DIGITAL INDUSTRIES SOFTWARE

Simcenter Cloud HPC – architecture and security

Delivering instant access to HPC resources for engineering simulation in the cloud using AWS global infrastructure

Executive summary
This white paper provides a technical overview of Simcenter™ Cloud HPC software, an application for running high-performance computing (HPC) simulation workloads in the cloud directly from a local client. Simcenter Cloud HPC is built using Amazon Web Services (AWS) infrastructure and services.

Leena Joseph
Siemens Digital Industries Software

Dnyanesh Digraskar
AWS

SIEMENS

Abstract

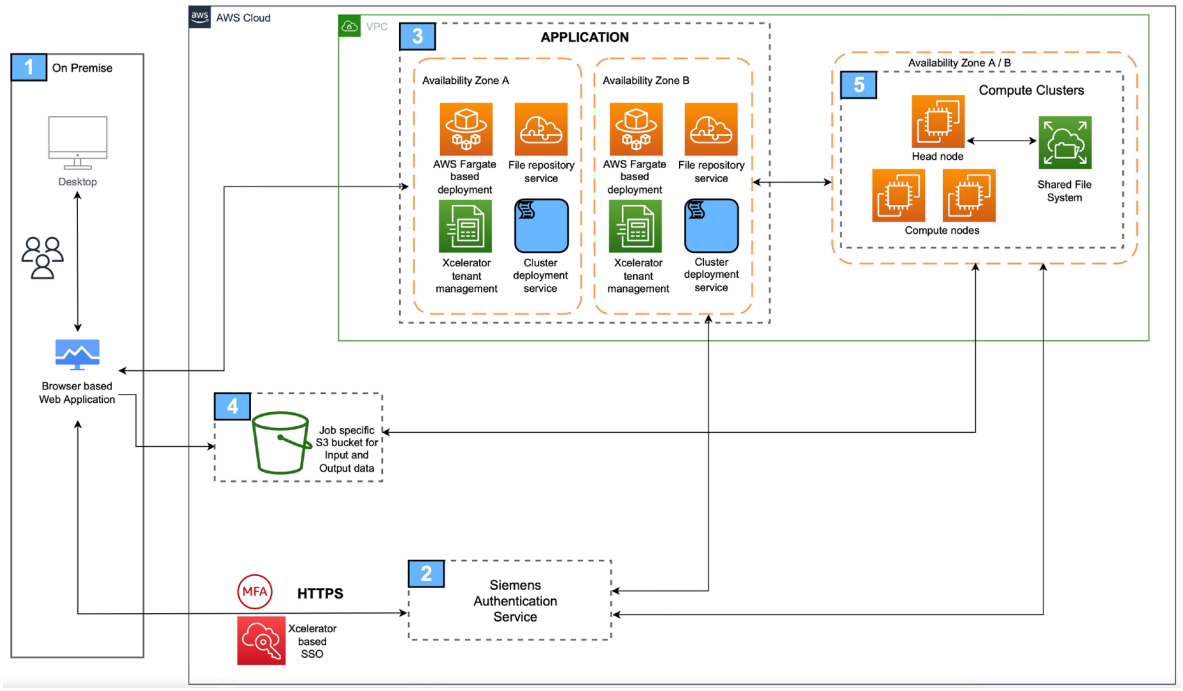
The AWS Well-Architected Framework provides guidance and best practices for AWS partners. It shares extensive experience and knowledge, enabling partners to build high-quality applications on AWS.

Simcenter Cloud HPC was developed in close collaboration with AWS following established best practices for security, reliability, performance and cost optimization. This solution is part of the Xcelerator portfolio, the comprehensive and integrated portfolio of software and services from Siemens Digital Industries Software.

