LİNUX AĞ KOMUTLARI

Mustafa NUMANOĞLU

Temel Ağ Komutları

- Linux işletim sistemlerinde kullanılan önemli ağ komutlarından bazıları şunlardır:
  - Telnet
  - Ftp
  - Mslookup
  - Whois
  - Netstat
  - Arp
  - Ping
  - Traceroute

Telnet Komutu

- Telnet yazılımı uzaktaki sunucu ile TELNET protokolü ile haberleşmeyi sağlayan bir programdır. Bu programla uzaktaki makinede kullanıcıya bir çalışma alanı açılır. Kullanıcının gerçekleştirdiği her işlem uzaktaki sunucuda gerçekleşir. Telnet komutunun en basit kullanım şekli aşağıdaki gibidir:
  - **telnet sunucu_ismi [port numarası]**
- Sunucu ismi parametresi bildirilmediği takdirde telnet yazılımı kullanıcıdan bir komut girmesini bekleyen interaktif modda açılır. Bu durumda aşağıdakine benzer bir çıktı gözükecektir.
  - **[root@musti /root]# telnet**
  - **telnet>**

Telnet Komutu

- Bu bilgi isteminde telnet yazılımı kullanıcıdan belli komutlar alabilmektedir. Bu komutların listesini görmek için help komutunu vermek yeterlidir. Herhangi bir telnet bağlantısı gerçekleştirmiş iken de bilgi istemi penceresine dönülebilir. Bunun için CTRL-] tuş kombinasyonunun kullanılması yeterlidir.

Ftp Komutu

- FTP protokolü uzaktaki sunucudan dosya transferi için kullanılan bir protokoldür. Bu protokol kullanılarak uzaktaki ftp sunucusu ile dosya transferi yapmayı sağlayan birçok istemci bulunmaktadır. Bu istemcilerden en yaygın olanı ftp yazılımıdır. Bir çok işletim sisteminde hemen hemen aynı komutlar ve aynı ara yüze sahiptir. Ftp yazılımının temel kullanım şekli aşağıdaki gibidir:
  - **ftp ftp_sunucusu**
- Ftp sunucusunun ismi verilmediği takdirde ftp yazılımı aşağıdaki bilgi istemi durumunda bekleyecektir. Bu durumda iken o veya open komutu ile yeni bir ftp bağlantısı oluşturulabilir.

Ftp Komutu

- **[root@musti /root]# ftp**
- **ftp>**
- Yeni bir bağlantı yaratıldığı durumda, bağlantı yapılan ftp sunucusunun gönderdiği başlık gösterilir ve kullanıcı ismi ve şifre girilmesi istenir.
- Eğer kullanıcı ismi ve şifre girişi sırasında bir hata meydana gelirse, **user** komutu ile tekrar kullanıcı ismi ve şifre girilebilir.
- Kullanıcı ismi ve şifre doğrulatıldıktan sonra ftp yazılımı komut beklemek için bilgi istemi durumuna dönecektir. Bu durumda iken birçok komut kullanılabilir.

Ftp Komutu

- En çok kullanılan Ftp komutları:
- **ls**: Uzaktaki sunucuda bulunulan dizinin içeriğinin görülmesini sağlar.
- **dir**: ls ile aynı görevi görür. İki komutun çıktısı ftp sunucusuna göre değişebilir.
- **cd**: Uzaktaki sunucuda bulunulan dizini değiştirmek için kullanılır.
- **get**: Uzaktaki sunucudan bir dosya almak için kullanılır.
- **mget**: Uzaktaki sunucudan birden fazla dosya almak için kullanılır. Dosya isminin tam olarak verilmesine gerek yoktur. İsmi tamamlamak için *,? gibi özel karakterler kullanılabilir.

Ftp Komutu

- **put**: Uzaktaki sunucuya bir dosya koymak için kullanılır.
- **mput**: Uzaktaki sunucuya birden fazla dosya koymak için kullanılır.
- **prompt**: mget ve mput komutları kullanıldığı durumlarda her işlem yapılmadan önce kullanıcıdan onay beklenir. Onay beklenmeden işlemi yapmak isteniyor ise prompt komutu **off** argümanı ile çağırılmalıdır. Onay verme işlemini tekrar aktif yapmak için "**prompt on**" komutu verilmelidir.
- **bye**: Ftp bağlantısını kapatmak için kullanılır.

Nslookup Komutu

- Nslookup komutu DNS sunucusu ile haberleşip DNS sorgulamaları yapmak için kullanılmaktadır. En basit kullanım alanı makine isminden makine IP adresinin bulunmasıdır. Komutun temel kullanım şekli aşağıdaki gibidir:
  - **nslookup [seçenek] [sorgu]**
- Sorgu parametresi verilmediği takdirde nslookup interaktif modda çalışmaya başlayacaktır. İnteraktif modda iken istenilen sorgulama yapılabilmektedir. Varsayılan olarak düz ve ters kayıt sorgulama işlemleri yapılır. Yani makine ismi verilirse makinenin IP adresi, makine IP adresi verilirse makinenin ismi sorgulanır. Sorgulama tipi istendiği takdirde değiştirilebilir.

