SOUTHGATE TERMINAL

Port Operations Security Documentation

Service Account Authentication Response Procedures

Document Information

Document Type: Technical Response Framework
Intended Users: Technical Team, Operations Team
Usage Context: Service account authentication failures affecting automated systems
Related Scenarios: svc_gantry failures, automated system disruptions, container operations

---

Purpose

This document provides specific response procedures for service account authentication failures, particularly focusing on critical service accounts like svc_gantry that control automated port operations including container handling and crane systems.

When to Use These Procedures

- Service account authentication failures detected in system logs
- Automated systems failing to authenticate properly
- Gantry or crane control systems showing authentication errors
- Pattern of failed authentication attempts from service accounts
- Operational systems degrading due to authentication issues

Service Account Classification Matrix

TIER 1 CRITICAL SERVICE ACCOUNTS (Immediate Operational Impact)

svc_gantry

- **Function:** Controls automated gantry crane operations
- **Impact if Failed:** Container handling operations compromised
- **Dependencies:** Container placement, cargo movement, berth operations
- **Recovery Priority:** IMMEDIATE (0-15 minutes)

svc_crane

- **Function:** Controls automated crane positioning and safety systems
- **Impact if Failed:** Crane operations halt, safety systems compromised
- **Dependencies:** Container lifting, vessel loading/unloading
- **Recovery Priority:** IMMEDIATE (0-15 minutes)

svc_container

- **Function:** Controls automated container routing and tracking
- **Impact if Failed:** Container misrouting, tracking loss
- **Dependencies:** Port logistics, customer delivery schedules
- **Recovery Priority:** HIGH (15-30 minutes)

TIER 2 OPERATIONAL SERVICE ACCOUNTS (Significant Impact)

svc_ais

- **Function:** Handles AIS data processing and vessel tracking
- **Impact if Failed:** Navigation assistance degraded
- **Dependencies:** Vessel scheduling, berth assignment
- **Recovery Priority:** HIGH (30-60 minutes)

svc_cctv

- **Function:** Manages CCTV system access and recording
- **Impact if Failed:** Security monitoring compromised
- **Dependencies:** Safety monitoring, incident documentation
- **Recovery Priority:** MEDIUM (1-2 hours)

TIER 3 ADMINISTRATIVE SERVICE ACCOUNTS (Limited Operational Impact)

svc_backup

- **Function:** Automated backup operations
- **Impact if Failed:** Data backup interruption
- **Dependencies:** Data recovery capability
- **Recovery Priority:** LOW (2-4 hours)

Service Account Failure Response Protocols

Phase 1: Immediate Detection and Assessment (0-5 minutes)

Authentication Failure Indicators Technical Team Actions: - [ ] **Log Analysis:** Check authentication server logs for failure patterns - [ ] **Service Status:** Verify status of dependent automated systems - [ ] **Impact Assessment:**

Determine which operations are affected - [ ] **Timeline Analysis:** Establish when failures began and frequency

Key Log Investigation Commands:

```
# Check authentication logs for service account failures
grep "svc_gantry" /var/log/auth.log | tail -20
grep "authentication failure" /var/log/auth.log | grep "svc_"
journalctl -u authentication-service --since "1 hour ago" | grep "failed"

# Check system status of dependent services
systemctl status gantry-control.service
systemctl status crane-control.service
systemctl status container-routing.service
```

Operational Impact Assessment Operations Team Actions: - [ ] **System Status Check:** Verify which automated systems are still functioning - [ ] **Safety Assessment:** Determine if manual operations can safely replace automated systems - [ ] **Capacity Calculation:** Assess operational capacity reduction - [ ] **Crew Notification:** Alert relevant operational crews to authentication issues

Operations Assessment Questions: 1. **Are gantry cranes responding to control commands?** 2. **Can container movements be performed manually if needed?** 3. **What is the current container backlog and priority?** 4. **Are there any suspended loads that need immediate attention?**

Phase 2: Immediate Safety and Containment (5-15 minutes)

Critical Safety Actions for svc_gantry Failures IMMEDIATE SAFETY PROTOCOLS:

If Active Container Operations in Progress: - [ ] **Suspend New Lifts:** Do not begin any new container movements - [ ] **Complete Current Operations:** Safely complete any containers currently being moved - [ ] **Secure Equipment:** Ensure all cranes are in safe positions - [ ] **Area Clearance:** Clear personnel from automated operation zones

Manual Override Authorization: - [ ] **Assess Manual Capability:** Verify trained operators available for manual control - [ ] **Authority Verification:** Confirm authorization for manual override procedures - [ ] **Safety Protocol Implementation:** Implement enhanced safety procedures for manual operations - [ ] **Communication Enhancement:** Establish direct radio contact between all operators

System Isolation and Evidence Preservation Technical Team Actions:

```
# Preserve authentication logs immediately
cp /var/log/auth.log /tmp/auth_backup_$(date +%Y%m%d_%H%M%S).log
sha256sum /var/log/auth.log > /tmp/auth_hash_$(date +%Y%m%d_%H%M%S).txt

# Document system state
systemctl status --all | grep -E "(gantry|crane|container)" > /tmp/service_status_$(date +%Y

# Check for unauthorized access patterns
grep -i "svc_gantry" /var/log/auth.log | grep -v "authentication failure" > /tmp/svc_gantry_
```

Phase 3: Root Cause Investigation (15-30 minutes)

Authentication System Analysis Systematic Investigation Steps:

1. Account Status Verification:

```
# Check account lock status
chage -l svc_gantry
passwd -S svc_gantry

# Verify account permissions
id svc_gantry
groups svc_gantry

# Check password expiration
chage -l svc_gantry | grep "Password expires"
```

2. Authentication Server Analysis:

```
# Check authentication service status
systemctl status authentication-server
journalctl -u authentication-server --since "2 hours ago"

# Look for configuration changes
find /etc/ -name "*auth*" -mtime -1 -type f
find /etc/ -name "*ldap*" -mtime -1 -type f
```

3. Network and Connectivity Analysis:

```
# Check network connectivity to authentication servers
ping authentication-server.local
nslookup authentication-server.local

# Check for network issues affecting authentication
netstat -an | grep :389  # LDAP port
netstat -an | grep :636  # LDAPS port
```

Service Account Specific Investigation svc_gantry Investigation Pattern:

```
# Create investigation summary
cat > /tmp/svc_gantry_investigation_$(date +%Y%m%d_%H%M%S).txt <<EOF
SVC_GANTRY AUTHENTICATION FAILURE INVESTIGATION
Date: $(date)
Investigator: $(whoami)

FAILURE TIMELINE:
$(grep "svc_gantry" /var/log/auth.log | grep "failure" | tail -10)

ACCOUNT STATUS:
$(chage -l svc_gantry)
$(passwd -S svc_gantry)

DEPENDENT SYSTEMS STATUS:
$(systemctl status gantry-control.service --no-pager)
$(systemctl status crane-control.service --no-pager)

OPERATIONAL IMPACT:
- Gantry automation: [AFFECTED/OPERATIONAL]
- Container movements: [MANUAL/AUTOMATED]
- Safety systems: [OPERATIONAL/COMPROMISED]

EVIDENCE PRESERVED:
- Authentication logs backed up and hashed
- System status documented
- Account configuration recorded
EOF
```

Phase 4: Recovery Procedures (30-45 minutes)

Account Recovery Process Step-by-Step Recovery:

1. Account Unlock/Reset (if appropriate):

```
# ONLY if investigation shows legitimate account lock
# AND after coordination with incident coordinator

# Unlock account
sudo passwd -u svc_gantry

# Reset password if needed (coordinate with security policy)
sudo passwd svc_gantry
```

2. Service Restart Sequence:

```
# Restart authentication-dependent services in order
sudo systemctl restart authentication-server
sleep 30
```

```
# Test authentication before restarting dependent services
su - svc_gantry -c "echo 'Authentication test successful'"

# If successful, restart operational services
sudo systemctl restart gantry-control.service
sudo systemctl restart crane-control.service
```

