

The Last Line of Defense: Building a Resilient IBM i Architecture



Justin Loeber
Kisco Systems



Kaldip Sidhu
Rocket Software



Edward Moon
ProCern



Defense in Depth

Prevention

Hardening IBM i OS

- ✓ Current OS and PTFs
- ✓ User profile authorities
- ✓ Password level and policy
- ✓ Encrypted connections
- ✓ Object authorities
- ✓ NetServer authority lists
- ✓ Network hardening

Detection

Proactive Measures

- ✓ Security audit journal
- ✓ Exit point registrations
- ✓ Multifactor authentication
- ✓ Ransomware detection
- ✓ Monitoring & alerting

Recovery

Resilient architecture

- ✓ Immutable backups
- ✓ Disaster Recovery
- ✓ High Availability
- ✓ Monitoring
- ✓ Observability
- ✓ Testing

Example: Ransomware Defensive Layers

- Examine, **report on Security State**
- Email and SMS alerts
- SIEM integration and analysis

- Invest in tools that help you identify/Protect who is accessing your system from vulnerable points

- application-level security
- Manage power users an
- Monitoring and reduce the direct usage of power users
- **Monitor access of shared mapped access to data (IFS/FTP/Host Access)**
- **Minimize access points for data**
- **Automation and orchestration**
- Deny by default policy



- Regular **daily** verified **saves**
- Storing data in secure cloud facilities/offsite vaults(**Second LPAR**)
- **Utilization** of other monochrome, picture tools like flash Copy, Media backup.
- **iCluster Checkpoint functionality**
- Longer retention of IBMi data/audit logs

- Invest in tools that can react to security breaches
- Tools that enable replay data activates
- **Keep up to date with vendor patches** for your applications and host

- **Secure promotion of changes**
- Audit-driven reporting
- Process standardization
- Separation of Duties
- Policy enforcement through pre-configurations
- Audit-ready change management

Limit your download capabilities and add tighter access point controls to fight ransomware attacks



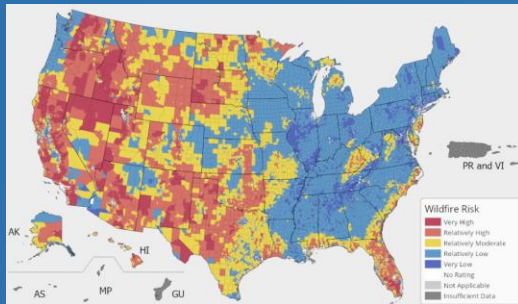
What is Resiliency?

A resilient IT architecture is one that can withstand and recover from failures, disruptions, and changing conditions while minimizing impact on users

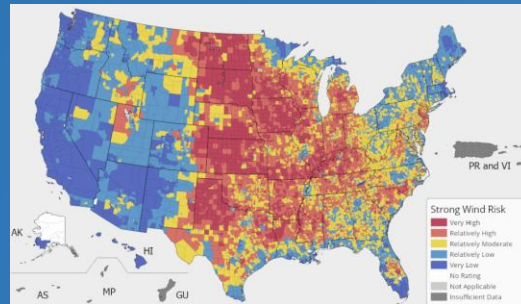
Resiliency Business Drivers

Business Continuity

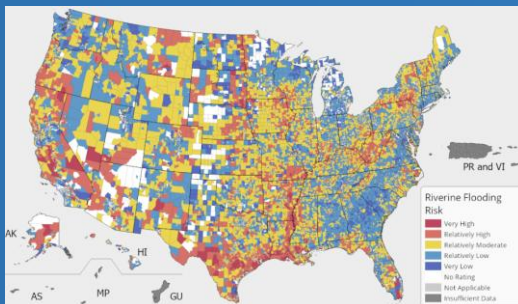
- Hardware failure
- OS issue
- High Uptime Req.
- Utility outage
- Natural disasters



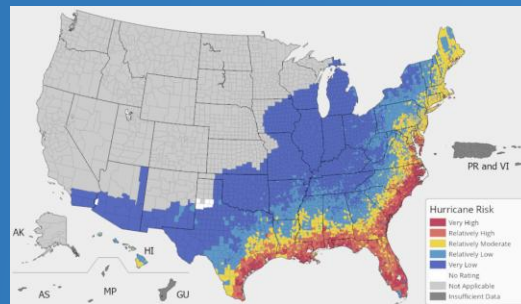
Wildfire



Strong Wind



Flooding



Hurricane

FEMA National Risk Index

<https://hazards.fema.gov/nri/natural-hazards>

Data Protection

- Cyber-incidents
- Loss of data
- Unauthorized changes

IT Compliance

Most compliance frameworks and regulations include resiliency requirements

- CMMC
- NIST
- ISO
- PCI
- DORA

Monitoring & Management

The ongoing monitoring and administration of IBM i systems to ensure performance, availability, security, and operational stability through proactive alerts, maintenance, and issue resolution.

