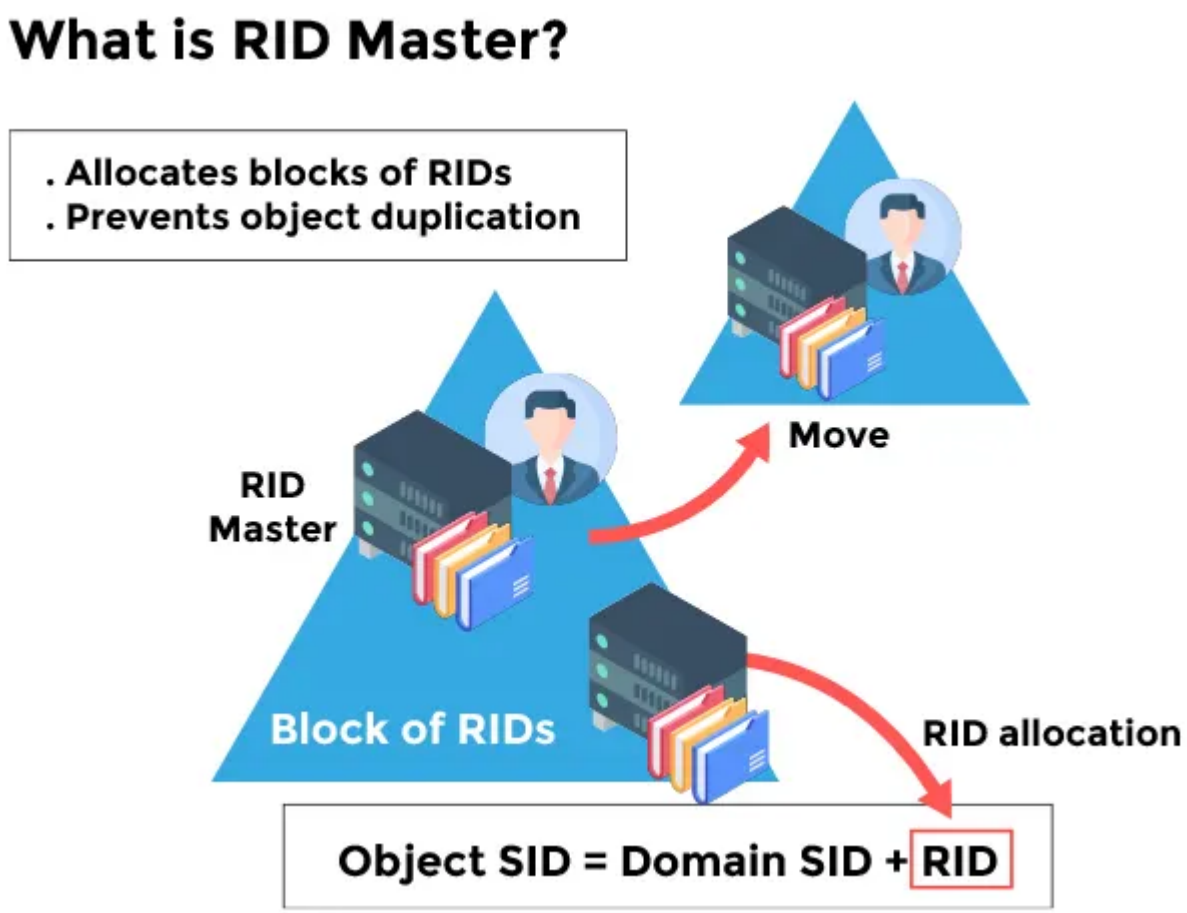
Relative Identifier Master (RID Master) is a domain-level role; there is one RID Master in each domain in an AD forest. It is responsible for allocating active and standby RID pools to DCs in its domain. RID pools consist of a unique, contiguous range of RIDs, which are used to generate a unique security identifier (SID) for a newly created object. Accordingly, it is important to ensure that all DCs, including those in remote or staging sites, have network connectivity to the RID Master so they are reliably able to obtain RID pools. The RID Master is also responsible for moving objects from one domain to another within a forest.

Generally, the RID Master role is assigned to the primary domain controller (PDC) in a domain because the PDC typically receives the most attention from administrators and therefore has high availability. In mature domains, the overhead generated by the RID Master role is negligible.

The loss of a domain's RID Master will eventually lead to an inability to create new objects in the domain, since the RID pools in the other DCs will become depleted. However, in mature environments, this would take a considerable length of time — there are relatively few object creation events, and each DC is assigned a pool of 500 RIDs and requests more whenever it has consumed half of them.

Bringing a RID Master back online after having seized its role can introduce duplicate RIDs into the domain, so this role should be seized only if the DC that owns it cannot be brought back online.



PDC Emulator (PDCE)

Primary Domain Controller (PDC Emulator or PDCE) is a domain level role; there is one PDC Emulator in each domain in an Active Directory forest.

PDC emulator controls authentication such as, Kerberos and NTLM, within the domain. More broadly, it is responsible for the following crucial operations:

Backward compatibility. In the older single-master model of Active Directory, only one DC in the domain is allowed to process updates. The PDCE mimics the single-master behavior of a Windows NT primary domain controller. To provide backward compatibility, the PDCE registers as the target DC for legacy applications that perform writable operations and certain administrative tools that are unaware of the multi-master behavior of DCs.

Time synchronization. Each PDCE serves as the master time source within its domain; all the other DCs in the domain synchronize their clocks to it. The PDCE in the forest root domain serves as the preferred Network Time Protocol (NTP) server in the forest; the PDCE in every other domain