

Windows 系统安全





第11课 安全策略

- 理解域安全策略
- 掌握密码策略
- 掌握账户锁定策略
- 掌握审核策略



- 可以影响整个域中的计算机的安全设置
- 打开方式
 - 【域安全策略】
- 帐户策略
 - 密码策略
 - 帐户锁定策略
- 本地策略
- `gpupdate /force`强制刷新



- 帐户策略设置需求
 - 域账户密码长度至少7个字符
 - 密码符合复杂性要求
 - 密码至少30天修改一次
 - 设置密码锁定策略：输入5次密码不正确就锁定该用户帐户



审核事件	说明
账户登录事件	审核域用户从域中的计算机登录时，域控制器收到的验证信息 I
登录事件	审核所有计算机用户的登录和注销事件
对象访问	审核用户访问某个对象的事件，例如文件、文件夹、注册表项、打印机等
账户管理	审核计算机上的每一个帐户管理事件，包括：创建、更改或删除用户帐户或组；重命名、禁用或启用用户帐户；设置或更改密码
目录服务访问	审核用户访问活动目录对象的事件
系统事件	审核用户重新启动或关闭计算机时或者对系统安全或安全日志有影响的事件



- 理解域安全策略
- 掌握密码策略
- 掌握账户锁定策略
- 掌握审核策略



The image features a central figure of a person wearing a black hoodie, with their right hand pressed against their forehead in a gesture of stress or concern. The background is a vibrant blue digital landscape. It includes a glowing globe on the right side, a network of interconnected nodes and lines, and several padlock icons scattered throughout, symbolizing security and technology. A horizontal semi-transparent bar is positioned across the middle of the image, containing the text.

谢谢观赏