Nslookup Komutu

Temel sorgulama tipleri:

- **A**: Makine isminden IP adresi sorgulaması için,
- **PTR**: Makine IP adresinden makine ismi sorgulaması için,
- **NS**: Verilen alan için yetkili DNS sunucularının listesini görmek için kullanılır.
- **MX**: Verilen alan veya sunucu için gönderilen e-postaları kabul eden sunucuları görmek için kullanılır.
- **ANY**: Tüm sorgulama tiplerini kullanarak gerekli bilgileri almak için kullanılır.
- **SOA**: Alandan sorumlu kişi, TTL süresi, alanın seri numarası gibi bilgileri almak için kullanılır.

- Sorgulama tipini değiştirmek için interaktif modda "set query=sorgu_tipi" veya "set type=sorgu_tipi" komutu verilmelidir.

Whois Komutu

- Whois komutu bir IP adresinin hangi ağa dahil olduğunu ve o ağdan sorumlu kişilerin e-posta adresleri, posta adresleri, telefonları gibi bilgileri gösteren bir komuttur. Temelde bir IP bloğu alındığı takdirde, bloğu satın alan ile ilgili bilgiler alınır ve bu bilgiler whois sunucularında tutulurlar. Whois komutu ile bu sunucular sorgulanır. Komutun temel kullanımı aşağıdaki gibidir:
  - **whois IP_adresi[@whois_sunucusu]**
- Whois sunucuları genelde IP adresi dağıtmaya hakkı bulunan kuruluşlarda bulunur. Her sunucu belli bölgeler için geçerli bilgileri tutmaktadır. Bu nedenle her sunucudan cevap alınamayabilir.

Netstat Komutu

- Netstat komutu ağ bağlantıları, yönlendirme tablosu, ara yüz istatistikleri gibi ağ ile ilgili temel bilgileri göstermeye yarayan bir programdır. Temel olarak kullanımı aşağıdaki gibidir:
  - **netstat [seçenekler]**
- Hiç bir seçenek verilmediği takdirde netstat yazılımı sistemde kullanımda olan soketler hakkında bilgi verecektir. Bu durumda yapılmış ağ bağlantıları ile ilgili olan bilgiler gözükecektir.
- Netstat komutu çıktısının "Active Internet Connections" bölümünde bulunan sütunlar ve anlamları şöyledir:
- **Proto**: Soket tarafından kullanılan protokolü belirtir. Tcp , udp veya raw değerlerini içerebilir.
- **Recv-Q**: Bu soketi kullanan programa kopyalanmayan verinin büyüklüğünü byte olarak belirtir.

Netstat Komutu

- **Send-Q**: Karşıdaki sistem tarafından alındığı onaylanmayan verinin büyüklüğünü byte olarak belirtir.
- **Local Adress**: Soketin yedek uçtaki IP adresi ve port numarasını belirtir. Eğer netstat yazılımı –n seçeneği ile çalıştırılmamış ise IP adresi ve port numarası için çözümleme yapılır.
- **Foreign Adress**: Soketin uzak uçtaki IP adresi ve port numarasını belirtir. Eğer netstat yazılımı –n seçeneği ile çalıştırılmamış ise IP adresi ve port numarası için çözümleme yapılır.
- **State**: Soketin durumunu belirtir. Soketler aşağıdaki durumlarda olabilirler:

Netstat Komutu

- ESTABLISHED: Soket bağlantı gerçekleştirmiş durumdadır.
- SYN_SENT: Soket bağlantı kurmaya çalışıyordur.
- SYN_RECV: Ağdan bir bağlantı isteği gelmiştir.
- FIN_WAIT1: Soket kapatılmış, bağlantı sonlandırılmak üzeredir.
- FIN_WAIT2: Bağlantı sonlandırılmıştır. Soket karşı ucun bağlantıyı sonlandırmasını beklemektedir.
- TIME_WAIT: Soket kapandıktan sonra gelebilecek paketleri alabilmek için beklemektedir.
- CLOSED: Soket kullanılmamaktadır.
- CLOSE_WAIT: Karşı uç bağlantıyı kapatmıştır. Soketin kapanması beklenmektedir.
- LAST_ACK: Karşı uç bağlantıyı sonlandırmış ve soketi kapatmıştır. Onay beklenmektedir.

Netstat Komutu

- LISTEN: Soket gelebilecek bağlantılar için dinleme konumundadır.
- CLOSING: Yerel ve uzak soketler kapatılmış fakat tüm verilerini göndermemiş durumdadırlar. Tüm veriler gönderilmeden soketler kapanmazlar.