This white paper discusses the following topics:

- Architecture and AWS services
- User workflow and data flow
- AWS regions and data residency
- Delivering high availability
- Tenancy
- Data retention and deletion
- Penetration testing and threat modeling
- Certifications

Architecture and AWS services



The different blocks of the architecture consist of:

1. User login via local standalone web browser or embedded inside Simcenter desktop application.
2. Authentication service using Siemens' Webkey.
3. AWS Fargate based application control and AWS Lambda based microservices including file repository service, billing and metering and HPC cluster orchestration.
4. Amazon Simple Storage Service (S3) buckets for storing simulation inputs/outputs.
5. Compute clusters offered in a range of sizes to suit different workloads. Based on the list of availability zones (AZ) in an AWS region, the cluster deployment service uses a round-robin approach to look for availability of instances in an AZ, then deploys clusters accordingly.

User workflow and data flow

Simcenter Cloud HPC is a web application that can be accessed in two ways – via an embedded Chromium browser in the Simcenter STAR-CCM+™ software desktop client or via a standalone browser such as Google Chrome or Mozilla Firefox.

The typical workflow involves starting from a loaded Simcenter STAR-CCM+ model. From the model navigator/tree, the user can choose to launch the simulation in Simcenter Cloud HPC, which loads the Simcenter Cloud HPC web application. If necessary, the user can sign in using their Siemens Webkey credentials.

Having signed in, the user can specify a job name and select the required resources from the four cluster options available. The user can choose to upload a Simcenter STAR-CCM+ Java macro file to be run when the job starts if desired. Finally, the user can also upload any other files if the job requires, such as reference data in a comma separated values (CSV) file.

If the user has a positive credit balance, they will be able to submit the job. Credit balance can be seen on the Simcenter Cloud HPC homepage and on the submit job page. The user can see their job status change through creation, upload, cluster provisioning and running. During this process, the input files are first uploaded to a dedicated Amazon S3 bucket. The cluster is provisioned on a number of Amazon Elastic Compute Cloud (Amazon EC2) compute nodes depending on the size of cluster. Once provisioned, the files are copied from the bucket to the cluster and the Simcenter STAR-CCM+ application is used to execute the job. The provisioned cluster is dedicated to the job and isolated from other clusters.

During the run, the user can monitor the job in real time, but they cannot modify or download any associated files. All files remain on the EC2 cluster during the run.

Upon job completion or interruption using the stop and save option, the relevant files are copied from the cluster back to the Amazon S3 bucket and are visible to the user in the job folder in Simcenter Cloud HPC. This includes all the original files uploaded during the job submission and any output files. Once the files are copied, the EC2 cluster is torn down and all temporary files are deleted.

The user can review the files in the corresponding folder in the Simcenter Cloud HPC job list and download files back to a specified folder on the local client at any point after the job is complete. It is also possible to delete the entire job if the files are no longer required.

AWS regions and data residency

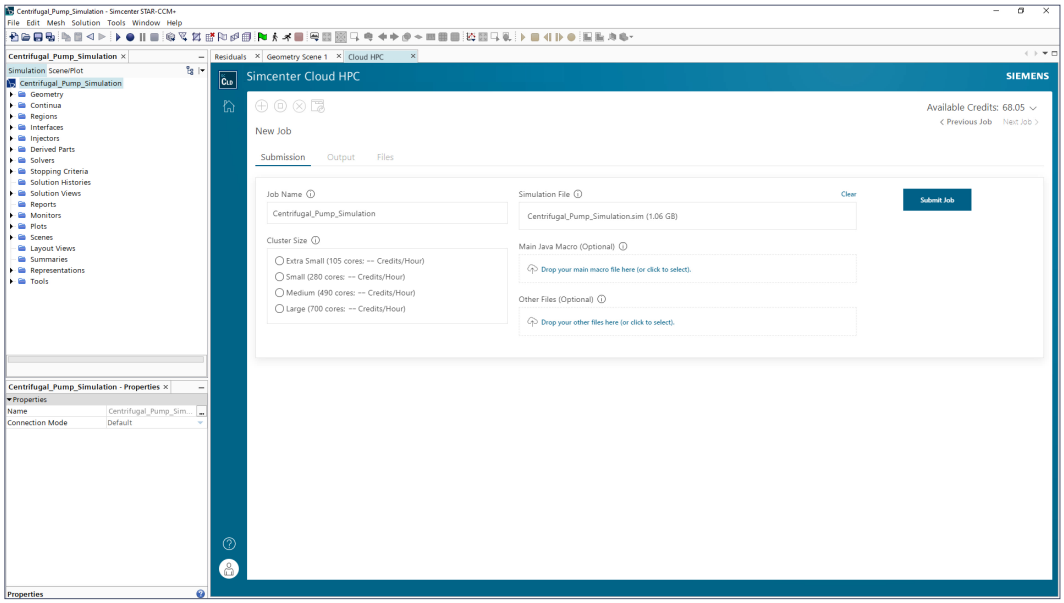
AWS is structured by region, which is a physical location around the world with multiple data centers. AWS infrastructure regions meet the highest level of security, compliance and data protection.

