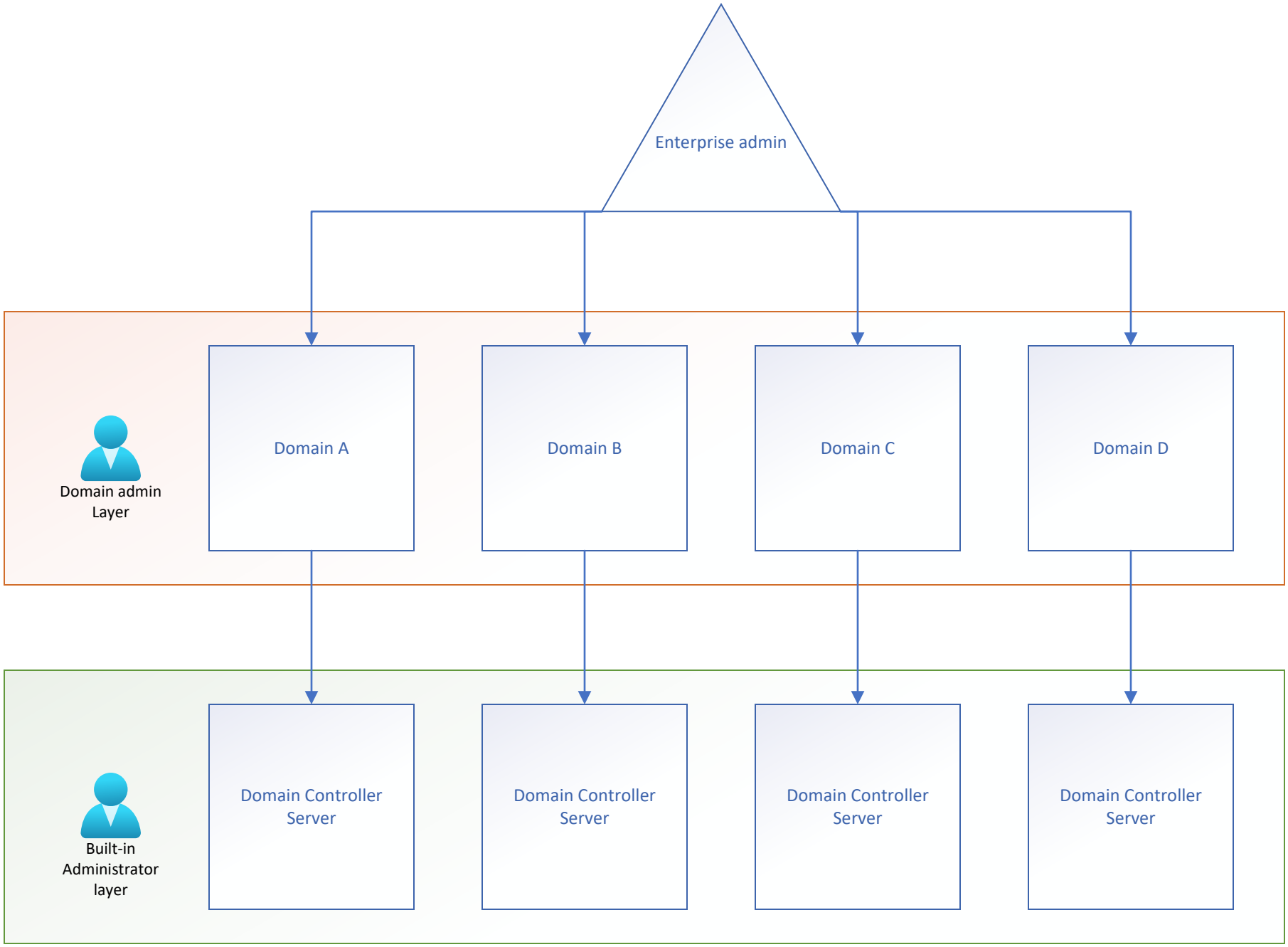
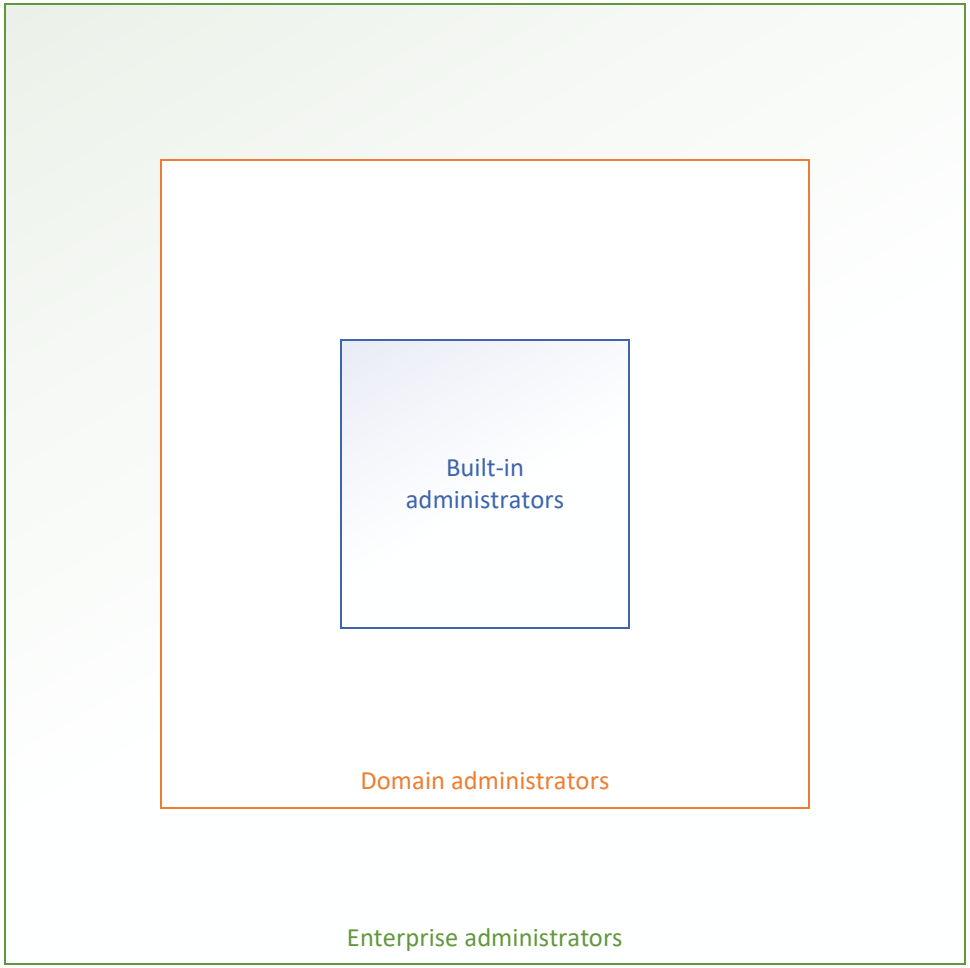