- Eğer netstat **–e** seçeneği ile çalıştırılmış ise User sütunu ile soketi kullanan yazılımın çalıştığı kullanıcı kimlik numarası veya kullanıcı ismi bilgisini içerir. Eğer netstat **–p** seçeneği ile çalıştırılmış ise "PID/Program name" sütunu soketi kullanan yazılımın süreç kimlik numarası ve program ismini gösterecektir. Her kullanıcı sadece kendi programları için bu bilgiyi alabilir. Root kullanıcısı ise tüm soketler için bu bilgiyi alma hakkına sahiptir.

Arp Komutu

- Arp komutu sistemin arp önbelleği ile ilgili işlevlerin yapılmasını sağlar.
- Yapılabilecek temel işlemler arasında arp tablosunu incelemek, arp tablosundan kayıt silmek ve arp tablosuna kayıt eklemek bulunmaktadır.
- Sistemin arp tablosunda, IP adresi–fiziksel adres çiftleri için kayıtlar bulunmaktadır.
- Sistemde bulunan arp tablosunu görmek için sadece arp komutunun çalıştırılması yeterlidir. İstendiği takdirde **–a** seçeneği de kullanılabilir. **–a** parametresi kullanıldığı takdirde istenilen makinenin MAC adresi öğrenilebilir.

Ping Komutu

- Ping komutu ICMP protokolü üzerinden **ECHO_REQUEST** göndermek için kullanılır. Bu isteği alan sunucu isteğe cevap gönderir. Arada geçen zaman hesaplanarak kullanıcıya gösterilir.
- Ping komutu çoğunlukla karşıdaki makinenin ayakta olup olmadığını kontrol etmek için kullanılır. Eğer ping isteğine cevap gelmiyor ise uzaktaki makine çalışmıyor olabilir. Aynı zamanda ping komutunun çıktısından iki makine arasındaki transferin ne kadar hızlı olabileceği hakkında tahmin yürütülebilir.
- Ping komutu ile aşağıdaki seçenekler kullanılabilir:
- **-c sayı**: Sayı ile belirtilen kadar ping paketi gönderdikten sonra programdan çıkılmasını sağlar. Bu seçenek kullanılmadığı takdirde ping yazılımı kullanıcıdan kapatma isteği gelene kadar çalışacaktır. En basit kapatma isteği **CTRL-C** tuşları ile verilir.

Ping Komutu

- **-f**: Çok hızlı olarak ping paketi üretilmesini sağlar. Sadece root kullanıcısı tarafından kullanılabilir. Ağ üzerinde yavaşlatıcı etken yapabileceğinden dikkatli kullanılması gerekmektedir.
- **-i süre**: Her bir ping paketinin gönderilmesi arasında geçmesi gereken sürenin ayarlanması için kullanılır. Belirtilen süre saniye cinsindendir. Bu seçenek kullanılmadığı takdirde her bir saniyede bir ping paketi gönderilir. –f seçeneği ile uyumsuzdur.
- **-n**: Bu seçenek kullanıldığı takdirde ping isteği gönderilen makineden gelen cevapların kullanıcıya gösterilmesi sırasında makinenin ismi yerine IP adresi kullanılır.
- **-s paket_büyüklüğü**: Gönderilecek ping paketinin büyüklüğünün ayarlanması için kullanılır. Varsayılan paket büyüklüğü 56 byte'tır. 8 baytlık ICMP başlık bilgisi ile paket boyu 64 byte'a çıkar.

Traceroute Komutu

- Traceroute komutu ile uzaktaki makineye giden yol hakkında bilgi alınır. Bu bilgilerden en temel olanı uzaktaki makineye giderken geçilen yönlendiricilerdir. Komutun temel kullanım şekli aşağıdaki gibidir:
- **traceroute [seçenekler] makine_ismi**
- Traceroute komutu varsayılan olarak UDP paketleri ile çalışır. UDP paketlerinde TTL (TimeToLive) değerlerini ayarlayarak geçilen geçitlerin ortaya çıkmasını sağlar. Bir yönlendirici üzerinden geçen paketi yönlendireceği zaman TTL değerini bir azaltır. Bu değer sıfır olduğu zaman paketi gönderen makineye ICMP “time exceeded” paketi gönderilir.

Traceroute Komutu

- Traceroute bu özelliği kullanarak yol bilgisini çıkarmaktadır. İlk olarak TTL değeri 1 olan bir UDP paketi yaratılır. Bu paket ilk yönlendiriciye geldiğinde yönlendirici kaynak makineye ICMP "time exceeded" paketi gönderir.
- Bu paket traceroute komutu tarafından işlenir. Daha sonra TTL değeri 2 olan bir paket gönderilir. Bu olay hedef makineye varana kadar devam eder.
- Başlangıç TTL değeri istendiği takdirde **–f** seçeneği ile ayarlanabilmektedir. UDP paketleri yerine ICMP paketleri kullanılabilmektedir. ICMP paketlerinin kullanılması için **–I** seçeneği kullanılmalıdır.