Backups

IBM i backups protect business data by creating recoverable copies that allow systems and information to be restored after loss or damage, but they do not provide instant system availability.

High Availability

High Availability ensures business-critical workloads stay online by maintaining a synchronized standby system that can take over quickly when the primary system is unavailable.

Disaster Recovery

Disaster Recovery is a strategy for swiftly restoring IT systems and data after a disaster to minimize downtime and data loss, ensuring business continuity.

Testing

The process of validating system changes, applications, and configurations in a controlled environment to ensure they function correctly, perform as expected, and do not impact production operations.

Backups

IBM i backups protect business data by creating recoverable copies that allow systems and information to be restored after loss or damage, but they do not provide instant system availability.

Full - A complete copy of all selected data at a specific point in time.

Incremental - Copies only data that has changed since the last backup of any type.

Cumulative - Copies all data changed since the last full backup.

Online (Save While Active) - Minimizes downtime by performing backup online

Full System Flash Copy - IBM Tools for automating backups using array-based snapshots

Immutable Backups - Backups that cannot be removed without a specific set of conditions

Air Gap - Physically / Logically isolated copies of backups.

3-2-1 Rule - 3 Copies, 2 Media Types, 1 Offsite

High Availability

High Availability ensures business-critical workloads stay online by maintaining a synchronized standby system that can take over quickly when the primary system is unavailable.

HA Measurement

99.9%, 99.99%, etc. – Percentage of system uptime guaranteed over a given period.

IASP (Independent Auxiliary Storage Pool)

Disk storage that can be switched between systems for high availability.

Clustering

Multiple IBM i systems linked to operate together for resilience and failover.

SPOF (Single Point of Failure)

A component whose failure would cause system downtime.

Disaster Recovery

Disaster Recovery is a strategy for swiftly restoring IT systems and data after a disaster to minimize downtime and data loss, ensuring business continuity.

- Comprehensive Plan - Documented strategy defining backup scope, schedules, retention, and recovery procedures.
- Regular Backups - Scheduled data copies to ensure recoverability after failure or loss.
- Testing & Validation - Verifying backups can be successfully restored and function properly.
- Offsite Storage - Storing backup copies outside the primary location for disaster protection.
- Business Awareness - Aligning backup and recovery priorities with business impact and critical systems.
- Resource Allocation - Assigning sufficient storage, bandwidth, and personnel to support backups.
- Risk Assessment - Identifying threats and potential impact to data and systems.
- Compliance & Regulations - Meeting legal, security, and industry requirements for data protection and retention.

DRaaS

DR As A Service. Cloud based service model that provides organizations with a comprehensive disaster recovery solution.

Backups v DR

"Backups are insurance for your data; Disaster Recovery is insurance for your Business's Continuity"

"High Availability is continuous operations to prevent downtime; Disaster Recovery is preparedness for unpredictable, large-scale events"

HA v DR

Disaster Recovery

Business Continuity Plan (BCP)

A blueprint for an organization to respond to disruptions, ensuring vital operations, minimizing downtime, and enabling efficient recovery.

Recovery Point Objective (RPO)

The maximum acceptable data loss a business can tolerate in a disaster.

Failover

An automatic or emergency transfer of IBM i workloads to a standby system when the primary system fails or becomes unavailable.

Single Point of Failure (SPOF)

A critical element whose failure can disrupt an entire system due to lack of redundancy.

Hot, Warm, Cold DR

Hot: Quick recovery with pre-provisioned resources. Warm: Reserved environment with available data. Cold: Delayed data availability without a defined restoration location.

Recovery Time Objective (RTO)

The maximum allowable downtime for systems and operations to be restored after a disaster

Capacity

Resources & infrastructure needed to support the recovery of IT systems and data in the event of a disaster

Switchover

A planned, controlled transfer of IBM i workloads from the primary system to a secondary system for maintenance, testing, or upgrades.

