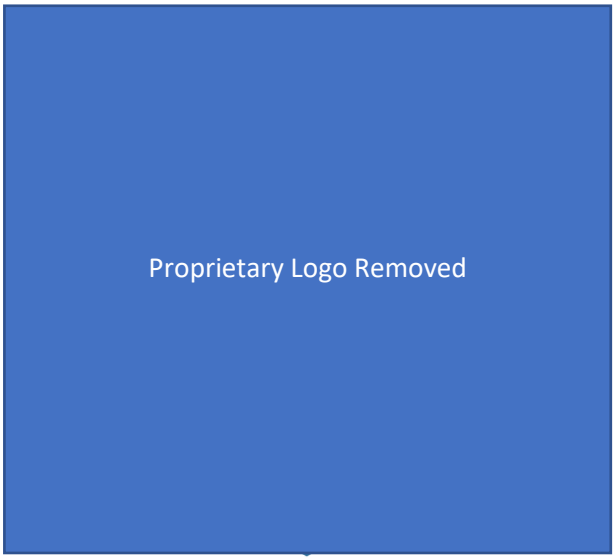
Solutions Architecture

Prepared for Proprietary, LLC

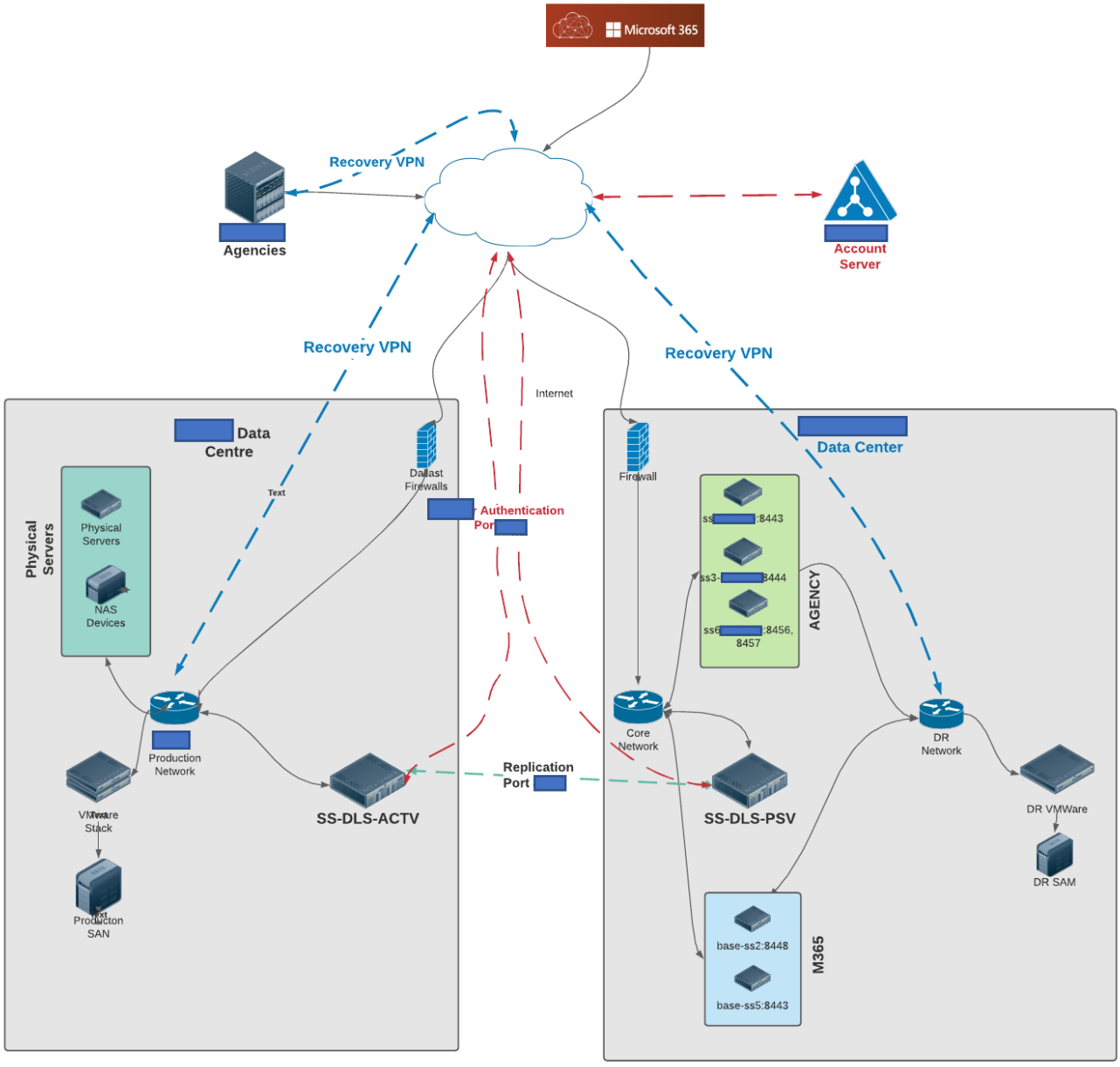


Contents

Contents 1
Solutions Overview 2
Solutions Architecture 4
Application Architecture 6
Appendix A 8

Solutions Overview

The solution is used to deploy a backup server in a Proprietary Data Center to protect all servers within the infrastructure. Backups flow from Agents on individual systems to the backup server. The data is then replicated to the backup server, which is hosted in the Proprietary Cloud DR (*disaster recovery cloud*).



Goals

- Protect all physical and virtual Proprietary servers so that applications and data can be fully recovered and restored.
- Allow for scheduled backups to reduce strain on resources and the physical server infrastructure.

Transition Expectations

Proprietary uses Veeam as the existing backup system. Veeam backups connect directly to the SAN (*storage area network*) that stores all VMDK (*Virtual Machine Disk*) files.

The following process is used for the transition:

1. Proprietary Agents are installed on all physical and virtual servers.
2. Server backups commence, starting with the first full backup (*seed*).
3. Nightly backup process completes consistently and successfully over three consecutive nights.
4. Veeam is disabled.

***Notes**:*
Current Veeam backups are not performed at the Hypervisor or guest level, so conflicts are not expected.
For optimal resource utilization, it is best to avoid existing and new backups from overlapping.
To effectively protect systems and data, technical assistance and adequate system resources are required.

Solutions Architecture

This section provides technical specifications and requirements details.

Hardware and Software Specifications

Manufacturer	Model	RAM	Storage
Dell	PowerEdge R740xd	64 GB	~80 TB
Proprietary	Backup Software		

Solutions Architecture Requirements

- **Data Center infrastructure, to be provided by Proprietary.**
  This includes rack-space, power, LAN (L*ocal Area Network)* and WAN (*Wide Area Network*), and smart-hands for the Proprietary Storage Server.
- **Proprietary Storage Server, to be provided by Proprietary.**
