Rubin at the Summit - observatory cyber infrastructure and security

Cristian Silva[a], Carlos Barría[a], Baden Erb[a], Ivan Gonzales[a],
Joshua Hoblitt[b], Guido Maulen[a], Hernan Stockebrand[a], Diego Tapia[a],
William O'Mullane[a]

[a]*Vera C." Rubin Observatory Avenida Juan Cisternas "#1500 La Serena Chile*
[b]*Vera C." Rubin Observatory Project Office 950 N." Cherry Ave. Tucson AZ 85719 USA*

Abstract

We describe the modern and dynamic infrastructure as code based system underlying operations of the Vera. C Rubin Observatory. We will also cover or extra efforts to be NIST standard compliant for cyber security.

Keywords: Vera C. Rubin Observatory

1. Introduction

The Vera C. Rubin Observatory[1] will go in to operations in 2025. During commissioning we have already seen our infrastructure as code based cyber system working well. In this paper we will describe the generic underlying hardware, deployments on that hardware of both bare metal and containerized applications, transmission of data to SLAC and our NIST[2] compliant security approach.

The Rubin summit may be viewed in terms os standard Cyber Infrastructure Layers. The layers are graphically depicted in Figure 1i which is a revised version of the diagram presented in [3]. Each layer is covered in a section below as follows:

1. The physical layer covered in Section 3
2. The network layer covered in Section 4
3. The computing layer covered in Section 5
4. The application layer covered in Section 6

2. Key Considerations

Before discussing the network infrastructure used for the Rubin Observatory, it is important to understand the conditions under which the Vera C. Rubin Observatory—and most observatories worldwide—operate.

Observatories typically have two operational sites: one in a city, where offices are located, and another where the actual observatory is situated. This latter site is by far more complex to design and operate.

At Rubin Observatory, we have multiple operational sites. There are two sites in La Serena, one in Tucson, and a data center at Stanford. However, the most challenging site to design, and the one requiring the highest level of precaution, is located on the mountain, one of the two sites in La Serena. This site is not only subject to unique climatic conditions—situated over 2,600 meters above sea level with lower oxygen levels and little humidity—but it is also difficult to access.

Traveling from the nearest city, La Serena, to Cerro Pachón takes approximately two hours. This means that if an urgent issue arises at the observatory—considering problems can occur at any time of day—those two hours must be factored into the response time. If physical intervention is needed and no staff are on-site, the response time could exceed three hours, factoring in the time required for someone to prepare and travel to the location. For any hardware, this delay could be catastrophic.

Some observatories operate on a shift-based schedule, ensuring someone is always closer to the site, which helps minimize accessibility issues. However, vendors do not maintain the same level of presence near these remote locations as in major cities. As a result, their ability to provide timely support remains constrained by the same logistical challenges of reaching the site.

Therefore, when designing the computing infrastructure of the observatory, the following key conditions had to be considered:

- Harsh environmental conditions. As a direct consequence, hardware failures are inevitable, making it essential for the observatory to be well-prepared for such incidents.

- Unreliable power grid. Power outages are almost unavoidable without a dedicated power station near the observatory.

- Limited accessibility in urgent situations. The time required for an engineer to reach the site after an alert is triggered must be considered.

At Rubin Observatory, this response time is at least three hours, which can be critical for hardware failures. While some observatories mitigate this challenge by implementing shift-based staffing, vendor support remains constrained by the same logistical barriers. As a result, shipping and delivery of replacement parts can take several days.

- Human factor. The difficulty in accessing the remote site, low oxygen levels, and the pressure to resolve issues quickly can affect the performance of the staff and increase the risk of errors. Therefore, solutions should be as simple as possible, requiring minimal effort and on the spot decision-making from the staff.

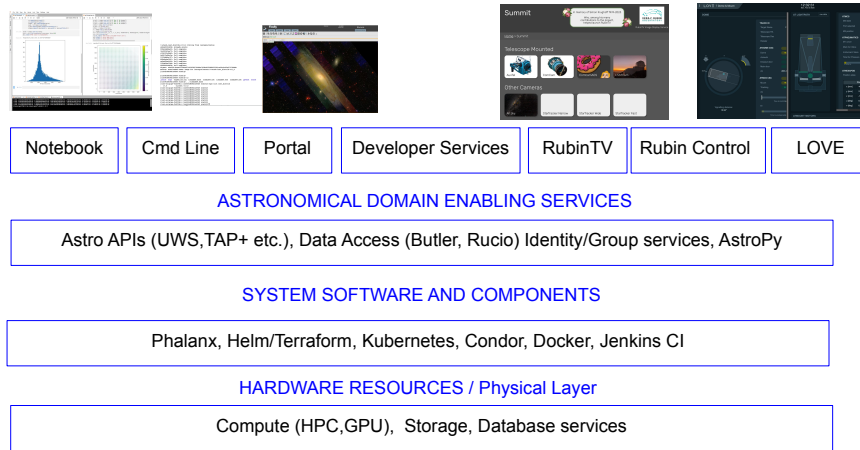All these factors were considered in the design of Rubin Observatory's computing infrastructure.

