Building a Disaster Recovery Plan

David Clinton

LINUX SYSTEM ADMINISTRATOR

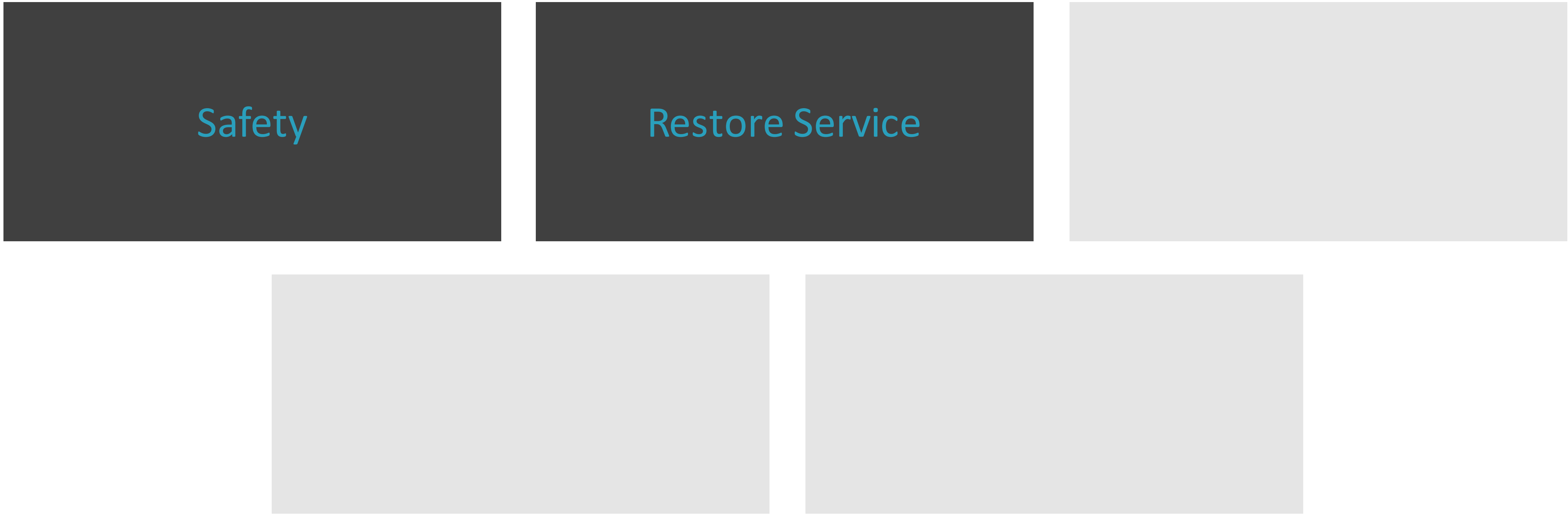
bootstrap-it.com/troubleshooting | @davidbclinton | linkedin.com/in/dbclinton

Business Continuity Plan (BCP)

Business Continuity Plan (BCP)

Safety

Business Continuity Plan (BCP)



Safety

Restore Service

Business Continuity Plan (BCP)

Safety

Restore Service

Restore All Operations

Business Continuity Plan (BCP)

Safety

Restore Service

Restore All Operations

Incident Management Protocol

Business Continuity Plan (BCP)

Safety

Restore Service

Restore All Operations

Incident Management Protocol

Disaster Recovery Plan

Disaster Recovery Plan

Disaster Recovery Plan

Minimize Damage

Disaster Recovery Plan

Minimize Damage

Restore Functionality

Incident Management Plan

Incident Management Plan

Minimize Damage

Incident Management Plan

Minimize Damage

Remove Threat

Developing an Incident Management Protocol

Incident Management Protocol

Incident Management Protocol

Alert: something's not right

Incident Management Protocol

Alert: something's not right

Initiate ticket or SIEM event

Incident Management Protocol

Alert: something's not right

Initiate ticket or SIEM event

Coordinate with all relevant parties

Incident Management Protocol

Alert: something's not right

Initiate ticket or SIEM event

Coordinate with all relevant parties

Close and review

Monitoring Solutions for Linux

collectd

Remote browser-based data collection

Nagios

Heavily customizable

Munin

Forensics analysis

Nmon

SSH-based visualizations

Graphs

Charts

Alerts

Monitoring Solutions

Developing a Disaster Recovery Plan

Disaster Recovery

Disaster Recovery

What Is Recovery?

Disaster Recovery

What Is Recovery?

What Will Your Recovery Require?

Disaster Recovery

What Is Recovery?

What Will Your Recovery Require?

How Will You Communicate Your Plan?

Disaster Recovery

What Is Recovery?

Disaster Recovery

What Is Recovery?

Recovery Time Objective:

Disaster Recovery

What Is Recovery?

Recovery Time Objective:

How long can you survive without IT service?

Disaster Recovery

What Is Recovery?

Recovery Time Objective:

How long can you survive without IT service?

Recovery Point Objective:

Disaster Recovery

What Is Recovery?

Recovery Time Objective:

How long can you survive without IT service?

Recovery Point Objective:

How much data can you afford to lose?

Disaster Recovery

What Will Your Recovery Require?

Disaster Recovery

Plan your backups

What Will Your Recovery Require?

Disaster Recovery

Plan your backups

Plan for failures - lots of 'em

What Will Your Recovery Require?

Disaster Recovery

Plan your backups

Plan for failures - lots of 'em

What Will Your Recovery Require?

Public cloud recovery plans:

Disaster Recovery

Plan your backups

Plan for failures - lots of 'em

What Will Your Recovery Require?

Public cloud recovery plans:

Data backups

Disaster Recovery

Plan your backups

Plan for failures - lots of 'em

What Will Your Recovery Require?

Public cloud recovery plans:

Data backups
Resource replacement templates

Disaster Recovery

Plan your backups

Plan for failures - lots of 'em

What Will Your Recovery Require?

Public cloud recovery plans:

Data backups
Resource replacement templates
Standby infrastructure

Disaster Recovery

How Will You Communicate Your Plan?

Disaster Recovery

Print and distribute:

How Will You Communicate Your Plan?

Disaster Recovery

Print and distribute:

Threats

How Will You Communicate Your Plan?

Disaster Recovery

Print and distribute:

Threats

Current system state

How Will You Communicate Your Plan?

Disaster Recovery

Print and distribute:

Threats

Current system state

Backup specs

How Will You Communicate Your Plan?

Disaster Recovery

Print and distribute:

Threats

Current system state

Backup specs

Team roster

How Will You Communicate Your Plan?

Disaster Recovery

Print and distribute:

Threats

Current system state

Backup specs

Team roster

Recovery tasks

How Will You Communicate Your Plan?

Summary

Summary

Business continuity plans

Summary

Business continuity plans

Incident management protocols

Summary

Business continuity plans

Incident management protocols

Disaster recovery plans