Hosting Platforms

# Hosting Platforms

We have developed a series of logging requirements for hosting platforms, such as virtualised and/or containered compute with associated supporting services such as database and queuing services at different maturity tiers in order to support defenisve cyber security, such as detecting breaches.

## Baseline Maturity Tier

### 1. User directory services

Log Collection Principle(s): 1, 2

User directory services must create and forward Authentication and Authorisation events from the directory service itself.

User directories within hosting environments can be rich and diverse, such technologies include:

* Active Directory (AD)
* Azure Active Directory
* OpenLDAP
* Amazon Web Services (Accounts and Incognito)
* Okta
* Auth0
* Github.com (acting as an identity provider)
* Google Workspace (acting as an identity provider)
* Local user stores within operating systems

These event types must be logged and forwarded:

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 (for example, role delegation through AWS IAM)
10. Multi-factor authentication state, such as:
    1. Enabled
    2. Disabled
    3. Reset/rotation
    4. Recovery method used

### 2. Bastion/Jump/Action-proxy services

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

Bastion/jump boxes that act as a management consolidation route and should be highly auditable therefore must create and forward security-related event data:

1. SSH keypair generation/revocation, including:
   1. Public key
   2. Keypair 'friendly name' / identifier
2. Account login attempts:
   1. Public key
   2. Username

### 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 should be created and forward and must, include the following variables:

1. Authenticated user name (if applicable)
2. Client identifiers:
   1. IP address
   2. Reverse lookup client name (if applicable)
3. HTTP method (for example, CONNECT GET)
4. Where available, full destination/target URL or SNI value
5. Connection return status code (for example, 200 or 403)
6. Size of response

### 5. Hypervisor events

Log Collection Principle(s): 3, 6

Hypervisors manage virtualised compute resources and are entrusted to segregate the same. All instructions to hypervisors should be highly auditable.

1. Virtual machine creation (including templates)
   1. Identifier(s)
   2. Operating system image information
2. Virtual machine 'power' events:
   1. Identifier(s)
   2. 'Power' on
   3. 'Power' off (including restart flag)
3. Virtual machine deletion
   * Identifier(s)
4. Virtual machine resource modification events:
   1. CPU addition/removal
   2. RAM addition/removal
   3. Networking additional/removal
   4. Storage mount/dismount/resize

### 6. Orchestrator events

Log Collection Principle(s): 3, 6

Orchestrators such as Cloud Foundry and Kubernetes create and manage a variety of technology resources to facilitate an application environment.

1. Resource creation (including templates)
   1. Identifier(s)
   2. Resource type
   3. Operating system image information (if applicable)
2. Container 'power' events
   1. Identifier(s)
   2. 'Power' on
   3. 'Power' off (including restart flag)
3. Resource deletion
   * Identifier(s)
4. Resource modification events:
   * Identifier(s)

### 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)

## 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. Security-related logs for all Windows-based end-user devices

Log Collection Principle(s): 6

Security-related logs, as defined by [NCSC's Logging Made Easy template](https://github.com/ukncsc/), from all end-user devices operating a Microsoft Windows operating system must be created and forwarded.

### 6. 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)

### 7. VPN concentrator activity data

Log Collection Principle(s): 3, 5

Where VPN services are 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

### 8. Pipeline events

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

Continuous integration and continuous deployment pipelines obey instructions to manage hosting environments and are a privileged position to oversee all tenant resources, they must be highly auditable to clarify activity and attribute the same.

1. Source identifier(s)
   1. User(s)
   2. Repository
2. Activity events
   1. Resource creation
   2. Resource destruction