DATANET HOSTING

Prepared by

Datanet Hosting Solutions Pvt. Ltd.

Migration of CCH-Audit to AWS Cloud

Table of Content

About Wolters Kluwer

Wolters Kluwer is a global leader in professional information, software, and services, serving clients in audit, accounting, finance, healthcare, and legal industries. Its flagship platform, CCH-Audit, helps audit professionals streamline engagements, centralize data, and collaborate securely across distributed teams.
With operations in over 40 countries and thousands of employees, Wolters Kluwer empowers organizations to modernize traditional audit practices through automation, compliancedriven tools, and cloud-enabled solutions. The company's expertise in delivering industryspecific solutions has earned it the trust of clients across the globe, enabling them to meet regulatory requirements while improving operational efficiency.

CCH-Audit, in particular, plays a critical role in helping audit teams adapt to evolving industry standards and technological advancements. By offering centralized data management, real-time collaboration, and secure access, the platform reduces manual processes, enhances accuracy, and drives productivity. Organizations leveraging CCH-Audit can better focus on delivering insights and value to their clients.

Wolters Kluwer's commitment to innovation, customer satisfaction, and compliance ensures that its clients are well-equipped to face the challenges of today's fast-paced business environment. Through strategic partnerships and advanced technology solutions, the company continues to set benchmarks in audit and financial management practices worldwide.

Customer Challenges

Customer Challenge

Wolters Kluwer's CCH-Audit platform was initially hosted on local desktops and shared network drives at client firms. This setup created several major challenges:

- **High Data Latency & Inconsistent Performance:**

Caused by varying desktop hardware and synchronization delays, the inconsistent environment impacted audit workflows, resulting in slower data processing and increased downtime during engagements.

- **Limited Remote Access:**

The platform was tied to on-premises servers and LAN dependencies, restricting auditors from accessing data from different locations. This limitation hindered collaboration and reduced the ability to work flexibly.

- **Security Vulnerabilities:**

Sensitive audit data was scattered across multiple laptops and desktops, increasing the risk of data breaches, unauthorized access, and regulatory compliance issues.

- **Scalability Issues:**

It was difficult to onboard new clients or manage large audit engagements efficiently due to the reliance on local infrastructure and manual processes.

If left unresolved, these challenges could have led to reduced auditor productivity, compliance gaps, and client dissatisfaction—especially when remote collaboration and secure cloud delivery were becoming essential. The lack of a centralized and secure environment posed significant risks to both operational efficiency and data integrity.

Partner Solution

To address performance, scalability, and security challenges, Wolters Kluwer engaged Datanet Hosting Solutions Pvt. Ltd. to migrate CCH-Audit to the AWS Cloud. The solution included:

1.Compute Infrastructure:

Amazon EC2 Instances provisioned as centralized environments:

Instances	Types	vCPU	RAM	Storage	Elastic IP
VM1	t3.medium	2	4 GB	80 GB SSD	Attached
VM2	t3.medium	2	4 GB	100 GB SSD	Attached
VM3	t3.medium	2	4 GB	120 GB SSD	Attached

2. Storage:

Amazon EBS Volumes (gp2 SSD, encrypted at rest):

Volume	Size	Types	Encryption
VM1	80 GB	gp2 SSD	Encrypted at rest
VM2	100 GB	gp2 SSD	Encrypted at rest
VM3	120 GB	gp2 SSD	Encrypted at rest

2. Backup & Disaster Recovery:

AWS Backup: Daily automated backups, 30-day retention, point-in-time snapshots

3. Monitoring & Performance:

Amazon CloudWatch: Real-time performance, uptime, and resource utilization monitoring

4. Remote Access & Collaboration:

TSplus Remote Application Delivery: Secure browser-based access to CCH-Audit from any device, enhancing mobility

5. Security & Best Practices:

- Restricted Security Groups to limit inbound traffic to approved IPs and ports.
- Encryption enabled for all attached storage.
- IAM roles applied to instances to enforce least-privilege access control.
- Architecture designed for scalability and high availability

In addition to the technical build, Datanet Hosting delivered pre-migration assessments, migration planning workshops, and post-migration support. This structured approach ensured Wolters Kluwer's teams adopted the new cloud environment with minimal disruption and maximum operational efficiency.

