


Database Redundancy Options

SER1001046

City of Mount Pleasant

1/22/2026

www.prime-controls.com
Prime Controls Corporate Office
Phone: 972.221.4849
1725 Lakepointe Drive | Lewisville, TX 75057

Revision History

Date	Approval	Description
01/22/2026	Kyle Dobson	Creation of Document
01/23/2026	Kyle Dobson	Updated and cleaned up document

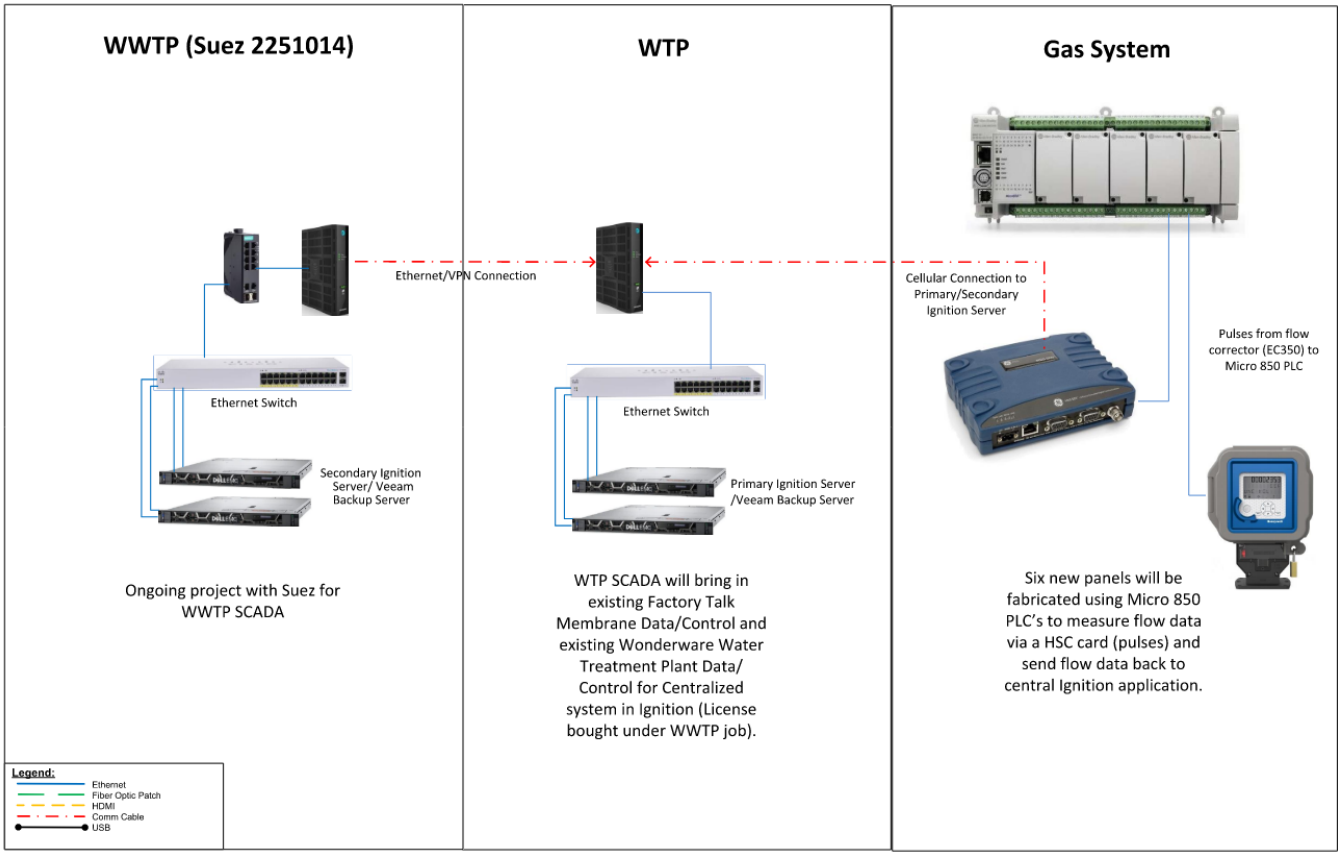
Overview

Provide a brief overview of the viable options for the City of Mount Pleasant to ensure minimal data loss. Existing hardware is currently one ESXi server running an Ignition VM and a MySQL VM along with a VEEAM backup server at Water Treatment Plant, known as Primary", and a another ESXi server running an Ignition VM and a MySQL VM along with a VEEAM backup server at Waste Water Treatment Plant, known as Secondary.

Ignition is currently set up with redundancy and will failover. MySQL is currently configured as a failover in Ignition, such that any time the Primary connection is dropped, Ignition will automatically write to the Secondary MySQL database.

The VEEAM servers are currently making a backups of their corresponding ESXi VMs daily at 10pm which can be restored in cases such as corruption.

GSA-055 Project Network Architecture



THIS PAGE IS INTENTIONALLY LEFT BLANK

Table of Contents

Revision History 2
Overview 3
Table of Contents 5
Option 1 – VEEAM Enhancements and Failovers 7
Option 2 – Option 1 with NAS 8
Option 3 – Offsite VEEAM for Spin-up 9
Option 4 – Database Clustering 10
Breakdown 11
Considerations 11
Known Issues 11

THIS PAGE IS INTENTIONALLY LEFT BLANK

Option 1 – VEEAM Enhancements and Failovers

Bottom Line: Lowest cost / fastest to implement

- **What's needed**
  - Use existing ESXi hosts at WTP and WWTP
  - Existing VEEAM servers configured for:
    - VM backups
    - VM replication between sites
    - Planned and unplanned failover
  - Network connectivity between sites with sufficient bandwidth and reliability
