Novi - Operational Documentation

Novi
Smart Commerce Suite

Generated on: 28/06/2025

Novi Operational Documentation

Operational procedures and maintenance guide for Novi Smart Commerce Suite

Ø=Þ€ System Operations

Overview

This document provides comprehensive operational procedures for maintaining and managing the Novi Smart Commerce Suite. It covers deployment, monitoring, maintenance, troubleshooting, and disaster recovery procedures.

Operational Principles

- Reliability First: Ensure 99.9% uptime for customer businesses
- Proactive Monitoring: Detect and resolve issues before they impact users
- Automated Operations: Minimize manual intervention through automation
- Security Focus: Maintain data protection and system security
- Scalability: Support business growth without performance degradation

---

Ø=ÜÊ Monitoring & Alerting

System Monitoring

Infrastructure Monitoring

Server Health

- CPU utilization (threshold: 80%)
- Memory usage (threshold: 85%)
- Disk space (threshold: 90%)
- Network connectivity
- Process status

Database Monitoring

- Connection pool status
- Query performance
- Lock contention
- Backup status
- Replication lag (if applicable)

Application Monitoring

- Response times
- Error rates
- Throughput metrics
- User session counts
- WhatsApp connection status

Monitoring Tools

Primary Monitoring Stack

- PM2: Process monitoring and management
- Custom Logging: Application-specific metrics
- Railway Dashboard: Infrastructure monitoring
- WhatsApp Web.js: Connection health monitoring

Alerting Configuration

```
const alertThresholds = {
cpu: 80,
memory: 85,
disk: 90,
errorRate: 5,
responseTime: 2000,
whatsappConnection: 'disconnected'
};
```

Log Management

Log Levels

- ERROR: System errors requiring immediate attention
- WARN: Potential issues that need monitoring
- INFO: General operational information
- DEBUG: Detailed debugging information

Log Rotation

```
const winston = require('winston');
require('winston-daily-rotate-file');
const logger = winston.createLogger({
```

```
transports: [
new winston.transports.DailyRotateFile({
filename: 'logs/application-%DATE%.log',
datePattern: 'YYYY-MM-DD',
maxSize: '20m',
maxFiles: '14d'
})
]
});
```

Log Analysis

Key Metrics to Monitor

- Error frequency and patterns
- Performance bottlenecks
- User activity patterns
- WhatsApp connection stability
- Database query performance

Ø=Ý' Maintenance Procedures

Daily Maintenance

Morning Checks (9:00 AM)

- System Health Review
- Check PM2 process status
- Verify WhatsApp connections
- Review error logs from overnight
- Confirm database connectivity
- Performance Metrics
- Review response times
- Check memory usage
- Monitor active user sessions
- Verify backup completion
- WhatsApp Integration
- Confirm all business connections active
- Check message processing queue
- Verify order parsing accuracy
- Monitor delivery status updates

Evening Checks (6:00 PM)

- Daily Summary
- Generate daily performance report
- Review system alerts
- Check scheduled maintenance tasks
- Update operational status
- Backup Verification
- Confirm database backup success
- Verify file backup completion
- Test backup restoration (weekly)
- Update backup logs

Weekly Maintenance

Performance Optimization

- Database Maintenance

```
VACUUM ANALYZE;

REINDEX DATABASE novi_db;
```

- Log Cleanup
- Archive old log files
- Compress archived logs
- Update log rotation settings
- Review log storage usage
- System Updates
- Review available security patches
- Plan update deployment
- Test updates in staging
- Schedule production deployment

Security Review

- Access Log Analysis
- Review failed login attempts
- Check for suspicious activity
- Verify user access patterns
- Update security rules
- Vulnerability Assessment
- Run security scans
- Review dependency updates
- Check SSL certificate status
- Update security configurations

Monthly Maintenance

Comprehensive Review

- Performance Analysis

- Review monthly performance trends
- Identify optimization opportunities
- Update capacity planning
- Adjust monitoring thresholds
- Security Audit
- Complete security assessment
- Update access controls
- Review compliance requirements
- Update security documentation
- Backup Strategy Review
- Test disaster recovery procedures
- Update backup retention policies
- Verify backup integrity
- Document recovery procedures

Ø=Þ¨ Incident Response

Incident Classification

Severity Levels

P1 - Critical

- Complete system outage
- Data loss or corruption
- Security breach
- WhatsApp integration failure

P2 - High

- Performance degradation
- Partial functionality loss
- High error rates
- Database connectivity issues

