



Replication Metadata

Ghosts in the Wire

Background

- When a change is made to a domain object on a domain controller in Active Directory, those changes are replicated to other domain controllers in the same domain
 - As part of the replication process, metadata about the replication is preserved in “two constructed attributes”
- Any domain user can enumerate these attributes!
- Why care?
 - Let’s us track some changes to AD objects WITHOUT enabling additional logging!
 - More info: <https://www.harmj0y.net/blog/defense/hunting-with-active-directory-replication-metadata/>

What attributes are replicated?

- Object attributes are themselves represented in the forest schema
- They include a **systemFlags** attribute that contains various meta-settings
 - This includes the FLAG_ATTR_NOT_REPLICATED flag, indicating that the given attribute should not be replicated
- So to search for attributes that ARE replicated:
 - The search base needs to be: **CN=schema,CN=configuration,DC=domain,...**
 - The objectClass needs to filter for **attributeSchema**
 - systemFlags is binary, so we need to use
(!systemFlags:1.2.840.113556.1.4.803:=1)

What attributes are replicated?

```
Windows PowerShell
PS C:\Users\harmj0y> $Searcher = [adsisearcher][adsi]"LDAP://CN=schema,CN=config
uration,DC=testlab,DC=local"
PS C:\Users\harmj0y> $Searcher.Filter = '(&(&(objectClass=attributeSchema)(!systemFlags:1.2.840.113556.1.4.803:=1)))'
PS C:\Users\harmj0y> $Searcher.PropertiesToLoad.Add('ldapdisplayname')
0
PS C:\Users\harmj0y> $Searcher.FindAll() | % {$_.Properties.ldapdisplayname}
accountExpires
accountNameHistory
aCSAggregateTokenRatePerUser
aCSAllocableRSVPBandwidth
acSCacheTimeout
acSDirection
acDSBMDeadTime
acDSBMPriority
acDSBMRrefresh
acSEnableACSService
acSEnableRSVPAccounting
acSEnableRSVPMessagelogging
acSEventLogLevel
aCSTidentityName
```

Non-PowerShell enumeration

- **REPADMIN /showobjmeta server “CN=objectDN,...”**
 - Output is text, and repadmin is only available on servers...