Disaster Recovery

DR Cloud Vendor Checklist

✓ Technical Capabilities

- Data Center Locations
- Data Backup & Retention
- Scalability & Compatibility
- Data Transfer & Bandwidth
- Redundancy & High Availability
- Compliance: SOC, PCI, HIPAA, ISO 27001, etc.

✓ Cost & Pricing

- Cost Structure
- Data Transfer Costs
- Variable Costs

✓ Disaster Recovery Specifics

- Failover & Failback Processes
- Testing and Reporting
- Disaster Recovery Plan Documentation

✓ Operational Considerations

- Experience with the IBM i platform. Offers more than IaaS
- Service Level Agreements (SLAs)
- Security & Compliance
- Support Service... 24/7 Monitoring & Management
- Redundancy & High Availability
- Disaster Recovery Testing
- Business Continuity Plan (BCP) Consulting

Monitoring

The continuous observation of system performance, availability, jobs, and resources to detect issues early, ensure stability, and maintain reliable operations.

Staffed NOC

Human Engagement - 24/7 team monitoring systems and responding to issues.

AI Ops

AI-driven analysis to automate detection and incident response.

Alert Thresholds

Set limits that trigger alerts when exceeded.

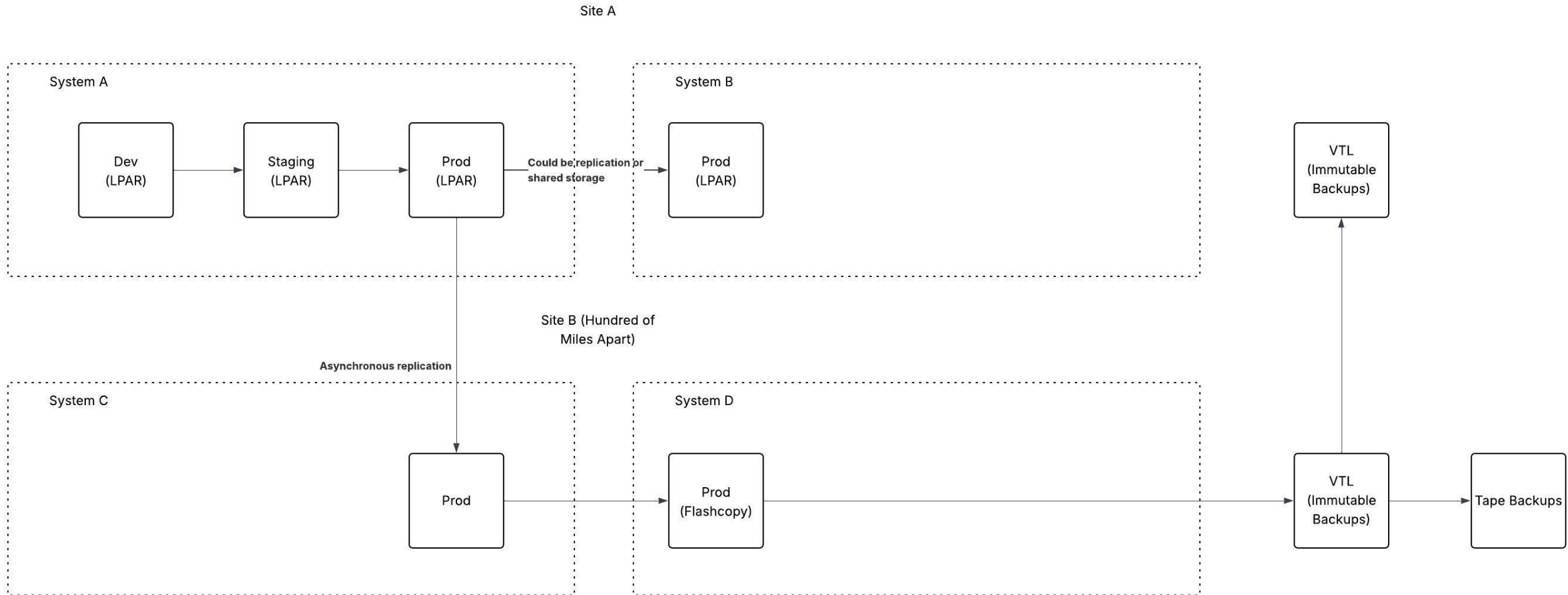
Performance Anomaly Detection (Observability)

Automatic detection of abnormal system behavior.

