Managing dbGaP Data with Stratus, a Research Cloud for Protected Data

Evan F. Bollig (bollig@umn.edu) Graham T. Allan Benjamin J. Lynch Yectli A. Huerta
Mathew Mix Brent Swartz Edward A. Munsell Joshua Leibfried Naomi Hospodarsky

Minnesota Supercomputing Institute
University of Minnesota
Driven to Discover℠

Introduction

Modern research computing needs at academic institutions are evolving. While traditional HPC has and continues to satisfy most workflows, a new generation of researchers has emerged looking for sophisticated, on-demand, and self-service control of compute infrastructure in a cloud-like environment. Furthermore, many also seek policy-compliant safe spaces to compute on sensitive or protected data.

To cater to these modern users, the Minnesota Supercomputing Institute is deploying a cloud service for research computing called Stratus. In its initial iteration, Stratus is designed expressly to satisfy the requirements set forth by the NIH Genomic Data Sharing (GDS) Policy for data from the Database of Genotypes and Phenotypes (dbGaP) [1].

Stratus is powered by the Newton version of the OpenStack cloud platform, and backed by Ceph storage. The subscription-based service is currently running in beta-test mode. In addition to data protection and compliance, the service offers three features not available on traditional HPC systems:

- on-demand availability of compute resources;
- long-running jobs (i.e., $>$ 30 days); and
- container-based computing with Docker.

Stratus Hardware

- 20x compute nodes with 2x Intel E5-2680v4 (14-core) CPUs, 256GB of RAM; 1120 cores and 5TB RAM total.
- 8x storage servers with 256GB memory, 2x 800GB Intel NVMe P3700 accelerator boards, and 198 TB raw capacity; 1.5 PB total raw capacity.
- 10x 8-core control servers with 32 GB RAM.

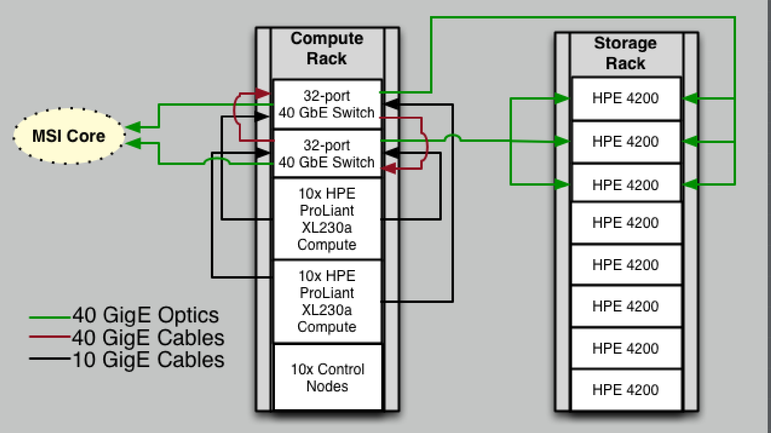

Figure 1: Stratus hardware footprint and connectivity.

Stratus Hardware Performance

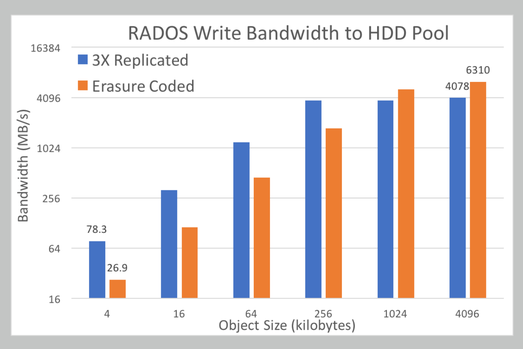

Figure 2: Stratus storage write bandwidth for both 3x replicated block device storage and erasure coded object storage.

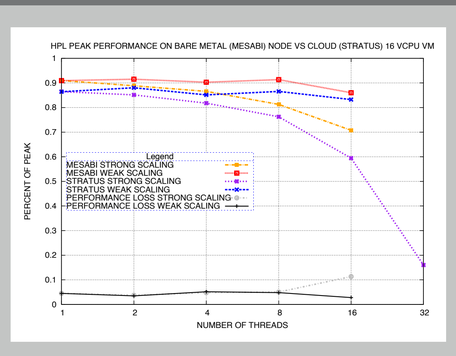

Figure 3: HPL benchmark comparison with Mesabi HPC. Virtualization sacrifices ∼5% of peak, but adds flexibility and long-running jobs. KVM accelerated virtualization, with oversubscription ratios for CPU and memory set to 2.0 and 1.2.

