Blocking Remote Use of Local Accounts

The use of local accounts for remote access in Active Directory environments is problematic for a number of reasons. By far, the biggest problem is that when an administrative local account has the same user name and password on multiple machines, an attacker with administrative rights on one machine can easily obtain the account’s password hash from the local Security Accounts Manager (SAM) database and use it to gain administrative rights over the other machines using “pass the hash” techniques.

Our latest security guidance responds to these problems by taking advantage of new Windows features to block remote logons by local accounts. Windows 8.1 and Windows Server 2012 R2 introduced two new security identifiers (SIDs), which are also defined on Windows 7, Windows 8, Windows Server 2008 R2 and Windows Server 2012 after installing [KB 2871997](http://support.microsoft.com/kb/2871997):

S-1-5-113: NT AUTHORITY\Local account

S-1-5-114: NT AUTHORITY\Local account and member of Administrators group

The former SID is added to the user’s access token at the time of logon if the user account being authenticated is a local account. The latter SID is also added to the token if the local account is a member of the BUILTIN\Administrators group. These SIDs can grant or deny access to all local accounts or all administrative local accounts – for example, in User Rights Assignments to “Deny access to this computer from the network” and “Deny log on through Remote Desktop Services”, as we recommend in our latest security guidance. Prior to the definition of these SIDs, you would have had to explicitly name each local account to be restricted to achieve the same effect.

In the initial release of the Windows 8.1 and Windows Server 2012 R2 guidance, we denied network and remote desktop logon to “Local account” (S-1-5-113) for all Windows client and server configurations, which blocks all remote access for all local accounts.

We have since discovered that Failover Clustering relies on a non-administrative local account (CLIUSR) for cluster node management and that blocking its network logon access causes cluster services to fail. Because the CLIUSR account is not a member of the Administrators group, replacing S-1-5-113 with S-1-5-114 in the “Deny access to this computer from the network” setting allows cluster services to work correctly while still providing protection against “pass the hash” types of attacks by denying network logon to administrative local accounts.

While we could keep the guidance as it is and add a “special case” footnote for failover cluster scenarios, we will instead opt to simplify deployments and change the Windows Server 2012 R2 Member Server baseline as follows:

|  |  |
| --- | --- |
| **Policy Path** | Computer Configuration\Windows Settings\Local Policies\User Rights Assignment |
| **Policy Name** | Deny access to this computer from the network |
| **Original Value** | Guests, Local account (\*) |
| **New Value** | Guests, Local account and member of Administrators group (\*) |

*(\*) The guidance also recommends adding Domain Admins and Enterprise Admins to these restrictions except on domain controllers and dedicated admin workstations. DA and EA are domain-specific and can’t be specified in generic GPO baselines.*

Note that this change applies only to the Member Server baseline and that the restriction on remote desktop logon is not being changed. Organizations can still choose to deny network access to “Local account” for non-clustered servers.

Note also that the restrictions on local accounts are intended for Active Directory domain-joined systems. Non-joined, workgroup Windows computers cannot authenticate domain accounts, so if you apply restrictions against remote use of local accounts on these systems, you will be able to log on only at the console.