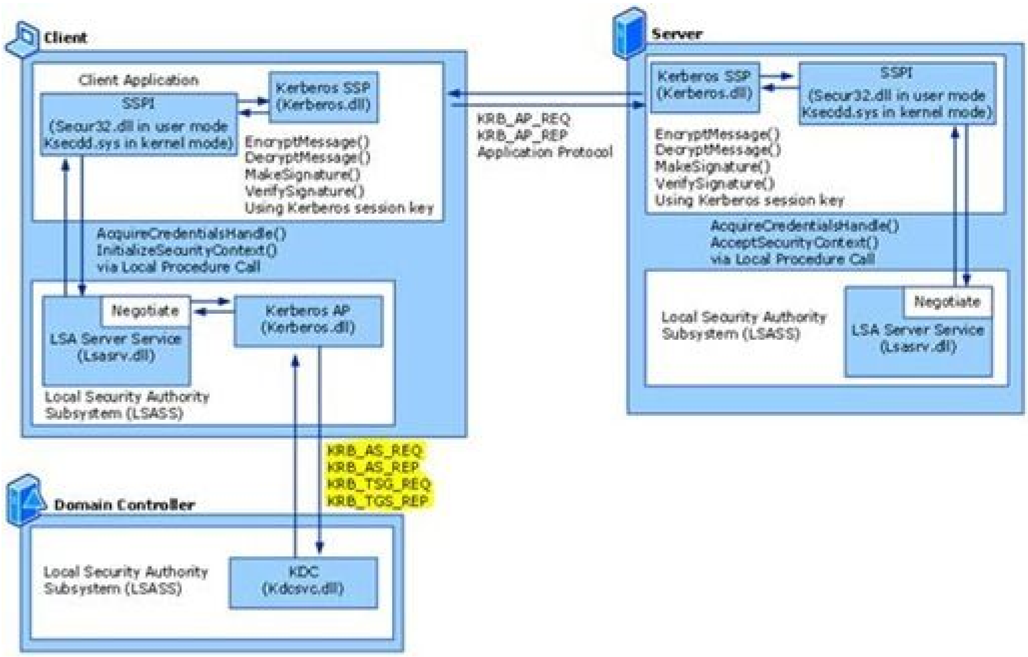
Understanding “Read Only Domain Controller” authentication

techcommunity.microsoft.com/t5/ask-the-directory-services-team/understanding-8220-read-only-domain-controller-8221/ba-p/395031

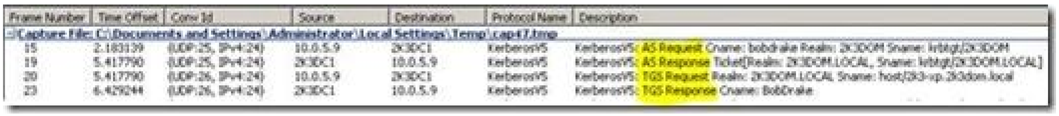
First published on TechNet on Jan 18, 2008

Hello there. Bob Drake here to discuss how Windows Server 2008 “Read Only Domain Controllers” (RODC’s) authenticate users differently from the way Windows Server 2003 and Windows Server 2008 standard domain controllers do. The “ Read Only Domain Controller ” is new to Windows Server 2008 and allows for the installation of a domain controller to accommodate common scenarios where users are authenticating over a wide area network (WAN) or there is a physical security concern for the domain controller, such as installations at branch office locations. Another new feature to Windows Server 2008 RODC’s is “ Password Replication Policy ” and depending on how they are configured determines how an RODC authenticates a user.

