

The hybrid cloud platform for HPE GreenLake

Audit logs



Contents

1. Introduction.....	3
2. What is an audit log?.....	3
Definition and importance.....	3
Key benefits of audit logs.....	3
Role in regulatory compliance and security.....	3
3. Features of audit logs on HPE GreenLake.....	4
Tracking of user and system activities.....	4
Centralized management of logs.....	4
Supported attributes in audit logs.....	4
Customization and export options.....	4
Retention policies.....	4
4. Use case: Security and forensic analysis.....	5
Role of audit logs in identifying the root cause.....	5
The power of RBAC in enhancing security.....	5
Benefits to the customer and preventive measures.....	5
5. Use case: MSPs and tenant logs.....	5
6. Retention and storage policies.....	6
7. Technical architecture of audit logs.....	6
Integration with CCS and external applications.....	7
8. Security and compliance.....	7
Audit logs as a pillar of security strategy.....	7
Ensuring compliance with GDPR and other regulations.....	7
Data protection mechanisms and encryption.....	7
9. Conclusion.....	8



1. Introduction

Audit logs are a fundamental component of any robust IT infrastructure, providing a comprehensive trail of all user and system activities. Within the HPE GreenLake cloud, audit logs serve not only as a record of actions but also as a critical tool for maintaining security, helping ensure compliance, and supporting operational efficiency. This white paper aims to provide a detailed overview of the audit logs feature on HPE GreenLake, exploring its capabilities, technical architecture, and practical applications.

2. What is an audit log?

Definition and importance

An audit log is a chronological record of events or actions that occur within a system. These logs are essential for tracking the activities of both users and systems, providing an immutable record that can be referenced in case of disputes, security incidents, or compliance audits. By capturing detailed information about every significant action, audit logs help ensure that there is a way to trace back and understand what occurred, when it occurred, and who was responsible.

Key benefits of audit logs



Figure 1. Key benefits of audit logs

- **Accountability:** Audit logs provide a clear trail of responsibility, helping ensure that users are held accountable for their actions within the platform.
- **Security:** By maintaining a detailed record of activities, audit logs help in identifying and mitigating security breaches, unauthorized access, and other potential threats.
- **Compliance:** Many regulations, such as the General Data Protection Regulation (GDPR) and the Health Insurance Portability and Accountability Act (HIPAA), require organizations to maintain detailed logs of user activities. Audit logs on HPE GreenLake help organizations meet these regulatory requirements.
- **Forensic analysis:** In the event of a security incident, audit logs provide the data needed to conduct a thorough investigation, identify the root cause, and take corrective action (Figure 1).

Role in regulatory compliance and security

In today's regulatory environment, organizations are required to maintain a high level of transparency and accountability. Audit logs play a crucial role in this by helping ensure that all actions within the platform and services are recorded and can be audited. This is especially important for industries with strict regulatory requirements, such as finance, healthcare, and government. HPE GreenLake audit logs feature is designed to meet these demands, providing the tools needed to help ensure compliance with a wide range of regulations.



3. Features of audit logs on HPE GreenLake

Tracking of user and system activities

Audit logs on HPE GreenLake provide detailed tracking of significant user and system activities within the platform. This includes actions such as logins, configuration changes, API calls, and more. Each action is recorded with relevant details, including the user who performed the action, the time it occurred, and the specific changes made. This level of detail is crucial for helping ensure accountability and transparency within the platform.

Centralized management of logs

One of the key features of HPE GreenLake audit logs is the ability to manage logs centrally for all users, whether they are stand-alone customers or managed service providers (MSPs). Stand-alone customers benefit from this feature by being able to view and manage logs across all their deployed services and regions from a single interface. This helps eliminate the need to log into different service consoles, such as HPE Aruba Networking, Data Services Cloud Console, or COM, making log management more efficient and streamlined without compromising security.

For MSPs, audit logs are fully integrated with both MSP and tenant workspaces. MSP users can view logs for all their tenants as well as their own actions, providing a centralized view of all activities across the different environments they manage. Tenants, on the other hand, have secure access to logs related only to their own workspace, helping ensure data privacy and integrity. This integration is especially crucial for MSPs managing multiple customer environments, as it allows them to monitor and manage activities across all tenants efficiently from one platform.

