Log and trace management in the Nuabee DRP solution

Security architecture · https://nuabee.com/documents/logs-traces-management-drp/

Introduction

Log and trace management is an essential component for the supervision and security of Cloud environments, particularly during a Disaster Recovery Plan (DRP).

Logs and traces enable system activity to be monitored, problems to be diagnosed, and compliance with security policies to be guaranteed. This document focuses on the log management solutions available in the OTC Cloud and their scope of application in the DRP space.

Importance of log and trace management

Log and trace management offers several crucial advantages, including:

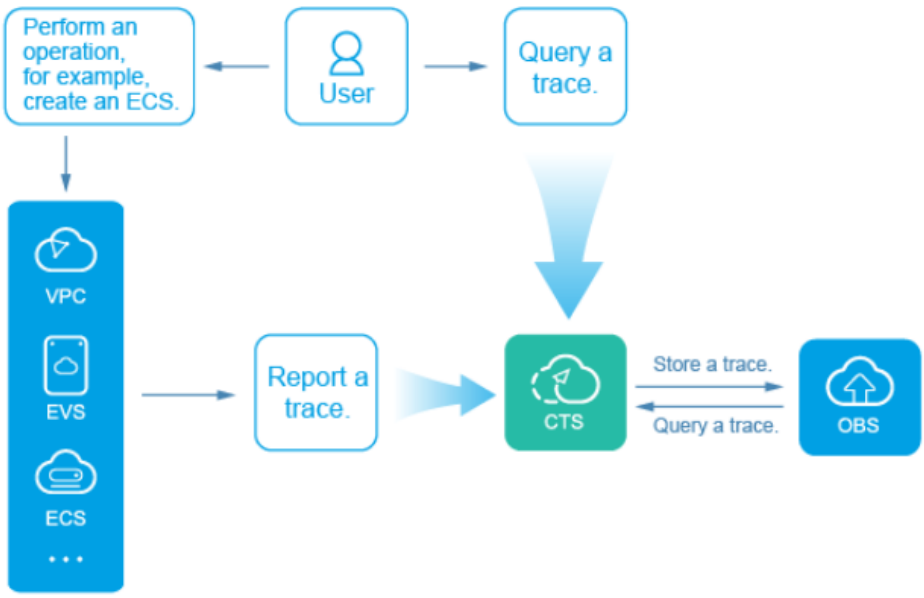
1. **Supervision and Monitoring**: Logs enable real-time monitoring of the status of Cloud resources, facilitating rapid detection of anomalies and failures.
2. **Diagnosis and troubleshooting**: In the event of an incident, detailed traces of system activity enable problems to be quickly identified and resolved.
3. **Security and Compliance**: Logs provide essential records for security audits and regulatory compliance, helping to prove that systems are being used in accordance with established security policies.
4. **Performance Analysis**: Log analysis can reveal opportunities to optimize system and application performance.

Log management solutions

Cloud OTC offers several solutions for log and trace management, tailored to the specific needs of ARP spaces.

The Cloud Trace Service (CTS) module

Cloud Trace Service (CTS) is an advanced solution for logging and monitoring activities in Cloud environments. It enables detailed tracing of actions carried out on Cloud resources, providing a complete, chronological view of operations. This visibility is crucial for security, incident diagnosis and regulatory compliance.



Activity log collection

CTS collects detailed activity logs for every operation carried out in the Cloud environment. These logs include information such as :

- **Operation type**: Operations such as resource creation, modification or deletion.
- **Timestamp**: Exact date and time of each event.
- **User IDs**: ID of the user or service initiating the operation.
- **IP addresses**: source and destination IPs for tracing the origin of requests.
- **Operation status**: Indications of successful or unsuccessful operations, including error codes and descriptive messages.

Log storage

Collected logs are securely stored in an S3 bucket or equivalent, with encryption measures to protect sensitive data. CTS supports configurable retention policies, enabling logs to be kept for specific durations to meet compliance requirements. These logs can be exported for in-depth

analysis or auditing purposes.