To understand the authentication difference between a standard domain controller and an RODC, we need to review the “ *How interactive Logon works* ” and “ *Kerberos authentication* ” TechNet articles. In the section *Domain Login (How interactive logon works article),* a user’s credentials are received by *Winlogon* and passed to the LSA (local security authority) which negotiates Kerberos and contacts the domain controller. The domain controller then returns the logon success to the local computers LSA which generates the user’s access token . The Kerberos authentication is seen in the following diagram (taken from the *Kerberos authentication* article):



To see the authentication on the wire, we would need to install a network capture application such as Netmon3.1 (or Wireshark , Ethereal , Packetyzer). In the following network trace, we see a client machine authenticate to a domain controller and is granted access with the “KRB_AS_REP” and “KRB_TGS_REP”:



Frame Number	Time Offset	Conv Id	Source	Destination	Protocol Name	Description
Capture File: C:\Documents and Settings\Administrator\Local Settings\Temp\cap47.tmp						
15	2.183139	{UDP:25, IPv4:24}	10.0.5.9	2K3DC1	KerberosV5	KerberosV5: AS Request Cname: bobdrake Realm: 2K3DOM Sname: krbtgt/2K3DOM
19	5.417790	{UDP:25, IPv4:24}	2K3DC1	10.0.5.9	KerberosV5	KerberosV5: AS Response Ticket[Realm: 2K3DOM.LOCAL, Sname: krbtgt/2K3DOM.LOCAL]
20	5.417790	{UDP:26, IPv4:24}	10.0.5.9	2K3DC1	KerberosV5	KerberosV5: TGS Request Realm: 2K3DOM.LOCAL Sname: host/2k3-xp.2k3dom.local
23	6.429244	{UDP:26, IPv4:24}	2K3DC1	10.0.5.9	KerberosV5	KerberosV5: TGS Response Cname: BobDrake

Now let’s take a look at the “ Password Replication Policies ” and how they affect the RODC authentication behavior. With the installation of an RODC, there are four new attributes and two built-in groups to support RODC operations:

- **msDS-Reveal-OnDemandGroup.** This attribute points to the distinguished name (DN) of the Allowed List. The credentials of the members of the Allowed List are permitted to replicate to the RODC.

- **msDS-NeverRevealGroup.** This attribute points to the distinguished names of security principals that are denied replication to the RODC. This has no impact on the ability of these security principals to authenticate using the RODC. The RODC never caches the credentials of the members of the Denied List. A default list of security principals whose credentials are denied replication to the RODC is provided. This helps ensure that RODCs are secure by default.

- **msDS-RevealedList.** This attribute is a list of security principals whose passwords have ever been replicated to the RODC.

- **msDS-AuthenticatedToAccountList.** This attribute contains a list of security principals in the local domain that have authenticated to the RODC. The purpose of the attribute is to help an administrator determine which computers and users are using the RODC for logon. This enables the administrator to refine the Password Replication Policy for the RODC.

- **Allowed RODC Password Replication Group.** This group is added to the msDS-Reveal-OnDemandGroup.

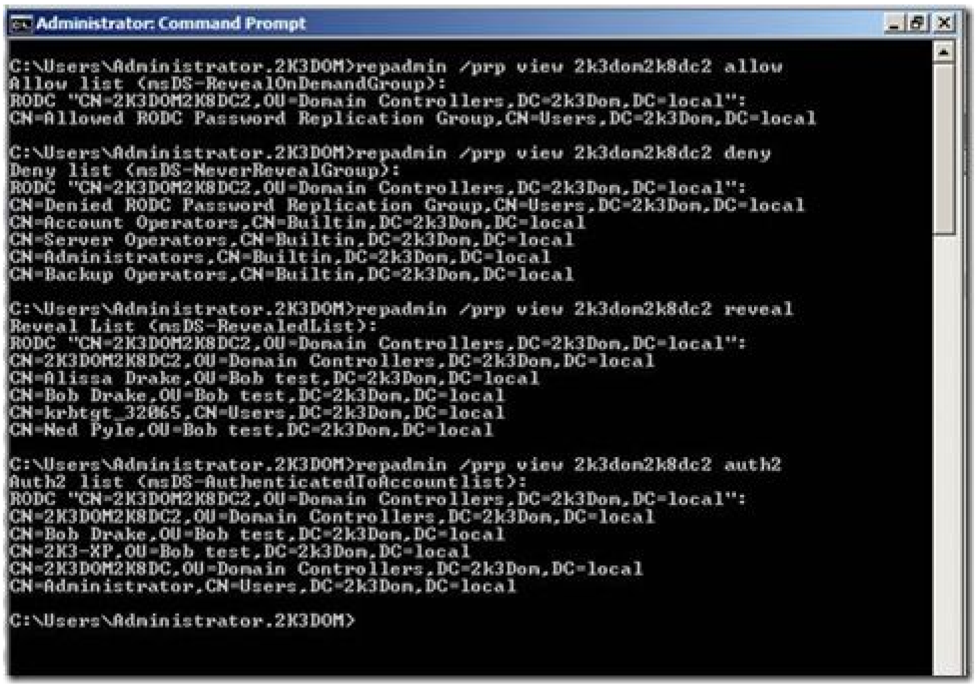
- **Denied RODC Password Replication Group.** This group is added to the msDS-NeverRevealGroup.

