SQL Instance Documentation

CLUSTER-2K19-2

CONTOSO TECHNICAL SERVICES

Date	02/11/2020 12:37:35
Author	DEMO2012R2\sysadmin
Version	1.03
Product	XIA Configuration Server [12.2.7.0]

Table of Contents

Disclaimer

SQL Instance Information

- Client Information 7
- Relationships 8
- Relationship Map 9

Compliance Benchmarks

- SQL Basic Compliance Benchmark [1.0.0.0] 11

Availability Groups

- Demonstration availability group 14
  - Availability Replicas 15
    - CLUSTER-2K19-1 16
    - CLUSTER-2K19-2 17
  - Listeners 18
    - ag-listener 19

Hosts

- CLUSTER-2K19-2 21

Management

- Database Mail 23
  - Demonstration account 24
- Maintenance Plans 25
  - Demonstration Maintenance Plan 26
- Resource Governor 27
  - Resource Pools 28
    - default 29
    - internal 30
  - External Resource Pools 31
    - default 32

Security

- Credentials 34

Demonstration credential 35
Cryptographic Providers 36
KeyVault 37
Logins 38
##MS_PolicyEventProcessingLogin## 39
##MS_PolicyTsqlExecutionLogin## 40
Demonstration login 41
NT AUTHORITY\SYSTEM 42
NT Service\MSSQLSERVER 43
NT SERVICE\SQLSERVERAGENT 44
NT SERVICE\SQLTELEMETRY 45
NT SERVICE\SQLWriter 46
NT SERVICE\Winmgmt 47
sa 48
TEST2019\sysadmin 49
Server Roles 50
bulkadmin 51
dbcreator 52
diskadmin 53
processadmin 54
public 55
securityadmin 56
serveradmin 57
setupadmin 58
sysadmin 59
Server Objects
Backup Devices 61
Endpoints 62
Server Properties
Advanced 65
Connections 66
Database Settings 67
Memory 68

Permissions 69
Processors 70
Security 71
Surface Area Configuration 72
SQL Server Agent
Alerts 74
Demonstration alert 75
Jobs 76
Demonstration Maintenance Plan.Subplan_1 77
Subplan_1 78
syspolicy_purge_history 79
Verify that automation is enabled. 80
Purge history. 81
Erase Phantom System Health Records. 82
Operators 83
Proxies 84
Demonstration proxy name 85
Version History

Disclaimer

This document is for authorised use by the intended recipient(s) only. It may contain proprietary material, confidential information and, or be subject to legal privilege. It should not be copied, disclosed to, retained or used by, any other party.

Microsoft, Windows and Active Directory are either registered trademarks or trademarks of Microsoft Corporation in the United States and/or other countries.

SQL Instance Information

Provides general information for this item.

General Information

Name	CLUSTER-2K19-2
Description	Microsoft SQL Server 2019 Enterprise Edition (64-bit)
Primary Owner Name	Technical Services
Primary Owner Contact	technicalservices@contoso.com

System Information

Item Path	Contoso Technical Services
Item ID	1115
Version ID	1.03
CheckOut Status	Available

Custom Item Details

This is a demonstration SQL Instance item.

Client Information

Provides information about the client that was used to generate the information and the data used by the client to uniquely identify this item.

Item Identifiers	
Primary Identifier	CLUSTER-2K19-2
Secondary Identifier	VMware-56 4d 6b 76 83 e4 76 64-14 7a 91 67 50 d3 2b ee
Tertiary Identifier	
Environment Identifier	

Client Information	
Client Machine Name	XCS-2K19-LIVE
Client Identifier	1167d6f3-3b76-4261-a236-72de1fc24be8
Client IP Address	192.168.131.201
Client Scan Date	02 November 2020 12:09 (today)
Client Service Username	TEST2019\sysadmin
Client Version	12.2.7.0

Scan Profile	
Target	CLUSTER-2K19-2
Profile Name	Scan SQL
Profile Identifier	5a1177b8-3296-466f-a8c9-c5198ff5c59c

Relationships

Provides a summary of the relationships between this item and other items in the environment.