Supported attributes in audit logs

The audit logs feature supports a wide range of attributes, each designed to capture specific details about an action. These attributes include:

Table 1. Attributes of audit logs

Attribute	Description
source	The name of the application generating the log
app_instance_id	A unique identifier for the instance of the application
application_customer_id	The customer ID associated with the application
category	The category of the event or action being logged
description	A short description of the log entry
username	The email address of the user who performed the action
audit_created_at	The time stamp of when the log was created
msp_application_customer_id	The MSP application customer ID, used specifically in tenant logs
account_type	Specifies whether the workspace is stand-alone, tenant, or MSP

These attributes provide a comprehensive view of each action, helping ensure that all relevant details are captured and can be analyzed as needed.

Customization and export options

Audit logs on HPE GreenLake can be customized to meet the specific needs of each organization. Users can filter logs based on various attributes, such as the source, category, or username, allowing them to focus on the information that is most relevant to them. Additionally, logs can be exported in CSV or PDF formats, making it easy to share them with auditors, compliance officers, or other stakeholders.

Retention policies

Logs are retained for a default period of three months on HPE GreenLake, but organizations can request for older logs up to one year by reaching out to our support team. This flexibility helps ensure that organizations can meet their compliance requirements while managing storage efficiently.



4. Use case: Security and forensic analysis

Scenario overview: Network device management with HPE Aruba Networking on HPE GreenLake

Imagine a scenario where a customer has deployed a networking device from HPE Aruba Networking within their HPE GreenLake environment. This device is crucial for maintaining the network's performance and security. One day, person X, an employee with administrative privileges, logs into the device through the HPE Aruba Networking Central application. Shortly after making some configuration changes, the device goes down, disrupting the network and causing significant operational issues.

Incident walkthrough: How the device failure occurred

Initially, the local logs from the device indicate that the failure was due to a configuration change. However, these logs do not provide detailed information about who made the change, what specific changes were made, or who granted the permissions. This lack of detail makes it difficult to understand the root cause of the issue and to take corrective action.

Role of audit logs in identifying the root cause

By leveraging the audit logs feature on HPE GreenLake, the IT team can access a detailed trail of actions taken by person X. The logs reveal exactly what configuration changes were made, the access level person X had, and who granted them this access. This level of detail is made possible by the platform's robust role-based access control (RBAC) policy, which helps ensure that all actions are logged with the appropriate context. Additionally, users do not need to switch between various service consoles to check the logs, as all logs are conveniently aggregated within HPE GreenLake.

The power of RBAC in enhancing security

The RBAC system on HPE GreenLake plays a crucial role in maintaining the security of the platform. By ensuring that only authorized users can perform certain actions, and by logging all actions with detailed context, the system helps prevent unauthorized access and configuration changes. In this case, the detailed audit logs enabled the IT team to quickly identify the root cause of the issue, take corrective action, and prevent similar incidents in the future.

Benefits to the customer and preventive measures

The ability to trace actions back to individual users and to understand the context in which those actions were taken is invaluable for maintaining security and operational integrity. By using audit logs, the customer was able to quickly resolve the issue, minimize downtime, and implement preventive measures to avoid similar incidents in the future.

5. Use case: MSPs and tenant logs

Story: A day in the life of an MSP managing multiple tenants

Let's imagine the daily operations of an MSP named TechPro Services, which manages IT environments for dozens of clients across various industries. Each client, or tenant, has its own set of servers, applications, and networking devices that need to be monitored, updated, and secured. The team at TechPro Services is responsible for ensuring that each tenant's environment runs smoothly and that any issues are resolved promptly.

One morning, the MSP administrator at TechPro Services logs into the HPE GreenLake to start their day on its platform. Without audit logs, the administrator would need to manually log into each tenant's workspace, check for any issues, and make the necessary updates. This process is not only time-consuming but also prone to errors, as the administrator might miss critical actions or fail to notice unauthorized access.

However, with the HPE GreenLake audit logs feature, the administrator's workflow is transformed. Instead of logging into each tenant's workspace individually, the administrator can view all tenant logs from a single, centralized interface. This means that they can quickly identify any issues, such as unauthorized access or failed updates, across all tenants without having to switch between multiple systems.

