Overview

As HPC adoption increases across industries and verticals, some companies face a difficult challenge. Their workload demands an upgrade to HPC, but their budget and staffing seems more suitable to a low-cost, low-maintenance and high-convenience cloud offering. Yet the nature of their business and competitive marketplace may also require all the rigorous security standards of an expensive, on-premise HPC environment. A European manufacturer in the automotive industry faced one such dilemma. They chose our HPCFLOW HPC-as-a-Service cloud solution, enabling them to maintain high security standards without compromising on job run time.

Objective

Ensure the highest level of security standards for HPC jobs run in the cloud – without compromising on processing time.

Requirements

- Highest quality HPC resources
- Secure transfer, storage and computation of sensitive company data
- Provision of HPC resources to multiple sites, all with the same high security restrictions
- Even distribution of HPC resources across these multiple sites

Approach

- HPCFLOW provides cloud-based, on-demand access to HPC resources from any site
- Project files are encrypted and uploaded via encrypted transfer methods, and access is highly restricted
- Automated job scheduling ensures even access to HPC resources across sites

Benefits

- Strong security, full encryption of most runtime and storage environments
- Flexible scalability to meet system demands at any given moment
- Convenience of cloud computing, enhanced processing power of HPC
- Minimal CAPEX required
The Challenge

When you’re a European manufacturer in the automotive industry, maintaining dozens of R&D centers around the world—and hundreds of production sites spread out over 30 countries—smart solutions are simply a requirement of doing business. With an R&D budget of nearly €2 billion, the company clearly prioritizes research and the need to innovate to remain on the cutting edge.

The highly competitive market and the company’s sensitive trade secrets mandated security and isolation of its HPC workloads. All transfer, storage and computation of their sensitive data demanded high security, often with full encryption.

Moreover, the company needed flexibility. Different teams at multiple sites needed to be able to upload their jobs to the HPC system. Of course, all teams would demand the same high performance and high security. Along with these strict privacy and security requirements, the company further required job scheduling to be automated, to ensure swift, fair and efficient distribution of the company’s HPC resources.

These were some of the basic constraints the company was working within when they searched for an IT solutions provider to upgrade a portion of their HPC environment in September of 2017. To meet their needs for both flexibility and remote access, the company was specifically interested in an HPC-as-a-Service offering rather than building a new cluster themselves.

But could HPC in the cloud meet their high security standards?

HPCFLOW: Secure-HPC as a Service

Encryption of the entire HPC cloud environment and workflow is, to be clear, not always enough of a priority for every company that they would be willing to build their HPC system around it. It’s reasonable to expect a 20% to 30% performance tradeoff for maintaining full encryption in every portion of the HPC environment.

On the other hand, 20-30% is a small premium to pay when the cost of not maintaining full security could mean millions of Euros in lost business and incalculable downstream consequences.

To meet the company’s needs, ADC brought to the table a purpose built bare metal HPC-as-a-Service (HPCaaS) offering, HPCFLOW. Using HPCFLOW, the company could scale their HPC resources up and down as needed, take advantage of faster deployment and hardware refreshes and enjoy easy deployment possibilities with integrated HPC applications.

To address the company’s security concerns, ADC proposed a dedicated HPC cloud solution, in which project files could be uploaded via encrypted transfer methods and remain encrypted for the entire life cycle. Access to the files would also be highly restricted, allowing only a single user to access them, preventing even root access.

Under this solution, Advania Data Centers’ HPC specialists would be able to give users feedback and assistance throughout the project. Crucially, though, no ADC personnel would ever have any access to the base data. This required a great amount of engineering and architecture to make sure just enough access enabled detailed feedback and help in the system’s automated job scheduling without providing any additional access to any data or results of computation.

Moreover, no unauthorized personnel — whether from ADC or anywhere else — would have the opportunity to access system data. Encryption, access controls and audit logging were utilized wherever possible.
In HPCFLOW, end to end encryption is a feature that you can leverage if you are running workloads that are sensitive. This feature allows customers to start leveraging HPC cloud in a secure and auditable manner while enjoying all the flexibility and scalability that HPCFLOW offers.

Gisli Kr., CCO, Advania Data Centers

Security as Pure OPEX

Ultimately, the company chose the zero-capital-expenditure (CAPEX) HPC choice that offered rigorous end-to-end security measures and full encryption of the entire HPC environment.

To execute projects using ADC’s HPCFLOW, the company’s teams prepared ZIP files for each project that contained all the files needed to run the computation. They uploaded the files to an internal server that then synchronized the files to the HPC platform. All transfers were done over an encrypted VPN tunnel to prevent unauthorized access to the data during transit.

Data files were then uploaded into an encrypted folder in ADC’s HPCFLOW platform. Using a proprietary solution controlled by the company’s internal administrators, this folder was only accessible to certain users when they logged in. As a result, the root user did not have access to the protected files, and indeed not even a system “superuser” could gain access to it either.

All access was logged and audited by the company, using Advania Data Centers’ proprietary solution. On the HPC platform, ADC further developed software that monitored the upload location for new files. New jobs were scheduled in the workload manager to assure fair access at all the company’s different sites. If one site uploaded multiple projects, they would not all be scheduled right away, so the next site could have access to HPC resources if they needed to upload a project as well.

The results of the computations were written to the same encrypted file system and finally synced back to the company. The source files were automatically deleted once the job had finished.
Powering Innovation Securely

The results speak for themselves. Even in the context of a highly secured HPC cloud environment, one in which performance might reasonably be expected to be sacrificed, the company was able to maintain its job queue times or even improve them. And even with strict security protocols in place, it was able to ensure that its engineers around the world could have access to secure and flexible HPC resources whenever they needed them.

In the rapidly evolving automotive marketplace, savvy and smarts are always required to continue supplying existing lines as well as get the next product line out and ahead of the competition. Now running ADC’s proprietary HPCFLOW solution, the company can more efficiently and securely power its research and development efforts. Smart HPC environments, these days, are just a requirement of doing business.

Get in touch

Customer Overview

Company
A European manufacturer in the automotive industry, providing a wide range of products to auto manufacturers and after-markets.

Industry
Automotive Manufacturing

Solution Specification
- Dedicated, purpose-built HPC cloud environment offers both bare-metal and virtualized HPC nodes
- All access to system logged and audited by customer via ADC proprietary solution
- File synchronization to HPC platform via encrypted VPN tunnel prevents unauthorized access to the data during transit
- ADC workload manager provides fair access to all customer's researchers and research centers seeking access to company HPC resources
- System scales easily to accommodate workload spikes

Case Study

Get in touch

Contact Us

Ægir Rafn Magnússon  
Head of Business Development  
eaegir.magnusson@advaniadc.com

Staffan Hansson  
HPC Sales Specialist, Scandinavia  
staffan.hansson@advaniadc.com

Hans Rickardt  
HPC Technical Director, Nordics  
hans.rickardt@advaniadc.com

Advania Data Centers  
Steinhella 10  
221 Hafnarfjörður  
Iceland  
hpc@advaniadc.com

For more information on what HPCFLOW can do for you, please don't hesitate to contact us.