9 Relationships

Item ID	Direction	Name	Type	Relationship Type
1116	Outbound	CLUSTER-2K19-2	Windows Server	Hosted On
1000	Outbound	Contoso Technical Services	Container	Contained Within
Internal	Outbound	AdventureWorksLT2019	Database	Hosts Database
Internal	Outbound	AdventureWorksLT2019_snapshot	Database	Hosts Database
Internal	Outbound	Demonstration database	Database	Hosts Database
Internal	Outbound	master	Database	Hosts Database
Internal	Outbound	model	Database	Hosts Database
Internal	Outbound	msdb	Database	Hosts Database
Internal	Outbound	tempdb	Database	Hosts Database

Relationship Map

Compliance Benchmarks

Compliance benchmarks provide the ability to compare the documented configuration of an item against a known security or compliance baseline.

Name	Version	Passed	Failed	Other
SQL Basic Compliance Benchmark	1.0.0.0	17	2	0

SQL Basic Compliance Benchmark [1.0.0.0]

This benchmark provides a basic security overview of an on-premises SQL instance.

Reference	Title	Configured Value
Section 1: Platform Settings		
1.01	Ensure that the SQL instance is running SQL version 11.0 or above	15.0
Section 2: Surface Area Configuration		
2.01	Disable ad hoc remote queries if not required	Disabled
2.02	Disable CLR integration if not required	Disabled
2.03	Disable database mail if not required	Enabled
2.04	Disable OLE automation if not required	Disabled
2.05	Disable remote DAC if not required	Disabled
2.06	Disable the service broker endpoint if not required	Disabled
2.07	Disable SOAP endpoints if not required	Disabled
2.08	Disable SQL mail if not required	Disabled
2.09	Disable XP CMD Shell if not required	Disabled
Section 3: Logins		
3.01	Rename the 'sa' account	sa
3.02	Disable the 'sa' account	True
3.03	Ensure no logins have a blank password	
Section 4: Security Properties		
4.01	Set the server authentication mode to 'Windows Authentication Mode'.	Windows Authentication Mode
4.02	Set the server login audit level to 'Failed Logins Only'.	Failed Logins Only
4.03	Disable cross database ownership chaining	Disabled
Section 5: Advanced Properties		
5.01	Disable scan for start-up procedures	Disabled
Section 6: Databases		
6.01	Ensure no databases are configured as TRUSTWORTHY	
Section 7: Network Protocols		

7.01	Disable Named Pipes if not required	Disabled

Availability Groups

An availability group supports a replicated environment for a discrete set of user databases, known as availability databases. You can create an availability group for high availability (HA) or for read-scale. An HA availability group is a group of databases that fail over together.

1 Availability Groups

Name	Type	Availability Databases
Demonstration availability group	Windows Server Failover Cluster	Demonstration database

Demonstration availability group

An availability group supports a replicated environment for a discrete set of user databases, known as availability databases. You can create an availability group for high availability (HA) or for read-scale. An HA availability group is a group of databases that fail over together.

General Settings

Cluster Type	Windows Server Failover Cluster
Required Synchronized Secondaries To Commit	0
Database Level Health Detection	False
Per Database DTC Support	False
Basic Availability Group	False

Availability Databases

Availability Databases	Demonstration database

Read-Only Routing

Server Instance	Read-Only Routing URL	Read-Only Routing List
CLUSTER-2K19-1	TCP://COMPUTER01.contoso.com:1433	
CLUSTER-2K19-2	TCP://COMPUTER01.contoso.com:1433	

Backup

Automated Backup Preference	Prefer Secondary

Replica Backup Priorities

Server Instance	Backup Priority	Exclude Replica
CLUSTER-2K19-1	50	False
CLUSTER-2K19-2	50	False

Permissions

There are no permissions defined.

Availability Replicas

An availability replica is an instantiation of an availability group that is hosted by a specific instance of SQL Server and maintains a local copy of each availability database that belongs to the availability group.