As the day progresses, the administrator receives an alert about a potential security breach in one of the tenant environments. Thanks to the detailed audit logs, the administrator can immediately see which user accessed the system, what actions they took, and whether those actions were authorized. This allows the administrator to quickly respond to the breach, mitigate the risk, and notify the affected tenant.

Later in the day, the administrator needs to perform a firmware update on several devices across multiple tenants. Without audit logs, this would require logging into each tenant's workspace to initiate the update. However, with centralized log management, the administrator can efficiently track and record the initiation of these updates across all tenants, saving time and ensuring accurate documentation of the process.

By the end of the day, the administrator at TechPro Services has efficiently managed multiple tenant environments, addressed potential security issues, and performed critical updates—all thanks to the power of audit logs on HPE GreenLake.



6. Retention and storage policies

Overview of retention periods and extended storage options (Figure 2)

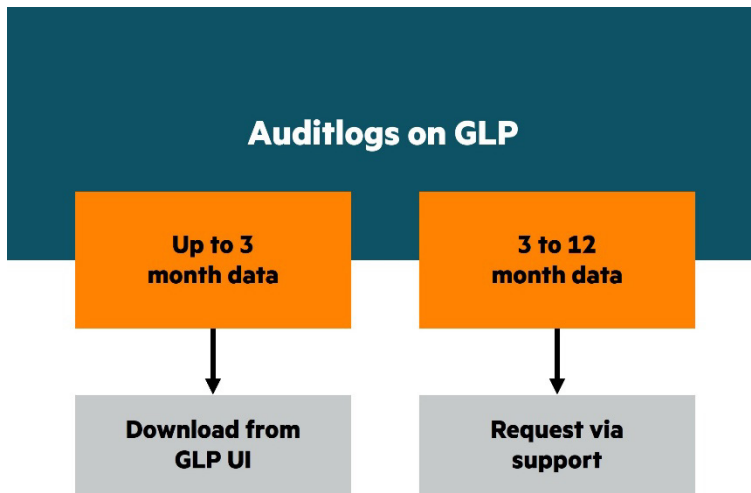


Figure 2. Retention policy

Audit logs on HPE GreenLake are retained for a default period of three months, helping ensure that recent activities are accessible for review and analysis. However, organizations with specific compliance or operational needs may require extended storage. To accommodate this, the platform offers the option to retain logs for up to one year upon request.

Technical details: Elasticsearch, DynamoDB, and Cassandra

The platform uses a combination of Elasticsearch, DynamoDB, and Cassandra to store and manage audit logs. Elasticsearch handles recent logs, providing fast and efficient search capabilities. For longer-term storage, DynamoDB is used in cloud environments while Cassandra is used for on-premises setups. Logs older than three months and up to 12 months are archived in a secure storage system and can be accessed through a support case. This hybrid approach helps ensure that logs are stored securely and can be retrieved quickly when needed.

Data flow and storage architecture

The architecture of the audit logs system is designed to help ensure data integrity and availability. Logs are generated by various applications and sent to the audit trail using a standardized format. They are then processed and stored in the appropriate database, depending on the retention period and storage requirements. This architecture helps ensure that logs are always accessible, even in large-scale, complex environments.

7. Technical architecture of audit logs

System components: Publisher, consumer, and user interface (Figure 3)

The technical architecture of the audit logs feature consists of three main components:

- **Publisher:** The service responsible for receiving logs generated by various services and applications—it validates the correctness of user details in the log before sending it to the audit trail. This component helps ensure that logs are consistent and contain all necessary attributes before they are processed by the consumer.
- **Consumer:** The component that processes and stores the logs—it validates the logs and helps ensure they are stored in the correct database for future retrieval.
- **User interface:** The interface through which users can access, search, and export logs in CSV or PDF format—this component provides advanced filtering and search capabilities, allowing users to find the information they need quickly and easily.



Data flow: From event generation to log storage

The data flow within the audit logs system begins with the generation of an event by the application/service, such as a user logging in or making a configuration change. This event is captured by the publisher component and sent to the audit trail. The consumer component then processes the log, validates the data, and stores it in the appropriate database. Finally, the log is made available through the user interface, where it can be searched, filtered, and analyzed.