IBM i monitoring data sources

Security Audit Journal, Message Queues, Performance Monitors, Network (exit points)

Typical High Resilience Deployment



Testing

The process of validating system changes, applications, and configurations in a controlled environment to ensure they function correctly, perform as expected, and do not impact production operations.

Parallel Testing / Isolation Testing

Validating DR systems without impacting production users, virtual role swap, Bubble testing

Full Interruption Failover

Stopping production to fully test DR takeover.

Testing Cadence

Quarterly? Semi-annually?

Use Cases Reviewed



Complete loss of system (catastrophic hardware failure, loss of site)



Cyber Incident



Transient event/temporary outage (weather, network provider outage?)



Planned Outage

Backups are paramount in every case

Virtual Tape Library (VTL) solutions play important roles in a layered defense strategy.

Immutable Backups (WORM)

- Many VTLs support Write-Once-Read-Many (WORM) functionality, making backup data immutable
- VTL can provide encryption in transit and at rest
- Ransomware cannot alter or delete these backups

Air-Gapped Backups

- VTLs can replicate data to offline or cloud storage, creating a "virtual air gap" that ransomware cannot reach.

Fast Recovery

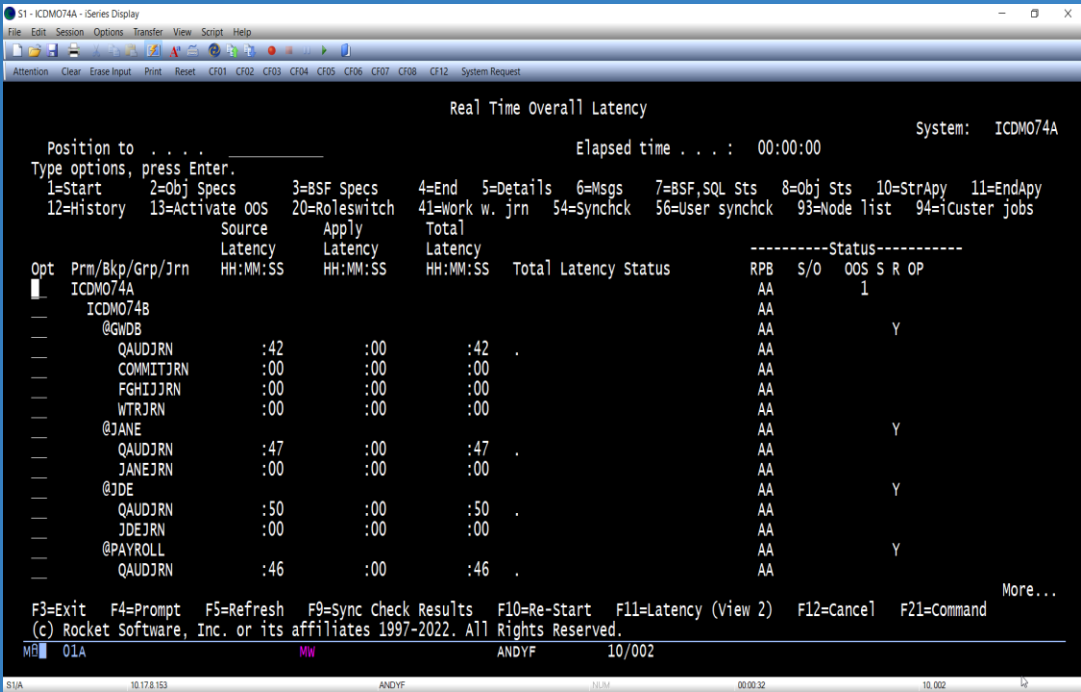
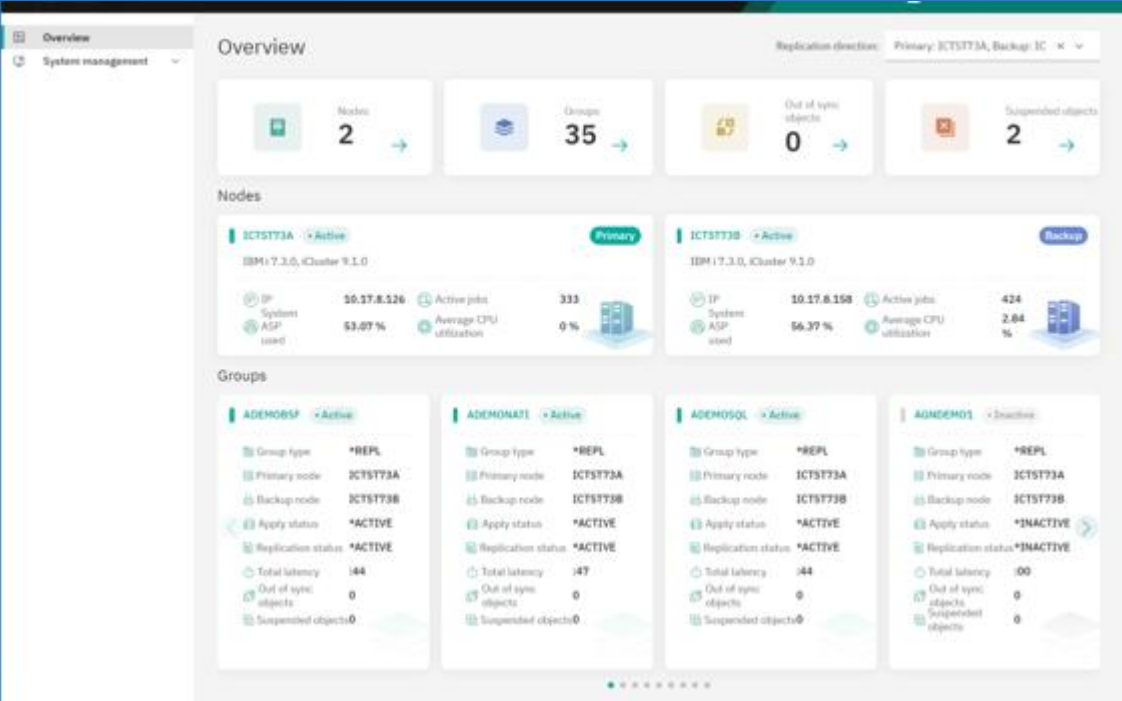
- In case of an attack, VTLs allow rapid restoration compared to physical tapes, minimizing downtime.