2 Availability Replicas

Name	Role	Availability Mode
CLUSTER-2K19-1	Secondary	Asynchronous Commit
CLUSTER-2K19-2	Primary	Asynchronous Commit

CLUSTER-2K19-1

An availability replica is an instantiation of an availability group that is hosted by a specific instance of SQL Server and maintains a local copy of each availability database that belongs to the availability group.

General Settings

Role	Secondary
Availability Mode	Asynchronous Commit
Failover Mode	Manual
Connections In Primary Role	Allow All Connections
Session Timeout (Seconds)	10
Endpoint URL	TCP://CLUSTER-2K19-1.test2019.net:5022

Read-Only Routing

Read-Only Routing Connection URL	TCP://COMPUTER01.contoso.com:1433
Read-Only Routing Replicas	

CLUSTER-2K19-2

An availability replica is an instantiation of an availability group that is hosted by a specific instance of SQL Server and maintains a local copy of each availability database that belongs to the availability group.

General Settings

Role	Primary
Availability Mode	Asynchronous Commit
Failover Mode	Manual
Connections In Primary Role	Allow All Connections
Session Timeout (Seconds)	10
Endpoint URL	TCP://CLUSTER-2K19-2.test2019.net:5022

Read-Only Routing

Read-Only Routing Connection URL	TCP://COMPUTER01.contoso.com:1433
Read-Only Routing Replicas	

Listeners

An availability group listener is a virtual network name (VNN) that clients can connect to in order to access a database in a primary or secondary replica of an Always On availability group. A listener allows a client to connect to a replica without having to know the physical instance name of the SQL Server.

1 Listeners

Name	Port	Addresses
ag-listener	1433	192.168.131.199/24

ag-listener

An availability group listener is a virtual network name (VNN) that clients can connect to in order to access a database in a primary or secondary replica of an Always On availability group. A listener allows a client to connect to a replica without having to know the physical instance name of the SQL Server.

General Settings

Port	1433
Addresses	192.168.131.199/24

Hosts

This section provides information about the host platforms.

1 Hosts

Name	Operating System	Service Pack	Serial Number
CLUSTER-2K19-2	Microsoft Windows Server 2019 Datacenter	None Installed	VMware-56 4d 6b 76 83 e4 76 64-14 7a 91 67 50 d3 2b ee

CLUSTER-2K19-2

This section provides information about the host platforms.

General Settings	
Computer Fully Qualified Domain Name	CLUSTER-2K19-2.test2019.net
Operating System Name	Microsoft Windows Server 2019 Datacenter
Service Pack	None Installed

Hardware	
Manufacturer	VMware, Inc.
Model	VMware Virtual Platform
Serial Number	VMware-56 4d 6b 76 83 e4 76 64-14 7a 91 67 50 d3 2b ee
Processors	Intel(R) Core(TM) i7-6700HQ CPU @ 2.60GHz

Management

Provides management related information including backup devices and endpoints.

Database Mail

Database Mail is an enterprise solution for sending e-mail messages from the SQL Server Database Engine or Azure SQL Database Managed Instance. Using Database Mail, your database applications can send e-mail messages to users.

General Settings

Enabled	True

1 Database Mail Accounts

Name	E-mail Address	Server Name	Authentication Type
Demonstration SMTP server	demonstration@email.com	SERVER01	Windows

Demonstration account

Database Mail is an enterprise solution for sending e-mail messages from the SQL Server Database Engine or Azure SQL Database Managed Instance. Using Database Mail, your database applications can send e-mail messages to users.

General Settings

Description	This is a demonstration account.
Display Name	Demonstration SMTP server
E-mail Address	demonstration@email.com
Name	Demonstration account
Reply E-mail	reply@email.com
Profile Names	Demonstration profile

Server Settings

Server Name	SERVER01
Port	25
Require Secure Connection (SSL)	False
Authentication Type	Windows

Maintenance Plans

Maintenance plans create a workflow of the tasks required to make sure that your database is optimized, regularly backed up, and free of inconsistencies.

