Enterprise IT - Infrastructure

# Enterprise IT - Infrastructure

We have developed a series of logging requirements for Enterprise IT infrastructure, such as underlying networks, network services and directory services at different maturity tiers in order to support defensive cyber security, such as detecting breaches.

## Baseline Maturity Tier

### 1. User directory services

Log Collection Principle(s): 1, 2

User directory services (such as Active Directory (AD), Azure Active Directory or OpenLDAP must create and forward Authentication and Authorisation events from the directory service itself. (Normal authentication and authorisation events for the underlying operating system and server should be forwarded as appropriate.)

For example:

* An administrator logging onto the AD server using the local end-user device's administrator account should result in an authentication event for the machine being sent.
* A directory admin logging on to the AD service from their end-user device without logging into the local machine should generate an authentication event for the directory.

These event types must be logged and forward:

1. Account creation
2. Account lockout
3. Account reinstatement
4. Account authentication failures
5. Account authentication successes after 1 or more failures
6. Account password changes
7. Group membership addition / deletion (in particular, any group that gives admin access)
8. Group creation
9. Privilege modification for users (changes to ACL's, granting of new roles in RBAC models)
10. Privilege escalation events (use of sudo, UAC)
11. Multi-factor authentication state, such as:
    1. Enabled
    2. Disabled
    3. Reset/rotation
    4. Recovery method used

### 2. Productivity Suite security logs

Log Collection Principle(s): 1, 2, 3, 6

Productivity suites (such as Google Workspace or Microsoft Office 365) must create and forward all security-related log data (as defined by the vendor), including unsuccessful Authentication and Authorisation events.

For example, within an Office 365 tenancy with Conditional Access enabled and set to require multi-factor authentication when a user device is perceived to be outside of the corporate network and such prompt is made and the outcome of that challenge.

### 3. Domain name service query logs

Log Collection Principle(s): 4

DNS query logs must be created and forwarded.

1. Client IP address
2. Query
3. Query response content including:
   1. Returned record(s) or NXDOMAIN
   2. Authoritative nameserver
4. Query response code
5. Zone and/or view identifier (if local zone response and/or multiview)

This remains true for where nodes (for example, servers) may bypass internal DNS services.

### 4. Web proxy access logs

Log Collection Principle(s): 5

Where web traffic proxies exist, access logs must be created and forward and must, include the following variables:

1. Authenticated user name
2. Client IP address
3. HTTP method (for example, CONNECT GET)
4. Full destination/target URL
5. Connection return status code (for example, 200 or 403)
6. Size of response

### 5. File server authentication, authorisation and access logs

Log Collection Principle(s): 6

Where file service exist, sufficient log data must be created and forwarded, including sufficient data to satisfy the following:

1. Detect permission changes and the user who changed such
2. Detect all file/folder changes and the user who changed such
3. Detect all file/folder read/open and the user who did such

### 6. Security-related event logs for all server operating systems

Log Collection Principle(s): 6

Security-related event logs from all servers (whether virtualised or physical) operating in a 'server' role:

* [additional information pending]

### 7. Allocation of IP address leases from DHCP services

Log Collection Principle(s): 3, 5

DHCP services must be configured to create and forward the following:

1. Successful client DHCP requests, including:
   1. Requesting client MAC address
   2. DHCP scope identifier
   3. IP address leased
   4. IP address lease duration
2. Unsuccessful client DHCP requests, including:
   1. Requesting client MAC address
   2. DHCP scope identifier (if applicable for unsuccessful request)

### 8. VPN concentrator activity data

Log Collection Principle(s): 3, 5

Where a end-user device VPN concentrator is in use, connection-related log data must be created and forwarded:

1. Success or unsuccess status
2. User/certificate identifier
3. Client IP address
4. Concentrator identifier

## Enhanced Maturity Tier

### 1. Firewall log data for denied network traffic

Log Collection Principle(s): 5

All firewall DENY log data must be forwarded:

1. Client IP address
2. Firewall/router identifier
3. Request response code
4. Request content, including:
   1. IP protocol (for example, ICMP)
   2. Destination/target port
   3. Destination/target IP address
   4. Destination/target hostname address (if reverse lookup performed)

### 2. Internal DNS namespace zone content

Log Collection Principle(s): 4

Internal domain name spaces must ultimate forward, in an [RFC5936 (DNS Zone Transfer Protocol (AXFR)](https://tools.ietf.org/html/rfc5936) compatible format including all information described in the RFC.

### 3. DHCP scopes (and the functional segmentation of each)

Log Collection Principle(s): 5

Machine-readable DHCP scope exports (and surrounding metadata/description of the purpose of each scope) must be created and forwarded.

### 4. Endpoint protection security logs

Log Collection Principle(s): 6

Security log data (as defined by the vendor) must be created and forwarded.

### 5. Mobile device enrollment activity

Log Collection Principle(s): 1, 2, 3, 6

Where a mobile device management solution is used and end-user devices register/enrol and de-register/de-enrol with it, enrollment data should be created in and forwarded:

1. Enrolment or un-enrolment event type
2. End-user device identifier(s), such as client IP address and/or MAC address and/or assigned DHCP name
3. End-user account name (if applicable)