P3 - Medium

- Minor functionality issues
- Performance impact
- User experience degradation
- Monitoring alerts

P4 - Low

- Cosmetic issues
- Documentation updates
- Feature requests
- General inquiries

Incident Response Process

Detection & Alerting

- Automated Detection
- System monitoring triggers alerts
- Error rate thresholds exceeded
- Performance degradation detected
- WhatsApp connection lost
- Manual Detection
- User reports issues
- Support team identifies problems
- Monitoring dashboard shows anomalies
- Log analysis reveals issues

Response Procedures

P1 Incident Response

```
- Alert on-call engineer
- Assess incident scope
- Implement immediate mitigation
- Notify stakeholders

2. Investigation (15-60 minutes)
- Root cause analysis
- Impact assessment
- Communication plan
- Recovery strategy

3. Resolution (1-4 hours)
- Implement fix
- Verify resolution
- Monitor system stability
- Update status

4. Post-Incident (24-48 hours)
- Incident review
- Documentation update
- Process improvement
- Stakeholder communication
```

P2/P3 Incident Response

```
- Review incident details
- Determine impact scope
- Assign response team
- Begin investigation

2. Resolution (30 minutes - 4 hours)
- Implement fixes
- Test solutions
- Deploy updates
- Verify resolution

3. Follow-up (24 hours)
- Document incident
- Update procedures
- Monitor for recurrence
- Team communication
```

Communication Procedures

Internal Communication

- Slack/Teams: Immediate team notification
- Email: Detailed incident reports
- Phone: Critical incident escalation
- Dashboard: Status page updates

Customer Communication

- Status Page: Real-time updates
- Email: Detailed incident reports
- WhatsApp: Direct customer notifications
- Social Media: Public updates

Ø=Ý Deployment Procedures

Deployment Strategy

Blue-Green Deployment

- Preparation
- Deploy new version to staging
- Run comprehensive tests
- Prepare rollback plan
- Notify stakeholders
- Deployment
- Deploy to production environment
- Run health checks
- Verify functionality
- Monitor performance
- Verification
- Confirm all features working
- Check performance metrics
- Verify WhatsApp integration
- Monitor error rates
- Rollback (if needed)
- Identify issues quickly
- Execute rollback plan
- Restore previous version
- Communicate status

Database Migrations

Migration Process

- Pre-Migration
- Backup production database
- Test migration in staging
- Review migration impact
- Schedule maintenance window
- Migration Execution
- Stop application services
- Run database migration

- Verify data integrity
- Restart services
- Post-Migration
- Verify application functionality
- Check data consistency
- Monitor performance
- Update documentation

Rollback Procedures

-- 20240320000010_rollback_add_new_column.sql

-- Rollback the new column addition

ALTER TABLE orders DROP COLUMN IF EXISTS new_column;

-- Verify rollback

SELECT column_name

FROM information_schema.columns

WHERE table_name = 'orders';

```
- Review incident details
- Determine impact scope
- Assign response team
- Begin investigation

2. Resolution (30 minutes - 4 hours)
- Implement fixes
- Test solutions
- Deploy updates
- Verify resolution

3. Follow-up (24 hours)
- Document incident
- Update procedures
- Monitor for recurrence
- Team communication
```

Configuration Management

Environment Configuration

const environments = {

development: {

database: 'novi_dev',

logLevel: 'debug',

whatsappTimeout: 30000

},

staging: {

database: 'novi_staging',

logLevel: 'info',

whatsappTimeout: 60000

},

production: {

database: 'novi_prod',

logLevel: 'warn',

whatsappTimeout: 120000

}

};

```
- Review incident details
- Determine impact scope
- Assign response team
- Begin investigation

2. Resolution (30 minutes - 4 hours)
- Implement fixes
- Test solutions
- Deploy updates
- Verify resolution

3. Follow-up (24 hours)
- Document incident
- Update procedures
- Monitor for recurrence
- Team communication
```

Feature Flags

const featureFlags = {

newOrderParser: process.env.ENABLE_NEW_PARSER === 'true',

advancedAnalytics: process.env.ENABLE_ANALYTICS === 'true',

realTimeTracking: process.env.ENABLE_TRACKING === 'true'

};


```
- Review incident details
- Determine impact scope
- Assign response team
- Begin investigation

2. Resolution (30 minutes - 4 hours)
- Implement fixes
- Test solutions
- Deploy updates
- Verify resolution

3. Follow-up (24 hours)
- Document incident
- Update procedures
- Monitor for recurrence
- Team communication
```