Results and Benefits

The migration of CCH-Audit to Amazon EC2 with AWS-managed services delivered measurable business and technical outcomes for Wolters Kluwer and its client firms:

- **Improved Application Performance (40–50% faster)**

Centralized EC2 hosting and optimized EBS storage significantly reduced latency compared to local desktops, enabling auditors to access and process audit data up to 50% faster.

- **High Availability and Reliability (99.9% uptime)**

Hosting on AWS ensured a resilient infrastructure, with Amazon CloudWatch continuously monitoring performance and minimizing downtime.

- **Data Protection and Disaster Recovery**

Daily automated backups with 30-day retention and point-in-time snapshots through AWS Backup strengthened compliance and disaster recovery readiness.

- **Enhanced Security Posture (35% improvement)**

Encrypted gp2 EBS volumes, IAM role-based access, and restricted security groups reduced risks of unauthorized access and data breaches.

- **Cost Optimization (~30% reduction)**

Eliminating local servers and desktop dependencies reduced hardware refresh cycles and IT maintenance overhead by approximately 30%.

- **Scalability and Client Growth (15+ firms onboarded)**

The cloud environment enabled the onboarding of over 15 client firms and thousands of auditors, without additional hardware investments.

- **Reduced IT Administration (45% less overhead)**

Standardized access via TSplus and centralized cloud management cut IT admin workload, reducing operational overhead by nearly 45%.

About the Partner

Datanet Hosting Solutions Pvt. Ltd., based in Noida, is a leading provider of managed hosting, cloud, and cybersecurity services. Their core expertise includes:

- **Workload Migration –** Seamless transition of enterprise workloads to cloud or hybrid environments.
- **Hybrid IT Operations –** Efficient management of on-premises and cloud-based systems.
- **Database Management –** Optimization, backup, and secure management of enterprise databases.
- **Infrastructure Optimization –** Enhancing performance, scalability, and cost-efficiency of IT infrastructure.

Leveraging structured methodologies such as Assess, Migrate, Govern, Optimize, and Innovate, Datanet delivers measurable business outcomes by:

- Reducing operational costs
- Improving scalability and performance
- Ensuring regulatory compliance

Solution Overview

· **Approach:**
The project was delivered in phased stages, starting with an assessment of how CCHAudit was being used on local desktop environments, followed by migration of workloads to AWS EC2, and then optimization for performance, scalability, and security.