| Notebook | Cmd Line | Portal | Developer Services | RubinTV | Rubin Control | LOVE |

ASTRONOMICAL DOMAIN ENABLING SERVICES

Astro APIs (UWS,TAP+ etc.), Data Access (Butler, Rucio) Identity/Group services, AstroPy

SYSTEM SOFTWARE AND COMPONENTS

Phalanx, Helm/Terraform, Kubernetes, Condor, Docker, Jenkins CI

HARDWARE RESOURCES / Physical Layer

Compute (HPC,GPU), Storage, Database services

Figure 1: Rubin Cyber infrastructure layers

3. Physical Layer

3.1. Design
Scalability, Open design

3.2. Legos
Blocks

4. Networking Layer

4.1. Reliability
4.2. Scalability

5. Computing Layer

5.1. Automatizing
IaC, GitOps, CI/CD

5.2. Monitoring
Health, Logs, Dashboards, Alerts

6. Application Layer

6.1. Deployments

Test Stands, Canary, Blue/Green

6.2. Security

Detections, Identities, Monitoring

7. Incidents Management

Alerts, Escalation,

8. Documentation

Technotes, Runbooks

Acknowledgments

References

[1] Ž. Ivezić, S. M. Kahn, J. A. Tyson, B. Abel, E. Acosta, R. Allsman, D. Alonso, Y. AlSayyad, S. F. Anderson, J. Andrew, J. R. P. Angel, G. Z. Angeli, R. Ansari, P. Antilogus, C. Araujo, R. Armstrong, K. T. Arndt, P. Astier, É. Aubourg, N. Auza, T. S. Axelrod, D. J. Bard, J. D. Barr, A. Barrau, J. G. Bartlett, A. E. Bauer, B. J. Bauman, S. Baumont, E. Bechtol, K. Bechtol, A. C. Becker, J. Becla, C. Beldica, S. Bellavia, F. B. Bianco, R. Biswas, G. Blanc, J. Blazek, R. D. Blandford, J. S. Bloom, J. Bogart, T. W. Bond, M. T. Booth, A. W. Borgland, K. Borne, J. F. Bosch, D. Boutigny, C. A. Brackett, A. Bradshaw, W. N. Brandt, M. E. Brown, J. S. Bullock, P. Burchat, D. L. Burke, G. Cagnoli, D. Calabrese, S. Callahan, A. L. Callen, J. L. Carlin, E. L. Carlson,

