Deployment Plan and rollback

SSL Certificate Deployment and Rollback Plan for XAMPP Apache

Document Information

- **Version**: 1.0
- **Date**: August 26, 2025
- **Environment**: Windows Server with XAMPP Apache
- **Prepared by**: System Administrator

DEPLOYMENT PLAN

1. Pre-Deployment Checklist

1.1 Environment Verification

☐ Verify XAMPP version and Apache status

- [ ] Confirm administrative access to Windows Server
- [ ] Ensure domain DNS is properly configured
- [ ] Verify current website functionality
- [ ] Check available disk space (minimum 100MB free)
- [ ] Confirm network connectivity and firewall settings

1.2 Certificate Validation

- [ ] Verify SSL certificate files are present and valid
- [ ] Check certificate expiration date (should be > 30 days)
- [ ] Validate private key matches the certificate
- [ ] Confirm intermediate/chain certificates are available
- [ ] Test certificate files with OpenSSL (if available)

1.3 Backup Preparation

- [ ] Create backup directory: `C:\xampp\backups\ssl-deployment-YYYYMMDD`
- [ ] Backup current Apache configuration files
- [ ] Backup current website files
- [ ] Document current Apache service status
- [ ] Take system snapshot (if virtualized)

2. Deployment Schedule

2.1 Recommended Deployment Window

- **Primary Window**: Sunday 02:00 AM - 06:00 AM (Local Server Time)
- **Alternative Window**: During scheduled maintenance window
- **Duration Estimate**: 2-3 hours (including testing)
- **Team Required**: 1-2 System Administrators

2.2 Pre-Deployment Communication

- [ ] Notify stakeholders 48 hours before deployment
- [ ] Send maintenance window notification to users
- [ ] Prepare status page updates
- [ ] Coordinate with DNS provider if needed

3. Deployment Steps

Phase 1: Preparation (30 minutes)

```
Start Time: T+0
Duration: 30 minutes
```

Step 1.1: Create Backup

```
# Create backup directory
mkdir C:\xampp\backups\ssl-deployment-%date:~-4,4%%date:~-10,2%%date:~-7,2%

# Backup configuration files
copy "C:\xampp\apache\conf\httpd.conf" "C:\xampp\backups\ssl-deployment-%date:~-4,4%%date:~-10,2%%date:~-7,2%\"
copy "C:\xampp\apache\conf\extra\httpd-vhosts.conf" "C:\xampp\backups\ssl-deployment-%date:~-4,4%%date:~-10,2%%date:~-7,2%\"
copy "C:\xampp\apache\conf\extra\httpd-ssl.conf" "C:\xampp\backups\ssl-deployment-%date:~-4,4%%date:~-10,2%%date:~-7,2%\"

# Backup htdocs if needed
robocopy "C:\xampp\htdocs" "C:\xampp\backups\ssl-deployment-%date:~-4,4%%date:~-10,2%%date:~-7,2%\htdocs" /MIR
```

Step 1.2: Document Current State

- [ ] Record current Apache version: `httpd.exe -v`
- [ ] Document loaded modules: `httpd.exe -M`
- [ ] Test current website functionality
- [ ] Record current port bindings: `netstat -an | findstr :80`

Phase 2: SSL Configuration (45 minutes)

```
Start Time: T+30
Duration: 45 minutes
```

Step 2.1: Certificate Installation

- [ ] Create SSL directory: `mkdir C:\xampp\apache\conf\ssl`
- [ ] Copy certificate files to SSL directory
- [ ] Set appropriate file permissions
- [ ] Verify certificate file integrity

Step 2.2: Apache Configuration

- [ ] Enable SSL module in `httpd.conf`
- [ ] Configure SSL settings in `httpd-ssl.conf`
- [ ] Update virtual hosts in `httpd-vhosts.conf`
- [ ] Enable rewrite module for redirects

Step 2.3: Configuration Validation

```
# Test Apache configuration
C:\xampp\apache\bin\httpd.exe -t
```

Expected Result: `Syntax OK`

Phase 3: Service Restart and Testing (45 minutes)

```
Start Time: T+75
Duration: 45 minutes
```

Step 3.1: Service Management

- [ ] Stop Apache service gracefully
- [ ] Wait 30 seconds for complete shutdown
- [ ] Start Apache service

- [ ] Verify service is running without errors
- [ ] Check Apache error logs for any issues

Step 3.2: Basic Functionality Testing

- [ ] Test HTTP access (should redirect to HTTPS)
- [ ] Test HTTPS access with SSL certificate
- [ ] Verify certificate chain is complete
- [ ] Test website functionality over HTTPS
- [ ] Check browser security indicators

Phase 4: Comprehensive Testing (30 minutes)

```
Start Time: T+120
Duration: 30 minutes
```

Step 4.1: SSL Certificate Verification

- [ ] Browser certificate validation
- [ ] SSL Labs test (if internet accessible)
- [ ] Certificate expiration date verification
- [ ] Mixed content checking