An availability zone is one or more discrete data center with redundant power, networking and connectivity in an AWS region. Each AWS region consists of multiple, isolated and physically separate AZs in a geographic area. Having access to multiple AZs enables customers to operate production applications and databases that are more available, fault-tolerant and scalable.

The AWS Control Plane, including application programming interfaces (APIs) and AWS Management Console, are distributed across AWS regions and uses a multi-AZ architecture in each region to deliver resilience and establish continuous availability. This enables customers to avoid depending on a single data center for a critical service. It also allows AWS to conduct maintenance activities without making any critical service temporarily unavailable to customers.

Simcenter Cloud HPC is architected to take full advantage of the AWS global infrastructure by deploying shared resources in a fault-tolerant and highly available manner. At first release, Simcenter Cloud HPC is deployed in the Northern Virginia region only; other regions will be added soon after launch. Users will determine the region to run their jobs in based on proximity.

Simcenter Cloud HPC stores customer data in the customer-selected AWS region of operation. Data is stored in unique buckets from which customers transfer it to their on-premises workstations. Customer-specific authentication information is stored in the Siemens authentication service that resides in the same region as the AWS services. The application backend resides in the Siemens tenant in the AWS region. Compute clusters are deployed in the Siemens tenant in one of the AZs in the selected region, depending on infrastructure availability.



Delivering high availability

Simcenter Cloud HPC uses Siemens' Xcelerator platform services, which are a constellation of microservices developed by Siemens for use across the Xcelerator portfolio. This enables a seamless user experience (UX) across Siemens' software-as-a-service (SaaS) applications by establishing common authorization and tenant management infrastructure. Service status and availability is closely monitored and managed by a dedicated RunOps team.

The Xcelerator platform relies on AWS managed services such as Amazon S3 for storage and Amazon DynamoDB for database, delivering robustness and high availability and incorporating AWS best practices. The Simcenter Cloud HPC backend is serverless and uses AWS Lambda so it has inherently high availability and scalability with no requirement to patch and manage server vulnerabilities. AWS Fargate, a serverless compute engine, is used for application control and deployment of the Amazon API Gateway. Together, this makes sure the application is resilient while the use of multiple AZs delivers a continuously available infrastructure.

Tenancy

As noted above, Simcenter Cloud HPC uses Siemens Xcelerator services for tenant management. All services are multi-tenant with enforced tenant data separation.

For each new job, a compute resource (HPC cluster) is created and dedicated to that job during execution. Upon completion, the cluster is torn down and destroyed. At all times, the cluster is isolated from other running clusters. Since no resources are shared, there is never a negative performance effect due to other tenants or jobs. Cluster isolation also minimizes the risk of malicious use.

The same principle applies to Amazon S3 storage; each job (folder) has a unique prefix, which means no data can be transferred between them. File upload and download is controlled by limited one-time, token-based user credentials issued by the file repository service based on their Siemens authentication service credentials. Each job can only be accessed by the job owner.

Protection against misconfigured infrastructure is provided by automatic and continuous services using AWS Control Tower with Cloud Custodian and AWS Security Hub.

