- Child to Forest Root using krbtgt hash
- We now have Enterprise Admin privileges.

```
ls //ps-dc.powershell.local/C$
```

Detection and Defense

- Do not allow or limit login of DAs to any other machine other than the Domain Controllers. If logins to some servers is necessary, do not allow other administrators to login to that machine.
- Do NOT run services with DA account. Many good credential reuse defenses are rendered useless because of it.

For Golden Ticket

- Some important Event ID:
- Event ID
  - 4624: Account Logon
  - 4672: Admin Logon

For silver ticket

- Event ID
  - 4624: Account Logon
  - 4634: Account Logoff
  - 4672: Admin Logon

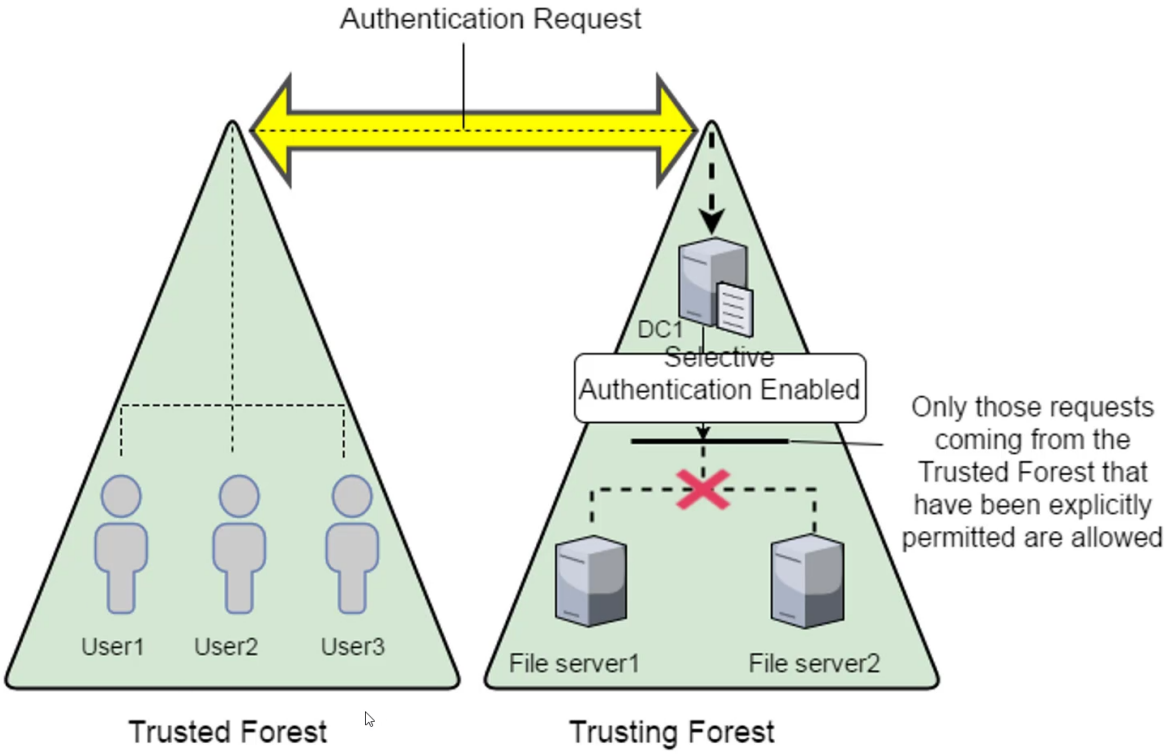
Kerberoast

- Events
  - Security Event ID 4769 – A Kerberos ticket was requested
- Mitigation
  - Service Account Passwords should be hard to guess (greater than 25 characters)
  - Use Managed Service Accounts (Automatic change of password periodically and delegated SPN Management)
  - https://technet.microsoft.com/en-us/library/jj128431(v=ws.11).aspx

Trust tickets

- SID Filtering
  - Avoid attacks which abuse SID history attribute (child to root domain privilege escalation, that is, DA from a Child to EA on forest root).
  - Enabled by default on all inter-forest trusts. Intra-forest trusts are assumed secured by default (MS considers forest and not the domain to be a security boundary).
  - But, since SID filtering has potential to break applications and user access, it is often disabled.

