Cloud resources monitoring in recovery mode

Security architecture · https://nuabee.com/documents/monitoring-resources-cloud-in-recovery-mode/

Introduction

Resource monitoring is an important component in ensuring resilience and service continuity in the DRP space.

When switching to Cloud backup mode, resources (servers, disks, gateways, etc.) need to be monitored in real time to detect anomalies and react quickly.

This article explores the CloudEye monitoring solution, native to the OTC Cloud, detailing how it works and its importance in a failover context.

Real-time resource monitoring: CloudEye

CloudEye is an OTC Cloud-native, advanced monitoring service that provides a comprehensive, real-time view of the status and performance of various cloud resources. Here's a detailed exploration of CloudEye's features for each resource type:

Server instances

CPU utilization: CloudEye continuously monitors the CPU utilization of server instances, providing detailed metrics on processor load. This includes:

- **Percentage Utilization**: Tracking the percentage of CPU utilization relative to total capacity. Spikes or prolonged loads may indicate overloading or an inefficient application.
- **CPU Wait Time**: Measures the time that processes wait for the CPU to become available, which may indicate performance problems.

Memory Usage: Monitoring of RAM usage.

- **Total and Used Memory**: Amount of total memory and used memory, as well as available memory.
- **Memory Leaks**: Detection of increasing memory usage that could indicate memory leaks in applications.

Disk performance: Measures the performance of attached storage volumes.

- **IOPS (Input/Output Operations Per Second)**: Number of read/write operations per second. A decrease in IOPS may indicate an overload or bottleneck.
- **Disk latency**: Response time for read/write operations. High latency can affect application performance.

Network resources: Monitoring of network interface usage.

- **Network throughput**: Amount of data entering and leaving instances, measured in bits per second (bps). Variations may reflect network problems or changes in traffic.
- **Network errors**: Track transmission errors and lost packets, indicating potential problems with network connectivity.

S3 storage

Storage volumes: CloudEye monitors the storage volumes attached to instances.

- **Space utilization**: the amount of space used in relation to the total capacity of the volume, enabling the detection of expansion needs or risks of saturation.
- **Volume performance**: Analysis of response times and IOPS to assess storage efficiency and identify bottlenecks.

File Systems: Monitor the integrity and performance of mounted file systems.

- **Used Space**: Monitor the amount of space used and available on mounted file systems.
- **File Errors**: Detection of read/write errors and file corruption problems.

Network

Bandwidth: Monitor the amount of data transferred across network interfaces:

- **Total Throughput**: Measurement of total throughput in and out for each network interface, providing a view of the amount of data exchanged.

- **Network utilization**: Analysis of bandwidth used versus total capacity, identifying periods of overload or excessive use.

Network Latency: Monitoring of network connection response times.

- **Response Time**: Measure of the time it takes for a request to travel between two points on the network, crucial for latency-sensitive applications.
- **Response times**: Monitoring of response times for services and applications, to identify connectivity problems.

Network errors: Monitoring of transmission errors

- **Lost packets**: Number of data packets lost during transmission, which may indicate connectivity or performance problems.
- **Transmission Errors**: Measure of errors in transmitted data, indicating potential problems with network interfaces.

Importance in a failover context

As part of a Disaster Recovery Plan (DRP), failover to backup mode is a crucial process for guaranteeing service continuity.

Resource monitoring plays an essential role at every stage of this process:

- **Proactive Problem Detection**: Real-time resource monitoring enables IT teams to spot potential problems before they cause a service interruption. This early detection facilitates a rapid response and enables corrective action to be initiated immediately, helping to reduce downtime and maintain continuity of operations in standby mode.
- **Post failover analysis**: After a failover to standby mode, it is imperative to examine the data collected by CloudEye in detail. This analysis helps diagnose potential problems by comparing performance trends with recorded activity. This helps identify any signs of compromise or anomaly, ensuring that restored systems are secure and operating correctly.
- **Failover validation**: CloudEye also plays a crucial role in validating failover to backup mode. It verifies that standby resources are operating as expected by monitoring performance metrics and analyzing activity logs. This validation ensures that services are fully operational and that data is consistent and complete after the transition.

Conclusion

Monitoring servers in a DRP space is crucial to ensuring rapid and effective recovery from an incident.

Solutions like CloudEye offer powerful tools for monitoring performance, managing alerts, and tracking actions taken.

By using this solution in failover mode, you strengthen your ability to detect, analyze and react to incidents, thus ensuring uninterrupted availability of Cloud services during a failover to standby mode.