All Siemens SaaS applications have privacy by design and adhere to the European Union's General Data Protection Regulations (GDPR). AWS also follows similar frameworks for data privacy and GDPR. The Siemens Trust Center is a useful resource for policies, compliance, transparency, availability and service.

Data retention and deletion

Data retention is governed by the terms of the Universal Customer Agreement (UCA); a customer must be able to access their data for at least 30 days after the subscription period expires. For credits, the subscription end date is when the last remaining credit expires (or would have expired if already consumed).

Data backup is governed by the terms of the cloud services support and service level framework. Simcenter Cloud HPC meets or exceeds all requirements of the standard tier.

There is currently no limit on data storage in Simcenter Cloud HPC while a customer holds an active subscription. The maximum size of an individual job (the total file size in a single job folder) is 1.2 terabytes (TB). Each individual user has control over their own data. Deleting a job from Simcenter Cloud HPC deletes the job folder and all associated files.

Penetration testing and threat modeling

Siemens works with an independent third party to conduct threat modeling and penetration testing activities. Threat modeling during the development cycle is used to identify and rectify any security weaknesses. All Siemens SaaS applications are regularly penetration tested to establish ongoing high levels of security.

Since Simcenter Cloud HPC is built on AWS, it benefits from the continuous security updates applied to all AWS services. Additionally, AWS provides a dedicated suite of fully managed security services, such as AWS Web Application Firewall (WAF), for distributed denial of service (DDoS) protection to reduce the potential for availability disruption. This includes protection from malicious use of Java macros or simulation files. Furthermore, the local redundancy provided by AZs deliver continuity of service in the event of an outage.

Network security groups and Amazon Virtual Private Cloud (VPC) are used to establish customer data confidentiality; VPCs are not accessible to incoming internet traffic.

Data is always encrypted at rest and in transit and API calls to AWS services are secured using the transport layer security (TLS) 1.2 standard, providing complete control over traffic access.

Certifications

Siemens has implemented a company-wide information security management system (ISMS) and Simcenter Cloud HPC complies with all requirements and practices. As part of this process, Siemens has achieved The International Organization for Standardization (ISO) 27001 security certification for SaaS services and is working toward certification for Simcenter Cloud HPC. ISO 27001 is the most widely known and accepted global standard for ISMS. Moreover, AWS already holds all related certifications including ISO 27017 for cloud security, ISO 27701 for privacy information management and ISO 27018 for cloud privacy.

Additionally, Siemens is working toward The American Institute of Certified Public Accountants (AICPA) System and Organization Controls (SOC) 2 type 1 and 2 certifications for Simcenter Cloud HPC. AWS is already SOC compliant.

The range of certifications held by Simcenter Cloud HPC is under continuous review and will be updated according to industry best practices and the specific needs of our customers. Some applicable certifications, such as Trusted Information Security Assessment Exchange (TISAX) and The Federal Risk and Authorization Management Program (FedRAMP) Moderate, are already held by AWS.

Conclusion

Simcenter Cloud HPC has been designed and architected to provide a robust and dependable HPC service for simulation users. Privacy, security and availability of the service are top priorities for Siemens' customers and Simcenter Cloud HPC incorporates the combined knowledge and best practices developed by Siemens and AWS. Additionally, the service follows industry standards on privacy and security and holds a range of certifications.

Siemens Digital Industries Software

Americas: 1 800 498 5351

EMEA: 00 800 70002222

Asia-Pacific: 001 800 03061910

For additional numbers, click here.

About Siemens Digital Industries Software

Siemens Digital Industries Software is driving transformation to enable a digital enterprise where engineering, manufacturing and electronics design meet tomorrow. Xcelerator, the comprehensive and integrated portfolio of software and services from Siemens Digital Industries Software, helps companies of all sizes create and leverage a comprehensive digital twin that provides organizations with new insights, opportunities and levels of automation to drive innovation. For more information on Siemens Digital Industries Software products and services, visit siemens.com/software or follow us on LinkedIn, Twitter, Facebook and Instagram. Siemens Digital Industries Software – Where today meets tomorrow.

siemens.com/software

84680-D3 6/22 H