S. Chandrasekharan, G. Charles-Emerson, S. Chesley, E. C. Cheu, H.-F. Chiang, J. Chiang, C. Chirino, D. Chow, D. R. Ciardi, C. F. Claver, J. Cohen-Tanugi, J. J. Cockrum, R. Coles, A. J. Connolly, K. H. Cook, A. Cooray, K. R. Covey, C. Cribbs, W. Cui, R. Cutri, P. N. Daly, S. F. Daniel, F. Daruich, G. Daubard, G. Daues, W. Dawson, F. Delgado, A. Dellapenna, R. de Peyster, M. de Val-Borro, S. W. Digel, P. Doherty, R. Dubois, G. P. Dubois-Felsmann, J. Durech, F. Economou, T. Eifler, M. Eracleous, B. L. Emmons, A. Fausti Neto, H. Ferguson, E. Figueroa, M. Fisher-Levine, W. Focke, M. D. Foss, J. Frank, M. D. Freemon, E. Gangler, E. Gawiser, J. C. Geary, P. Gee, M. Geha, C. J. B. Gessner, R. R. Gibson, D. K. Gilmore, T. Glanzman, W. Glick, T. Goldina, D. A. Goldstein, I. Goodenow, M. L. Graham, W. J. Gressler, P. Gris, L. P. Guy, A. Guyonnet, G. Haller, R. Harris, P. A. Hascall, J. Haupt, F. Hernandez, S. Herrmann, E. Hileman, J. Hoblitt, J. A. Hodgson, C. Hogan, J. D. Howard, D. Huang, M. E. Huffer, P. Ingraham, W. R. Innes, S. H. Jacoby, B. Jain, F. Jammes, M. J. Jee, T. Jenness, G. Jernigan, D. Jevremović, K. Johns, A. S. Johnson, M. W. G. Johnson, R. L. Jones, C. Juramy-Gilles, M. Jurić, J. S. Kalirai, N. J. Kallivayalil, B. Kalmbach, J. P. Kantor, P. Karst, M. M. Kasliwal, H. Kelly, R. Kessler, V. Kinnison, D. Kirkby, L. Knox, I. V. Kotov, V. L. Krabbendam, K. S. Krughoff, P. Kubánek, J. Kuczewski, S. Kulkarni, J. Ku, N. R. Kurita, C. S. Lage, R. Lambert, T. Lange, J. B. Langton, L. Le Guillou, D. Levine, M. Liang, K.-T. Lim, C. J. Lintott, K. E. Long, M. Lopez, P. J. Lotz, R. H. Lupton, N. B. Lust, L. A. MacArthur, A. Mahabal, R. Mandelbaum, T. W. Markiewicz, D. S. Marsh, P. J. Marshall, S. Marshall, M. May, R. McKercher, M. McQueen, J. Meyers, M. Migliore, M. Miller, D. J. Mills, C. Miraval, J. Moeyens, F. E. Moolekamp, D. G. Monet, M. Moniez, S. Monkewitz, C. Montgomery, C. B. Morrison, F. Mueller, G. P. Muller, F. Muñoz Arancibia, D. R. Neill, S. P. Newbry, J.-Y. Nief, A. Nomerotski, M. Nordby, P. O'Connor, J. Oliver, S. S. Olivier, K. Olsen, W. O'Mullane, S. Ortiz, S. Osier, R. E. Owen, R. Pain, P. E. Palecek, J. K. Parejko, J. B. Parsons, N. M. Pease, J. M. Peterson, J. R. Peterson, D. L. Petravick, M. E. Libby Petrick, C. E. Petry, F. Pierfederici, S. Pietrowicz, R. Pike, P. A. Pinto, R. Plante, S. Plate, J. P. Plutchak, P. A. Price, M. Prouza, V. Radeka, J. Rajagopal, A. P. Rasmussen, N. Regnault, K. A. Reil, D. J. Reiss, M. A. Reuter, S. T. Ridgway, V. J. Riot, S. Ritz, S. Robinson, W. Roby, A. Roodman, W. Rosing, C. Roucelle, M. R. Rumore, S. Russo, A. Saha, B. Sassolas, T. L. Schalk, P. Schellart, R. H.

Schindler, S. Schmidt, D. P. Schneider, M. D. Schneider, W. Schoening, G. Schumacher, M. E. Schwamb, J. Sebag, B. Selvy, G. H. Sembroski, L. G. Seppala, A. Serio, E. Serrano, R. A. Shaw, I. Shipsey, J. Sick, N. Silvestri, C. T. Slater, J. A. Smith, R. C. Smith, S. Sobhani, C. Soldahl, L. Storrie-Lombardi, E. Stover, M. A. Strauss, R. A. Street, C. W. Stubbs, I. S. Sullivan, D. Sweeney, J. D. Swinbank, A. Szalay, P. Takacs, S. A. Tether, J. J. Thaler, J. G. Thayer, S. Thomas, A. J. Thornton, V. Thukral, J. Tice, D. E. Trilling, M. Turri, R. Van Berg, D. Vanden Berk, K. Vetter, F. Virieux, T. Vucina, W. Wahl, L. Walkowicz, B. Walsh, C. W. Walter, D. L. Wang, S.-Y. Wang, M. Warner, O. Wiecha, B. Willman, S. E. Winters, D. Wittman, S. C. Wolff, W. M. Wood-Vasey, X. Wu, B. Xin, P. Yoachim, H. Zhan, LSST: From Science Drivers to Reference Design and Anticipated Data Products, ApJ873 (2) (2019) 111. `arXiv:0805.2366`, `doi:10.3847/1538-4357/ab042c`.

[2] R. Ross, V. Pillitteri, Special publication 800-171, protecting controlled unclassified information in nonfederal systems and organizations (May 2024).
URL `https://doi.org/10.6028/NIST.SP.800-171r3`

[3] W. O'Mullane, N. Gaffney, F. Economou, A. M. Smith, J. R. Thomson, T. Jenness, The demise of the filesystem and multi level service architecture, arXiv e-prints (2019) arXiv:1907.13060`arXiv:1907.13060`, `doi:10.48550/arXiv.1907.13060`.