Tiered Storage

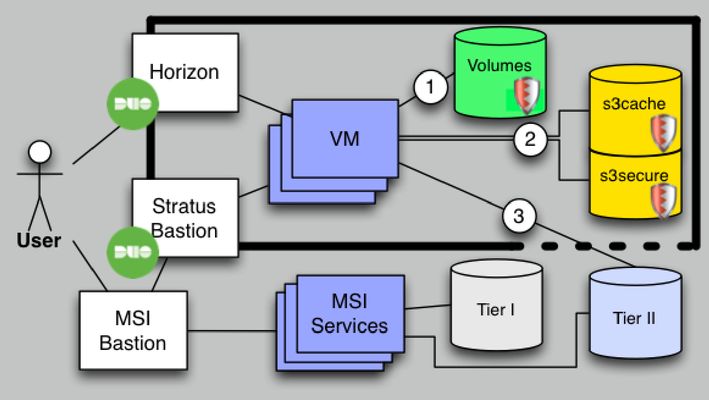

Figure 4: Stratus is sandboxed from other MSI services, but VMs have access to three tiers of storage. Shields denote storage suitable for dbGaP data. Analysis results, which are not subject to dbGaP requirements, can move to MSI Tier II for archive or public sharing.

Two-Factor Authentication

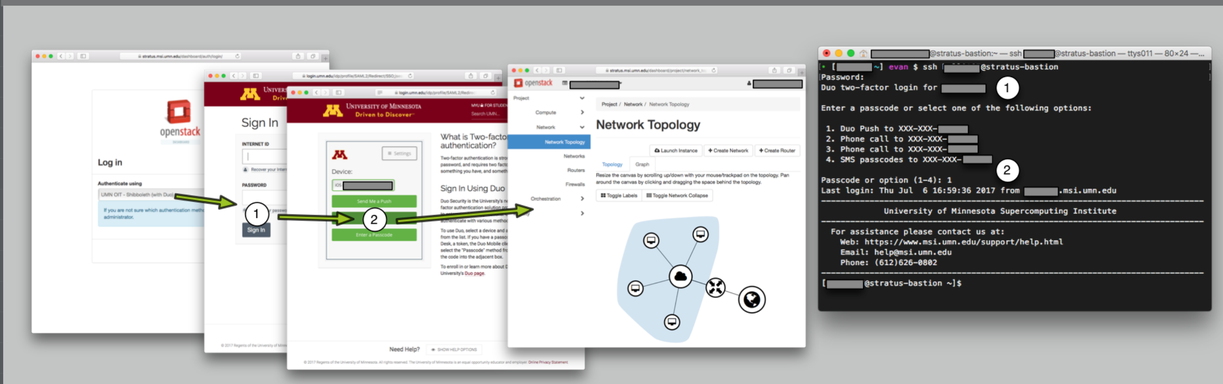

Figure 5: Two-factor Shibboleth authentication is required to access Stratus via Horizon and the Stratus-Bastion server. SSH to VMs requires connecting via the Bastion.

GDS Compliance

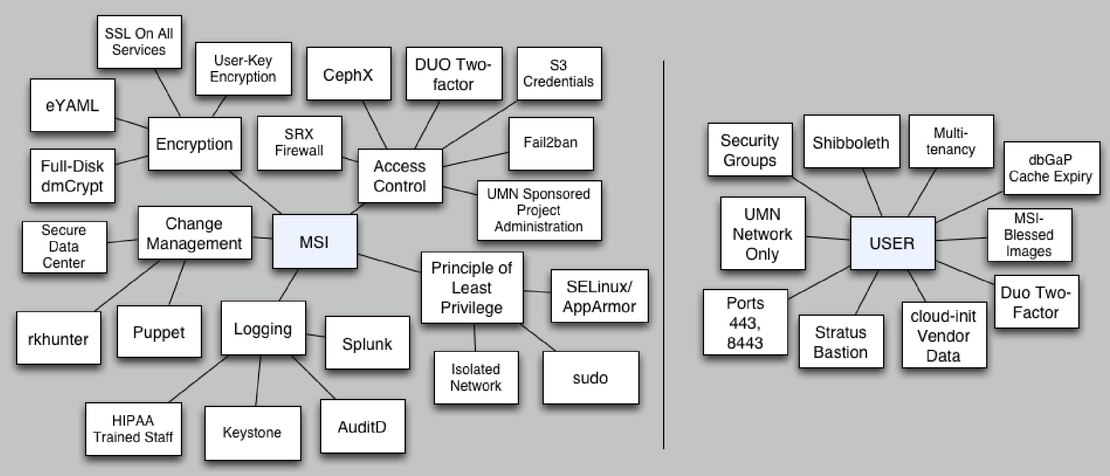

Figure 6: Compliance is met with an MSI-first policy that focuses on securing MSI, OpenStack, and Ceph. Going the extra mile, users are protected with sane defaults and network security, but they can opt-out of some protections at their own risk.

The NIH best practices guide for GDS data [2] was followed as a checklist. All bullets therein were treated as required controls. Note that the best practices go beyond what most large research computing facilities can or need to do.