Alerts and Notifications

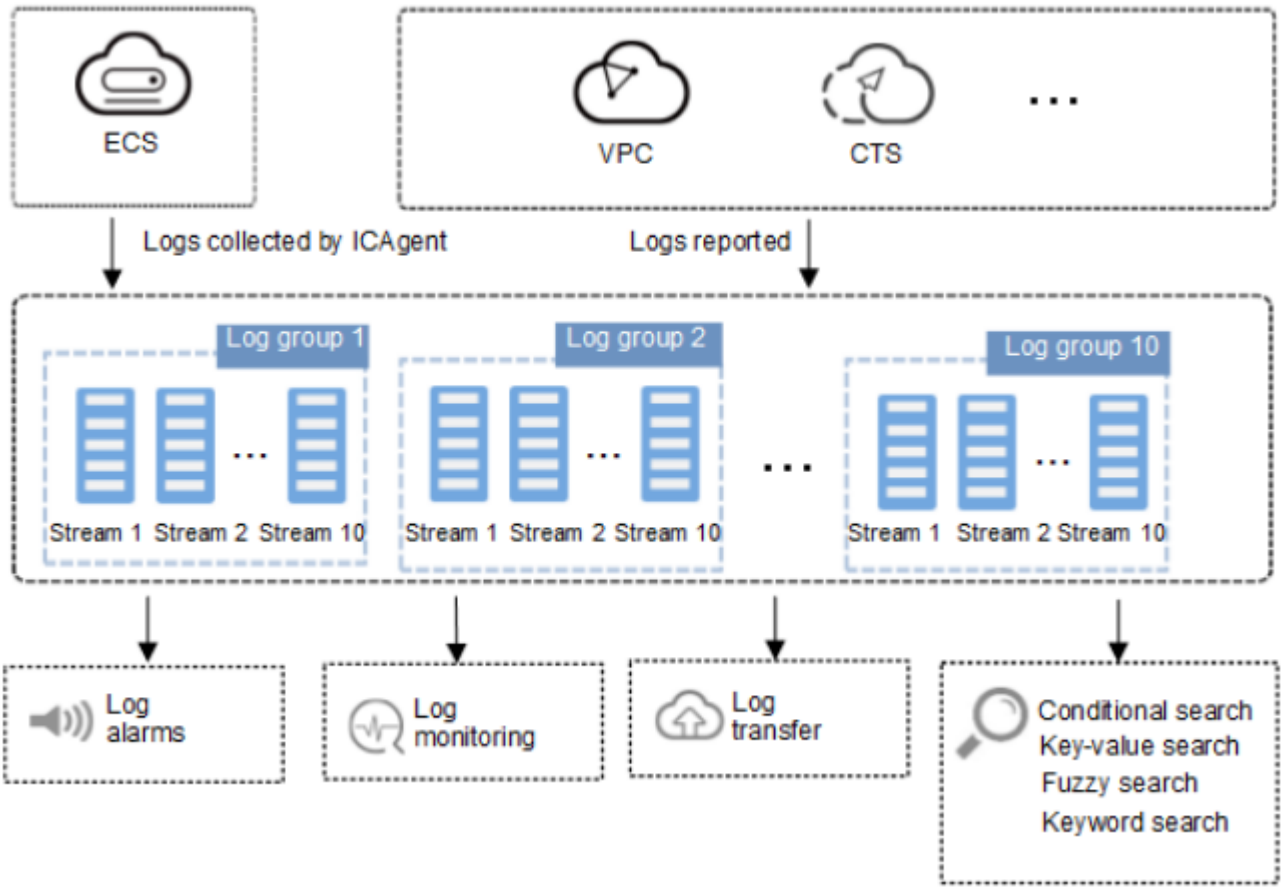
CTS offers real-time alert functionalities based on predefined criteria. For example, administrators can set up notifications for suspicious activities, such as repeated failed login attempts or unauthorized changes to critical configurations. These alerts can be sent via a variety of channels, including e-mail and instant messaging services.

Integration with SIEM solutions

CTS can be integrated with SIEM (Security Information and Event Management) solutions such as Splunk or Graylog, facilitating centralized analysis and correlation of security events. This integration enables the creation of customized reports and dashboards for greater visibility of potential threats.

Cloud Log Tank Service (LTS) module

Cloud Log Tank Service (LTS) is a robust log management solution designed to collect, store, analyze and manage logs generated within Cloud infrastructures. LTS plays a crucial role in continuous system monitoring, problem diagnosis and overall security enhancement.



Log collection

LTS supports comprehensive log collection from a variety of sources, including :

- **System logs**: Logs from the operating system and core services.
- **Application logs**: Logs generated by deployed applications, including error messages, stack traces and debugging information.
- **Network logs**: Logs relating to network traffic, capturing incoming and outgoing connections, firewalls and traffic routes.
- **Security logs**: Include security-related events such as unauthorized access attempts, IDS/IPS alerts, and security audits.

