查找域控制器

查看域控制器的机器名

执行如下命令,可以看到,域控制器的机器名

```
nltest /DCLIST:hack
```

```
C:\>nltest /DCLIST:hack
获得域“hack”中 DC 的列表(从“\\DC”中)。
    DC.hack.com [PDC]  [DS] 站点: Default-First-Site-Name
此命令成功完成
```

查看域控制器的主机名

执行如下命令,可以看到,域控制器的主机名

```
nslookup -type=SRV _ldap._tcp
```

```
C:\>nslookup -type=SRV _ldap._tcp
服务器:  UnKnown
Address:  192.168.41.10

_ldap._tcp.hack.com     SRV service location:
          priority       = 0
          weight         = 100
          port           = 389
          svr hostname   = dc.hack.com
dc.hack.com     internet address = 192.168.41.10
```

查看当前时间

在通常情况下,时间服务器为主域控制器。执行如下命令

```
net time /domain
```

```
C:\>net time /domain
\\DC.hack.com 的当前时间是 2022/3/31 15:26:36

命令成功完成。
```

查看域控制器组

执行如下命令,查看域控制器组。,其中有一台机器名为"DC"的域控制器`

```
net group "Domain Controllers" /domain
```

```
C:\>net group "Domain Controllers" /domain
这项请求将在域 hack.com 的域控制器处理。

组名     Domain Controllers
注释     域中所有域控制器

成员

-------------------------------------------------------------------------------
DC$
命令成功完成。
```

在实际网络中,一个域内一般存在两台或两台以上的域控制器,其目的是:一旦主域控制器发生故障,备用的域控制器可以保证域内的服务和验证工作正常进行。