Ø=Þáþ Security Operations

Access Control

User Access Management

- Account Provisioning
- Create user accounts
- Assign appropriate roles

- Set up authentication
- Provide access credentials
- Access Review
- Monthly access review
- Remove inactive accounts
- Update permissions
- Audit access logs
- Account Decommissioning
- Disable user accounts
- Revoke access permissions
- Archive user data
- Update documentation

API Security

```
const rateLimit = require('express-rate-limit');

const helmet = require('helmet');

// Rate limiting

const limiter = rateLimit({

windowMs: 15 * 60 * 1000, // 15 minutes

max: 100 // limit each IP to 100 requests per windowMs

});

// Security headers

app.use(helmet());

app.use(limiter);
```

```
- Review incident details
- Determine impact scope
- Assign response team
- Begin investigation

2. Resolution (30 minutes - 4 hours)
- Implement fixes
- Test solutions
- Deploy updates
- Verify resolution

3. Follow-up (24 hours)
- Document incident
- Update procedures
- Monitor for recurrence
- Team communication
```

Data Protection

Encryption

- At Rest: Database encryption
- In Transit: TLS/SSL encryption
- WhatsApp: End-to-end encryption (native)
- Backups: Encrypted backup storage

Data Retention

const retentionPolicies = {

orders: {

active: '2 years',

archived: '7 years',

deleted: '30 days'

},

logs: {

application: '90 days',

access: '1 year',

error: '2 years'

},

backups: {

daily: '30 days',

weekly: '12 months',

monthly: '7 years'

}

};

```
- Review incident details
- Determine impact scope
- Assign response team
- Begin investigation

2. Resolution (30 minutes - 4 hours)
- Implement fixes
- Test solutions
- Deploy updates
- Verify resolution

3. Follow-up (24 hours)
- Document incident
- Update procedures
- Monitor for recurrence
- Team communication
```

Security Monitoring

Threat Detection

- Intrusion Detection: Monitor for suspicious activity
- Anomaly Detection: Identify unusual patterns
- Vulnerability Scanning: Regular security assessments
- Compliance Monitoring: Ensure regulatory compliance

Incident Response

- Detection: Identify security incidents
- Containment: Limit incident impact

- Eradication: Remove threat sources
- Recovery: Restore normal operations
- Lessons Learned: Improve security posture

Ø=ÜÈ Performance Management

Performance Monitoring

Key Performance Indicators (KPIs)

Application Performance

- Response time (target: <2 seconds)
- Throughput (requests per second)
- Error rate (target: <1%)
- Availability (target: 99.9%)

Database Performance

- Query execution time
- Connection pool utilization
- Lock wait time
- Cache hit ratio

WhatsApp Integration

- Message processing time
- Connection stability
- Order parsing accuracy
- Delivery notification success

Performance Optimization

Database Optimization

ANALYZE orders;

VACUUM orders;

REINDEX TABLE orders;

-- Performance monitoring queries

SELECT

schemaname,

tablename,

attname,

n_distinct,

correlation

FROM pg_stats

WHERE tablename = 'orders';

```
- Review incident details
- Determine impact scope
- Assign response team
- Begin investigation

2. Resolution (30 minutes - 4 hours)
- Implement fixes
- Test solutions
- Deploy updates
- Verify resolution

3. Follow-up (24 hours)
- Document incident
- Update procedures
- Monitor for recurrence
- Team communication
```

Application Optimization

const performanceMetrics = {

responseTime: [],

memoryUsage: [],

cpuUsage: [],

errorRate: []

};

// Cache optimization

const cacheConfig = {

ttl: 3600,

maxSize: 1000,

evictionPolicy: 'lru'

};


```
- Review incident details
- Determine impact scope
- Assign response team
- Begin investigation

2. Resolution (30 minutes - 4 hours)
- Implement fixes
- Test solutions
- Deploy updates
- Verify resolution

3. Follow-up (24 hours)
- Document incident
- Update procedures
- Monitor for recurrence
- Team communication
```


Capacity Planning

Resource Monitoring

- CPU Usage: Monitor processor utilization
- Memory Usage: Track memory consumption
- Disk Space: Monitor storage usage
- Network: Track bandwidth utilization

Scaling Strategies

- Vertical Scaling: Increase server resources
- Horizontal Scaling: Add more servers
- Database Scaling: Read replicas, sharding
- Caching: Redis, CDN implementation

Ø=Ý Backup & Recovery

Backup Strategy

Database Backups

backup-database.sh

Daily backup

pg_dump -h localhost -U novi_user -d novi_db > /backups/daily/novi_$(date +%Y%m%d).sql

