

# Abuse of Domain Accounts, Detection Strategy DET0210

Archived: 2026-04-05 16:47:56 UTC

## AN0590

Detection of suspicious logon behavior using valid domain accounts across multiple hosts, off-hours, or simultaneous sessions from geographically distant locations.

### Log Sources

### Mutable Elements

Field	Description
TimeWindow	Tune for detection of off-hours or abnormal logon spikes.
UserContext	Scope to sensitive domain accounts (e.g., Domain Admins).
LogonType	Distinguish between interactive, service, and network logons.

## AN0591

Use of domain accounts via sssd or winbind for logon activity outside of typical patterns, especially on sensitive systems or with lateral movement tools.

### Log Sources

### Mutable Elements

Field	Description
HostnameScope	Filter to high-value systems (e.g., domain-joined servers).
AccountDomain	Identify trusted domains versus external or misconfigured domains.

## AN0592

Domain logins using network accounts or mobile accounts via Open Directory or Active Directory plugins, especially outside business hours or on atypical endpoints.

### Log Sources

### Mutable Elements

Field	Description
UserLocation	Geo-IP or VPN source context for abnormal remote access.
LogonMethod	Control for expected services (e.g., GUI login vs. SSH).

### AN0593

Login to vSphere or ESXi hosts using domain accounts, especially those associated with vpxuser or unexpected group memberships.

#### Log Sources

#### Mutable Elements

Field	Description
AccountType	Prioritize detection on accounts with elevated access.
LoginInterface	Distinguish interactive UI login from API or SSH access.

---

Source: <https://attack.mitre.org/detectionstrategies/DET0210>