How to Protect Credentials in Windows Server 2016

Adam Stetson
Systems Engineer, Security Expert

Credentials are the keys to an account. By harvesting credentials, attackers can enter your network, move laterally and escalate their privileges to steal your data. Windows Server 2016 has several features for minimizing the chance that attackers will be able to harvest credentials;

Using the Protected Users Group

Putting users, especially highly privileged users, in the "Protected Users" group helps you protect against compromise of their credentials by disabling authentication options that are less secure. For example, Windows does not cache the credentials of members of this group locally, so they are never left on workstations for attackers to harvest. In addition, user accounts that are members of this group cannot:

- Use default credentials delegation
- Use Windows Digest
- Use NTLM
- Use Kerberos long-term keys
- Sign on offline
- Use NT LAN Manager (NTLM) for authentication
- Use DES for Kerberos pre-authentication
- Use RC4 cipher suites for Kerberos pre-authentication
- Be delegated privileges using constrained delegation
- Be delegated privileges using unconstrained delegation
- Renew user ticket-granting tickets (TGTs) past the initial 240-minute lifetime

Using Account Preferences

User Accounts

For user accounts that need less stringent protection, you can use the following security options, which are available for any AD account:

- **Logon Hours** — Enables you to specify when users can use an account.
- **Logon Workstations** — Enables you to limit the computers the account can sign in to.
- **Password Never Expires** — Absolves the account from the "Maximum password age" policy setting; don't configure this option for privileged accounts.
- **Smart card is required for interactive logon** — Requires a smart card to be presented for the account to sign in.
- **Account is sensitive and cannot be delegated** — Ensures that trusted applications cannot forward the account's credentials to other services or computers on the network.
- **This account supports Kerberos AES 128-bit encryption** — Allows Kerberos AES 128-bit encryption.
- **This account supports Kerberos AES 256-bit encryption** — Allows Kerberos AES 256-bit encryption. Use this option for privileged accounts.
- **Account expires** — Enables you to specify an end date for the account.

Computer Accounts

In addition to controlling user accounts, you also need to understand and manage the reach of computer and service accounts. When you join a computer to the domain for the first time, Windows creates a computer account in Active Directory in the "Computers" container and automatically assigns it a password. AD manages these passwords and updates them automatically every 30 days.

To manage the permissions of computer accounts and control which Group Policies are applied to them, you can add them to groups and move them to different OUs. You can also disable and reset computer accounts:

- **Disabling** a computer account means that the computer cannot connect to the domain anymore. If you delete a computer account and the computer is still operational, you'll need to rejoin the computer to the domain if you want it to regain domain membership.
- **Resetting** a computer account removes the connection between the computer and the domain.

Service Accounts

Service accounts are a special type of account that Windows services use to interact with the operating system and resources on the network. (It's also possible to create user accounts and configure them to run as service accounts, but that is not convenient.)

There are three types of built-in service accounts:

- **Local system** — The NT AUTHORITY\SYSTEM account has privileges equivalent to the local Administrators group on the computer.
- **Local service** — The NT AUTHORITY\LocalService account has privileges equivalent to the local Users group on the computer.
- **Network service** — The NT AUTHORITY\NetworkService account has privileges equivalent to the local Users group on the computer.

To protect these accounts, ensure a sysadmin updates their passwords on a regular basis. This is a manual process if you use native tools.

Group Managed Service Accounts and Virtual Accounts

A Group Managed Service Account is a special type of service account; AD automatically updates the passwords of these accounts. A virtual account is the computer-specific local equivalent of a Group Managed Service Account.

Using Windows Defender Credential Guard

Windows Defender Credential Guard is a new technology in Windows 10 and Windows Server 2016 that helps to protect credentials from attackers who try to harvest them by using malware. Windows Defender Credential Guard uses virtualization-based security that allows you to isolate secrets, such as cached credentials, so that only privileged software can access them.

In virtualization-based security, the specific processes that use credentials or data, and the memory associated with those processes, run in a separate operating system parallel with, but independent of, the host operating system. This virtual operating system protects processes from attempts by any external software to read the data that those processes store and use. Windows Defender Credential Guard takes advantage of hardware security, including secure boot and virtualization.

You can manage Windows Defender Credential Guard using Group Policy, Windows Management Instrumentation (WMI), or Windows PowerShell.

Windows Defender Credential Guard does not allow the use of:

- Unconstrained Kerberos delegation
- NT LAN Manager version 1 (NTLMv1)
- Microsoft Challenge Handshake Authentication Protocol (MS-CHAPv2)
- Digest
- Credential Security Support Provider (CredSSP)
- Kerberos DES encryption

Using the Local Administrator Password Solution

Microsoft's Local Administrator Password Solution (LAPS) provides a secure central repository for the passwords all built-in local Administrator accounts and automates proper management of those passwords. In particular, LAPS:

- Ensures that local administrator passwords are unique on each computer
- Automatically changes all local administrator passwords every 30 days
- Provides configurable permissions to control access to passwords
- Transmits passwords to the client in a secure, encrypted manner

Using the Active Directory Administrative Center

The Active Directory Administrative Center enables you to search your Active Directory for accounts that are ripe for takeover by attackers. In particular, you should regularly look for the following types of accounts:

- **User accounts whose passwords never expire** — You should avoid configuring accounts with fixed passwords because they are less secure than accounts with passwords that users have to update periodically.
- **Inactive user accounts** — Inactive user accounts usually belong to a person who has left the organization. The Active Directory Administrative Center console enables you to find accounts that haven't signed in for a specified number of days.

Deleting or disabling these user accounts prevents them from being misused by outside attackers or malicious insiders.