3. System Verification:

```
# Verify service account authentication working
grep "svc_gantry" /var/log/auth.log | tail -5

# Check operational system status
systemctl status gantry-control.service
systemctl status crane-control.service

# Test automated operations (coordinate with operations team)
```

Operational Recovery Coordination Operations Team Actions: - [ ] **Test Manual Systems:** Verify manual overrides are working correctly - [ ] **Gradual Automation Return:** Slowly return to automated operations with monitoring - [ ] **Enhanced Monitoring:** Monitor all automated systems for 2 hours after recovery - [ ] **Backlog Management:** Develop plan to handle any operational backlog created during manual operations

Phase 5: Enhanced Monitoring and Prevention (45+ minutes)

Post-Recovery Monitoring Technical Monitoring (First 2 Hours):

```
# Enhanced authentication monitoring
watch -n 60 'grep "svc_gantry" /var/log/auth.log | tail -5'

# Service status monitoring
watch -n 300 'systemctl status gantry-control.service crane-control.service --no-pager'

# Create ongoing monitoring script
cat > /tmp/svc_monitor.sh <<EOF
#!/bin/bash
while true; do
    echo "$(date): Service Account Status Check"
    grep "svc_gantry.*failure" /var/log/auth.log | tail -1
    systemctl is-active gantry-control.service
    systemctl is-active crane-control.service
    echo "---"
    sleep 300
done
```

```
EOF
chmod +x /tmp/svc_monitor.sh
```

Operational Monitoring: - Monitor automated system performance for signs of recurring issues - Track operational capacity and efficiency compared to pre-incident levels - Document any unusual behavior or performance degradation - Maintain ready access to manual override procedures

---

Specific Service Account Scenarios

Scenario: svc_gantry Repeated Authentication Failures

Indicators:

- Authentication failures every few minutes from svc_gantry account
- Gantry control systems showing connection errors
- Container movements experiencing delays or failures
- Operations team reporting automated system unresponsiveness

Immediate Response (0-10 minutes):

```
# Quick assessment
grep "svc_gantry" /var/log/auth.log | tail -20
systemctl status gantry-control.service

# If multiple recent failures, preserve evidence immediately
cp /var/log/auth.log /tmp/svc_gantry_incident_$(date +%Y%m%d_%H%M%S).log
```

Investigation Priority:

1. **Credential Compromise:** Check for unauthorized password changes
2. **Account Lock:** Verify account is not locked due to failed attempts
3. **Configuration Drift:** Check for authentication server configuration changes
4. **Network Issues:** Verify connectivity between gantry systems and auth server
5. **Timing Issues:** Check for clock synchronization problems

Recovery Approach:

- **Conservative:** Reset account credentials after coordination with security team
- **Aggressive:** Temporarily bypass authentication if operational emergency
- **Balanced:** Reset credentials while implementing enhanced monitoring

Scenario: Multiple Service Account Failures

Indicators:

- svc_gantry, svc_crane, and svc_container all showing authentication failures
- Pattern suggests systematic issue rather than individual account problems
- Multiple operational systems affected simultaneously

Response Escalation:

- **Immediate:** Treat as potential coordinated attack
- **Technical:** Full authentication system investigation
- **Operational:** Prepare for extended manual operations
- **Legal:** Consider breach notification requirements
- **Executive:** Prepare for potential operations halt decision

Investigation Focus:

1. **Authentication Server Compromise:** Full audit of authentication infrastructure
2. **Credential Database Integrity:** Verify credential storage hasn't been tampered with
3. **Network Attack:** Check for authentication traffic interception or manipulation
4. **Insider Threat:** Consider possibility of deliberate credential compromise

---

Cross-Team Coordination Procedures

Technical-Operations Coordination

Communication Protocol: Every 15 minutes during active incident: - **Technical to Operations:** Authentication recovery progress update - **Operations to Technical:** Operational impact and manual operation status - **Bi-directional:** Any new symptoms or system behavior changes