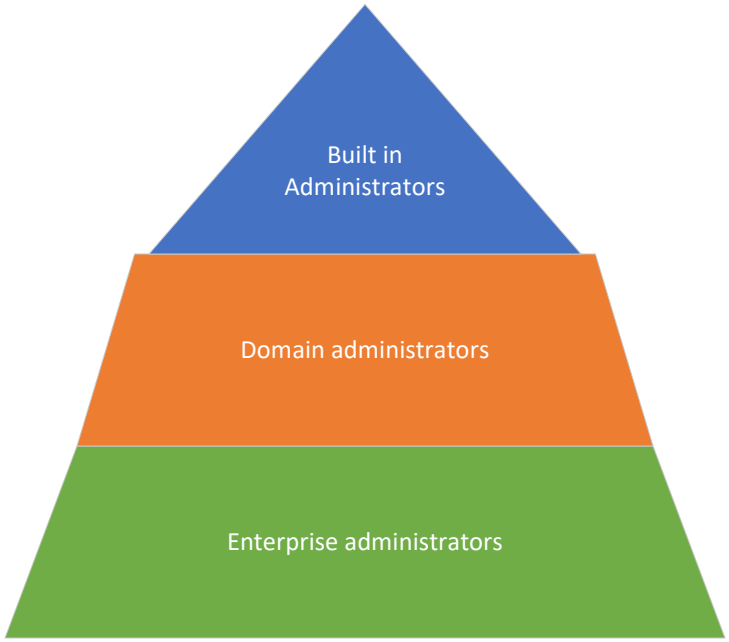
