Vera C. Rubin Observatory
Rubin Observatory Project Office

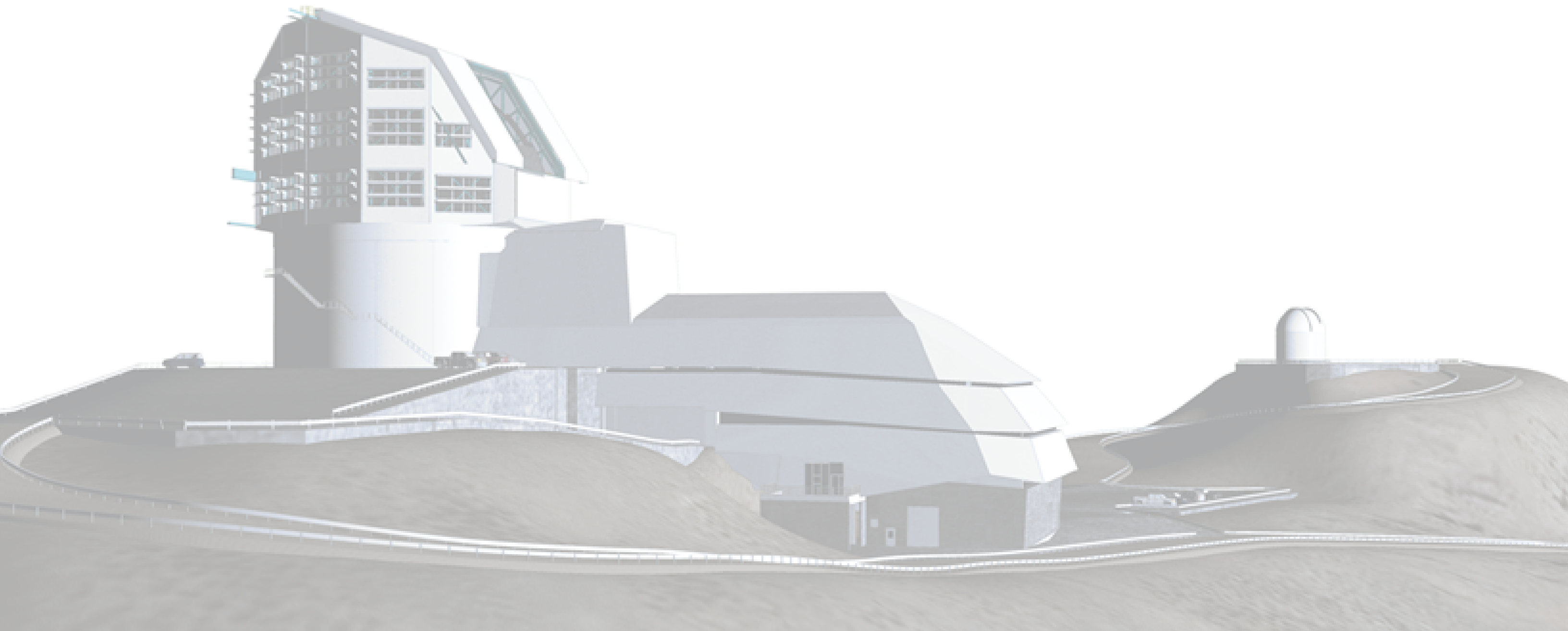
Disaster Recovery - Network

Cristian Silva

ITTN-056

Latest Revision: 2023-11-28

DRAFT



Abstract

Details of network devices Disaster Recovery plan

Change Record

Version	Date	Description	Owner name
1	2023-03-02	Unreleased.	Cristian Silva
1	2023-11-20	Early draft	Cristian Silva

Document source location: `https://github.com/lsst-it/ittn-056`

Contents

Disaster Recovery - Network

1 Introduction

This Technical Disaster Recovery Document is crafted as a response against events that may cause disruptions of our operations. We aim not only to mitigate the impact of potential crises but to ensure the rapid restoration of critical technical systems.

2 Risk Assessment

Identify potential risks and threats to the organization's IT infrastructure. Categorize risks based on severity and likelihood.

3 Backup and Recovery Procedures

The following outlines the backup schedules for critical data and systems, and the data restoration strategy

3.1 Backup Procedure

The network backup is scheduled to run twice daily on both summit and base devices. The backup encompasses Switches, routers, and Firewalls. It's specifically designed to exclude any sensitive information like keys or passwords. Once completed, the backup is pushed to a private repository.

3.2 Restore Procedures

In the event of device failure or replacement, the restoration process offers three options:

3.2.1 Manual Restoration

Access the repository to retrieve the last backup of the device. Manually reconfigure the new device based on the retrieved backup. Suitable for situations requiring a manual review and setup of a new device.

3.2.2 Zero-Touch Provisioning (In Progress)

Utilize a preliminary configuration on new devices. Upon startup, the device automatically updates its software and retrieves the latest backup from the repository. Simplifies and automates the restoration process for newly deployed devices.

3.2.3 Infrastructure as Code (In Progress)

Leveraging the repository network, a sequence of tasks is designed to reconstruct and upgrade device configurations. Embraces an infrastructure-as-code approach, allowing for streamlined rebuilding and upgrading of devices.

4 Emergency Response Team

Designate roles and responsibilities for the Emergency Response Team. Establish communication channels and protocols during a crisis.

4.1 Incident Commander (IC)

- Assumed control, coordinating with technical experts and relevant stakeholders.
- Prioritized resolution tasks to restore network functionality swiftly.

IC should usually be the Devops Manager, in his absence a Network team member can take the role.

4.2 Communications

- Facilitated the rapid deployment of technical resources and tools.
- Established a centralized communication hub for real-time updates.

Communications will be taken care by Devops Manager, in his absence another team member, not performing technical tasks can take the role.

4.3 Technical Support and Analysis

- Diagnosed the root cause of the incident and devised an action plan.
- Collaborated with vendors and internal teams to implement corrective measures.

5 Infrastructure Resilience

Implement measures to enhance infrastructure resilience. Ensure redundancy in critical systems and data storage.

6 Testing and Training

Conduct regular disaster recovery drills to assess the efficiency of procedures. Provide ongoing training for the response team.

7 Detection

Identify the occurrence of a disaster or disruption. Validate the severity and impact on IT systems.

8 Declaration

Upon detection of an incident a declaration will be done announcing it in the Summit channel selected for announcements. The declaration will be done by the IC.

The declaration will contain the following information

- Incident description
- Incident commander in charge
- Confirmation of slack channel to follow up the incident.
- Estimated resolution time (if possible)

9 Response

Response will be adecuated depending of the type of incident.

The following are responses thay could be executed:

- Local or total network isolation
- Servers shutdown
- Blocking of credentials
- Disable services
- Full restore of a system
- Partial restore of a system

10 Communication

Communications with stakeholders will be done in the usual Slack channel to request support from Chile. The communication lead will not provide updates on any other channel and will not be answering direct messages.

In the situation of a larger incident, emails will be sent to all stakeholders.

A References

B Acronyms

Acronym	Description
IT	Information Technology
ITTN	IT Technote
PMO	Project Management Office