Note: *The “Allowed RODC Password Replication Group” has no members by default, and the “Denied RODC Password Replication Group” contains all the ‘VIP’ accounts (Enterprise Administrators, Cert Publishers, Schema Administrators, Etc). As with most things, Deny always trumps Allow.*

Using the commands for “ Repadmin.exe ” (this is built into Windows Server 2008) an administrator can modify the Password Replication Policy groups. To view the current PRP for a specified user:

Repadmin /prp view <RODC> {<List_Name >|<User>}

The following shows the settings for the groups on the RODC through several commands:



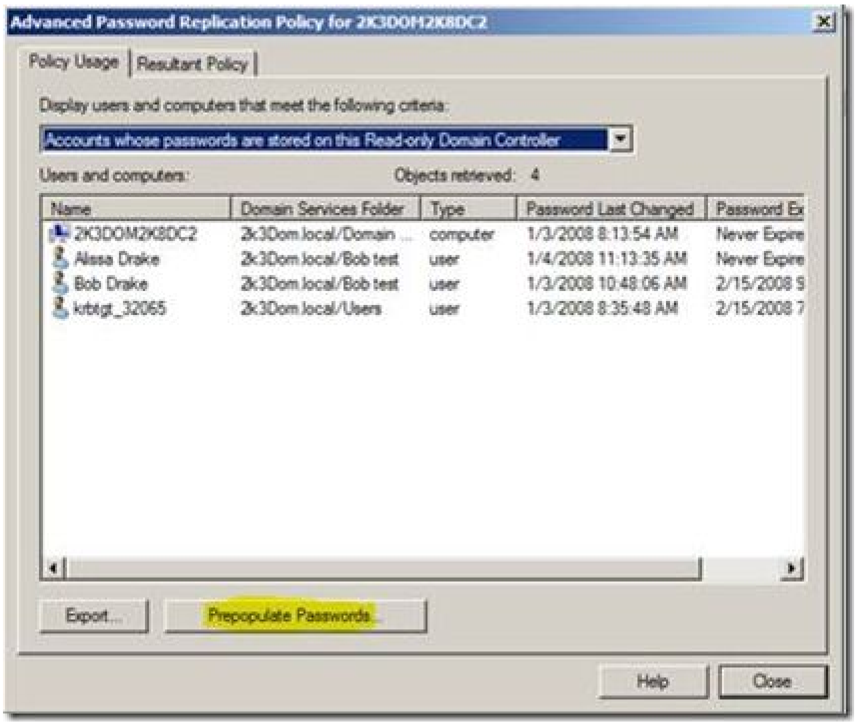
```
C:\Users\Administrator.2K3DOM>repadmin /prp view 2k3dom2k8dc2 allow
Allow list (msDS-RevealOnDemandGroup):
RODC "CN=2K3DOM2K8DC2,OU=Domain Controllers,DC=2k3Dom,DC=local":
CN=Allowed RODC Password Replication Group,CN=Users,DC=2k3Dom,DC=local

C:\Users\Administrator.2K3DOM>repadmin /prp view 2k3dom2k8dc2 deny
Deny list (msDS-NeverRevealGroup):
RODC "CN=2K3DOM2K8DC2,OU=Domain Controllers,DC=2k3Dom,DC=local":
CN=Denied RODC Password Replication Group,CN=Users,DC=2k3Dom,DC=local
CN=Account Operators,CN=Builtin,DC=2k3Dom,DC=local
CN=Server Operators,CN=Builtin,DC=2k3Dom,DC=local
CN=Administrators,CN=Builtin,DC=2k3Dom,DC=local
CN=Backup Operators,CN=Builtin,DC=2k3Dom,DC=local

C:\Users\Administrator.2K3DOM>repadmin /prp view 2k3dom2k8dc2 reveal
Reveal List (msDS-RevealedList):
RODC "CN=2K3DOM2K8DC2,OU=Domain Controllers,DC=2k3Dom,DC=local":
CN=2K3DOM2K8DC2,OU=Domain Controllers,DC=2k3Dom,DC=local
CN=Alissa Drake,OU=Bob test,DC=2k3Dom,DC=local
CN=Bob Drake,OU=Bob test,DC=2k3Dom,DC=local
CN=krbtgt_32065,CN=Users,DC=2k3Dom,DC=local
CN=Ned Pyle,OU=Bob test,DC=2k3Dom,DC=local

C:\Users\Administrator.2K3DOM>repadmin /prp view 2k3dom2k8dc2 auth2
Auth2 list (msDS-AuthenticatedToAccountlist):
RODC "CN=2K3DOM2K8DC2,OU=Domain Controllers,DC=2k3Dom,DC=local":
CN=2K3DOM2K8DC2,OU=Domain Controllers,DC=2k3Dom,DC=local
CN=Bob Drake,OU=Bob test,DC=2k3Dom,DC=local
CN=2K3-XP,OU=Bob test,DC=2k3Dom,DC=local
CN=2K3DOM2K8DC,OU=Domain Controllers,DC=2k3Dom,DC=local
CN=Administrator,CN=Users,DC=2k3Dom,DC=local

C:\Users\Administrator.2K3DOM>
```