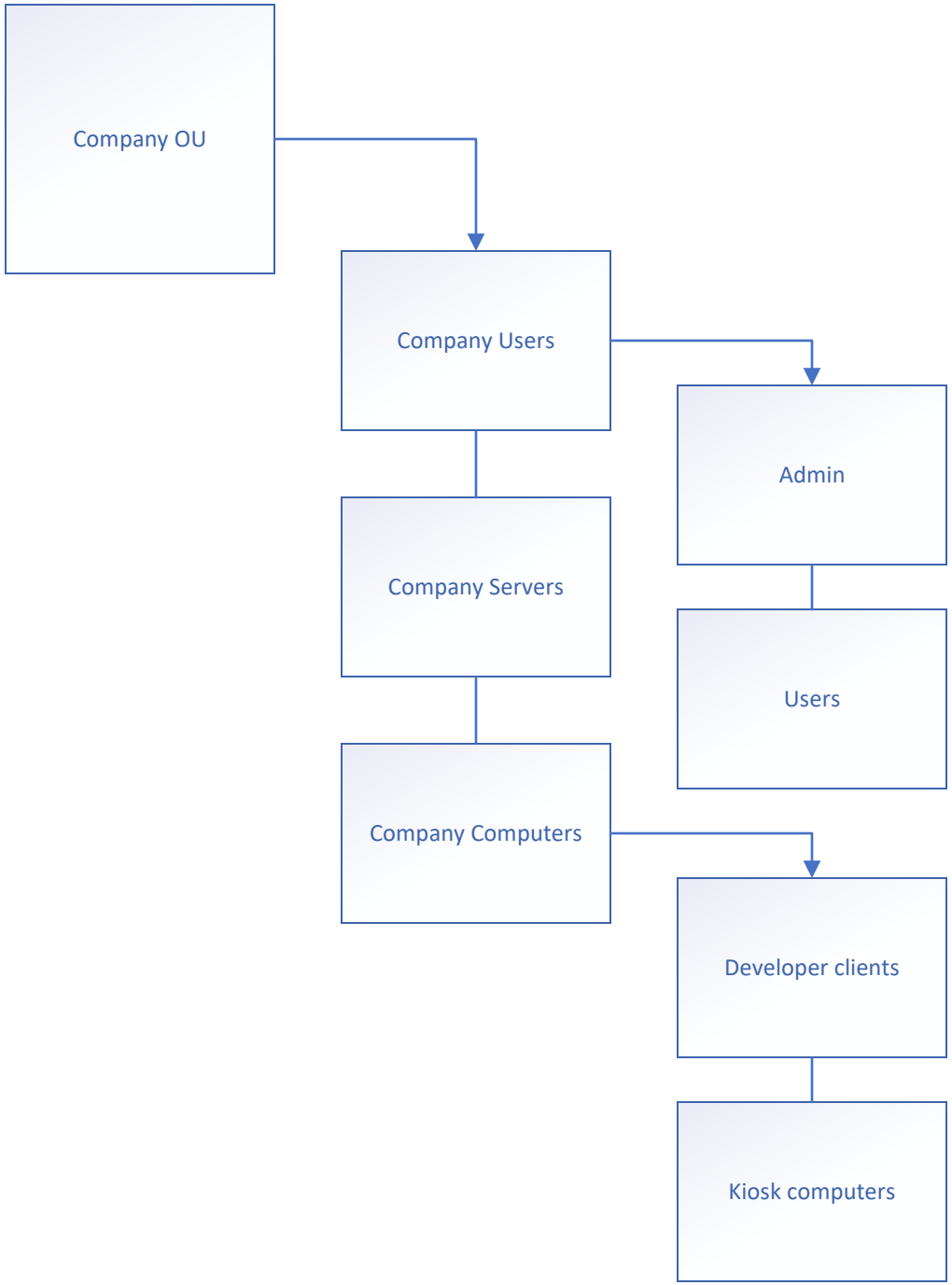
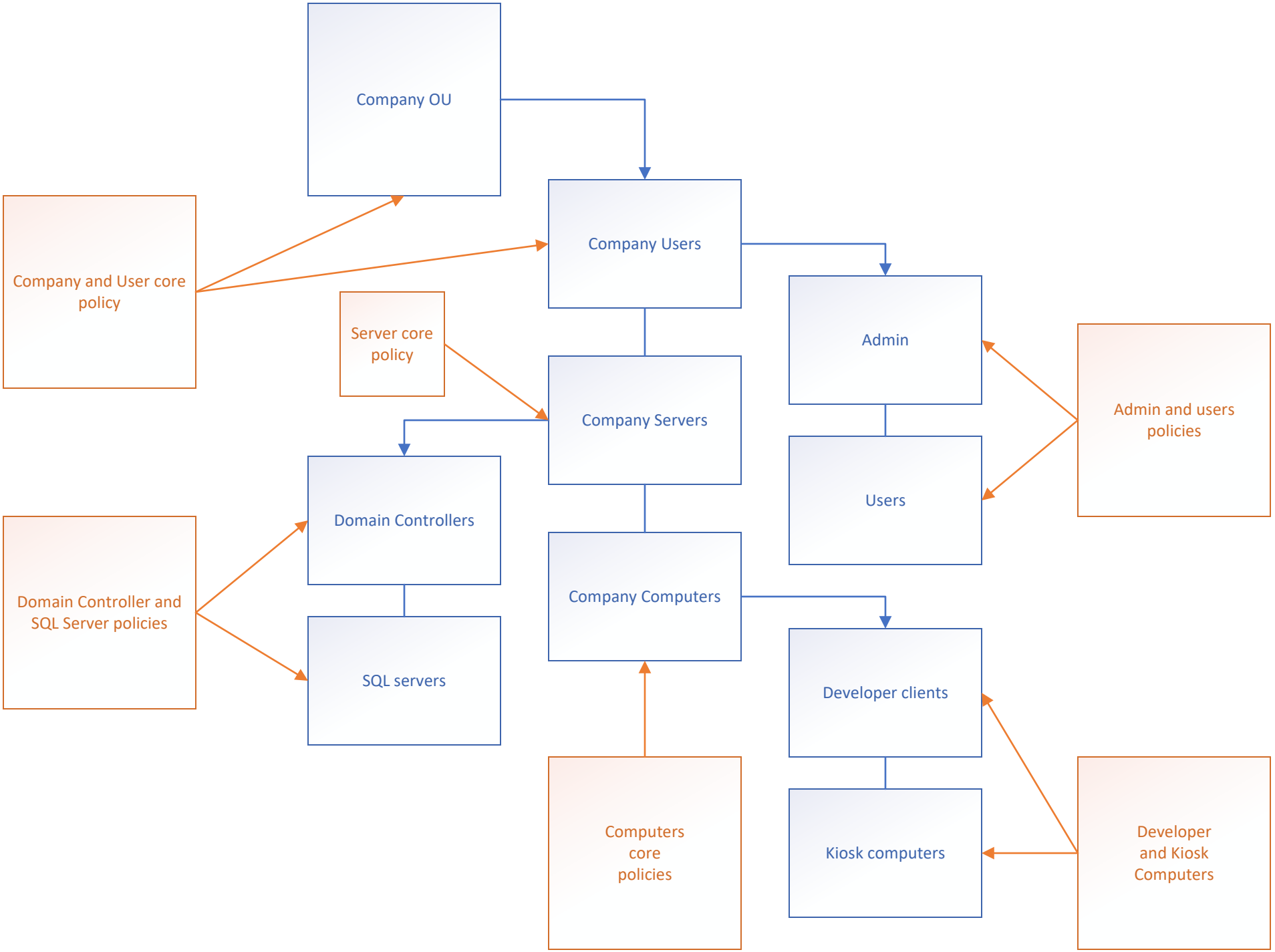