- Selective Authentication
  - In an inter-forest trust, if Selective Authentication is configured, users between the trusts will not be automatically authenticated. Individual access to domains and servers in the trusting domain/forest should be given.



ATA

- Microsoft ATA (Advanced Threat Analytics).
  - Traffic destined for Domain Controller(s) is mirrored to ATA sensors and a user activity profile is build over time – use of computers, credentials, log on machines etc.
  - Collects Event 4776 (The DC attempted to validate the credentials for an account) to detect credential replay attacks.
  - Can detect Behavior anomalies.

- Useful for detecting:
  - Recon: Account enum, Netsession enum
  - Compromised Credentials Attacks: Brute force, High privilege account/service account exposed in clear text, Honey token, unusual protocol (NTLM and Kerberos)
  - Credential/Hash/Ticket Replay attacks.

- Bypassing ATA:
  - ATA, for all its goodness, can be bypassed and avoided.
  - The key is to avoid talking to the DC as long as possible and make appear the traffic we generate as attacker normal.

Architectural Changes

- LAPS (Local Administrator Password Solution)
  - Centralized storage of passwords in AD with periodic randomizing where read permissions can be access controlled.
  - Storage in **clear text**, transmission is encrypted.
  - LAPS intro: https://technet.microsoft.com/en-us/mt227395.aspx
  - Abusing LAPS feature: https://blog.netspi.com/running-laps-around-cleartext-passwords/

Privileged Administrative Workstations (PAWs)

- A hardened workstation for performing sensitive tasks like administration of domain controllers, cloud infrastructure, sensitive business functions etc.
- Can provides protection from phishing attacks, OS vulnerabilities, credential replay attacks.

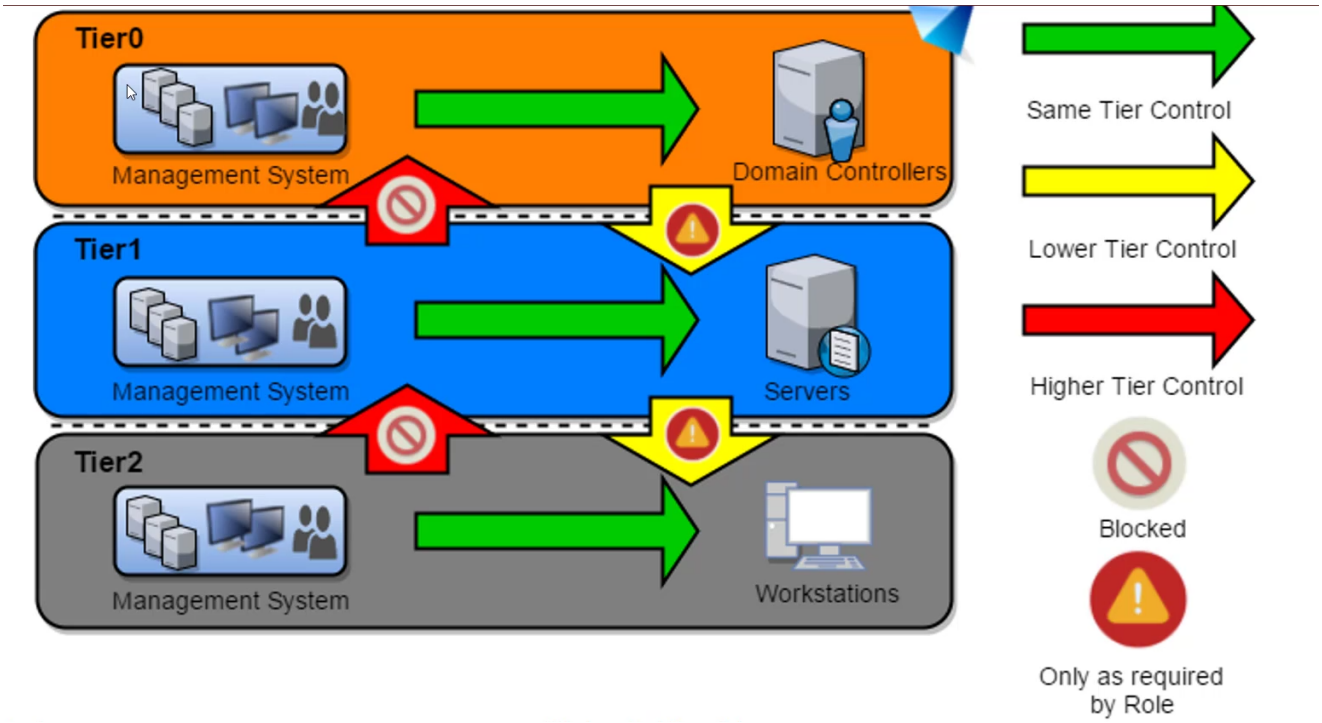
Privileged Administrative Workstations (PAWs)