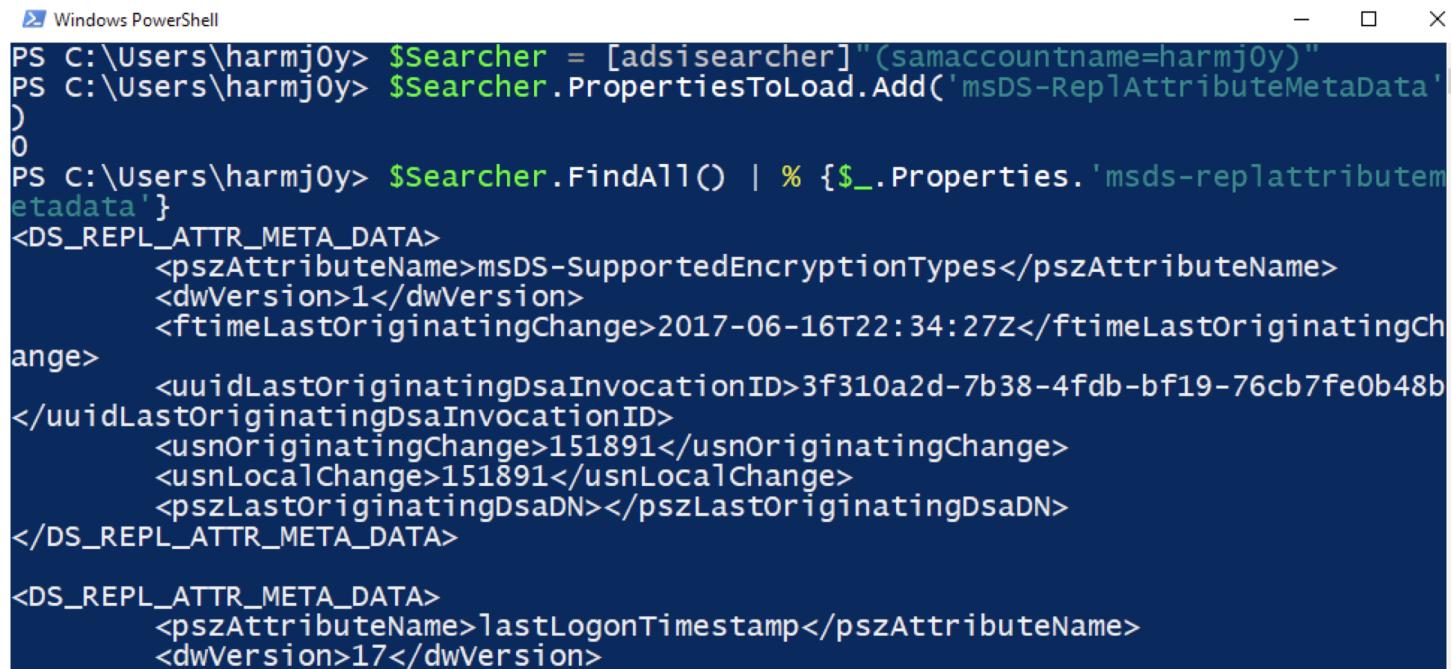
```
Windows PowerShell
PS C:\Users\dfm.a> repadmin /showobjmeta primary "CN=harmj0y,CN=Users,DC=testlab,DC=Local"
30 entries.
Loc.USN          Originating DSA  Org.USN  Org.Time/Date    Ver Attribute
=====          ====== =====  ======  ====== ====== =====
25630 3f310a2d-7b38-4fdb-bf19-76cb7fe0b48b 25630 2017-03-07 11:56:27 1 objectClass
25630 3f310a2d-7b38-4fdb-bf19-76cb7fe0b48b 25630 2017-03-07 11:56:27 1 cn
25630 3f310a2d-7b38-4fdb-bf19-76cb7fe0b48b 25630 2017-03-07 11:56:27 1 givenName
25630 3f310a2d-7b38-4fdb-bf19-76cb7fe0b48b 25630 2017-03-07 11:56:27 1 instanceType
25630 3f310a2d-7b38-4fdb-bf19-76cb7fe0b48b 25630 2017-03-07 11:56:27 1 whenCreated
25630 3f310a2d-7b38-4fdb-bf19-76cb7fe0b48b 25630 2017-03-07 11:56:27 1 displayName
197049 3f310a2d-7b38-4fdb-bf19-76cb7fe0b48b 197049 2017-07-25 01:16:58 15 nTSecurityDescriptor
iptor
25630 3f310a2d-7b38-4fdb-bf19-76cb7fe0b48b 25630 2017-03-07 11:56:27 1 name
151904 3f310a2d-7b38-4fdb-bf19-76cb7fe0b48b 151904 2017-06-16 15:36:32 6 userAccount
rol
25631 3f310a2d-7b38-4fdb-bf19-76cb7fe0b48b 25631 2017-03-07 11:56:27 1 codePage
25631 3f310a2d-7b38-4fdb-bf19-76cb7fe0b48b 25631 2017-03-07 11:56:27 1 countryCode
25632 3f310a2d-7b38-4fdb-bf19-76cb7fe0b48b 25632 2017-03-07 11:56:27 2 dBcspwd
25631 3f310a2d-7b38-4fdb-bf19-76cb7fe0b48b 25631 2017-03-07 11:56:27 1 logonHours
25632 3f310a2d-7b38-4fdb-bf19-76cb7fe0b48b 25632 2017-03-07 11:56:27 2 unicodePwd
25632 3f310a2d-7b38-4fdb-bf19-76cb7fe0b48b 25632 2017-03-07 11:56:27 2 ntPwdHistory
25632 3f310a2d-7b38-4fdb-bf19-76cb7fe0b48b 25632 2017-03-07 11:56:27 2 pwdLastSet
25631 3f310a2d-7b38-4fdb-bf19-76cb7fe0b48b 25631 2017-03-07 11:56:27 1 primaryGroup
25633 3f310a2d-7b38-4fdb-bf19-76cb7fe0b48b 25633 2017-03-07 11:56:27 1 supplement
```