Enterprise admin
Domain admin Layer
Domain A
Domain B
Domain C
Domain D
Built-in Administrator layer
Domain Controller Server
Domain Controller Server
Domain Controller Server
Domain Controller Server

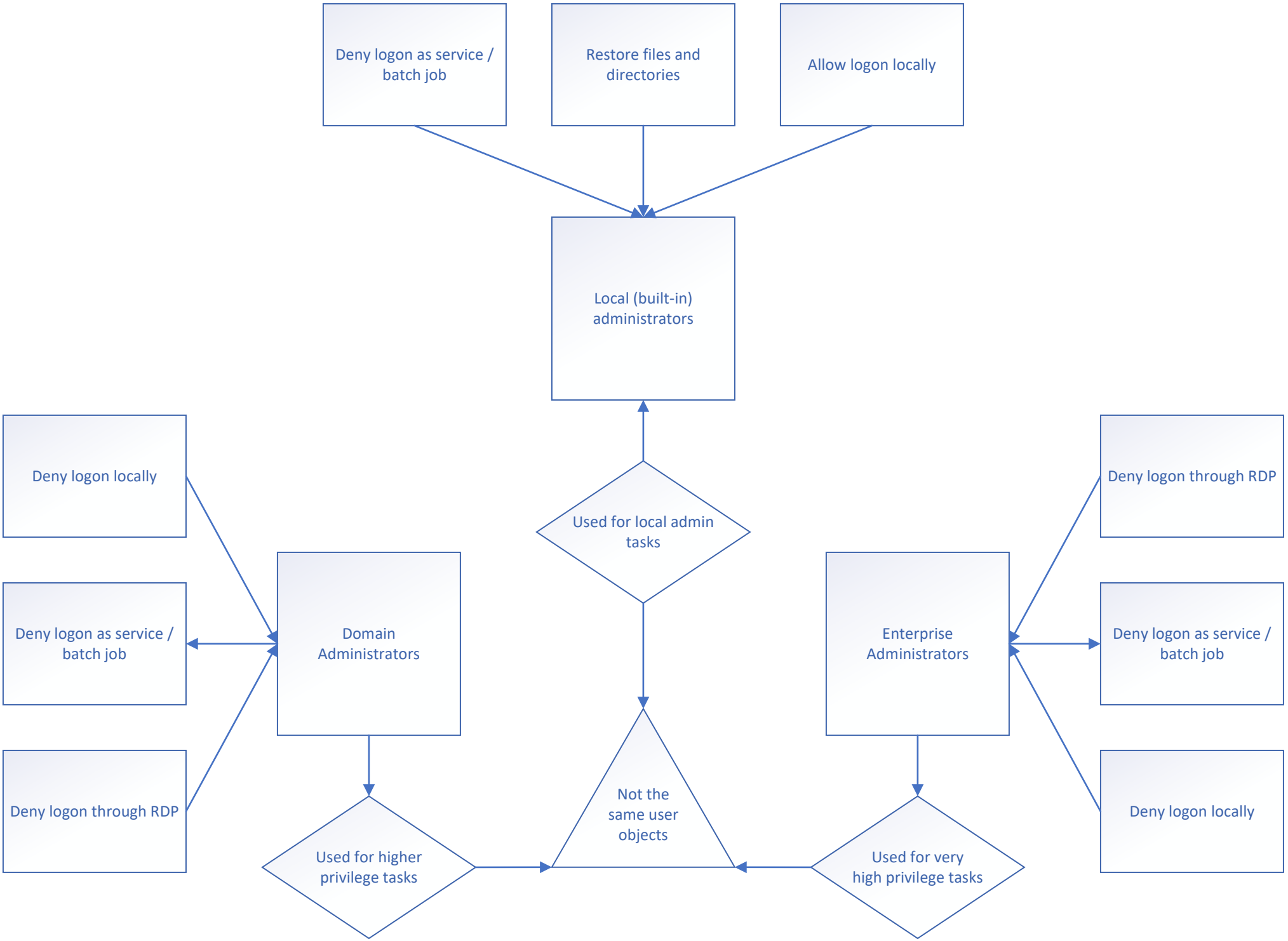

Access this computer from the network
Adjust memory quotas for a process
Back up files and directories
Allow log on locally
Bypass traverse checking
Change the system time
Create a pagefile
Shut down the system
Debug programs
Enable computer and user accounts to be trusted for delegation
Manage auditing and security log
Profile system performance
Restore files and directories
Remove computer from docking station
Load and unload device drivers
Increase scheduling priority
Profile single process
Modify firmware environment values
Force a shutdown from a remote system
Take ownership of files or other objects
Administrator privileges


Built-in
administrators
Domain administrators
Enterprise administrators


Built in
Administrators
Domain administrators
Enterprise administrators


Company OU