- Multiple strategies
  - Separate privilege and hardware for administrative and normal tasks.
  - Admin Jump servers to be accessed only from a PAW.
  - Having a VM on a PAW for user tasks.

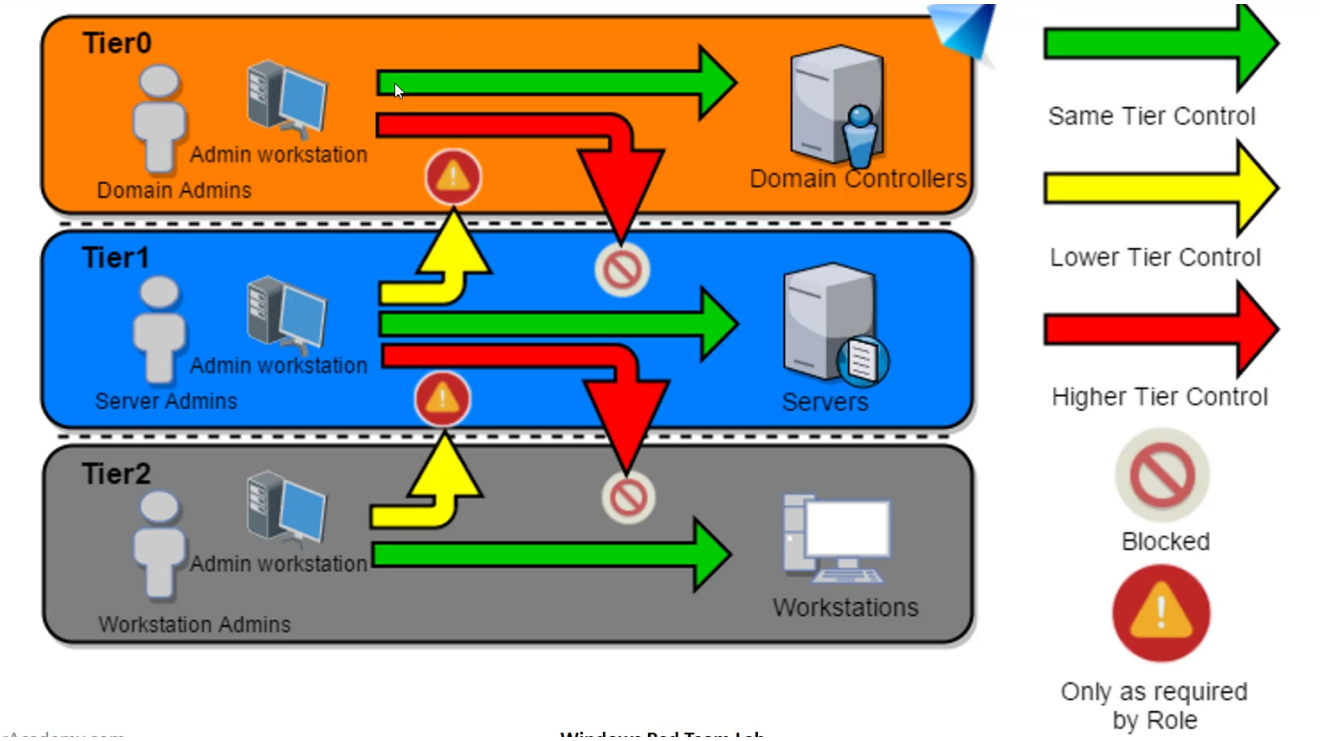
Active Directory Administrative Tier Model

- Composed of three levels only for administrative accounts:
  - Tier 0 – Accounts, Groups and computers which have privileges across the enterprise like domain controllers, domain admins, enterprise admins. .
  - Tier 1 - Accounts, Groups and computers which have access to resources having significant amount of business value. A common example role is server administrators who maintain these operating systems with the ability to impact all enterprise services.
  - Tier 2 - Administrator accounts which have administrative control of a significant amount of business value that is hosted on user workstations and devices. Examples include Help Desk and computer support administrators because they can impact the integrity of almost any user data.