Role-Based Access Control

- VTL appliances often enforce strict access policies, reducing the risk of unauthorized changes.

Recovering From An Unplanned Complete System Loss

With HA in place a failover is performed when system loss detected. There may be some data loss based on the current latency.



Without HA system recovery will be restoration of last full system save along with the most recent cumulative or incremental saves.

Determining A Recovery Path

Figure 3: Recovery Paths for Failed State (Part 1)

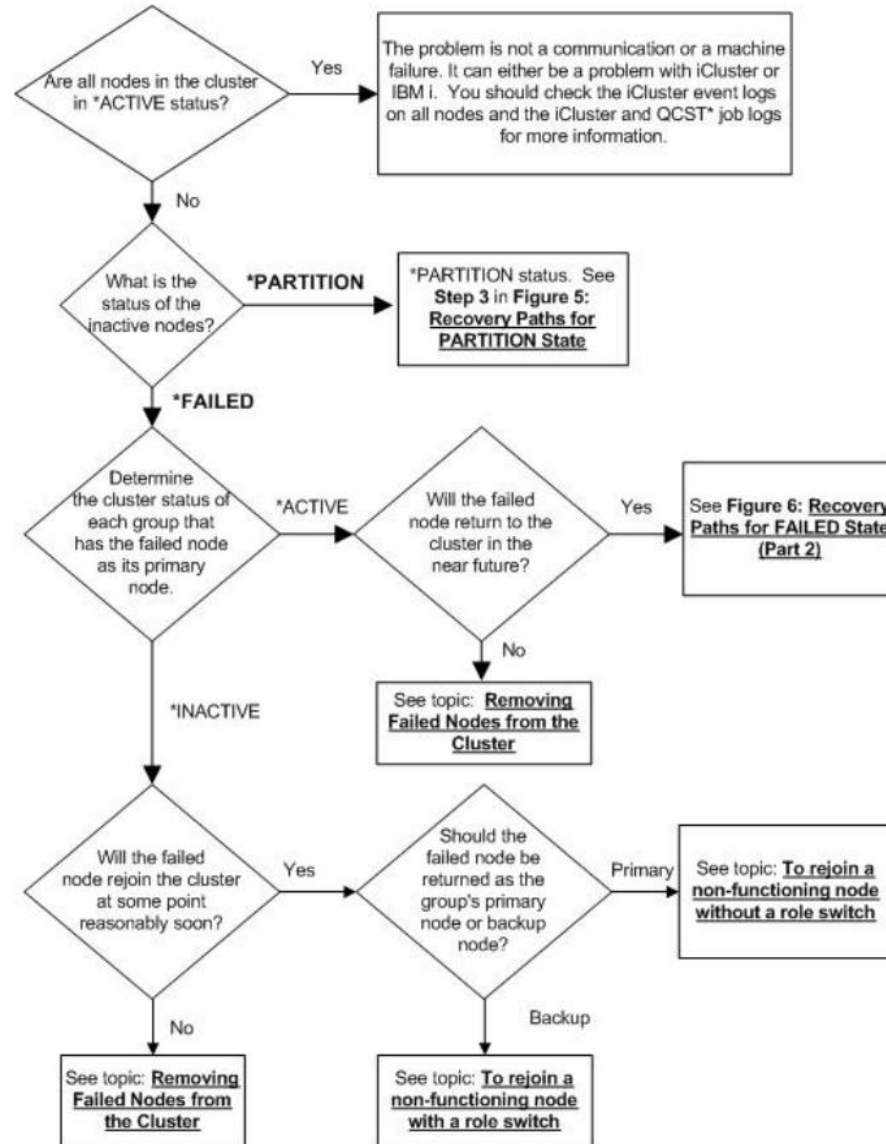
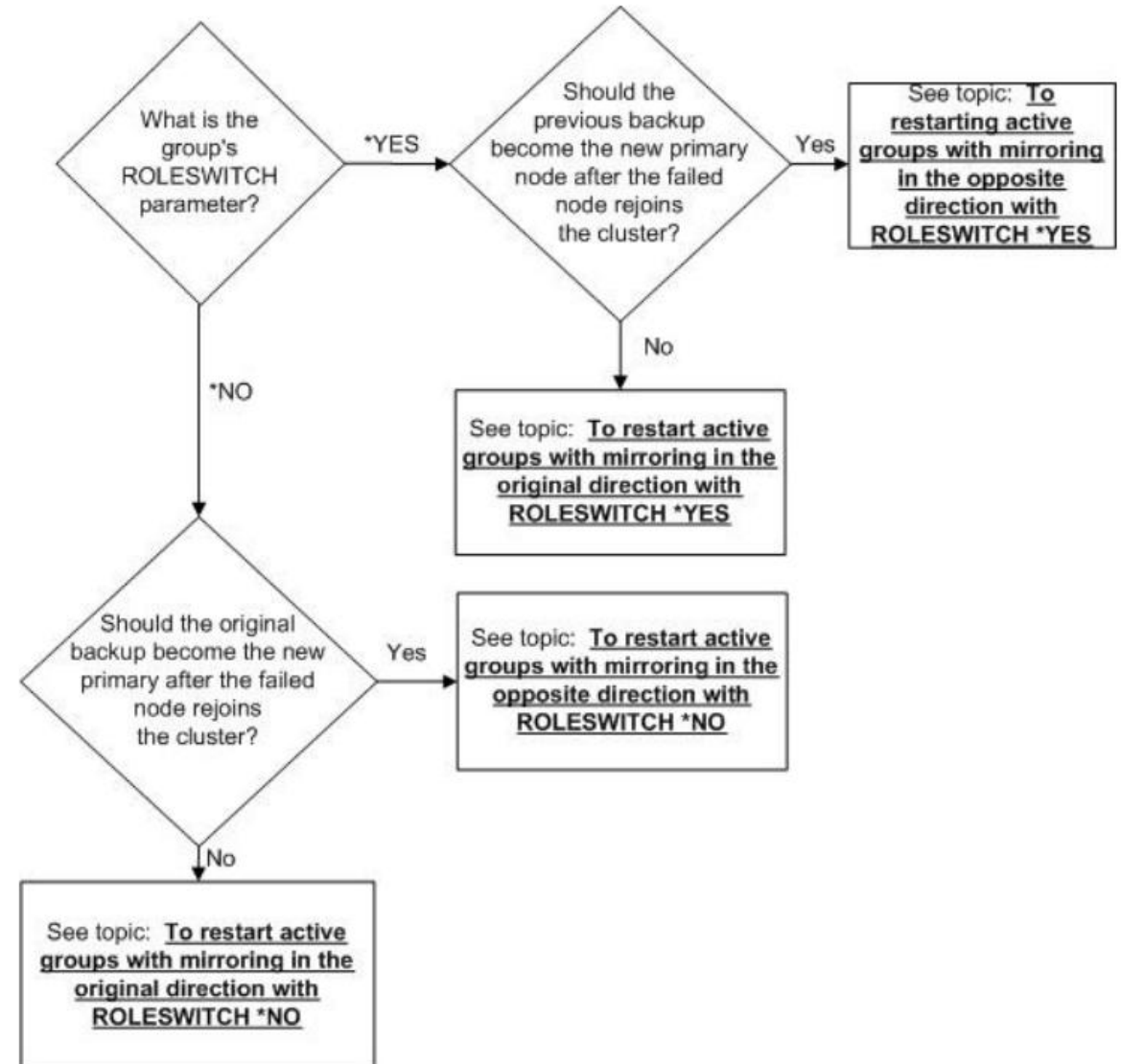


