SAP National Security Services Secure HANA Cloud on AWS GovCloud (US)

Address the most stringent U.S. government security and compliance requirements

SAP National Security Services (SAP NS2) is collaborating together with Amazon Web Services (AWS) to offer customers a comprehensive cloud solution designed to deliver SAP innovation to organizations that require the utmost security compliance. SAP NS2 Secure HANA Cloud (SHC) offers an end to end cloud solution that combines the capabilities and expertise of SAP NS2 personnel, leveraging secure AWS GovCloud (US) infrastructure. The SHC solution provides customers support for both SAP and non-SAP workloads on enterprise scale architecture that is tailored fit by SAP NS2 experts based on customers storage, networking, security, operating system, database, and application management needs.

Secure, reliable, and extensive cloud infrastructure

SAP NS2 offers Secure HANA Cloud customers service levels that are relevant to the business community and measure the SAP application uptime. As opposed to other cloud providers that only deliver infrastructure uptime SLAs, the SHC solution success is calculated based on the ability to keep the application up and running. In the instance of infrastructure SLA's, the virtual machines could be running successfully but the applications could be down. SHC provides this level of performance because we believe customers deserve the highest standard of support and performance. Customer investment into the SHC solution requires the highest commitment.

Key Benefits

The SAP NS2 team has extensive experience migrating, deploying, tuning, and securing SAP workloads on AWS. The following list provides insight into our methodology:

Quick & Secure Deployment

SHC uses expertly tuned AWS Machine Images (AMIs) specifically designed to run SAP solutions for highly regulated customers in a rapid and repeatable deployment. This means your SAP workloads will be deployed and configured more quickly than any other providers and meet the security and compliance requirements of the demanding frameworks such as FedRAMP Moderate and High, CJIS, IRS 1075, and DoD IL 2, 4, and 5.

Encryption At Rest At All Layers

AWS Key Management Service (AWS KMS) can protect block storage on Amazon Elastic Block Store (Amazon EBS), Amazon Elastic File System (Amazon EFS) as well as object storage on Amazon Simple Storage Service (Amazon S3). These keys are validated by the FIPS 140-2 Cryptographic Module Validation Program and meet the standards of most compliance frameworks. We also use compliant TLS cipher suites to protect encrypt and protect data in transit.

Maintain Data Protection

Secure HANA Cloud continuously maintains the data protection requirements of SAP workloads. SAP NS2 leverages SAP native tooling as well as AWS managed services like AWS Backup and Amazon S3 Cross Region Replication to meet RPO and RTO requirements.

Stay Up To Speed With Cloud Workloads Best Practices

SAP NS2 has a deep partnership with AWS. We constantly evolve our design to take advantage of the latest offerings and best practices of running cloud workloads.

Leverage Prebuilt Network Security Tools

SAP NS2 developed prebuilt cloud native network security tools including firewalls, security groups, and network access control lists designed to run SAP solutions in order to ensure only the communication necessary for your workload to function is allowed.

Securely Connect Your On-Premise Environment To Your Cloud Deployments

AWS Direct Connect and AWS Cloud VPN is set up by SAP NS2 experts to securely connect your on-premises environment to your cloud deployments of SAP applications. The SAP NS2 team also connects your SAP workload to the AWS environment securely using AWS Transit Gateway or VPC peering, without the need to leave the AWS network.

Avoid Public Internet

SAP NS2 deploys preconfigured Amazon Virtual Private Clouds (Amazon VPCs) designed to run SAP solutions and limit unneeded egress traffic. The SHC design can accommodate connections to your resources without traversing the public internet.

Use SAP NS2 Experts To Manage Cloud Native Configuration Management Tools

SHC uses SAP NS2 experts to manage cloud native configuration management tools to support the underlying operating systems of your workload. This includes patch management, performance tuning, and OS hardening.

Monitor Your Workloads And Mitigate Disruptions

AWS CloudWatch as well as other tools are leveraged by SAP NS2 to monitor your workloads. We combine this with cloud native recovery options such as Amazon EC2 Auto Recovery to respond and mitigate disruptions to your environment quickly.

Meet The Standards Of Most Compliance Frameworks

SHC on AWS GovCloud (US) gives customers the flexibility to architect secure cloud solutions that comply with the FedRAMP High baseline; the DOJ's Criminal Justice Information Systems (CJIS) Security Policy; U.S. International Traffic in Arms Regulations (ITAR); and other compliance regimes.

SAP National Security Services Overview

SAP NS2 is an independent subsidiary of SAP founded to help protect and secure the critical data of our nation. Our team is made up of 100% United States persons on United States soil managing enterprise scale cloud infrastructure across many different cloud applications. SAP NS2 provides the unique capability for customers in the a U.S. federal, defense, and aerospace industries to run market leading SAP applications without having to sacrifice innovation or cost.

More on AWS GovCloud (US)

AWS GovCloud (US) provides specific compliance and regulatory needs of U.S. government agencies at the federal, state, and local levels, as well as U.S. commercial organizations. Designed to host sensitive data and regulated workloads in the cloud, AWS GovCloud (US) Regions are isolated AWS regions operated by employees who are U.S. citizens on U.S. soil.

Get started: Visit AWS Marketplace or https://sapns2.com/cloud/ to learn more.