msDS-ReplAttributeMetaData

- The constructed **msDS-ReplAttributeMetaData** property is associated with every user/group/computer/etc.
 - *As long as you have the right to read an object, you can read its metadata!*
- This metadata includes things like
 - The name of the attribute that changed on the object
 - When the attribute changed
 - The number of times the attribute changed
 - The “Directory System Agent” (traceable to a domain controller) that initiated the change

msDS-ReplAttributeMetaData

- To retrieve, just use **PropertiesToLoad.Add('msDS-ReplAttributeMetaData')** with your searcher:



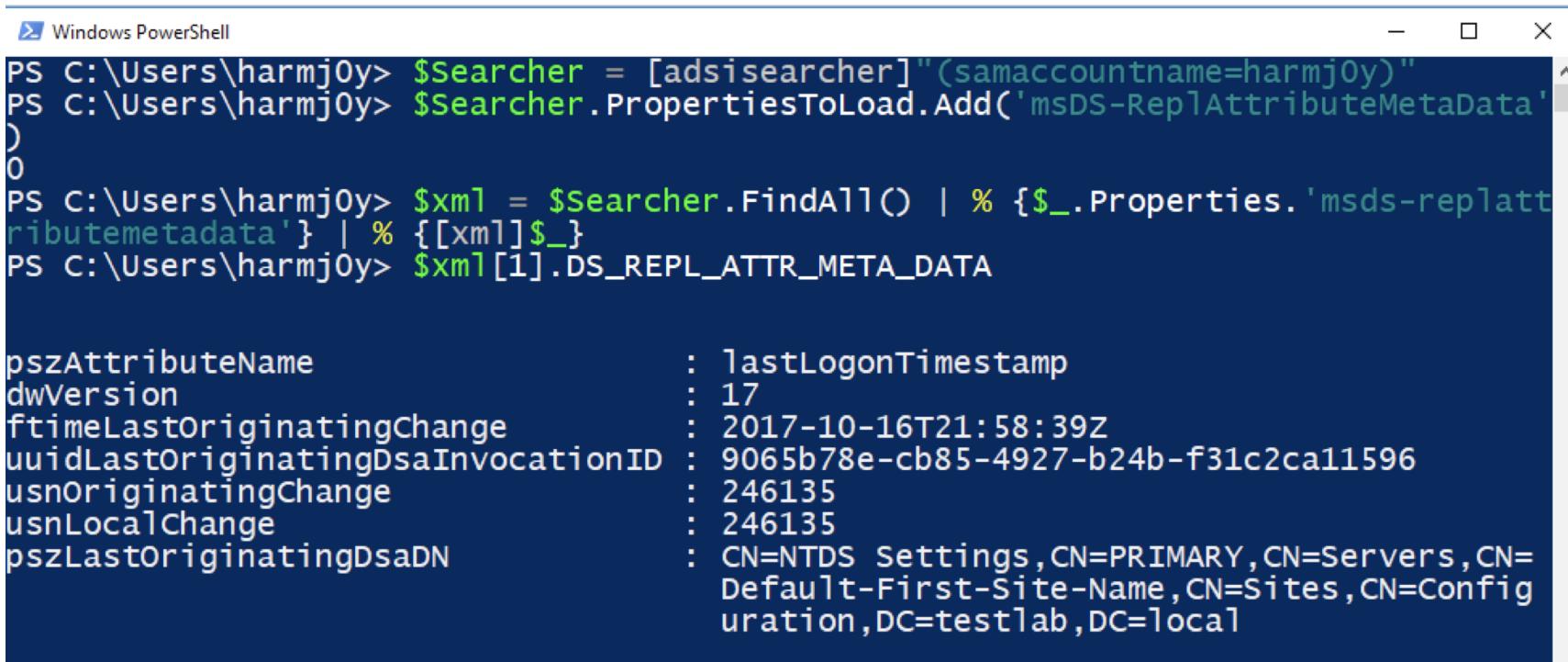
A screenshot of a Windows PowerShell window titled "Windows PowerShell". The command shown is:

```
PS C:\Users\harmj0y> $Searcher = [adsisearcher]"(samaccountname=harmj0y)"
PS C:\Users\harmj0y> $Searcher.PropertiesToLoad.Add('msDS-ReplAttributeMetaData')
)
0
PS C:\Users\harmj0y> $Searcher.FindAll() | % {$_ .Properties .'msds-replattributemetadata'}
<DS_REPL_ATTR_META_DATA>
    <pszAttributeName>msDS-SupportedEncryptionTypes</pszAttributeName>
    <dwVersion>1</dwVersion>
    <ftimeLastOriginatingChange>2017-06-16T22:34:27Z</ftimeLastOriginatingChange>
    <uuidLastOriginatingDsaInvocationID>3f310a2d-7b38-4fdb-bf19-76cb7fe0b48b
</uuidLastOriginatingDsaInvocationID>
    <usnOriginatingChange>151891</usnOriginatingChange>
    <usnLocalChange>151891</usnLocalChange>
    <pszLastOriginatingDsaDN></pszLastOriginatingDsaDN>
</DS_REPL_ATTR_META_DATA>

<DS_REPL_ATTR_META_DATA>
    <pszAttributeName>lastLogonTimestamp</pszAttributeName>
    <dwVersion>17</dwVersion>
```