Company Users
Admin
Company Servers
Users
Company Computers
Developer clients
Kiosk computers


Company OU
Company and User core policy
Company Users
Server core policy
Company Servers
Admin
Admin and users policies
Users
Domain Controllers
Domain Controller and SQL Server policies
SQL servers
Company Computers
Developer clients
Computers core policies
Kiosk computers
Developer and Kiosk Computers


Deny logon as service / batch job
Restore files and directories
Allow logon locally
Local (built-in) administrators
Deny logon locally
Used for local admin tasks
Deny logon through RDP
Deny logon as service / batch job
Domain Administrators
Enterprise Administrators
Deny logon as service / batch job
Deny logon through RDP
Not the same user objects
Deny logon locally
Used for higher privilege tasks
Used for very high privilege tasks

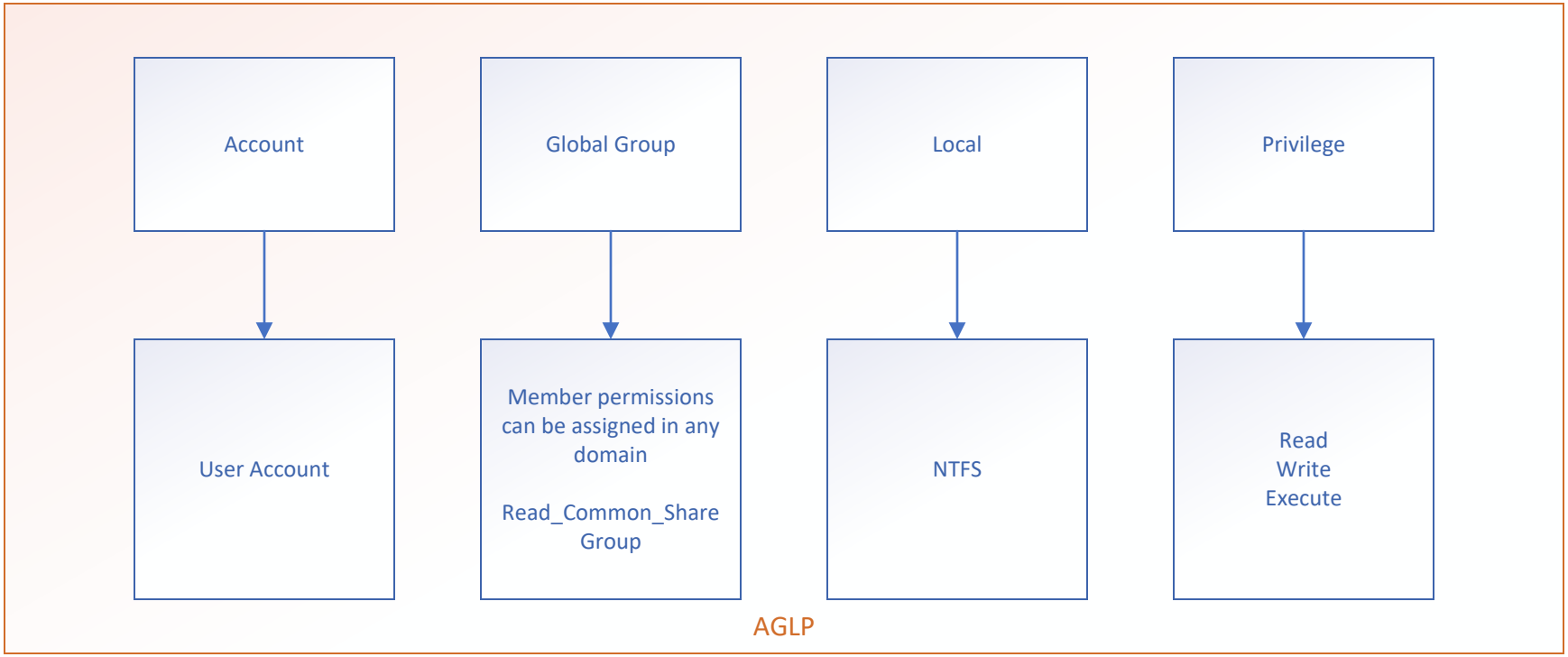
Controls for Built-in Administrator Accounts
For the built-in Administrator account in each domain in your forest, you should configure the following settings:

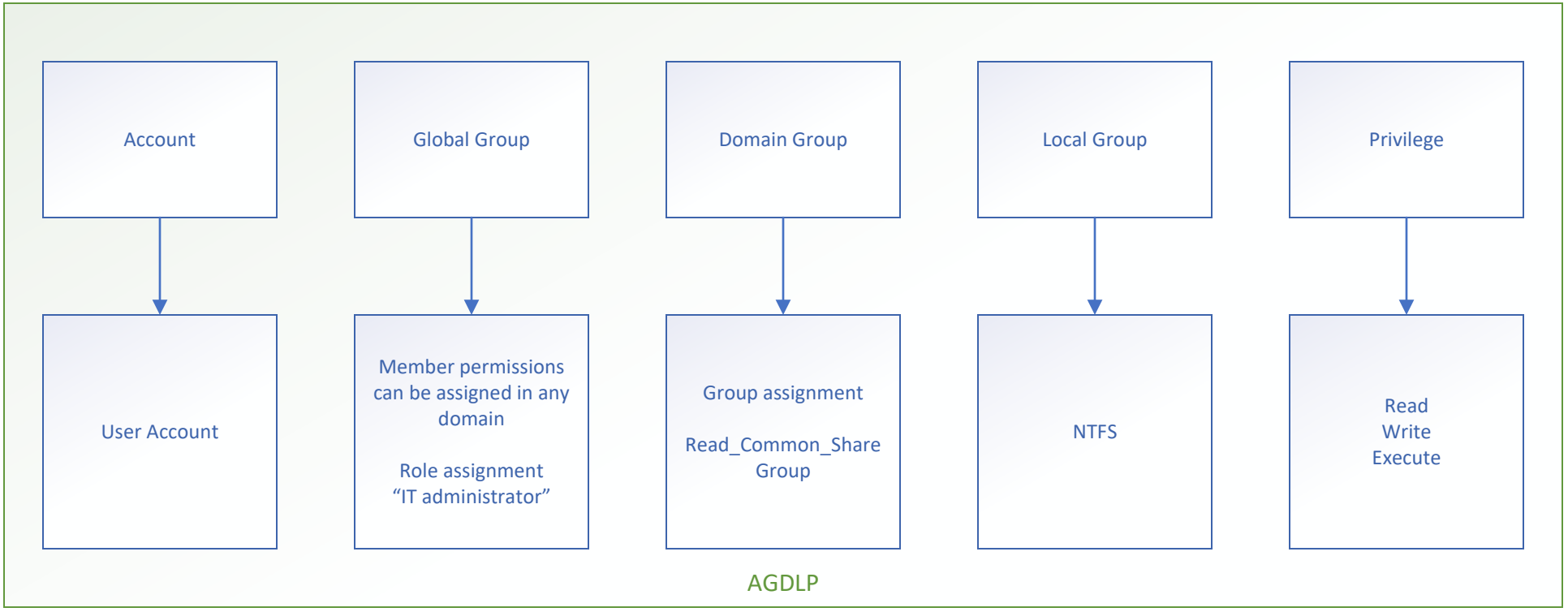
- Enable the **Account is sensitive and cannot be delegated** flag on the account.
- Enable the **Smart card is required for interactive logon** flag on the account.
- Configure GPOs to restrict the Administrator account's use on domain-joined systems:
    - In one or more GPOs that you create and link to workstation and member server OUs in each domain, add each domain's Administrator account to the following user rights in **Computer Configuration\Policies\Windows Settings\Security Settings\Local Policies\User Rights Assignments**:
        - Deny access to this computer from the network
        - Deny log on as a batch job
        - Deny log on as a service
        - Deny log on through Remote Desktop Services
- Configure Auditing of Administrator accounts
    - GPO linked to DC's
        - Access this computer from the network
        - Allow log on locally
        - Allow log on RDP