Control Restrictions on tier model

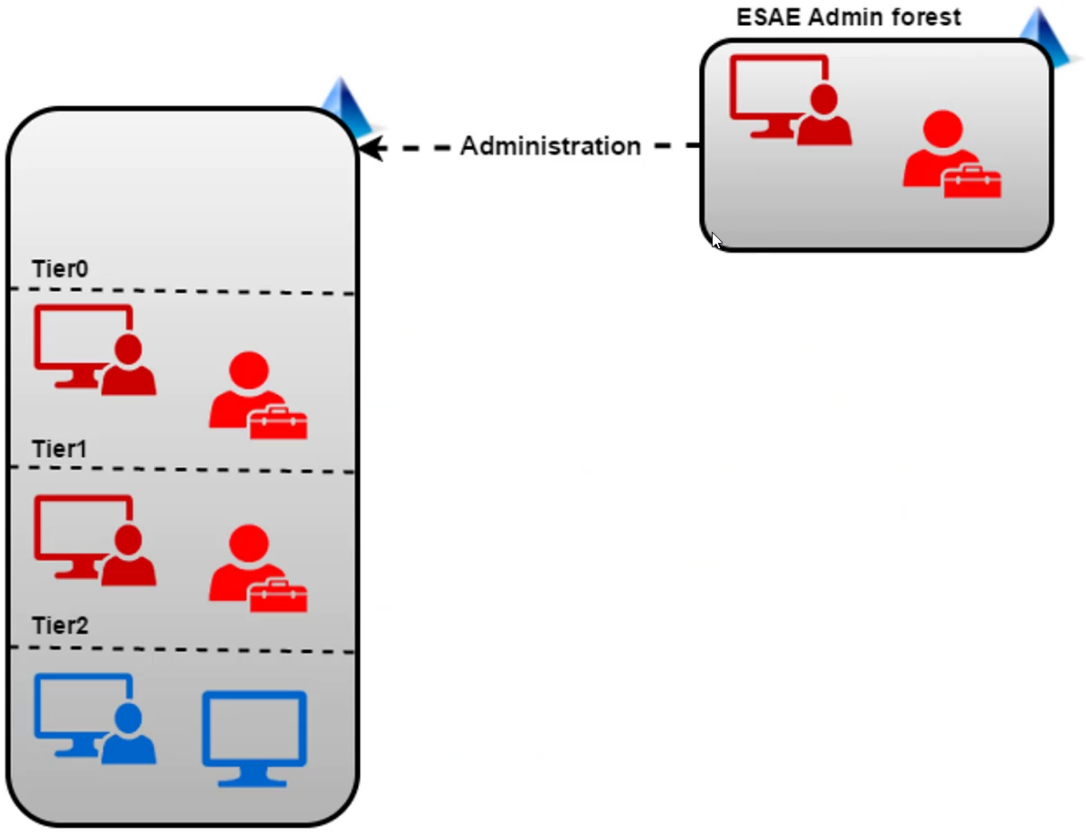


Logon Restrictions on tier model



Red forest

- ESAE (Enhanced Security Admin Environment)
- Dedicated administrative forest for managing critical assets like administrative users, groups and computers.
- Since a forest is considered a security boundary rather than a domain, this model provides enhanced security controls.
- The administrative forest is also called the Red Forest.
- Administrative users in a production forest are used as standard non-privileged users in the administrative forest.
- Selective Authentication to the Red Forest enables stricter security controls on logon of users from non-administrative forests.



- Securing Privileged Access: https://technet.microsoft.com/en-us/windows-server-docs/security/securing-privileged-access/securing-privileged-access
- MS Paper - Best Practices for Securing Active Directory: http://aka.ms/bpsadtrd