1 Maintenance Plans

Name	Owner	Description
Demonstration Maintenance Plan	TEST2019\sysadmin	This is a demonstration maintenance plan.

Demonstration Maintenance Plan

Maintenance plans create a workflow of the tasks required to make sure that your database is optimized, regularly backed up, and free of inconsistencies.

General Settings

Creation Date	10/09/2020 14:03:09
Description	This is a demonstration maintenance plan.
Owner	TEST2019\sysadmin

1 Subplans

Name	Description	Job Name
Subplan_1	Subplan_1	Demonstration Maintenance Plan.Subplan_1

Resource Governor

SQL Server Resource Governor is a feature that you can use to manage SQL Server workload and system resource consumption. Resource Governor enables you to specify limits on the amount of CPU, physical I/O, and memory that incoming application requests can use.

General Settings

Enabled	True
Classifier Function Name	

Resource Pools

A resource pool represents a subset of the physical resources of an instance of the Database Engine.

2 Resource Pools

Name	System	Min CPU %	Max CPU %	Min Memory %	Max Memory %
default	True	0	100	0	100
internal	True	0	100	0	100

default

A resource pool represents a subset of the physical resources of an instance of the Database Engine.

General Settings

System Object	True
Minimum CPU %	0
Maximum CPU %	100
Minimum Memory %	0
Maximum Memory %	100

1 Workload Groups

Name	Importance	Max Requests	CPU Time (sec)	Memory Grant %	Grant Timeout (sec)	Degree Of Parallelism
default	Medium	0	0	25	0	0

internal

A resource pool represents a subset of the physical resources of an instance of the Database Engine.

General Settings

System Object	True
Minimum CPU %	0
Maximum CPU %	100
Minimum Memory %	0
Maximum Memory %	100

1 Workload Groups

Name	Importance	Max Requests	CPU Time (sec)	Memory Grant %	Grant Timeout (sec)	Degree Of Parallelism
internal	Medium	0	0	25	0	0

External Resource Pools

An external pool is used to define resources for external processes.

1 External Resource Pools

Name	System	Max CPU %	Max Memory %	Maximum Processes
default	True	100	20	0

default

An external pool is used to define resources for external processes.

General Settings

Is System Object	True
Maximum CPU %	100
Maximum Memory %	20
Maximum Processes	0

Security

Provides security related information.

Credentials

A credential is a record that contains the authentication information (credentials) required to connect to a resource outside SQL Server. This information is used internally by SQL Server.

1 Credentials

Name	Identity	Use Encryption Provider
Demonstration credential	TEST2019\Administrator	True

Demonstration credential

A credential is a record that contains the authentication information (credentials) required to connect to a resource outside SQL Server. This information is used internally by SQL Server.

General Settings

Date Created	10/09/2020 14:12:02
Date Last Modified	10/09/2020 14:15:00
Identity	TEST2019\Administrator
Use Encryption Provider	True
Encryption Provider Name	KeyVault

Cryptographic Providers

Cryptographic providers allow third-party Extensible Key Management (EKM) providers to be registered and used within SQL Server.

1 Cryptographic Providers

Name	Authentication Type	Enabled	Version
KeyVault	Basic	True	1.0.5.0

KeyVault

Cryptographic providers allow third-party Extensible Key Management (EKM) providers to be registered and used within SQL Server.

General Settings

Authentication Type	Basic
DLL Path	C:\Program Files\SQL Server Connector for Microsoft Azure Key Vault\Microsoft.AzureKeyVaultService.EKM.dll
Enabled	True
Version	1.0.5.0

Logins

A login is a security principal, or an entity that can be authenticated by a secure system. Users need a login to connect to SQL Server.