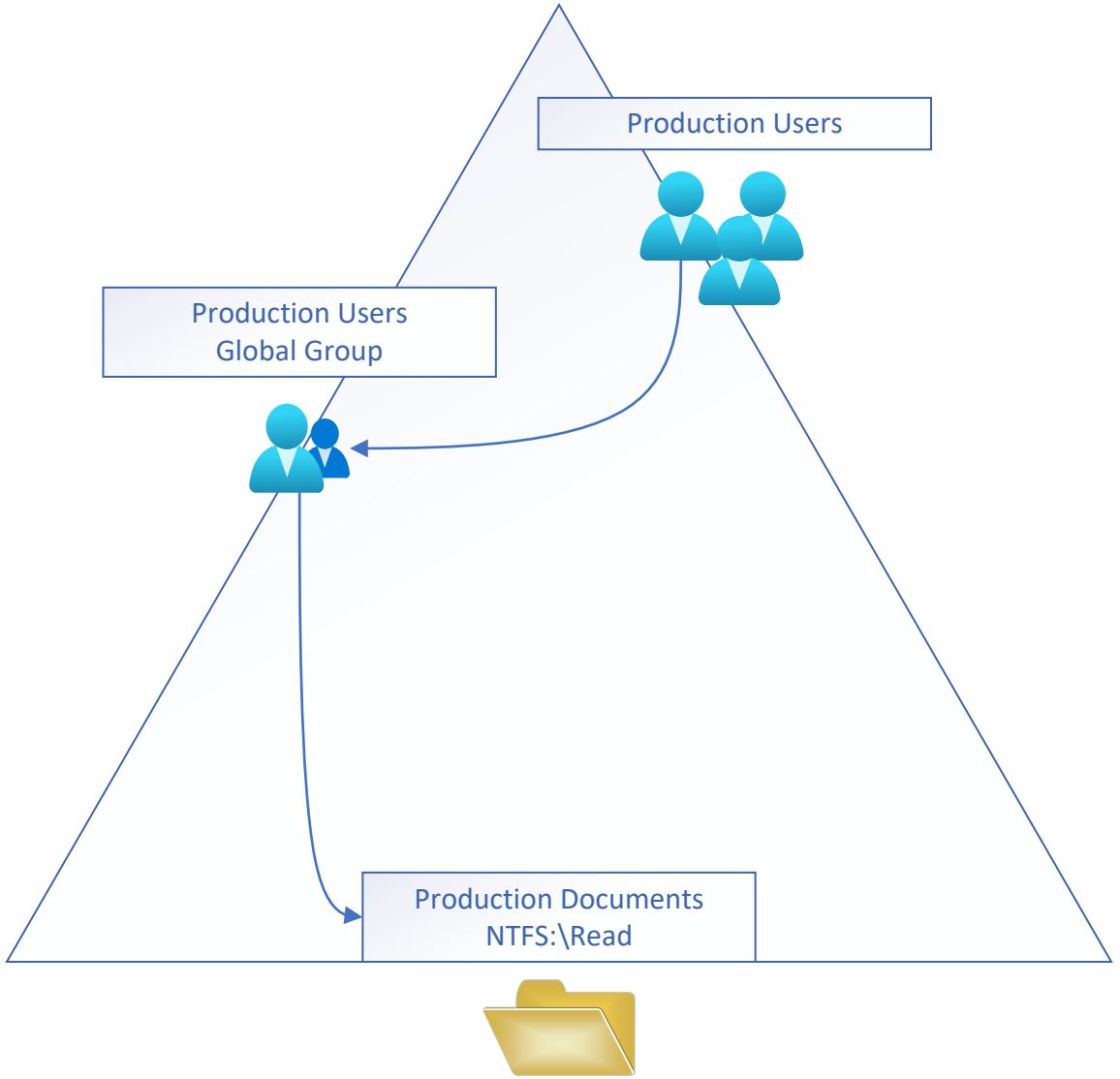
Controls for Domain Administrator users:
DA users should adhere to:
- Enable the Account is sensitive and cannot be delegated flag on the account.