  - Runbooks for failover/failback procedures
- **How it works**
  - VEEAM continuously replicates VMs (Ignition + MySQL) between sites.
  - In a failure, replicas are powered on at the opposite site.
  - Failback is manual or semi-automated once the primary site is restored.
- **Pros**
  - **Lowest capital cost**
  - No new major hardware required
  - Works well for site-level disasters
  - Simple architecture, easy to understand and support
  - Minimal disruption to current environment
- **Cons**
  - **RPO is not zero** (data loss possible between replication intervals)
  - Failover is not instantaneous
  - Database consistency depends on snapshot timing
  - Not true "high availability" — more like *disaster recovery*
  - Manual intervention required during incidents
- **Additional hardware**
  - None (assuming current storage and networking are adequate)

Option 2 – Option 1 with NAS

Bottom Line: Improved data durability, still DR-focused

- **What's needed**
  - Redundant NAS at WTP
  - Redundant NAS at WWTP
    - RAID 6 / RAID 10
    - Dual controllers preferred
  - VEEAM configured to:
    - Back up local VMs to local NAS
    - Optionally copy backups between sites
  - Adequate inter-site bandwidth
- **How it works**
  - VMs are backed up to local NAS instead of (or in addition to) local disks.
  - Backups can be copied to the opposite site for extra protection.
  - Restores occur from NAS to ESXi.
- **Pros**
  - Significantly improved backup reliability
  - Faster restore times than off-host backups
  - Protects against local storage failure
  - Modular and scalable
  - Still relatively simple to manage
- **Cons**
  - Still not real-time replication
  - No automatic failover
  - NAS is not application-aware (database still restored from backups)
  - Additional hardware and maintenance cost
- **Additional hardware**
  - 2× Redundant NAS systems
  - Possible 10Gb networking (recommended)

