基于RODC的身份验证过程 PDF转换可能丢失图片或格式，建议阅读原文 https://www.100test.com/kao_ti2020/275/2021_2022__E5_9F_BA_E4_BA_8ERODC_c67_275003.htm 以下场景帮助解释了基于RODC的身份验证过程。在这个场景中： 用户Bob想要登录到名称为BOB_WS的工作站。 安装BOB_WS工作站子网由一台RODC提供服务。 Bob的用户账户被允许在RODC上缓存凭据，但是凭据当前还没有缓存。 计算机账户BOB_WS被允许在RODC上缓存凭据，但是凭据当前还没有缓存。 Bob尝试在工作站（BOB_WS）上登录。首先，必须从域控制器处获得TGT。在本场景中TGT的获得过程如下图所示 1. RODC在分支机构宣告成为KDC。这意味着当BOB_WS搜索域控制器来认证Bob的登录请求时，它将找到并使用RODC作为KDC。BOB_WS 的Kerberos认证包准备了TGT请求并将它发送给RODC 2. RODC收到来至BOB_WS的TGT请求。因为RODC不知道Bob的账户密码，所以不能为Bob创建TGT。随后RODC将TGT请求传递给运行Windows Server 2008的可写域控制器。 3. 运行Windows Server 2008的可写域控制器验证请求。 4. 随后结果返回给RODC。如果Bob提供了正确的凭据，那么结果就是获得TGT。如果Bob的凭据验证失败，将会导致一条错误信息。在这个场景中，如果Bob在登录时输入了正确的用户名及密码，那么验证过程将获得成功。 5. 同时，可写域控制器返回TGT给RODC，它也向RODC计算机账户msDS-AuthenticatedToAccountList属性添加了Bob账户的相对可分辨名称（distinguished name，DN）。RODC创建了一条Bob已经被验证的记录。 6. 随后RODC将结果传递

给BOB_W S。 7. 在RODC将TGT发送回BOB_WS以后，它也向可写域控制器请求将Bob的凭据复制至它的活动目录数据库的副本区（replica） 8. 当可写域控制器收到将Bob的凭据复制到RODC的请求时，它会检查密码复制策略来查看RODC是否被允许缓存Bob账户的凭据。 9. 如果检查表明凭据能被缓存，那么可写域控制器将会允许复制Bob账户的凭据至RODC。 10. 在可写域控制器发送RODC请求的凭据的同时，可写域控制器在RODC计算机账户的msDS-RevealedList属性中写入Bob账户的相对可分辨名称（DN）。这创建了一条说明Bob的账户凭据已被缓存在RODC上的记录。 11. RODC在活动目录数据库的用户的合适属性中储存了Bob的凭据。 此时： 在可写域控制器上有一条允许复制Bob的凭据至RODC的记录。 Bob账户凭据在RODC上已被缓存。 Bob拥有可写域控制器产生的TGT。 