What is DS-Replication-Get-Changes?

DS-Replication-Get-Changes, and its more dangerous partner DS-Replication-Get-Changes-All, are Active Directory extended rights that allow an account to request replicated directory data from a Domain Controller. Domain Controllers hold these rights so they can sync with each other. The risk is that the rights also enable DCSync: any account that holds them can ask a real DC to hand over an account password hash, including KRBTGT, without ever running code on the DC. Because the request looks like normal DC-to-DC traffic, auditing exactly which accounts hold these rights is one of the highest-value Active Directory checks.

HOW IT WORKS

01 The attack it enables: DCSync

DCSync is the abuse of these replication rights. An attacker whose account holds DS-Replication-Get-Changes-All does not need malware on a Domain Controller. They simply ask a DC to replicate an account's secrets to them, exactly as another DC would.

The DC complies, because the request is legitimate replication traffic. The attacker can name any account, up to and including every Domain Admin and the KRBTGT account whose hash unlocks Golden Tickets. One permission, granted carelessly, becomes the key to the whole domain.

02 How the attack runs

With the replication right in hand, DCSync is a single command:

- `lsadump::dcsync /domain:corp.local /user:krbtgt` (Mimikatz)
- `secretsdump.py -just-dc corp.local/user@dc-ip` (Impacket dumps every hash)

Attackers also chain it the other way: if they can write permissions on the domain object (for example through WriteDACL), they grant their own account the replication right first, then run DCSync. That is why both holding and being able to grant these rights matter.

HOW TO DEFEND

- Enumerate who holds the rights. List every principal with DS-Replication-Get-Changes-All on the domain object. The answer should be Domain Controllers and a tiny set of admin groups, nothing else.
- Remove stale grants to old sync tools, service accounts, or migrated objects.
- Protect the domain ACL so attackers cannot grant themselves the right via WriteDACL or GenericAll.
- Monitor for replication requests from any source IP that is not a Domain Controller. That is the clearest DCSync detection signal.

SOURCES

[1] MITRE ATT&CK Enterprise Matrix

[2] Microsoft: Best Practices for Securing Active Directory

[3] NIST SP 800-115 Technical Guide to Security Testing

THE TWO QUESTIONS TO ASK

For every non-DC account, ask: can it use DS-Replication-Get-Changes-All, and can it grant that right to itself by editing the domain ACL? Either answer being yes is a path to full compromise.