

Experienced

Engineer

Modules & Polymer Products - Motherson Technology Services Limited (MTSL) - Noida, India

At Motherson, we’re committed to creating long-term jobs and advancing global careers. Featured on TIME’s World’s Best Companies list, we are a diversified global design, engineering, manufacturing, assembly and logistics specialist, delivering full-system solutions to customers across industries. With a focus on innovation, quality and sustainability, we strive to be a trusted industrialisation partner and an employer that nurtures a diverse, inclusive workplace.

Our Modules and Polymer division leads automotive innovation, producing everything from plastic components to complex integrated systems. Trusted by major OEMs worldwide, we also specialise in mould design, tooling, and high-quality upholstery for passenger vehicles. Join us in shaping the future of mobility.

What you'll do

- Monitor and manage AWS cloud infrastructure across Production and Non-Production environments. Provide 24x7 operational support through rotational shifts. Troubleshoot and resolve infrastructure, application, and network-related incidents. Manage AWS services including EC2, VPC, IAM, RDS, S3, ELB, Route 53, CloudWatch, CloudTrail, Lambda, and Auto Scaling. Perform server patching, upgrades, backup verification, and disaster recovery activities. Monitor system performance and ensure high availability of cloud resources. Implement security best practices and respond to security alerts. Automate routine operational tasks using Shell scripting, Python, or AWS CLI. Investigate systemic failures rather than simply treating symptoms. Perform deep log analysis and event correlation using AWS CloudWatch Logs Insights, AWS CloudTrail, and VPC Flow Logs to deliver comprehensive RCA reports for clients. Troubleshoot state and performance degradation across Amazon EC2 Auto Scaling groups, Amazon ECS/EKS container environments, and Amazon RDS Multi-AZ databases (identifying locking issues, IOPS exhaustion, and connection limits). Troubleshoot state and performance degradation across Amazon EC2 Auto Scaling groups, Amazon ECS/EKS container environments, and Amazon RDS Multi-AZ databases (identifying locking issues, IOPS exhaustion, and connection limits). Review and actively remediate security alerts and configuration flaws flagged by AWS Security Hub, Guard Duty, Macie, and AWS Inspector. Maintain environments aligned with CIS Benchmarks and local regulatory frameworks (e.g. RBI/CERT-In guidelines). Participate in on-call support and scheduled maintenance activities. Collaborate with application, database, and DevOps teams during deployments and incident resolution.

What we are looking for

- Monitor and manage AWS cloud infrastructure across Production and Non-Production environments. Provide 24x7 operational support through rotational shifts. Troubleshoot and resolve infrastructure, application, and network-related incidents. Manage AWS services including EC2, VPC, IAM, RDS, S3, ELB, Route 53, CloudWatch, CloudTrail, Lambda, and Auto Scaling. Perform server patching, upgrades, backup verification, and disaster recovery activities. Monitor system performance and ensure high availability of cloud resources. Implement security best practices and respond to security alerts. Automate routine operational tasks using Shell scripting, Python, or AWS CLI. Investigate systemic failures rather than simply treating symptoms. Perform deep log analysis and event correlation using AWS CloudWatch Logs Insights, AWS CloudTrail, and VPC Flow Logs to deliver comprehensive RCA reports for clients. Troubleshoot state and performance degradation across Amazon EC2 Auto Scaling groups, Amazon ECS/EKS container environments, and Amazon RDS Multi-AZ databases (identifying locking issues, IOPS exhaustion, and connection limits). Troubleshoot state and performance degradation across Amazon EC2 Auto Scaling groups, Amazon ECS/EKS container environments, and Amazon RDS Multi-AZ databases (identifying locking issues, IOPS exhaustion, and connection limits). Review and actively remediate security alerts and configuration flaws flagged by AWS Security Hub, Guard Duty, Macie, and AWS Inspector. Maintain environments aligned with CIS Benchmarks and local regulatory frameworks (e.g. RBI/CERT-In guidelines). Participate in on-call support and scheduled maintenance activities. Collaborate with application, database, and DevOps teams during deployments and incident resolution.

What we offer

- Career growth
- Inclusive workplace culture