Awesome information here! We can see who is on the allowed list (msDS-RevealOnDemand), who is on the deny list (msDS-NeverRevealGroup), who is actually revealed (msDS-RevealedList) and who actually has authenticated to the RODC (msDS-AuthenticatedToAccountlist).

The configuration of a Password Replication Policy is pretty straight forward. Open Active Directory Users and Computers snap-in and select the RODC in the Domain Controllers organizational unit. On the “Password Replication Policy” tab, there are the two groups:

“Allowed RODC Password Replication Group” and “Denied RODC Password Replication Group”. A user can be added to either of the desired groups.

Another really cool feature is the “Prepopulate the password cache for an RODC” button. This button (pictured) allows an administrator to pre-add users that will be authenticating to the RODC.



Advanced Password Replication Policy for 2K3DOM2K8DC2

Display users and computers that meet the following criteria:

Accounts whose passwords are stored on this Read-only Domain Controller

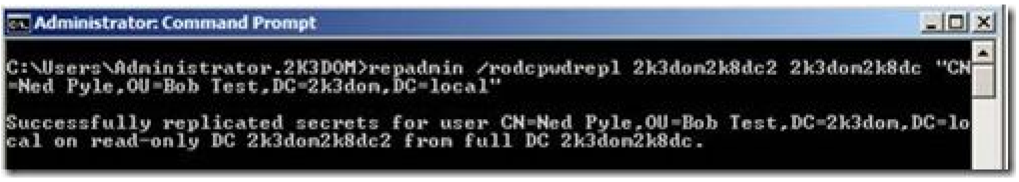
Users and computers: Objects retrieved: 4

Name	Domain Services Folder	Type	Password Last Changed	Password Ex
2K3DOM2K8DC2	2k3Dom.local/Domain ...	computer	1/3/2008 8:13:54 AM	Never Expire
Alissa Drake	2k3Dom.local/Bob test	user	1/4/2008 11:13:35 AM	Never Expire
Bob Drake	2k3Dom.local/Bob test	user	1/3/2008 10:48:06 AM	2/15/2008 9
krbtgt_32065	2k3Dom.local/Users	user	1/3/2008 8:35:48 AM	2/15/2008 7

An administrator could also use the “ Repadmin ” utility to populate the password cache with the following command:

Repadmin /rodcpwdrepl [DSA_LIST] <Hub DC> <User1 Distinguished Name> [<Computer1 Distinguished name> <User2 Distinguished Name>…].