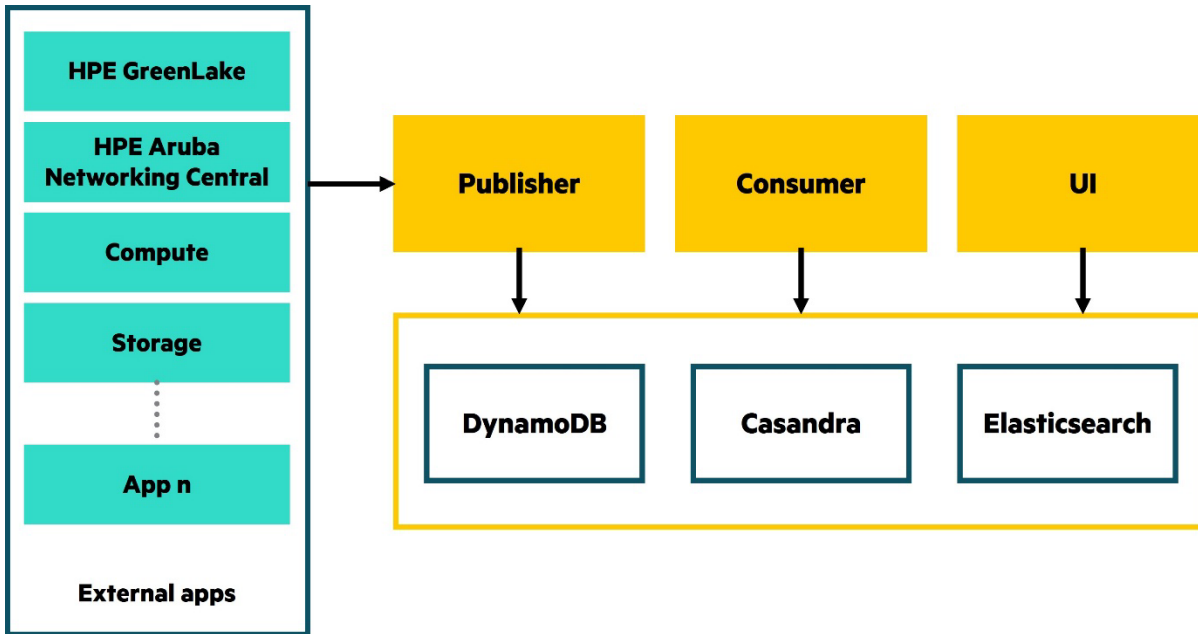


Figure 3. High-level architecture of the audit log mechanism

Integration with CCS and external applications

The audit logs feature is fully integrated with HPE GreenLake Common Cloud Services (CCS) and can be extended to external applications through APIs. This integration allows for seamless log management across multiple environments and helps ensure that all relevant activities are captured and stored.

8. Security and compliance

Audit logs as a pillar of security strategy

Audit logs are a critical component of HPE GreenLake security strategy. By providing a detailed record of all actions within the platform, audit logs help to identify and mitigate security breaches, unauthorized access, and other potential threats. The ability to trace actions back to individual users helps ensure that accountability is maintained, and any suspicious activities can be investigated promptly.

Ensuring compliance with GDPR and other regulations

In addition to enhancing security, audit logs also play a crucial role in helping ensure compliance with various regulations, including GDPR, HIPAA, and more. These regulations require organizations to maintain detailed logs of user activities, and the HPE GreenLake audit logs feature is designed to meet these requirements. Logs are stored securely, with robust encryption and access controls, helping ensure that sensitive data is protected at all times.

Data protection mechanisms and encryption

To protect the integrity and confidentiality of the data captured in audit logs, HPE GreenLake employs a range of data protection mechanisms. These include encryption of log data both in transit and at rest, access controls to enable that only authorized users can view logs, and regular security audits to identify and address potential vulnerabilities. These measures help ensure that audit logs remain a secure and reliable source of information.



9. Conclusion

Audit logs on HPE GreenLake provide a powerful tool for enhancing security, compliance, and operational efficiency. By offering detailed tracking of user and system activities, centralized log management, and robust integration with MSP and tenant workspaces, the audit logs feature helps organizations maintain transparency and accountability across their IT environments. As Hewlett Packard Enterprise continues to innovate and enhance the platform, audit logs will remain a critical component of the HPE GreenLake offering, helping organizations meet their security and compliance needs.

Learn more at

[HPE GreenLake for Audit Logs developer guide](#)

Explore **HPE GreenLake** 

 **Chat now (sales)**