

Disaster Recovery Plan (DRP)

Overview

Client: TGI Entertainment

Infrastructure: 2x ESXi Hosts with VM backups via Acronis Backup Cloud

Backup Schedule: Daily incremental at 03:00 AM, retention policy (Daily: 2 days, Weekly: 1 week, Monthly: 1 month)

Recovery Target: Restore all critical VMs to operational state within 24 hours

Inventory of Critical Systems

VM Name	Purpose	Priority	Host
prod-db	Database Server	High	CY Production
PROD-FW1	Firewall VM	High	CY Production
PROD-MASTER	Main Application Master	High	CY Production
PROD-SLAVE	Application Slave	Medium	CY Production
PROD-WEB	Production Web Server	High	CY Production
DBSAM01	Secondary DB Server	Medium	AMS Stage
MasterCache	Cache System Master	Medium	AMS Stage
Slave Cache	Cache System Slave	Low	AMS Stage
Monitor	Monitoring Tools	Medium	AMS Stage
pf1	Secondary Firewall/Test	Low	AMS Stage
Web Server	Test/Backup Web Server	Medium	AMS Stage

Backup Configuration Summary

- Scope: Entire VM backups
- Type: Always incremental (after first full backup)
- Time: 03:00 AM
- Retention:
 - Daily backups: 2 days
 - Weekly backups: 1 week
 - Monthly backups: 1 month
- Storage Location: Acronis Cloud Storage

Recovery Scenarios

- Scenario A: Single VM Failure
 - Action: Restore latest backup from Acronis Console to the same ESXi host.
 - RTO: < 2 hours
 - RPO: ≤ 24 hours (incremental backup at 03:00 AM)
- Scenario B: Complete ESXi Host Failure
 - Action: Boot VMs from backup to the surviving ESXi host (if capacity allows).
 - Preparation: Confirm resource availability on remaining host, keep ESXi install ISO on hand.
- Scenario C: Acronis Cloud Unavailable
 - Mitigation: Enable local backups or secondary offsite location. (e.g. S3 object storage)
 - Log ticket with Acronis support immediately.
- Scenario D: Both ESXi hosts failure
 - Action: Spin up new infrastructure (on-prem or cloud), restore VMs from Acronis Cloud.
 - RTO: ≤ 24 hours
 - RPO: Last successful incremental backup

DR Tools & Access

- Admin Console: Acronis Cyber Protect Cloud
- VM Host Access: vSphere/ESXi consoles
- Cloud Access: Credentials stored securely in password manager

- Documentation: System documentation with VM roles, IPs, access stored offsite

Test & Update Schedule

- Test Restore: Quarterly (test restore a VM and/or a file)
- Update DR Plan: Biannually or after major infra changes

Roles and Responsibilities

Role	Person/Team	Responsibilities
DR Coordinator	IT Manager / NOC	Oversee recovery execution, escalation
Backup Operator	Sysadmin/NOC	Monitor backup jobs, trigger restores
Network Admin	Firewall Team	Reconfigure routing, IPs, and DNS as needed
Cloud Vendor	Acronis Support	Assist with backup issues and cloud recovery