msDS-ReplAttributeMetaData

- The array of XML blobs can be parsed using the [xml] accelerator:



```
Windows PowerShell
PS C:\Users\harmj0y> $Searcher = [adsisearcher]"(samaccountname=harmj0y)"
PS C:\Users\harmj0y> $Searcher.PropertiesToLoad.Add('msDS-ReplAttributeMetaData')
PS C:\Users\harmj0y> $xml = $Searcher.FindAll() | % {$_.Properties.'msds-replattributemetadata'} | % {[xml]$_}
PS C:\Users\harmj0y> $xml[1].DS_REPL_ATTR_META_DATA

{
    pszAttributeName : lastLogonTimestamp
    dwVersion : 17
    ftimeLastOriginatingChange : 2017-10-16T21:58:39Z
    uuidLastOriginatingDsaInvocationID : 9065b78e-cb85-4927-b24b-f31c2ca11596
    usnOriginatingChange : 246135
    usnLocalChange : 246135
    pszLastOriginatingDsaDN : CN=NTDS Settings,CN=PRIMARY,CN=Servers,CN=Default-First-Site-Name,CN=Sites,CN=Configuration,DC=testlab,DC=local
}
```

Interpreting msDS-ReplAttributeMetaData

- **pszAttributeName** : the name of the attribute that changed
- **dwVersion** : the number of times the attribute has changed
- **ftimeLastOriginatingChange** : the time (in UTC) the attribute changed
- **pszLastOriginatingDsaDN** : the “directory services agent” the change originated from

Sidenote: Linked Attributes

- In order to understand how/why the second attribute is different, you need to be aware of “linked value replication”
 - *“allows individual values of a multivalued attribute to be replicated separately”*
 - **In English:** Active Directory calculates the value of a given attribute, referred to as the *back link*, from the value of another attribute, referred to as the *forward link*
- The **member** property of a group is a *forward link*, while the **memberof** property of a group/user is a *back link*
 - Note: only *forward links* are writable!