  The Proprietary Storage Server is located onsite at the City Data Center.
- **Proprietary Mirror Server, to be provided by Proprietary.**
  The Proprietary Mirror Server is hosted in the Proprietary Cloud DR.

Solutions Architecture Assumptions

- A dedicated virtual LAN will be provided for the Proprietary Storage Server. Only specific ports will be opened for use. Will be supplied during implementation phase.
- Proprietary Storage Server will not be joined to any Proprietary domain. This protects against infiltration by compromised domain credentials.
- Proprietary Storage Server will use Proprietary remote management and monitoring tools, as specified by Proprietary.

Availability and Reliability

The architecture is deployed as an active-passive replica peer, making backups available even in the event of unavailability of one node. Servers are built for redundancy and have dual power supplies and RAID 6 volumes for data storage. Data is immediately replicated offsite.

Business Continuity and Disaster Recovery

This solution enables you to replicate servers, including all data and history, into a backup copy that is stored offsite. Recoveries of all types can be initiated in the Proprietary Cloud DR. If the onsite storage server becomes compromised, the base setup of the server can be recovered, and replication can be reversed to populate the onsite storage server to its uncompromised state.

Capacity

The initial capacity of the server is 80 TB. This is sufficient to protect approximately 70 TB of native Proprietary data for one year of retention. Additional storage capabilities can be enacted as needed.

The initial memory capacity of the server is 64 GB RAM. The capacity adheres to Proprietary guidance of 8 GB RAM and 1 GB per million files of the largest server.

Additional memory can be added as needed.

Security Architecture

The onsite backup server exists behind Proprietary's firewall and is within the scope of Proprietary's security framework. Refer to Proprietary for security standards.

Proprietary Storage Server uses only local system security credentials and will not be a part of any Proprietary Active Directory domain.

