

SQLskills Immersion Event

IE0: Accidental/Junior DBA

Module 8: Checklists



Hardware Checklist

- **Processor selection based on workload**
 - OLTP – faster single-threaded performance and clock speed over cores
 - DW/DSS – higher core counts for parallel task processing
- **Maximize memory based on edition**
 - Install 72GB+ RAM for Standard Edition – allows SQL to use all 64GB
- **Storage configuration**
 - Configure storage based on performance requirements not size in GB
 - Isolate transaction logs on RAID 10 where practical/possible
 - Verify performance baseline using SQLIO before production use

Installation Checklist (1)

- **Hardware and OS**
 - ❑ Update BIOS, hardware firmware, device drivers
 - ❑ Windows Updates applied
 - ❑ Power Management configured for High Performance
 - ❑ Lock Pages in Memory and Perform Volume Maintenance added to service account in Local Security Policy
- **SQL Server setup**
 - ❑ Only install required services
 - ❑ Configure Service Accounts with low privilege local or domain account
 - ❑ Authentication mode – Windows vs Mixed
 - ❑ Default paths for data, log, tempdb, and backups changed from C:

Installation Checklist (2)

- **Instance configuration settings**
 - ❑ Enable remote DAC
 - ❑ Remove BUILTIN\Administrators group
 - ❑ Configure 'max server memory', 'max degree of parallelism', 'cost threshold for parallelism', 'compress backup', and 'optimize for ad hoc workloads' sp_configure options
 - ❑ Configure tempdb files
 - ❑ Configure fixed TCP port and firewall rules for the instance
 - ❑ Configure ;-T3226 and ;-T1118 startup parameters for service
 - ❑ Configure SQL Agent to start automatically for stand alone instances
 - ❑ Configure Database Mail and necessary firewall or anti-virus rules
 - ❑ Configure SQL Operator in SQL Agent for notifications
 - ❑ Configure SQL Agent Alerts for high severity errors

Security Checklist (1)

- **Server security**

- Physically secured with limited access to hardware
- Reviews of server access lists and Windows logins annually
- Principal of least privilege applied to service accounts
- Anti-virus software installed with exclusions configured
- Backup media stored securely

- **Authentication**

- Separate accounts used for administration purposes
- Password policies and expiration enforced for logins
- Secure 'sa' account password if using mixed mode authentication
- Limit access to fixed server roles; sysadmin and securityadmin specifically
- Configure failed login auditing

Security Checklist (2)

- **Authorization**
 - Principal of least privilege applied
 - Database roles created to simplify permissions management
- **Auditing**
 - Compliance auditing enabled according to requirements
- **Database encryption**
 - Backup database encryption key, server certificate and master key
 - Restore database backup to validate encryption key backup and steps required to recover from a disaster
 - Perform periodic test restores to ensure the database encryption key backup is still correct for the encrypted database (key rotation may change the key)

Disaster Recovery Checklist

- **Service Level Agreements**
 - Downtime SLA established and tracked against for outages
 - Data-loss SLA established and tested against
 - Redundant components tested to validate configuration routinely
 - SLAs reviewed at least annually to ensure they continue to meet business requirements and remain realistic for the workload
- **Disaster recovery planning**
 - Requirements gathering
 - Requirements ordering
 - Limitations gathering
 - Trade-off/compromise
 - Technology evaluation and choice
 - Implementation
 - Testing and validation (repeatedly on a schedule)

Maintenance Checklist

- **Critical maintenance tasks automated**
 - Backups
 - Consistency checks with DBCC CHECKDB
 - Index fragmentation removal
 - Update statistics
- **Logging and alerts configured for jobs**