Centralized storage

Logs are stored centrally in an elastic storage system, often based on technologies such as S3 object storage. LTS allows you to define retention policies to keep logs according to specific business needs, ranging from a few weeks to several years.

Analysis and visualization

LTS includes tools for analyzing and visualizing log data. Administrators can use interactive dashboards, advanced filters and search queries to explore the data.

Machine learning and anomaly detection features can also be integrated to identify unusual behavior or security incidents.

Access management and security

LTS incorporates strict access management mechanisms, ensuring that only authorized persons can access and analyze logs. Role-based access controls (RBAC), multi-factor authentication (MFA), and encryption of data in transit and at rest are common measures implemented to protect sensitive data.

Alerting and monitoring

Like CTS, LTS lets you configure alert rules to monitor logs in real time. Alerts can be triggered by specific events, defined thresholds, or anomaly patterns detected in logs. These alerts are crucial for proactive response to security incidents or operational problems.

Integration with other services

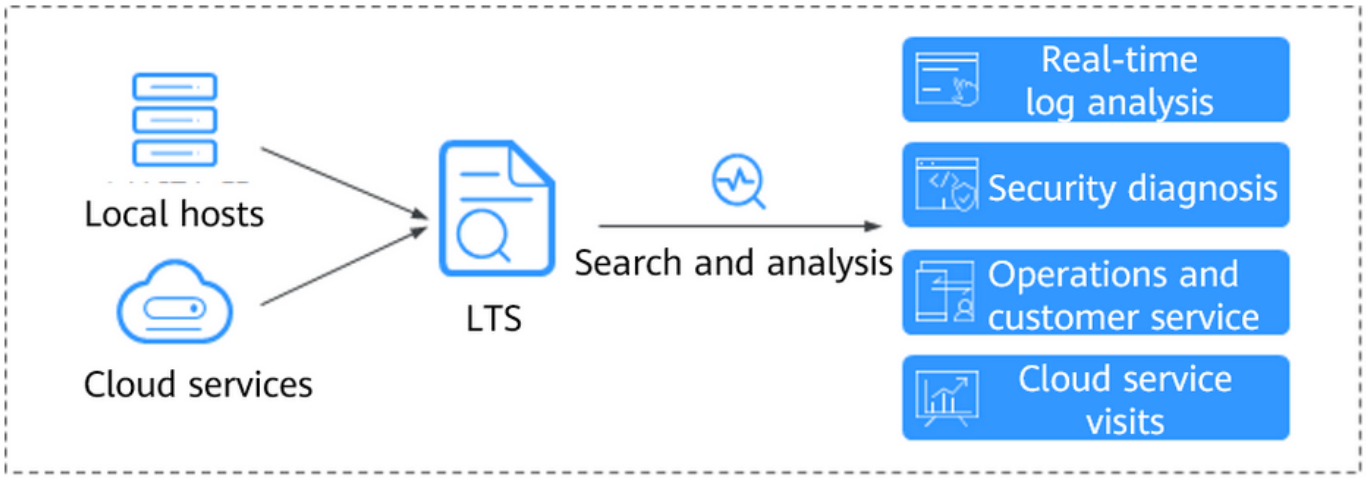
LTS is designed for seamless integration with other Cloud services and third-party monitoring tools. For example, it can connect with SIEM systems for consolidated analysis, or with DevOps tools to integrate logs into CI/CD pipelines.

This integration enhances the ability to monitor and manage logs across diverse environments and technologies.

CTS integration with LTS

The integration of Cloud Trace Service (CTS) with Cloud Log Tank Service (LTS) offers a robust solution for comprehensive log and trace management. CTS records user activities and operations performed on Cloud resources, generating detailed event logs. These logs can then be centralized and stored in LTS, where they can be accessed for in-depth analysis. This integration makes it easy to correlate security events and system activities, facilitating incident tracking and compliance auditing. What's more, by combining the collection and monitoring capabilities of CTS

with the log analysis and management features of LTS, we gain a complete and consistent overview of the DRP space, optimizing system security and performance.



Conclusion

Cloud OTC's **Cloud Trace Service (CTS)** and **Cloud Log Tank Service (LTS)** offer comprehensive coverage for log and trace management in the DRP space.

CTS focuses on activity logs and traceability of operations carried out in the Cloud, while LTS provides a global solution for the collection, storage and analysis of logs from various sources.

Together, these services form a solid foundation for security, compliance and operational management of cloud resources.

Further information: OTC log management documentation