11 Logins

Name	Type	Default Database	Language
##MS_PolicyEventProcessingLogin##	SQL authentication	master	English
##MS_PolicyTsqlExecutionLogin##	SQL authentication	master	English
Demonstration login	Mapped to certificate	master	English
NT AUTHORITY\SYSTEM	Windows authentication	master	English
NT Service\MSSQLSERVER	Windows authentication	master	English
NT SERVICE\SQLSERVERAGENT	Windows authentication	master	English
NT SERVICE\SQLTELEMETRY	Windows authentication	master	English
NT SERVICE\SQLWriter	Windows authentication	master	English
NT SERVICE\Winmgmt	Windows authentication	master	English
sa	SQL authentication	master	English
TEST2019\sysadmin	Windows authentication	master	English

##MS_PolicyEventProcessingLogin##

A login is a security principal, or an entity that can be authenticated by a secure system. Users need a login to connect to SQL Server.

General Settings

ID	256
Login Type	SQL authentication
Date Created	24/09/2019 14:21:53
Date Last Modified	09/09/2020 11:29:40
Default Database	master
Language Display Name	English

SQL Login

Locked	False
Password Expired	False
Must Change Password	False
Enforce Password Expiration	False
Enforce Password Policy	True

Mapped Credentials

Mapped Credentials	

Status

Connect Permission	True
Disabled	True

Server Roles

Server Roles	public

##MS_PolicyTsqlExecutionLogin##

A login is a security principal, or an entity that can be authenticated by a secure system. Users need a login to connect to SQL Server.

General Settings

ID	257
Login Type	SQL authentication
Date Created	24/09/2019 14:21:53
Date Last Modified	09/09/2020 11:29:40
Default Database	master
Language Display Name	English

SQL Login

Locked	False
Password Expired	False
Must Change Password	False
Enforce Password Expiration	False
Enforce Password Policy	True

Mapped Credentials

Mapped Credentials	

Status

Connect Permission	True
Disabled	True

Server Roles

Server Roles	public

Demonstration login

A login is a security principal, or an entity that can be authenticated by a secure system. Users need a login to connect to SQL Server.

General Settings

ID	266
Login Type	Mapped to certificate
Date Created	10/09/2020 14:13:15
Date Last Modified	10/09/2020 14:13:15
Default Database	master
Language Display Name	English

Certificate Login

Certificate	DemonstrationCertificate

Mapped Credentials

Mapped Credentials	Demonstration credential

Status

Connect Permission	True
Disabled	False

Server Roles

Server Roles	public

NT AUTHORITY\SYSTEM

A login is a security principal, or an entity that can be authenticated by a secure system. Users need a login to connect to SQL Server.

General Settings

ID	263
Login Type	Windows authentication
Date Created	09/09/2020 11:29:40
Date Last Modified	09/09/2020 11:29:40
Default Database	master
Language Display Name	English

Windows Login

Security Identifier (SDDL)	S-1-5-18

Mapped Credentials

Mapped Credentials	

Status

Connect Permission	True
Disabled	False

Server Roles

Server Roles	public

NT Service\MSSQLSERVER

A login is a security principal, or an entity that can be authenticated by a secure system. Users need a login to connect to SQL Server.

General Settings

ID	262
Login Type	Windows authentication
Date Created	09/09/2020 11:29:40
Date Last Modified	09/09/2020 11:29:40
Default Database	master
Language Display Name	English

Windows Login

Security Identifier (SDDL)	S-1-5-80-3880718306-3832830129-1677859214-2598158968-1052248003

Mapped Credentials

Mapped Credentials	

Status

Connect Permission	True
Disabled	False

Server Roles

Server Roles	public sysadmin

NT SERVICE\SQLSERVERAGENT

A login is a security principal, or an entity that can be authenticated by a secure system. Users need a login to connect to SQL Server.

General Settings

ID	264
Login Type	Windows authentication
Date Created	09/09/2020 11:29:40
Date Last Modified	09/09/2020 11:29:40
Default Database	master
Language Display Name	English

Windows Login

Security Identifier (SDDL)	S-1-5-80-344959196-2060754871-2302487193-2804545603-1466107430

Mapped Credentials

Mapped Credentials	

Status

Connect Permission	True
Disabled	False

Server Roles

Server Roles	public sysadmin

NT SERVICE\SQLTELEMETRY

A login is a security principal, or an entity that can be authenticated by a secure system. Users need a login to connect to SQL Server.