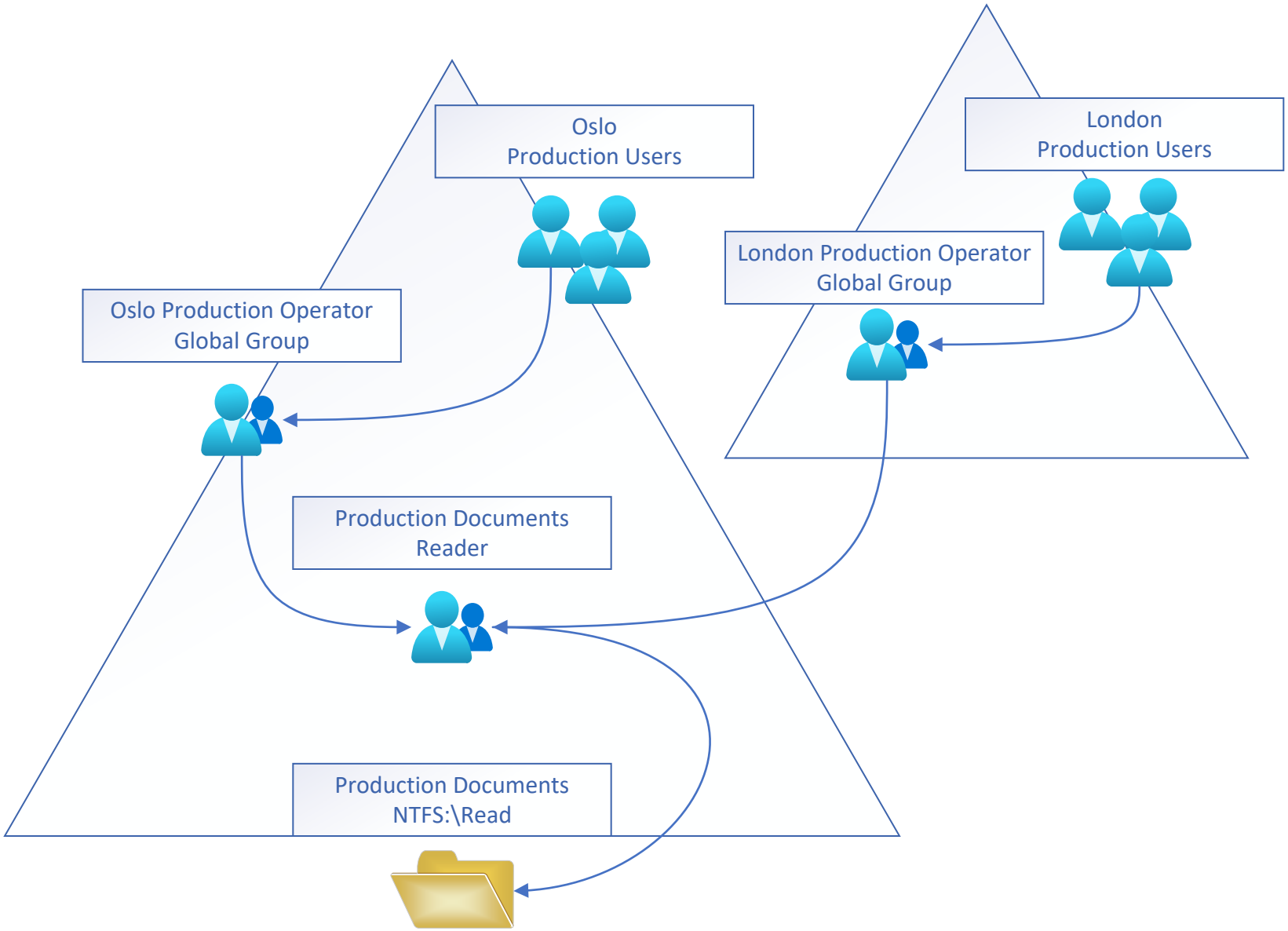
- GPO's linked to servers and workstations
    - Deny access to this computer from the network
    - Deny log on as batch job
    - Deny log on as a service
    - Deny log on locally
    - Deny log on through RDP user rights
- Remove as many as possible
- Configure Auditing of Domain Administrator accounts
- GPO linked to DC's
    - Deny log on locally
    - Deny log on through Remote Desktop Services

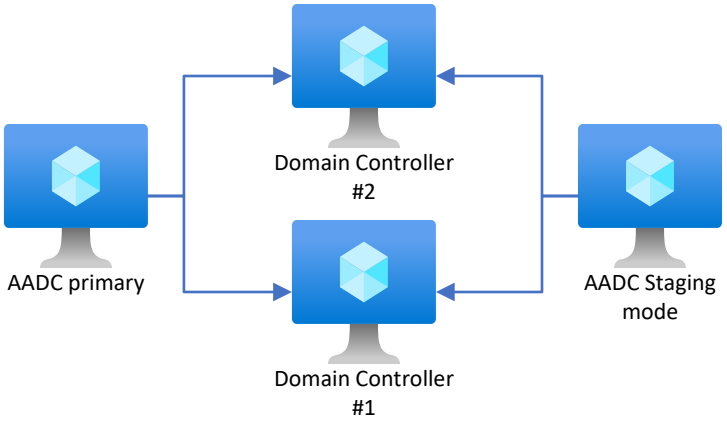
- Controls for Enterprise Administrators users should adhere to:
  - Enable the **Account is sensitive and cannot be delegated** flag on the account.
  - GPO's linked to servers and workstations
        - Deny access to this computer form the network
        - Deny log on as a batch job
        - Deny log on as a service
        - Deny log on locally
        - Deny log on through RDP
  - Activate auditing
  - Remove as many as possible
  - GPO linked to DC's
    - Deny log on locally
    - Deny log on through Remote Desktop Services


Account
Global Group
Local
Privilege
User Account
Member permissions can be assigned in any domain
Read_Common_Share Group
NTFS
Read
Write
Execute
AGLP


Account
Global Group
Domain Group
Local Group
Privilege
User Account
Member permissions can be assigned in any domain
Role assignment
“IT administrator”
Group assignment
Read_Common_Share Group
NTFS
Read
Write
Execute
AGDLP


Production Users
Production Users
Global Group
Production Documents
NTFS:\Read


Oslo
Production Users
London
Production Users
London Production Operator
Global Group
Oslo Production Operator
Global Group
Production Documents
Reader
Production Documents
NTFS:\Read


Domain Controller #2
AADC primary
AADC Staging mode
Domain Controller #1