SDSC SHERLOCK CLOUD OVERVIEW

The SDSC Sherlock Cloud infrastructure was established as a means to provide secure data storage and computing to academic and government partners. Sherlock Cloud is both HIPAA and FISMA compliant and was developed in accordance with hundreds of NIST controls governing system access, information control, and management processes. Sherlock Cloud addresses federal Cloud First requirements and is undergoing FedRAMP Infrastructure as a Service (IaaS) Cloud Service Provider (CSP) certification, a requirement for many new and existing federal contracts and grants.

Sherlock Cloud currently supports National Institutes of Health (NIH), Centers for Medicare & Medicaid Services (CMS) and University of California (UC) initiatives and complies with the specific requirements of each agency. Sherlock Cloud offers a flexible and scalable compute and storage platform for a variety of research and data projects requiring a secure, access-controlled environment.

FOR RESEARCHERS

Sherlock Cloud was built to support researchers and their projects. Sherlock Cloud programmers and staff at the San Diego Supercomputer Center (SDSC) understand the requirements of research computing, and how the needs of professors and investigators may differ from those of the typical end users of commercial cloud platforms. Sherlock Cloud offers the ability to partner on a project basis, improving economies-of-scale based on shared infrastructure, processes, and documentation, and providing expertise in supporting FISMA, HIPAA, and more agile environments. Sherlock Cloud provides researchers a competitive advantage in their proposals, in the execution of their awards, and in the ongoing enhancement of their capabilities.

FOR IT ORGANIZATIONS

Sherlock Cloud prides itself in the ability to provide a full suite of services to researchers. Sometimes, however, the researcher can be better accommodated by IT staff institutionally closer to the project. For this reason, Sherlock Cloud partners with IT organizations to develop a custom framework for supporting projects. Together, we develop a comprehensive joint service model that defines roles, responsibilities, processes, and methods that will be used to support projects. Permutations can range from Sherlock Cloud operating as a service “island” to integration with campus account provisioning and deprovisioning systems and institutional branding. Sherlock Cloud is flexible to support the needs of partner institutions within security compliance requirements.

WHERE TO FIND SHERLOCK CLOUD

Sherlock Cloud’s resources are physically located within SDSC’s Data Center, and, where needed for redundancy, in a secure data center in Northern California. SDSC’s Data Center is staffed around the clock and protected with controlled access systems, backup power, advanced fire suppression systems, and other safety measures.

Sherlock Cloud systems interconnect with a 10Gb/s (gigabits per second) network fabric within the SDSC Data Center, and wide-area networking utilizes more than 100Gb/s of high-bandwidth connections to the Internet and research networks such as Internet2, National Lambda Rail (NLR), and the Corporation for Education Network Initiatives in California (CENIC). More information can be found at http://sdsc.sherlock.edu.

SAN DIEGO SUPERCOMPUTER CENTER (SDSC)

In 1985, General Atomics established SDSC at the University of California, San Diego (UC San Diego) with funding awarded by the National Science Foundation (NSF); SDSC was one of two national supercomputer centers for academia. SDSC transitioned to UC San Diego management in 1997.

SDSC is an Organized Research Unit at UC San Diego with a staff of more than 300 scientists, software developers, and support personnel. It has major programs with:

- Centers for Medicare and Medicaid Services (CMS)
- National Institute of Health (NIH)
- National Science Foundation
- Department of Defense
- Universities and other Organized Research Units around the country

SDSC is leading the way in developing a national cyberinfrastructure that will provide the technological foundation for the next generation of science and engineering advances. More information can be found at http://www.sdsc.edu.

WHAT CAN SHERLOCK CLOUD DO FOR YOU?

Sherlock Cloud offers users the robust, academically oriented support that one would expect from UC San Diego. Further, Sherlock Cloud’s value proposition is uniquely suited to computing and includes:

- Support for research and academic space
- Partnership on a project or institutional basis
- Sharing of economies-of-scale across projects
- Experience in supporting FISMA, HIPAA, and agile environments (i.e., compliance to regulatory requirements)
- Support from resource or program perspective
- Managed/shared services
- Ownership of the stack – it is your data
GETTING STARTED

Our team of expert information technology specialists will guide you through the process of determining the “next steps” for working with Sherlock Cloud.

Step 1: Determining Your Project’s Background and Scope

Before we can initiate a new project, we must understand the project’s background and scope and any specific user needs.

- What regulatory requirements must be met? (e.g., FISMA, HIPAA)
- Who will need access to your project’s data?
- What is your understanding of the project’s security?
- What is your understanding of the project’s security requirements?
- What can we do to help you?

Step 2: Understanding Your Project’s Compliant Hosting Requirements

For this step, we will need to know a few details about your specific computing requirements, such as:

- Applications
- Compute and Storage
- Account Management
- Development, Testing, and Production Environment
- Second-site, Backup, and Offsite
- Monitoring Framework
- Systems Development Life Cycle
- On-call User Support
- Service-level Agreements

Step 3: Proposing and Building a Platform

Next, we will work with your team to:

- Define and Test a Proof-of-Concept (PoC) Implementation (if requested)
- Upon PoC Approval, Discuss Costing Options
- Develop Proposal, including Deliverables and Timelines
- Initiate Platform Deployment upon Contract Award

Step 4: Providing Ongoing Operations and Maintenance Support

We want your project to be successful from initiation to completion and every step in between. To aid in your success, we provide ongoing:

- Infrastructure Support
- System Maintenance
- Change Management
- Security/CISO Support
- Overall Program Management

PRICING

The following table provides pricing for compute, storage, and a few examples of standard software components typically deployed for compliant hosting. This is not a comprehensive list but is intended to provide an estimate on pricing for commonly used software/applications/tools.

*The costs listed below are for demonstrative purposes and subject to change based on requirements.

<table>
<thead>
<tr>
<th>Offering</th>
<th>Rate</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Compute and Storage</strong></td>
<td></td>
</tr>
<tr>
<td>VM Base Cost (per VM-Month)</td>
<td>$12</td>
</tr>
<tr>
<td>VM Resources (per CPU Core or 3GB RAM Hour)</td>
<td>$0.05</td>
</tr>
<tr>
<td>Primary Storage (per allocated GB-Month)</td>
<td>$0.15</td>
</tr>
<tr>
<td>Backups (per GB-Month)</td>
<td>$0.12</td>
</tr>
<tr>
<td>Data Transfer Costs (Free)</td>
<td>$0</td>
</tr>
<tr>
<td>Physical Servers (per Hour)</td>
<td>$0.20</td>
</tr>
<tr>
<td><strong>Example Software/ODCs</strong></td>
<td></td>
</tr>
<tr>
<td>Antivirus (per server)</td>
<td>$30</td>
</tr>
<tr>
<td>SecurID Fobs (each)</td>
<td>$86</td>
</tr>
<tr>
<td>Windows Licensing (Annual)</td>
<td>$40</td>
</tr>
<tr>
<td>RDS Licensing (Annual)</td>
<td>$8</td>
</tr>
<tr>
<td>Zerto Replication (per VM-year)</td>
<td>$30</td>
</tr>
<tr>
<td><strong>Labor</strong></td>
<td></td>
</tr>
<tr>
<td>Baseline Environment Labor Costs (per hour): Includes support for: infrastructure support, account provisioning, VPN, etc.</td>
<td>$80</td>
</tr>
</tbody>
</table>

KEY SLEUTHS

For more information, please contact Sherlock Cloud’s Key Sleuths:

- Sandeep Chandra, Division Director: chandras@sdsc.edu
- Winston Armstrong, Chief Information Security Officer: warmstrong@sdsc.edu