Option 3 – Offsite VEEAM for Spin-up

Bottom Line: Best DR posture without full clustering

- **What's needed**
  - Third physical site (new location)
  - ESXi or physical server for VEEAM
  - Redundant NAS at:
    - WTP
    - WWTP
    - Third site
  - VEEAM Backup Copy Jobs configured for immutability (if supported)
  - Secure WAN/VPN connectivity between all sites
- **How it works**
  - Local backups at WTP and WWTP
  - Backup copies sent to the third site
  - Optional immutable storage for ransomware protection
  - Failover still occurs between WTP and WWTP; third site is recovery-only
- **Pros**
  - Strong protection against ransomware and site loss
  - Meets best-practice 3-2-1 backup rule
  - Data survives catastrophic multi-site events
  - Allows air-gapped or immutable backups
  - Excellent audit and compliance story
- **Cons**
  - Higher capital and operational cost
  - More complex to manage
  - Still DR-based, not high availability
  - Restore times from third site can be longer
- **Additional hardware**
  - 1× VEEAM server at third site
  - 3× Redundant NAS systems (if not already added)
  - WAN upgrades likely required

Option 4 – Database Clustering

Bottom Line: Zero-data-loss, zero-downtime goal – True High Availability

- **What's needed**
  - Redesign of database architecture with MySQL InnoDB Cluster
  - Witness/arbiter server (third site or cloud)
  - Low-latency, high-bandwidth links between sites
  - Synchronized time (NTP), reliable DNS
  - Possible redesign of Ignition architecture
  - Continued VEEAM backups for disaster recovery
- **How it works**
  - Databases replicate synchronously
  - Writes are committed to multiple nodes before success
  - Automatic failover with no data loss
  - Witness prevents split-brain scenarios
- **Pros**
  - Near-zero RPO and RTO
  - Automatic failover
  - True high availability
  - Minimal operator involvement during failures
  - Best option for mission-critical control data
- **Cons**
  - Most expensive
  - High complexity
  - Strict network requirements (latency sensitive)
  - Existing hardware/software may not be compatible
  - Requires expert setup and ongoing care
  - Not all Ignition/database features behave well in clustered DBs – Ignition rework required
- **Additional hardware**
  - Dedicated DB nodes (may not be current ESXi VMs)
  - Witness server (physical, virtual, or cloud)
  - Network upgrades (low latency is critical)
  - Potential licensing upgrades

*Note: there are other high availability options available i.e. Galera Cluster

Breakdown

Option	Cost	Complexity	RPO (Recovery Point Objective)	RTO (Recovery Time Objective)	Staff Intervention	Maintenance Overhead
1	$	Low	5-15 Minutes	15-60 Minutes	Yes	Low
2	$$	Low-Medium	5-15 Minutes	30-90 Minutes	Yes	Medium
3	$$$	Medium	5-15 Minutes	1-4 Hours	Yes	Medium-High
4	$$$$	High	~0	~0	No	High

Considerations

As these servers are in a production environment, scheduling staff support for taking servers offline for rework will be necessary.

For the most robust system, 10GB network connection is recommended in most applications to allow faster transfer of data between sites and reduce any downtime.

Known Issues

1. ~~ESXi is currently running the Primary SQL Server VM is a disjointed Datastore. Essentially a recovery was made to a new datastore which needs to be cleaned up. This will require the Primary SQL Server VM to be turned off and reconfigured to merge into the main datastore. Ignition will failover to the Secondary Ignition (redundany) gateway, and the data will be written to the Secondary MySQL Server. Once the VM is fixed, the data from Secondary will need to be merged back into the Primary database.~~ This has been fixed as of 1/23/2026.
2. ~~The Primary SQL Server VM is currently configured as thick provisioning. This essentially means the configured space (currently 1.5TB) is being taken up in full instead of growing. Backups, restores, and replicas are all affected by this as any transfer of data is the entire 1.5TB on a network.~~ This has been fixed as of 1/23/2026.
3. Network does now allow WTP or GAS devices to reach secondary gateway.
    a. 192.168.125.101 cannot reach 192.168.8.10, etc.
4. iDRAC does not have remote access. Network cable was installed, but there's no way to reach through VPN.