# ntds.dit文件的介绍

## Ntds.dit介绍

ntds.dit为ad的数据库，内容有域用户、域组、用户hash等信息，域控上的ntds.dit只有可以登录到域控的用户（如域管用户、DC本地管理员用户）可以访问。ntds.dit包括三个主要表：数据表、链接表、sd表。所以只要在域渗透中能够获取到ntds.dit就可以获取到所有域用户的用户名和对应的hash，它和SAM文件一样，被windows系统锁死

## Ntds.dit位置

```
C:\Windows\NTDS
```