Decision Points: Technical Team Decision: "Authentication system appears compromised, recommend full manual operations" **Operations Team Decision:** "Manual operations unsustainable, need authentication recovery or operations halt" **Joint Decision:** "Risk-benefit analysis of temporary authentication bypass vs. operations halt"

Legal-Technical Coordination

Evidence Preservation:

- Technical team preserves all authentication logs and system status information
- Legal team provides guidance on evidence handling and retention requirements
- Joint documentation of any security implications and breach classification

Regulatory Notifications:

- If service account failures indicate security breach, legal team initiates notification procedures
- Technical team provides detailed technical impact assessment for regulatory reports
- Coordination on external communications about authentication system status

---

Service Account Security Hardening

Post-Incident Improvements

Authentication Monitoring Enhancements:

```
# Implement real-time service account monitoring
cat > /etc/rsyslog.d/50-service-accounts.conf <<EOF
# Service account authentication monitoring
:programname, isequal, "sshd" /var/log/service-auth.log
:msg, contains, "svc_" /var/log/service-auth.log
& stop
EOF

# Restart rsyslog to apply changes
systemctl restart rsyslog
```

Automated Alert System:

```
# Create service account failure alert script
cat > /usr/local/bin/service-account-monitor.sh <<EOF
#!/bin/bash
LOGFILE="/var/log/auth.log"
ALERT_THRESHOLD=3
LAST_CHECK_FILE="/tmp/last_service_check"

# Check for service account failures in last 5 minutes
CURRENT_TIME=\$(date +%s)
FIVE_MIN_AGO=\$((CURRENT_TIME - 300))

if [ -f "\$LAST_CHECK_FILE" ]; then
```

```
    LAST_CHECK=\$(cat \$LAST_CHECK_FILE)
else
    LAST_CHECK=\$FIVE_MIN_AGO
fi

# Count failures since last check
FAILURE_COUNT=\$(grep "authentication failure" \$LOGFILE | grep "svc_" | awk -v start=\$LAST

if [ \$FAILURE_COUNT -ge \$ALERT_THRESHOLD ]; then
    echo "ALERT: \$FAILURE_COUNT service account authentication failures detected"
    # Send alert to incident coordinator
    echo "Service account authentication failures: \$FAILURE_COUNT" | mail -s "URGENT: Servi
fi

echo \$CURRENT_TIME > \$LAST_CHECK_FILE
EOF

chmod +x /usr/local/bin/service-account-monitor.sh

# Add to cron for every 5 minutes
echo "*/5 * * * * root /usr/local/bin/service-account-monitor.sh" >> /etc/cron.d/service-mon
```

Recovery Readiness Procedures

Pre-positioned Recovery Tools:

- Service account password reset procedures pre-approved and documented
- Manual override activation procedures tested and ready
- Emergency contact information for authentication system vendors
- Backup authentication methods tested and available

Regular Testing:

- Monthly service account authentication testing
- Quarterly manual override procedure drills
- Annual authentication system failover testing
- Regular review and update of service account procedures

Success Criteria for Service Account Response

Immediate Response Success

- Service account failures detected within 5 minutes of occurrence
- Safety protocols implemented immediately to prevent operational accidents
- Evidence preserved before any recovery attempts
- All affected systems identified and assessed within 15 minutes

Investigation and Recovery Success

- Root cause of authentication failures identified within 30 minutes
- Service account functionality restored within 45 minutes (if technically feasible)
- No compromise of operational safety during manual operations
- Complete documentation of incident and recovery actions

Coordination Success

- Effective communication maintained between technical and operations teams
- Legal requirements for evidence preservation and breach notification met
- Executive team kept informed of status and decision points
- External stakeholders appropriately informed without compromising security

Long-term Improvement Success

- Enhanced monitoring implemented to prevent similar incidents
- Authentication system hardening completed within 30 days
- Staff training updated to reflect lessons learned
- Incident procedures refined based on actual response experience

---

Owner: Technical Team Lead / Operations Manager
Reference: TECH-SVC-01
Version: 1.0
Approved by: Cyber-Ops Coordination Cell