The following shows the user “Ned Pyle” being added to the password cache using Repadmin:

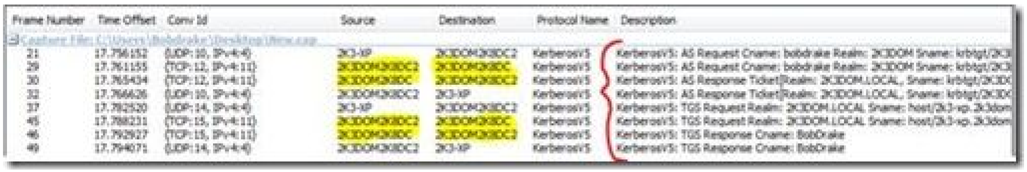


Administrator: Command Prompt

```
C:\Users\Administrator.2K3DOM>repadmin /rodcpwdrepl 2k3dom2k8dc2 2k3dom2k8dc "CN
=Ned Pyle,OU=Bob Test,DC=2k3dom,DC=local"

Successfully replicated secrets for user CN=Ned Pyle,OU=Bob Test,DC=2k3dom,DC=lo
cal on read-only DC 2k3dom2k8dc2 from full DC 2k3dom2k8dc.
```

So how does this affect the RODC? When a user authenticates to an RODC a check is performed to see if the password is cached. If the password is cached, the RODC will authenticate the user account locally. If the user's password is not cached, then the RODC forwards the authentication request to a writable Windows Server 2008 Domain Controller which in turn authenticates the account and passes the authenticated request back to the RODC. Once the user account is authenticated, the RODC makes another request for the replication of the user's password in a unidirectional replication providing the account has been configured to allow replication.

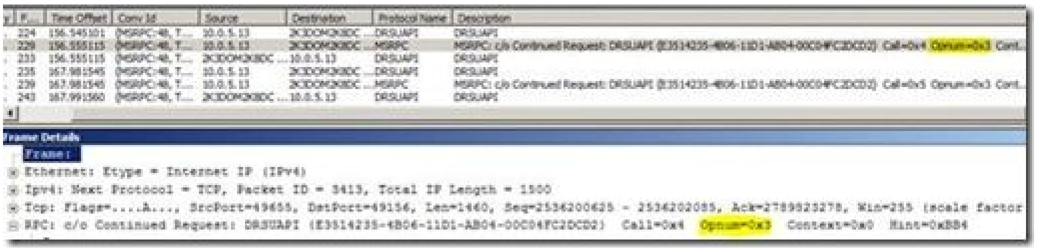
This finally brings us to seeing the difference in authentication. For the following NetMon 3.1 trace, I have configured a user account whose password has been denied replication to the RODC. The user authenticates to the RODC (*2k3DOM2k8DC2*) and the RODC forwards the request to the writable domain controller (*2k3DOM2k8DC*). We see the extra traffic since the user's password has not been cached:



Capture File: C:\Users\Bobdrake\Desktop\New.cap

Frame Number	Time Offset	Conv Id	Source	Destination	Protocol Name	Description
21	17.756152	{UDP:10, IPv4:4}	2K3-XP	2K3DOM2K8DC2	KerberosV5	KerberosV5: AS Request Cname: bobdrake Realm: 2K3DOM Sname: krbtgt/2K3
29	17.761155	{TCP:12, IPv4:11}	2K3DOM2K8DC2	2K3DOM2K8DC	KerberosV5	KerberosV5: AS Request Cname: bobdrake Realm: 2K3DOM Sname: krbtgt/2K3
30	17.765434	{TCP:12, IPv4:11}	2K3DOM2K8DC	2K3DOM2K8DC2	KerberosV5	KerberosV5: AS Response Ticket[Realm: 2K3DOM.LOCAL, Sname: krbtgt/2K3DC
32	17.766626	{UDP:10, IPv4:4}	2K3DOM2K8DC2	2K3-XP	KerberosV5	KerberosV5: AS Response Ticket[Realm: 2K3DOM.LOCAL, Sname: krbtgt/2K3DC
37	17.782520	{UDP:14, IPv4:4}	2K3-XP	2K3DOM2K8DC2	KerberosV5	KerberosV5: TGS Request Realm: 2K3DOM.LOCAL Sname: host/2k3-xp.2k3dom
45	17.788231	{TCP:15, IPv4:11}	2K3DOM2K8DC2	2K3DOM2K8DC	KerberosV5	KerberosV5: TGS Request Realm: 2K3DOM.LOCAL Sname: host/2k3-xp.2k3dom
46	17.792927	{TCP:15, IPv4:11}	2K3DOM2K8DC	2K3DOM2K8DC2	KerberosV5	KerberosV5: TGS Response Cname: BobDrake
49	17.794071	{UDP:14, IPv4:4}	2K3DOM2K8DC2	2K3-XP	KerberosV5	KerberosV5: TGS Response Cname: BobDrake

For the last trace I have allowed the user password to be cached by configuring the Password Replication Policy. The user authentication is the same as above, with the exception to what the RODC does after authenticating the user. Now see the RODC make the request for the user's password to be replicated, but in subsequent logins the password replication request would not be seen since it has been cached:



F...	Time Offset	Conv Id	Source	Destination	Protocol Name	Description
224	156.545101	{MSRPC:48, T...	10.0.5.13	2K3DOM2K8DC ...	DRSUAPI	DRSUAPI
229	156.555115	{MSRPC:48, T...	10.0.5.13	2K3DOM2K8DC ...	MSRPC	MSRPC: c/o Continued Request: DRSUAPI {E3514235-4B06-11D1-AB04-00C04FC2DCD2} Call=0x4 Opnum=0x3 Cont...
233	156.555115	{MSRPC:48, T...	2K3DOM2K8DC ...	10.0.5.13	DRSUAPI	DRSUAPI
235	167.981545	{MSRPC:48, T...	10.0.5.13	2K3DOM2K8DC ...	DRSUAPI	DRSUAPI
239	167.981545	{MSRPC:48, T...	10.0.5.13	2K3DOM2K8DC ...	MSRPC	MSRPC: c/o Continued Request: DRSUAPI {E3514235-4B06-11D1-AB04-00C04FC2DCD2} Call=0x5 Opnum=0x3 Cont...
243	167.991560	{MSRPC:48, T...	2K3DOM2K8DC ...	10.0.5.13	DRSUAPI	DRSUAPI

Frame Details

```
Frame:
+ Ethernet: Etype = Internet IP (IPv4)
+ Ipv4: Next Protocol = TCP, Packet ID = 3413, Total IP Length = 1500
+ Tcp: Flags=....A..., SrcPort=49655, DstPort=49156, Len=1460, Seq=2536200625 - 2536202085, Ack=2789523278, Win=255 (scale factor
- RPC: c/o Continued Request: DRSUAPI (E3514235-4B06-11D1-AB04-00C04FC2DCD2)  Call=0x4  Opnum=0x3  Context=0x0  Hint=0xBB4
```

Note : If the Wide Area Network (WAN) is down and the user account and password has NOT been cached, then the user account will fail to authenticate.

To wrap it up, when a user account is not cached, the RODC forwards the authentication to a writable Domain Controller which does the authentication. If the Users password is allowed to be cached, then the RODC will pull that through a replication request. Once the user has been authenticated, and their password has been cached, any subsequent login can then be handled by the RODC alone. Some people may see an increase in Wide Area Network (WAN) traffic with the introduction to an RODC, but after caching user passwords there should be a significant reduction in traffic and a more secure environment. In my next blog I will discuss how account lockout thresholds affect this process and what Administrators might run into with them.

-Bob Drake