General Settings

ID	265
Login Type	Windows authentication
Date Created	09/09/2020 11:29:41
Date Last Modified	09/09/2020 11:29:41
Default Database	master
Language Display Name	English

Windows Login

Security Identifier (SDDL)	S-1-5-80-2652535364-2169709536-2857650723-2622804123-1107741775

Mapped Credentials

Mapped Credentials	

Status

Connect Permission	True
Disabled	False

Server Roles

Server Roles	public

NT SERVICE\SQLWriter

A login is a security principal, or an entity that can be authenticated by a secure system. Users need a login to connect to SQL Server.

General Settings

ID	260
Login Type	Windows authentication
Date Created	09/09/2020 11:29:40
Date Last Modified	09/09/2020 11:29:40
Default Database	master
Language Display Name	English

Windows Login

Security Identifier (SDDL)	S-1-5-80-1402415987-66678372-3059512406-1823130485-2345841878

Mapped Credentials

Mapped Credentials	

Status

Connect Permission	True
Disabled	False

Server Roles

Server Roles	public sysadmin

NT SERVICE\Winmgmt

A login is a security principal, or an entity that can be authenticated by a secure system. Users need a login to connect to SQL Server.

General Settings

ID	261
Login Type	Windows authentication
Date Created	09/09/2020 11:29:40
Date Last Modified	09/09/2020 11:29:40
Default Database	master
Language Display Name	English

Windows Login

Security Identifier (SDDL)	S-1-5-80-3750560858-172214265-3889451188-1914796615-4100997547

Mapped Credentials

Mapped Credentials	

Status

Connect Permission	True
Disabled	False

Server Roles

Server Roles	public sysadmin

sa

A login is a security principal, or an entity that can be authenticated by a secure system. Users need a login to connect to SQL Server.

General Settings

ID	1
Login Type	SQL authentication
Date Created	08/04/2003 09:10:35
Date Last Modified	09/09/2020 11:29:40
Default Database	master
Language Display Name	English

SQL Login

Locked	False
Password Expired	False
Must Change Password	False
Enforce Password Expiration	False
Enforce Password Policy	True

Mapped Credentials

Mapped Credentials	

Status

Connect Permission	True
Disabled	True

Server Roles

Server Roles	public sysadmin

TEST2019\sysadmin

A login is a security principal, or an entity that can be authenticated by a secure system. Users need a login to connect to SQL Server.

General Settings

ID	259
Login Type	Windows authentication
Date Created	09/09/2020 11:29:40
Date Last Modified	09/09/2020 11:29:40
Default Database	master
Language Display Name	English

Windows Login

Security Identifier (SDDL)	S-1-5-21-1597374802-183462725-2612050851-1103

Mapped Credentials

Mapped Credentials	

Status

Connect Permission	True
Disabled	False

Server Roles

Server Roles	public sysadmin

Server Roles

SQL Server provides server-level roles to help you manage the permissions on a server. These roles are security principals that group other principals. Server-level roles are server-wide in their permissions scope.

9 Server Roles

Name	Fixed Role	Member Names
bulkadmin	True	
dbcreator	True	
diskadmin	True	
processadmin	True	
public	False	
securityadmin	True	
serveradmin	True	
setupadmin	True	
sysadmin	True	NT Service\MSSQLSERVER NT SERVICE\SQLSERVERAGENT NT SERVICE\SQLWriter NT SERVICE\Winmgmt sa TEST2019\sysadmin

bulkadmin

SQL Server provides server-level roles to help you manage the permissions on a server. These roles are security principals that group other principals. Server-level roles are server-wide in their permissions scope.