System Management, Monitoring and Administration

Proprietary uses the following technologies:

- **Monitoring**: Zabbix
- **Remote Assist Access:** Zoho
- **SEIM** (*Security Information and Event Management*) **capabilities**: Bitlyft

<Removed***: Graphic of Proprietary Storage Server overview>***

Application Architecture

This section identifies, describes, and defines the major solution components and their relationships. Components defined and specified by the models may include both custom and COTS *(Commercial off the Shelf)* components integrated into the solution architecture. The application also identifies existing common services used by the solution.

System Architecture

System Architecture is an enterprise architecture solution for visualizing, analyzing, and communicating enterprise architecture and business process analysis. This solution provides decision support, process optimization, and integration into solution delivery. System Architecture addresses all aspects of an organization's enterprise architecture, including modeling, publishing, analysis, and execution.

<Removed: ***System Architecture Scenario Graphic***>

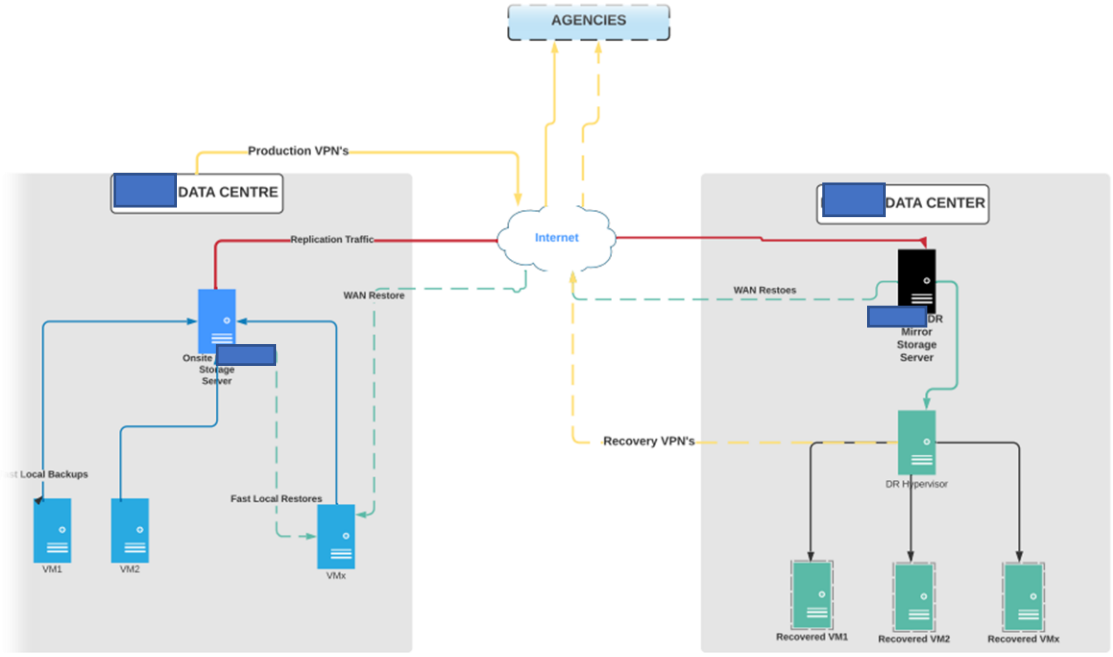
Application Layer

Proprietary backup software consists of:

- Agents installed on each physical or virtual server
- Proprietary storage server installed on Proprietary's onsite storage server and on the mirror server in the Proprietary Cloud DR. Proprietary Mirroring engine provides simple and reliable porting between hardware platforms.

Models and Diagrams

Component Relationship Diagrams



Per-Agent Resources

- **Memory:** 500 MB for Agent
- **CPU:** 4-70% of available CPU
- **Daily backup Size:** 1-2% of total data
- **Install Space:** 200 MB + 300 MB per 1 million files

Legend

- Backups
- Restores
- Replication
- VPN's

Appendix A

The table below provides definitions and explanations for terms and acronyms relevant to the content presented in this document.

Term	Definition
Cloud DR	Disaster Recovery Cloud
SAN	Storage Area Network
VMDK	Virtual Machine Disk
LAN	Local Area Network
WAN	Wide Area Network
RAID	Redundant Array of Individual Disks
SEIM	Security Information and Event Management

Table A.1: Key Terms