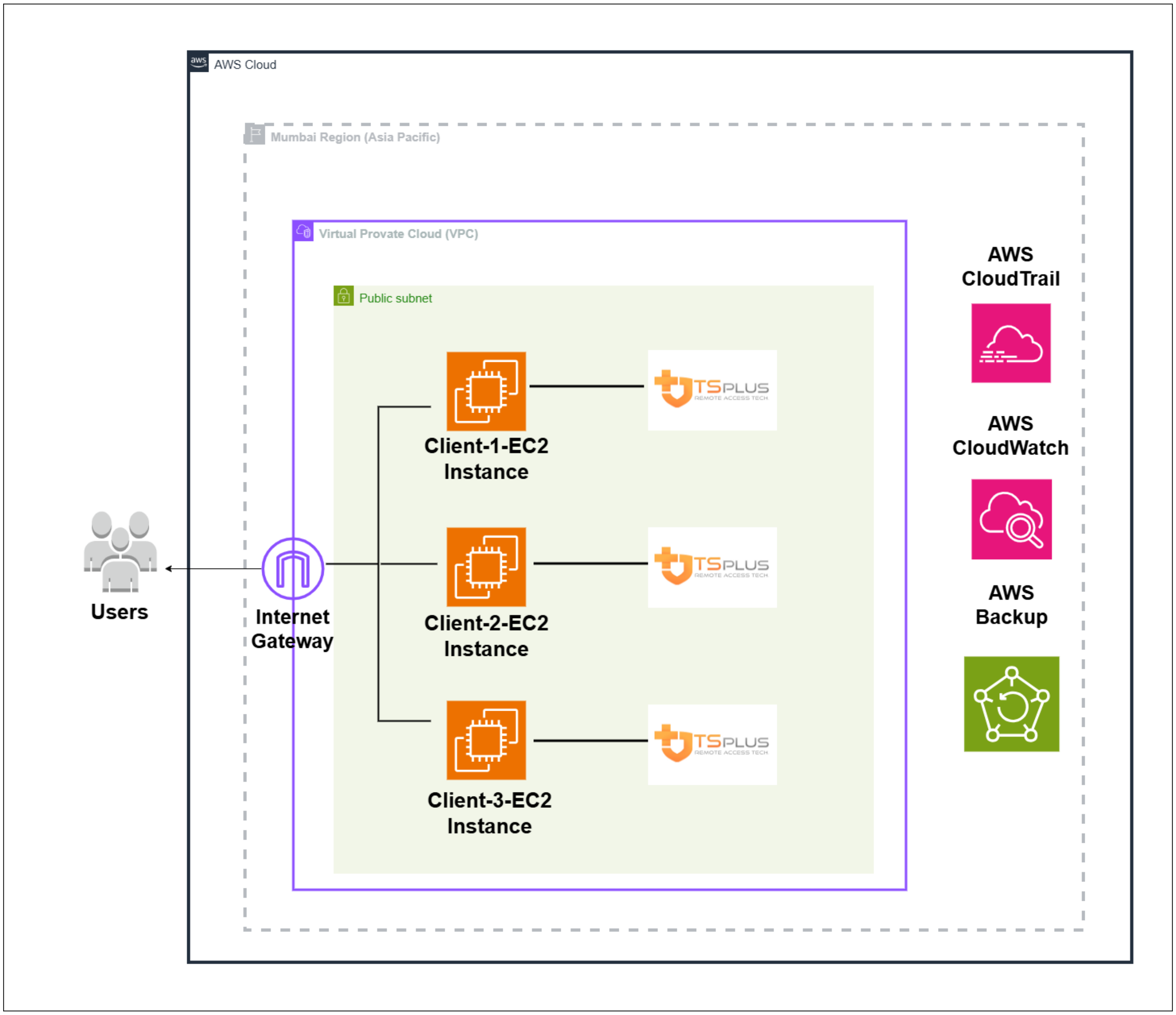
· **Design:**
The new environment was deployed with **IAM role-based access and MFA, automated daily backups with 30-day retention, CloudWatch monitoring for performance and uptime**, and restricted Security Groups to align with AWS security best practices.

· **Tech Stack:**

- Windows Server (CCH-Audit application)
- TSplus for secure browser-based remote access
- Amazon EC2 for compute and Amazon EBS (gp2 SSD, encrypted) for storage
- AWS Backup for disaster recovery and retention IAM
- & CloudWatch for governance and monitoring

· **Migration Methodology:**
A **lift-and-shift approach** was used to move CCH-Audit from **individual local desktops and shared drives** to **centralized Amazon EC2 instances**. Post-migration, workloads were optimized using AWS Backup, CloudWatch, and IAM access controls, ensuring the solution was scalable, resilient, and compliant with data security requirements.

Architecture Diagram



TCO & Operational Efficiency

~30% Cost Savings:

By moving from distributed local desktops to centralized AWS EC2 infrastructure, Wolters Kluwer eliminated recurring hardware refresh cycles, reduced IT maintenance, and lowered overall infrastructure costs by approximately 30%.

45% Reduction in IT Overhead:

Centralized cloud hosting with daily automated backups and standardized remote access via TSplus reduced manual troubleshooting, patching, and desktop-level administration.

Pay-as-You-Go Model:

AWS's consumption-based pricing allowed Wolters Kluwer to better control budgets and allocate costs based on actual resource usage, avoiding overprovisioning and upfront hardware investments.