General Settings

Date Created	13/04/2009 12:59:06
Date Last Modified	13/04/2009 12:59:06
Is Fixed Role	True
Owner	sa

Membership

There are no members defined for this server role.

dbcreator

SQL Server provides server-level roles to help you manage the permissions on a server. These roles are security principals that group other principals. Server-level roles are server-wide in their permissions scope.

General Settings

Date Created	13/04/2009 12:59:06
Date Last Modified	13/04/2009 12:59:06
Is Fixed Role	True
Owner	sa

Membership

There are no members defined for this server role.

diskadmin

SQL Server provides server-level roles to help you manage the permissions on a server. These roles are security principals that group other principals. Server-level roles are server-wide in their permissions scope.

General Settings

Date Created	13/04/2009 12:59:06
Date Last Modified	13/04/2009 12:59:06
Is Fixed Role	True
Owner	sa

Membership

There are no members defined for this server role.

processadmin

SQL Server provides server-level roles to help you manage the permissions on a server. These roles are security principals that group other principals. Server-level roles are server-wide in their permissions scope.

General Settings

Date Created	13/04/2009 12:59:06
Date Last Modified	13/04/2009 12:59:06
Is Fixed Role	True
Owner	sa

Membership

There are no members defined for this server role.

public

SQL Server provides server-level roles to help you manage the permissions on a server. These roles are security principals that group other principals. Server-level roles are server-wide in their permissions scope.

General Settings

Date Created	13/04/2009 12:59:06
Date Last Modified	13/04/2009 12:59:06
Is Fixed Role	False
Owner	sa

Membership

There are no members defined for this server role.

securityadmin

SQL Server provides server-level roles to help you manage the permissions on a server. These roles are security principals that group other principals. Server-level roles are server-wide in their permissions scope.

General Settings

Date Created	13/04/2009 12:59:06
Date Last Modified	13/04/2009 12:59:06
Is Fixed Role	True
Owner	sa

Membership

There are no members defined for this server role.

serveradmin

SQL Server provides server-level roles to help you manage the permissions on a server. These roles are security principals that group other principals. Server-level roles are server-wide in their permissions scope.

General Settings

Date Created	13/04/2009 12:59:06
Date Last Modified	13/04/2009 12:59:06
Is Fixed Role	True
Owner	sa

Membership

There are no members defined for this server role.

setupadmin

SQL Server provides server-level roles to help you manage the permissions on a server. These roles are security principals that group other principals. Server-level roles are server-wide in their permissions scope.

General Settings

Date Created	13/04/2009 12:59:06
Date Last Modified	13/04/2009 12:59:06
Is Fixed Role	True
Owner	sa

Membership

There are no members defined for this server role.

sysadmin

SQL Server provides server-level roles to help you manage the permissions on a server. These roles are security principals that group other principals. Server-level roles are server-wide in their permissions scope.

General Settings

Date Created	13/04/2009 12:59:06
Date Last Modified	13/04/2009 12:59:06
Is Fixed Role	True
Owner	sa

Membership

Members	NT Service\MSSQLSERVER NT SERVICE\SQLSERVERAGENT NT SERVICE\SQLWriter NT SERVICE\Winmgmt sa TEST2019\sysadmin

Server Objects

Provides server object related information.

Backup Devices

During a backup operation on a SQL Server database, the backed up data (the backup) is written to a physical backup device.

1 Backup Devices

Name	Type	Location
Demonstration backup device	Disk	C:\Program Files\Microsoft SQL Server\MSSQL15.MSSQLSERVER\MSSQL\Backup\Demonstration backup device.bak

Endpoints

An endpoint is a service that can listen natively for requests.

6 Endpoints

Name	System	Type	State	TCP Listener Port
Dedicated Admin Connection	True	TSQL	Started	
Hadr_endpoint	False	Database Mirroring	Started	5022
TSQL Default TCP	True	TSQL	Started	
TSQL Default VIA	True	TSQL	Started	
TSQL Local Machine	True	TSQL	Started	
TSQL Named Pipes	True	TSQL	Started	

Server Properties

This section provides information about the SQL Server properties.