Weekly backup

if [$(date +%u) -eq 1]; then

pg_dump -h localhost -U novi_user -d novi_db > /backups/weekly/novi_$(date +%Y%m%d).sql

fi

Monthly backup

if [$(date +%d) -eq 01]; then

pg_dump -h localhost -U novi_user -d novi_db > /backups/monthly/novi_$(date +%Y%m).sql

fi

```
- Review incident details
- Determine impact scope
- Assign response team
- Begin investigation

2. Resolution (30 minutes - 4 hours)
- Implement fixes
- Test solutions
- Deploy updates
- Verify resolution

3. Follow-up (24 hours)
- Document incident
- Update procedures
- Monitor for recurrence
- Team communication
```

File Backups

- Session Data: WhatsApp session files
- Uploads: User uploaded files
- Logs: Application and system logs
- Configuration: System configuration files

Recovery Procedures

Database Recovery

restore-database.sh

Stop application

pm2 stop novi-commerce

Restore database

psql -h localhost -U novi_user -d novi_db < /backups/daily/novi_20240315.sql

Verify restoration

psql -h localhost -U novi_user -d novi_db -c "SELECT COUNT(*) FROM orders;"

Restart application

pm2 start novi-commerce

```
- Review incident details
- Determine impact scope
- Assign response team
- Begin investigation

2. Resolution (30 minutes - 4 hours)
- Implement fixes
- Test solutions
- Deploy updates
- Verify resolution

3. Follow-up (24 hours)
- Document incident
- Update procedures
- Monitor for recurrence
- Team communication
```

Full System Recovery

- Infrastructure Recovery
- Restore server configuration
- Reinstall dependencies
- Configure networking
- Restore SSL certificates
- Application Recovery
- Deploy application code
- Restore configuration files
- Restart services
- Verify functionality
- Data Recovery
- Restore database from backup
- Restore file uploads
- Restore session data
- Verify data integrity

Disaster Recovery

Recovery Time Objectives (RTO)

- Critical Systems: 4 hours
- Business Functions: 8 hours
- Full Recovery: 24 hours

Recovery Point Objectives (RPO)

- Database: 1 hour (transaction log backup)
- Files: 24 hours (daily backup)
- Configuration: 1 week (version control)

Ø=ÜË Operational Checklists

Daily Operations Checklist

Morning (9:00 AM)

- Check system health status
- Review overnight error logs
- Verify WhatsApp connections
- Confirm database connectivity
- Check backup completion
- Review performance metrics
- Update status dashboard

Evening (6:00 PM)

- Generate daily performance report
- Review system alerts
- Check scheduled tasks
- Update operational logs
- Plan next day activities
- Communicate status updates

Weekly Operations Checklist

Monday

- Review weekly performance trends
- Check security updates
- Review user access logs
- Update operational documentation
- Plan maintenance activities

Wednesday

- Database maintenance
- Log file rotation
- Performance optimization
- Security review
- Backup verification

Friday

- Weekly summary report
- Team communication

- Process improvement review
- Next week planning
- Stakeholder updates

Monthly Operations Checklist

First Week

- Monthly performance analysis
- Security audit
- Capacity planning review
- Backup strategy review
- Compliance check

Second Week

- System updates deployment
- Configuration review
- Documentation updates
- Training sessions
- Process optimization

Third Week

- Disaster recovery testing
- Performance optimization
- Security hardening
- Monitoring improvements
- Automation enhancements

Fourth Week

- Monthly operational review
- Stakeholder reporting
- Budget review
- Strategic planning
- Team development

Ø<ß¯ Continuous Improvement

Performance Optimization

Regular Reviews

- Weekly: Performance metrics review
- Monthly: Optimization opportunities
- Quarterly: Architecture improvements
- Annually: Strategic technology planning

Automation Opportunities

- Deployment: Automated CI/CD pipelines

- Monitoring: Automated alerting and response
- Backup: Automated backup verification
- Security: Automated vulnerability scanning

Process Improvement

Feedback Collection

- User Feedback: Customer satisfaction surveys
- Team Feedback: Internal process reviews
- Metrics Analysis: Performance data review
- Incident Reviews: Post-incident analysis

Implementation

- Quick Wins: Immediate improvements
- Medium Term: Process optimization
- Long Term: Strategic improvements
- Continuous: Ongoing refinement

Novi Operational Excellence

Ensuring reliable, secure, and scalable operations