In architecting the **POSSE Cloud** environments, we recognized that systems may fail due to various factors, and clients must be able to continue working when this happens. To deal with this reality, POSSE Cloud environments are designed with data and system services redundancy. This is further supplemented by running client systems on highly available Kubernetes clusters where workloads are dynamically moved within the cluster without impacting live client activities. Further, each cluster is built with enough excess capacity (compute, memory, and storage) so that any host node can be down, and the remaining host nodes have sufficient reserve to continue operating without client impact.

Data Backup

Data stored as part of POSSE Cloud agreements belongs to the client, and its safekeeping is of the utmost importance to Computronix. As such, Computronix has architected a backup solution that meets industry best practices using Microsoft Azure.

The following is a summary of the data backup solution:

Database

The Oracle database is at the heart of the POSSE Cloud solution and contains all structured data and configuration metadata. Backing up the POSSE database secures all the information and metadata stored within it. All completed transactions on the database (inserting data, changing data, deleting data) are logged to the Oracle transaction log (Oracle Redo Log). Three independent copies of the logs are retained on separate disks to reduce the risk of data loss.

Azure Site Recovery (ASR) is configured to continuously replicate the Oracle services (including data) to the Azure Disaster Recovery (DR) site. The continuous nature of Computronix's ASR configuration ensures that the transactions are streamed to the DR site as they are written to the Oracle transaction log files. This ensures that data is available on the DR site within the **Recovery Point Objective (RPO)** of 4 hours.

Using ASR configuration Computronix has found that we are able to exceed the RPO and transactions are frequently available in DR within minutes of the completion of Oracle processing.

The health of the replication process is monitored and configured to alert if it becomes unhealthy. Remediation of unhealthy conditions is initiated promptly.

At least daily, Oracle Recovery Manager (RMAN), the industry-standard utility for backing up Oracle, autonomously creates a backup on **Geographically Redundant Storage (GRS)**. GRS provides replication between the primary data center and the DR data center and delivers reliability of 16 9s (99.99999999999999%) over a given year.

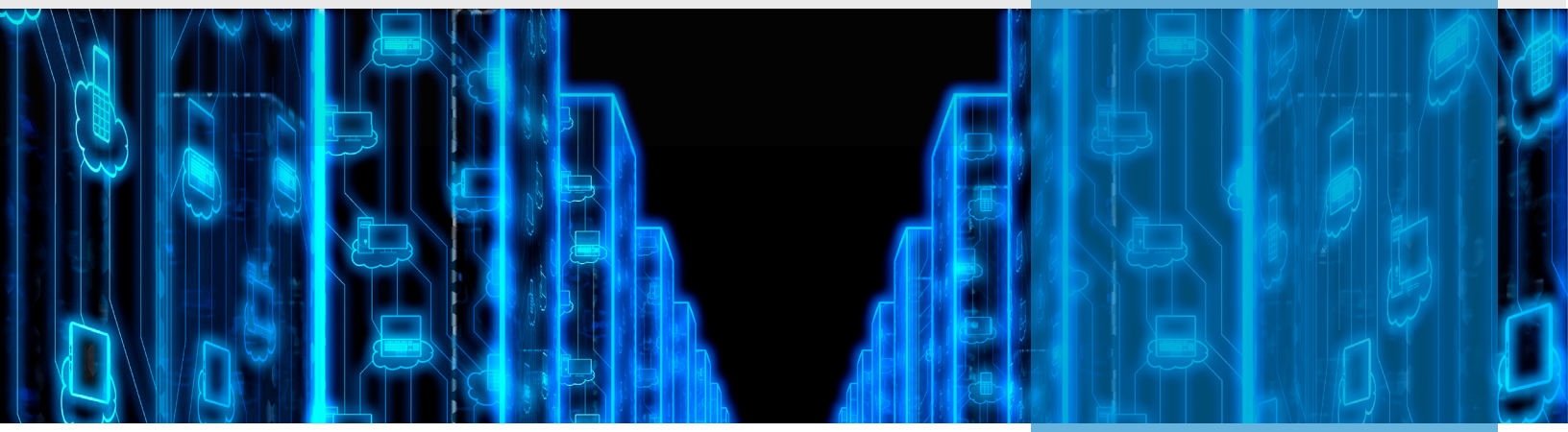
PADD

The **POSSE Alternate Document Datastore (PADD)** is a repository for documents. Similar to Oracle data storage, PADD uses GRS storage, to achieve 99.99999999999999% file reliability over a given year.

Security Compliance Audits

POSSE Cloud recognizes that there are many aspects to securely protecting our customers business. This includes Role Base Access, Privileged Access Management, remediating vulnerabilities, and many more.

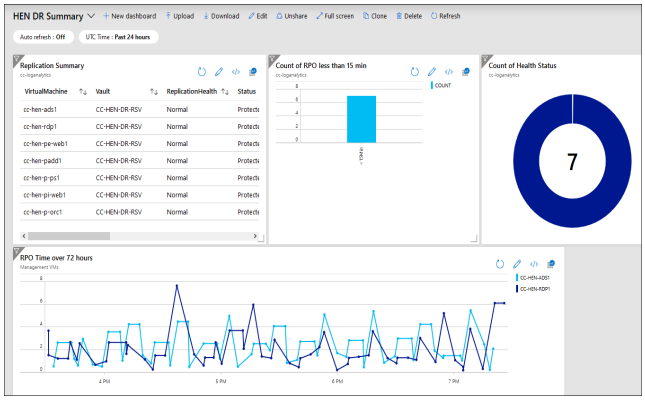
To address these and many other security concerns, POSSE Cloud is designed, implemented and maintained to be compliant with NIST 800-53 Moderate assessment using FedRAMP Moderate parameters. To ensure compliance with this standard and to be transparent with our customers, POSSE Cloud engages a FedRAMP certified auditor (3PAO) to complete an annual audit. The results of the audits are made available to our customers.



Disaster Recovery

All services within a Client environment are built using pipeline technology; whenever DR is tested or executed, all services are created by executing the environment build pipeline and attaching the replicated storage to the new environment. Ensuring continuity in client operations in the event of loss of the primary hosting site is not only a key provision within POSSE Cloud agreements, it is also a primary objective of the Hosting Team. To that end, each client is provided with a geographically distinct disaster recovery environment in a Microsoft Azure data center completely independent of the primary hosting site.

In the event of a catastrophic failure of the primary hosting site, Computronix would coordinate efforts with the client staff to reroute access and networking for the client's primary system interfaces to the disaster recovery environment. Computronix ensures that all security, compliance, and system performance requirements are maintained in the disaster recovery environment. This ensures client staff maintain continuity in conducting business functions following the recovery process. In compliance with NIST 800-53, Computronix performs annual testing of the DR process including testing of client data recovery and system functionality.



The Azure Portal Dashboard indicates current replication health and RPO (Recovery Point Objective) times.

Encryption

Data at rest and data in transit is encrypted using FIPS 140-2 algorithms. This ensures that sensitive data is not available to unauthorized entities. It also ensures that data has not been altered while in transit or at rest.

Modern Software. Timeless Values.
computronix.com

Join the growing number of Computronix customers who have chosen POSSE Cloud for hosting their POSSE solutions.

computronix.com

Computronix (U.S.A.) , Inc.
Denver, CO

Phone: 720.962.6300
Toll free: 866.962.6300

Computronix (Canada) Ltd.
Edmonton, AB

Phone: 780.454.3700
Toll free: 800.359.3758