msDS-ReplValueMetaData

- Because of how forward/back links are replicated, the previous values of these attributes are stored in replication metadata!
 - This means if we user is added and then removed from a group, we can retrieve the value of the deleted user name!
- Replication metadata is stored as an XML blob (again, only for linked attributes) in the **msDS-ReplValueMetaData** property
- Can be retrieved by adding this property to your searcher, same as **msDS-ReplAttributeMetaData**

msDS-ReplValueMetaData

```
Windows PowerShell
PS C:\Users\harmj0y> $Searcher = [adsisearcher]"(samaccountname=Domain Admins)"
PS C:\Users\harmj0y> $Searcher.PropertiesToLoad.Add('msds-replvaluemetadata')
0
PS C:\Users\harmj0y> $xml = $Searcher.FindAll() | % {$_.Properties.'msds-replvaluemetadata'} | % {[xml]$_}
PS C:\Users\harmj0y> $xml[0].DS_REPL_VALUE_META_DATA

pszAttributeName : member
pszObjectDn   : CN=user,CN=Users,DC=testlab,DC=local
cbData          : 0
pbData          :
ftimeDeleted   : 2017-09-17T19:47:27Z
ftimeCreated   : 2017-09-17T19:46:57Z
dwVersion      : 2
ftimeLastOriginatingChange : 2017-09-17T19:47:27Z
uuidLastOriginatingDsaInvocationID : 9065b78e-cb85-4927-b24b-f31c2ca11596
usnOriginatingChange : 238205
usnLocalChange  : 238205
pszLastOriginatingDsaDN   : CN=NTDS Settings,CN=PRIMARY,CN=Servers,CN=Default-First-Site-Name,CN=Sites,CN=Configuration,DC=testlab,DC=local
```

Interpreting msDS-ReplValueMetaData

- **dwObjectDn** : the member that was added
- **ftimeDeleted** : the time (UTC) the member has been removed (0 if the object is currently still a member)
- **ftimeCreated** : the time (UTC) the member was first added
- **dwVersion** : the number of times the attribute has changed
 - odd if the user is still a member of the group
 - even if the user was added and then removed

PowerView Implementations

- **Get-DomainObjectAttributeHistory**
 - Retrieves the 'msds-replattributemetadata' data and parses the XML to proper object output
- **Get-DomainObjectLinkedAttributeHistory**
 - Retrieves the 'msds-replvaluemetadata' data for linked attributes and parses the XML to proper object output
- **Get-DomainGroupMemberDeleted**
 - Retrieves any users who were removed from groups by wrapping **Get-DomainObjectLinkedAttributeHistory**'s functionality
- All of these, by default, retrieve this data for every object in the domain

Resolving **LastOriginatingDsaDN**

- The object has a **NTDS-DSA** category, and is linked to a server topology reference (`objectclass=msDSR-Member`) through the **serverreferencebl** property
- This msDSR-Member object:
 - has a **serverrefrence** property that matches the **LastOriginatingDsaDN**
 - has a list of server distinguished names in its **msdfscomputerreference** property, which refer to the actual domain controllers
- So we can resolve a LastOriginatingDsaDN by:
 - Using an LDAP filter of “`(serverreference=$LastOriginatingDsaDN)`”
 - Extracting the **msdfscomputerreference** property
 - Re-querying the domain to return the compelte object

Resolving LastOriginatingDsaDN

```
Windows PowerShell
PS C:\Users\harmj0y> $User = Get-DomainGroupMemberDeleted | Select -First 1
PS C:\Users\harmj0y> $User

GroupDN          : CN=Domain Admins,CN=Users,DC=testlab,DC=local
MemberDN         : CN=user,CN=Users,DC=testlab,DC=local
TimeFirstAdded   : 2017-09-17T19:46:57Z
TimeDeleted      : 2017-09-17T19:47:27Z
LastOriginatingChange : 2017-09-17T19:47:27Z
TimesAdded       : 1
LastOriginatingDsaDN : CN=NTDS Settings,CN=PRIMARY,CN=Servers,CN=Default-First-Site-Name,CN=Sites,CN=Configuration,DC=testlab,DC=local

PS C:\Users\harmj0y> Get-DomainObject -LDAPFilter "(&(serverreference=$($User.LastOriginatingDsaDN))" | % {Get-DomainObject $_."msdfscomputerreference" -Properties 'dnshostname'}
dnshostname
-----
PRIMARY.testlab.local
```

This would be a good time to
attempt Lab: Replication Metadata