WINDOWS DOMAIN CONTROLLER

Limit physical access

Encrypt the disks on which the domain controller runs on

Secure the Directory Services Restore Mode password

What	Why
1. User Configuration	Protect your credentials.
2. Network Configuration	Establish communications.
3. Features and Roles Configuration	Add what you need, remove what you don't.
4. Update Installation	Patch vulnerabilities.
5. NTP Configuration	Prevent clock drift.
6. Firewall Configuration	Minimize your external footprint.
7. Remote Access Configuration	Harden remote administration sessions.
8. Service Configuration	Minimize your attack surface.
9. Further Hardening	Protect the OS and other applications.
10. Logging and Monitoring	Know what's happening on your system.

Secure the Directory Services Restore Mode password

Directory Services Restore Mode (DSRM) is a special mode for fixing Active Directory offline when something's gone wrong. The DSRM password is a special back door that provides administrative access to the directory. You use this in an offline, text mode state. Protect this password like it's the one thing that can sink your forest, because it is just that.

```
ntdsutil "set dsrm password" "sync from domain account <DomainAdminAccount>" q q
```

References:

https://technet.microsoft.com/en-us/library/cc755321(WS.10).aspx

https://docs.microsoft.com/en-us/windows-server/identity/ad-ds/plan/security-best-practices/securing-domain-controllers-against-attack

https://adsecurity.org/?p=3377

https://blogs.technet.microsoft.com/askpfeplat/2012/09/26/what-can-be-used-to-keep-active-directory-data-secure/

https://www.concurrency.com/blog/w/enable-bitlocker,-automatically-save-keys-to-activ

https://www.upguard.com/blog/the-windows-server-hardening-checklist

http://www.itprotoday.com/management-mobility/5-steps-secured-active-directory