Step 4.2: Performance and Security Testing

- [ ] Page load time comparison
- [ ] Security headers verification
- [ ] HSTS functionality test
- [ ] Cross-browser compatibility check

4. Post-Deployment Tasks

4.1 Monitoring Setup

- [ ] Configure SSL certificate expiration monitoring
- [ ] Set up log monitoring for SSL errors
- [ ] Update monitoring dashboards
- [ ] Schedule regular SSL health checks

4.2 Documentation Update

- [ ] Update system documentation
- [ ] Record SSL certificate details and expiration
- [ ] Update network diagrams
- [ ] Create maintenance schedules

4.3 Communication

- [ ] Send deployment success notification
- [ ] Update status pages
- [ ] Notify stakeholders of completion
- [ ] Schedule post-deployment review

ROLLBACK PLAN

1. Rollback Triggers

1.1 Critical Issues Requiring Immediate Rollback

- SSL certificate validation failures
- Website completely inaccessible via HTTPS
- Apache service failing to start
- Significant performance degradation (>50% slower)
- Critical functionality broken

1.2 Non-Critical Issues (Monitor and Fix)

- Minor SSL warnings in some browsers
- Non-critical mixed content warnings
- Minor performance impact (<20% slower)
- Cosmetic SSL indicator issues

2. Rollback Decision Matrix

Issue Severity	Impact Level	Action Required	Time Frame
Critical	High	Immediate Rollback	15 minutes
Major	Medium	Rollback within 1 hour	60 minutes
Minor	Low	Monitor and schedule fix	Next maintenance

3. Rollback Procedures

Quick Rollback (Emergency - 15 minutes)

Step 1: Stop Apache Service

```
# Stop Apache immediately
net stop apache2.4
# or via XAMPP Control Panel
```

Step 2: Restore Configuration Files

```
# Restore backup configurations
copy "C:\xampp\backups\ssl-deployment-YYYYMMDD\httpd.conf" "C:\xampp\apache\conf\"
copy "C:\xampp\backups\ssl-deployment-YYYYMMDD\httpd-vhosts.conf"
"C:\xampp\apache\conf\extra\"
copy "C:\xampp\backups\ssl-deployment-YYYYMMDD\httpd-ssl.conf" "C:\xampp\apache\conf\extra\"
```

Step 3: Start Apache Service

```
# Test configuration
C:\xampp\apache\bin\httpd.exe -t

# Start Apache service
net start apache2.4
```

Full Rollback (Comprehensive - 45 minutes)

Step 1: Complete Service Shutdown

- ☐ Stop Apache service
- ☐ Terminate any remaining Apache processes
- ☐ Clear any temporary files

Step 2: Full Configuration Restore

- ☐ Restore all Apache configuration files
- ☐ Remove SSL certificate files
- ☐ Restore original virtual host configurations
- ☐ Restore original htdocs if modified

Step 3: Verification and Testing

- ☐ Test Apache configuration syntax
- ☐ Start Apache service
- ☐ Verify HTTP website functionality
- ☐ Test all critical website features
- ☐ Monitor error logs for 15 minutes

4. Rollback Verification Checklist

4.1 Service Level Checks

- [ ] Apache service is running
- [ ] Website accessible via HTTP
- [ ] All website functionality working
- [ ] No errors in Apache error logs
- [ ] Performance metrics restored to baseline

4.2 Business Continuity Checks

- [ ] Critical business functions operational
- [ ] User access restored
- [ ] Database connectivity confirmed
- [ ] External integrations working

5. Post-Rollback Activities

5.1 Immediate Actions (0-2 hours)

- [ ] Document rollback reason and timeline
- [ ] Notify stakeholders of rollback completion
- [ ] Update status pages
- [ ] Begin root cause analysis

5.2 Follow-up Actions (2-24 hours)

- [ ] Complete incident report
- [ ] Schedule post-mortem meeting
- [ ] Plan remediation strategy
- [ ] Update deployment procedures if needed

5.3 Recovery Planning (24-72 hours)

- [ ] Analyze failed deployment
- [ ] Correct identified issues

- [ ] Plan new deployment approach
- [ ] Schedule retry deployment

RISK ASSESSMENT

1. Risk Matrix

Risk	Probability	Impact	Mitigation Strategy
Certificate validation failure	Medium	High	Thorough pre-deployment testing
Apache configuration error	Low	High	Configuration backup and testing
DNS propagation issues	Low	Medium	Verify DNS before deployment
Performance degradation	Medium	Medium	Load testing and monitoring
User access interruption	Medium	High	Deployment during low-usage hours

2. Contingency Plans

2.1 Certificate Issues

- Keep old certificate as backup
- Have certificate authority contact information ready
- Prepare temporary self-signed certificate if needed

2.2 Configuration Issues

- Maintain multiple backup copies
- Have Apache expert on standby
- Prepare minimal working configuration

2.3 Service Interruption

- Implement health checks during deployment
- Have alternative access methods ready
- Prepare user communication templates

Revision #3
Created 26 August 2025 06:33:47 by Admin
Updated 26 August 2025 08:12:45 by Admin