MSI-Blessed Images

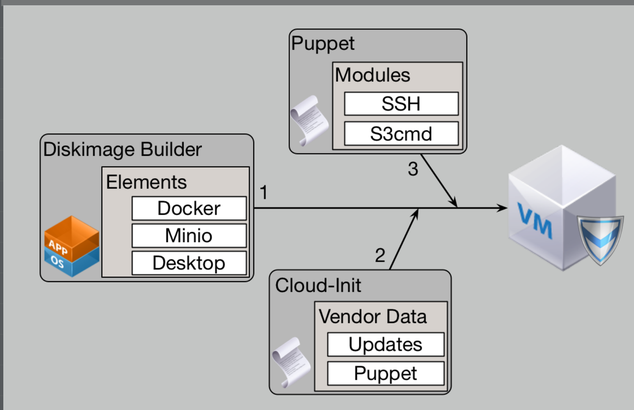

Figure 7: Secure VMs start with "MSI-blessed" images constructed by DiskImage Builder. Cloud-Init and Puppet ensure that VMs are updated with the latest security patches and configured for compliance at boot.

Name	Type	Status	Visibility
Centos7_dbgap_blessed	Image	Active	Public
Centos7_dbgap_blessed_desktop	Image	Active	Public
Centos7_vanilla	Image	Active	Public
Centos7_vanilla_desktop	Image	Active	Public
cirros035	Image	Active	Public
Debian8_dbgap_blessed	Image	Active	Public
Debian8_vanilla	Image	Active	Public

Figure 8: Users choose from a variety of cloud-ready operating systems, including variants for graphical remote desktops, and variants tailored for dbGaP data.

Network Isolation

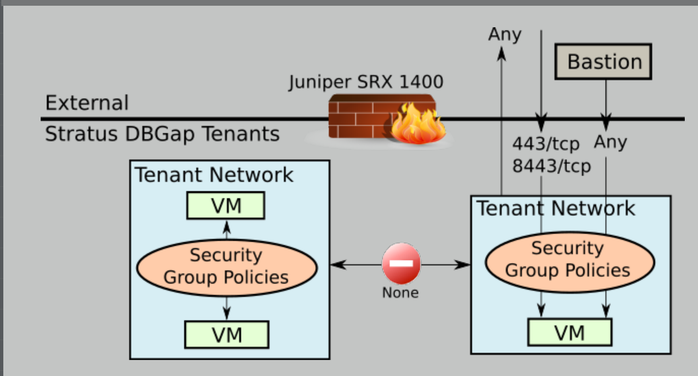

Figure 9: Tenants are isolated from one another. Traffic outside of the tenant is governed by the enterprise stateful firewall rules in Table 1. Egress traffic is unrestricted for general internet connectivity.

Table 1: The Juniper SRX Firewall ensures traffic originates from UMN networks. Even when Ingress is allowed, users must opt-out by modifying their OpenStack Security Group policies.

Scope	Ingress	Egress
World	None	ALL
UMN	443, 8443 with SSL[1]	ALL
Stratus	ALL via Stratus Bastion[1]	ALL
Project	ALL	ALL

[1] requires Security Group exceptions

Stratus Subscription

Base subscription:

- 16 vCPUs across one or more VMs
- 2 TB Block Storage for VMs and attached Volumes
- Access to dbGaP Cache, an S3 Short-term Protected Object Store
- Access to MSI-blessed VM images
- Root-level control to install software

Table 2: Stratus' fee-based services require a base subscription, which can be expanded à la carte with additional vCPUs and storage.

Service Name	Unit	Cost/Year
Stratus base subscription	Pkg	$626.06
Additional CPU Cores	vCPU	$20.13
Additional Block Storage	TB	$151.95
Persistent Secure Object Storage	TB	$70.35

Fee structure is based on zero-profit cost recovery. Services are limited to UMN researchers only.

Acknowledgments

Stratus is piloted as part of the MSI Beta program. The authors extend their thanks to Drs. Claudia Neuhauser, James Wilgenbusch, Jeffrey McDonald, Josh Baller, and Michael Milligan for their support of the Stratus project. Additionally, Ms. Raychel Benson for her insightful critique of operational security.

References

[1] Matthew D. Mailman, Michael Feolo, Yumi Jin, Masato Kimura, Kimberly Tryka, Rinat Bagoutdinov, Luning Hao, Anne Kiang, Justin Paschall, Lon Phan, Natalia Popova, Stephanie Pretel, Lora Ziyabari, Moira Lee, Yu Shao, Zhen Y. Wang, Karl Sirotkin, Minghong Ward, Michael Kholodov, Kerry Zbicz, Jeffrey Beck, Michael Kimelman, Sergey Shevelev, Don Preuss, Eugene Yaschenko, Alan Graeff, James Ostell, and Stephen T. Sherry. The NCBI dbGaP database of genotypes and phenotypes. Nature genetics, 39(10):1181–1186, October 2007.

[2] NIH. NIH Security Best Practices for Controlled-Access Data Subject to the NIH Genomic Data Sharing (GDS) Policy, March 2015.