Figure 4: Recovery Paths for FAILED State (Part 2)



Mitigating A Temporary Outage

Trigger Events

- Hardware failure (including extended replacement timelines)
- Power outage
- Network or broader infrastructure outage

Operational Response

- Initiate failover to the High Availability (HA) environment
- Continue running production workloads in the HA system
- Monitor and stabilize operations during the outage

Recovery & Return

- Restore the primary site once infrastructure is available
- Perform a controlled switchover to the primary prod system

Business Impact

- Minimal data loss
- Reduced downtime
- Proper planning

Routine testing significantly minimizes user disruption

Recover From A Ransomware Attack

MONITORING

- Early detection and containment (FCM 4 / IBM FlashSystem / Exit Points)
- Kisco SafeNet Ransomware Detection and Automation
- Network monitoring
- 24/7 Operations Engagement

Suspend Replication: Use SafeNet external hooks to automatically halt replication processes

System Restore: Restore the system from the most recent unaffected full system save

Journal Restore: Restore the most recent unaffected journal receivers

Receiver Placement: Store journal receivers on an iASP to enable frequent capture and minimize data loss

Immutable Protection: Protect journal receivers with immutable backups or snapshots

Recovery Completion: Roll forward journaled changes

Planned Outage

Trigger Events

- Hardware or software maintenance requiring downtime on primary hardware
- Site or facility maintenance
- Proactive action for a predicted natural disaster (hurricane, flooding, etc.)

Response

- Perform a planned switchover to the HA system and run production there
- Once the outage has ended and all-clear is given, switch back to the production system
- No data loss and minimal user impact

Flexible Resiliency Options

Bronze

Backups
Hardware HA (manual)
Replicated Backups Only
High RPO / High RTO
Annual DR Test
Minimum Engineering Support
Operational Monitoring

Silver

Backups
Hardware HA (manual) - Local
Replication
Medium RPO / Medium RTO
Bi-Annual DR Test
Expanded Engineering Support
Expanded Monitoring

Gold

Backups
Expanded HA Technology
Replication
Low RPO / Low RTO
Quarterly DR Test
Custom Engineering Support
Monitoring and Observability

Resiliency Infrastructure Resources



IBM i cybsersecurity

- Security testing & readiness
- IBM i monitoring & alerting
- Exit point monitoring
- Ransomware detection
- iCluster status monitoring

More information

Contact:
alicia@kisco.com



IBM i HA/DR solutions

- Cost-effective IBM i HA/DR
- Optimizing skills & efficiency
- Modernization
- Seamless on-prem/cloud connectivity

More information

Contact:
ksidhu1@rocketsoftware.com



Managed services

- IBM i & Enterprise Hosting
- Managed SOC/SIEM
- Cyber Compliance
- Solution Architecture
- Strategic leadership

More information

Contact:
info@procern.com

Thank you!

Any Questions? Want to learn more?

Schedule a one-to-one conversation:

Book a Meeting

or email Alicia@kisco.com