SECURING WINDOWS SERVICES

Windows Server 2008 expands the number of service accounts from three to six, with more granular controls to limit service privileges and mitigate potential damage of compromised systems.

Pre-Windows Server 2008/Vista service accounts

LocalService Account	Has minimum privilege on the local computer and presents anonymous credentials on the network.
NetworkService Account	Has minimum privileges on the local computer and acts as the computer on the network. By default, the remote token contains SIDs for the Everyone and Authenticated User groups.
LocalSystem Account	Has extensive privileges on the local computer and acts as the computer on the network. Its token includes the NT AUTHORITY\SYSTEM and BUILTIN\Administrator SIDs, which have permissions to most system objects.

Windows Server 2008/Vista service accounts

LocalService Account (Fully Restricted)	Has no access to resources (e.g., TCP/IP NetBIOS Helper service).
LocalService Account (No Network Access)	Restricted to local resources; no network access (e.g., Peer Name Resolution Protocol service).
NetworkService Account	Has minimum privileges on the local computer; can present itself to the network (e.g., Windows Event Collector service).
NetworkService Account (Fully Restricted)	Still has network access, but it is limited by the Network Firewall policy in the Windows Firewall. Cannot access system resources (e.g., IPsec Policy Agent service).
LocalSystem Account	Has extensive privileges on the local computer and can present itself to the network (e.g., Background Intelligent Transfer Service).
LocalSystem Account (Firewall Restricted)	Still has extensive privileges on the local computer but network access is restricted by the Network Firewall policy in the Windows Firewall (e.g., Diagnostic System Host service).