proc/cpuinfo | sort | uniq | wc -l)
vcpu=$(grep "^processor" /proc/cpuinfo | wc -l)
fram=$(free -m | awk '$1 == "Mem:" {print $2}')
uram=$(free -m | awk '$1 == "Mem:" {print $3}')
pram=$(free | awk '$1 == "Mem:" {printf("%.2f"), $3/$2*100}')
fdisk=$(df -Bg | grep '^/dev/' | grep -v '/boot$' | awk '{ft += $2} END {print ft}')
udisk=$(df -Bm | grep '^/dev/' | grep -v '/boot$' | awk '{ut += $3} END {print ut}')
pdisk=$(df -Bm | grep '^/dev/' | grep -v '/boot$' | awk '{ut += $3} {ft+= $2} END {printf("%d"), ut/ft*100}')
cpul=$(top -bn1 | grep '^%Cpu' | cut -c 9- | xargs | awk '{printf("%.1f%%"), $1 + $3}')
lb=$(who -b | awk '$1 == "system" {print $3 " " $4}')
lvmt=$(lsblk | grep "lvm" | wc -l)
lvmu=$(if [ $lvmt -eq 0 ]; then echo no; else echo yes; fi)
#You need to install net tools for the next step [$ sudo apt install net-tools]
ctcp=$(cat /proc/net/sockstat | awk '$1 == "TCP:" {print $3}')
ulog=$(users | wc -w)
ip=$(hostname -I)
mac=$(ip link show | awk '$1 == "link/ether" {print $2}')
cmds=$(journalctl _COMM=sudo | grep COMMAND | wc -l) # journalctl should be running as sudo but our script is running as root so we don't need in sudo here
wall "  #Architecture: $arc
        #CPU physical: $pcpu
        #vCPU: $vcpu
        #Memory Usage: $uram/${fram}MB ($pram%)
        #Disk Usage: $udisk/${fdisk}Gb ($pdisk%)
        #CPU load: $cpul
        #Last boot: $lb
        #LVM use: $lvmu
        #Connexions TCP: $ctcp ESTABLISHED
        #User log: $ulog
        #Network: IP $ip ($mac)
        #Sudo: $cmds cmd" # broadcast our system information on all terminals
```

 # Cron nedir?

——> cron nedir?

Cron, adı Yunanca zaman kelimesi olan Chronos'tan gelen bir saat arka plan programıdır(deamon). Kullanıcıların belirli zaman aralıklarında komutların, komut dosyalarının (bir grup komut) veya programların yürütülmesini otomatikleştirmesini sağlar.

Cron, Linux kullanıcılarının herhangi bir görevi zamanlamasına yardımcı olan bir sistemdir. Ancak, bir cron işi, belirli bir zaman diliminde çalıştırılacak tanımlanmış herhangi bir görevdir. Bir kabuk betiği veya basit bir bash komutu olabilir. Cron işi, rutin görevlerimizi otomatikleştirmemize yardımcı olur, saatlik, günlük, aylık vb.

 # Her 10dk bir çalışan kod nasıl kuruldu?

> sudo crontab -u root -e

```
# m h  dom mon dow   command
*/10 * * * * bash /usr/local/bin/monitoring.sh
```

 # Her 1dk bir çalışması için 10 -> 1 yapılır ve kaydedilir.

 # Komut satırı değiştirilmeden cron nasıl durdurulur?

> “sudo /etc/init.d/cron stop”