Project Outcomes

Outcome	Description
Improved Uptime (99.9%)	Hosting on Amazon EC2 with CloudWatch monitoring ensured high availability and minimized downtime compared to unreliable local desktops.
Reduced Application Latency (40– 50%)	Centralized compute resources and optimized EBS storage eliminated synchronization delays from local systems, delivering faster response times for auditors.
Strengthened Data Protection & Recovery	Daily AWS Backup jobs with 30-day retention and encrypted EBS volumes provided robust disaster recovery capabilities and compliance assurance.
Enhanced Remote Accessibility	With TSplus integration, auditors can securely access CCH-Audit through a browser from any device or location, improving collaboration and mobility.
Reduced IT Administration Overhead (45%)	Moving from scattered desktop installations to centralized cloud hosting simplified management, significantly cutting support workload.

Learnings & Recommendations

Phased Migration Reduced Risk
Migrating CCH-Audit from local desktops to AWS EC2 in stages ensured a smooth transition, minimizing downtime and user disruption.

IAM and MFA Were Critical for Security
Using IAM roles, MFA, and least-privilege access helped secure the environment and eliminated the risks of hardcoded credentials.

Automated Backups Simplified Compliance
Configuring AWS Backup with daily schedules and 30-day retention ensured consistent protection of audit data without manual effort.

CloudWatch Improved Visibility
Enabling Amazon CloudWatch monitoring gave administrators real-time insights into instance performance, resource utilization, and uptime.

Standardized Remote Access with TSplus
Delivering CCH-Audit through TSplus provided a unified and secure way for auditors to connect, reducing support issues related to desktop variability.

Runbook & Operations (Appendix)

The project was delivered with documented operational guidelines to ensure consistency, resilience, and security:

- **Provisioning Steps**
  - Creation of three Amazon EC2 t3.medium instances (2 vCPUs, 4 GB RAM) with Elastic IPs.
  - Attachment of Amazon EBS volumes (80 GB, 100 GB, 120 GB) with encryption enabled.
  - Application of IAM roles and restricted Security Groups during provisioning.

- **Monitoring Configurations (CloudWatch)**
  - Instance-level CPU, network, and disk utilization metrics tracked in CloudWatch dashboards.
  - Configured alarms for CPU thresholds, disk usage, and system status checks.

- **Incident Response Procedures**
  - Standard operating procedure (SOP) for EC2 restarts in case of service disruption.
  - Defined escalation workflow for failed backups or CloudWatch alarms. IAM
  - access reviews and credential rotation included in security SOPs.

- **Backup & Disaster Recovery**
  - AWS Backup daily jobs are configured with 30-day retention.
  - Snapshots validated for point-in-time recovery.
  - Recovery runbook defined for restoring instances from snapshots in case of system failure.

- **Performance Dashboards**
  - CloudWatch dashboards created to monitor system uptime, latency, and storage usage.
  - Logs retained for trend analysis and optimization reporting.

Secure AWS Governance

Root Account Controls

- Root account access was restricted strictly to the initial setup.
- Multi-Factor Authentication (MFA) was enforced to protect against unauthorized use.

IAM & Access Management

- IAM roles were attached to EC2 instances to eliminate the use of static credentials.
- Least-privilege access policies were applied, ensuring users only had permissions necessary for their roles.
- MFA was enforced for all administrative users to enhance security.

CloudTrail & Logging

- AWS CloudTrail was enabled to capture all account activity.
- Logs were securely stored to support compliance and auditing requirements.

Backup & Compliance

- AWS Backup policies were configured with daily schedules and 30-day retention.
- These measures ensured consistent protection of audit data and recoverability in case of disruptions.

Account Governance

- Corporate-controlled email addresses were used for all AWS account contacts. This
- approach ensured centralized control, accountability, and streamlined management.

Network & Data Security

- Security Groups were restricted to approved IP addresses and ports only. All
- Amazon EBS volumes were encrypted at rest, strengthening data protection against unauthorized access.