General Settings	
Product	Microsoft SQL Server 2019
Edition	Enterprise Edition (64-bit)
Engine Type	On-Premises
Version	15.0.2000.5
Product Level	RTM
Collation	Latin1_General_CI_AS
Is Full-Text Installed	True
Is HADR Enabled	True
Named Pipes Enabled	False
TCP Enabled	True
Is XTP Supported	True
Language	English (United States)
Root Directory	C:\Program Files\Microsoft SQL Server\MSSQL15.MSSQLSERVER\MSSQL

Clustering	
Clustered	False

Service	
Service Account	NT Service\MSSQLSERVER
Service Start Mode	Automatic

Platform

Operating System	6.3 (17763)
Physical Memory (MB)	2,047
Platform	NT x64
Processors	4

Advanced

This section provides information about the SQL Server advanced properties.

Containment	
Enable Contained Databases	False

FILESTREAM	
FILESTREAM Effective Access Level	Full access enabled
FILESTREAM Share Name	MSSQLSERVER

Miscellaneous	
Allow Triggers To Fire Others	True
Blocked Process Threshold	0
Boost SQL Server Priority	False
Cursor Threshold	-1
Default Full Text Language	1033
Default Language Name	English
Full-Text Upgrade Option	Import
Max Text Replication Size	65,536
Optimize Adhoc Workloads	False
Scan For Startup Procs	False
Two Digit Year Cutoff	2049
Use Windows Fibers (Lightweight Pooling)	False

Network	
Network Packet Size	4,096
Remote Login Timeout	10

Parallelism	
Cost Threshold For Parallelism	5
Locks	0
Max Degree Of Parallelism	4
Query Wait	-1

Connections

This section provides information about the connections settings assigned to the instance.

Connections	
Maximum Concurrent Connections	Unlimited
Query Governor	Disabled
Allow Remote Connections	True
Remote Query Timeout	600 seconds
Require Distributed Transactions	False

Default Connection Options	
Implicit Transactions	False
Cursor Close On Commit	False
ANSI Warnings	False
ANSI Padding	False
ANSI NULLs	False
Arithmetic Abort	False
Arithmetic Ignore	False
Quoted Identifier	False
No Count	False
ANSI NULL Default On	False
ANSI NULL Default Off	False
Concatenate NULL Yields NULL	False
Numeric Round Abort	False
XACT Abort	False

Database Settings

This section provides information about the database settings assigned to the instance.

Database Settings	
Compress Backup	False
Default Index Fill Factor	0
Default Backup Media Retention (Days)	0
Recovery Interval (Minutes)	0

Path Settings	
Default Backup Path	C:\Program Files\Microsoft SQL Server\MSSQL15.MSSQLSERVER\MSSQL\Backup
Default Database Path	C:\Program Files\Microsoft SQL Server\MSSQL15.MSSQLSERVER\MSSQL\DATA\
Default Log Path	C:\Program Files\Microsoft SQL Server\MSSQL15.MSSQLSERVER\MSSQL\DATA\

Memory

This section provides information about the memory related settings assigned to the instance.

Memory	
Minimum Server Memory (MB)	0
Maximum Server Memory (MB)	2,147,483,647
Index Creation Memory (KB)	0
Minimum Memory Per Query (KB)	1,024

Permissions

This section provides information about the permissions assigned to the instance.

29 Permissions

Name	Grantor	Permission	State
sa	sa	CONNECT SQL	Grant
public	sa	VIEW ANY DATABASE	Grant
##MS_SQLResourceSigningCertificate##	sa	VIEW ANY DEFINITION	Grant
##MS_SQLReplicationSigningCertificate##	sa	AUTHENTICATE SERVER	Grant
##MS_SQLReplicationSigningCertificate##	sa	VIEW ANY DEFINITION	Grant
##MS_SQLReplicationSigningCertificate##	sa	VIEW SERVER STATE	Grant
##MS_SQLAuthenticatorCertificate##	sa	AUTHENTICATE SERVER	Grant
##MS_PolicySigningCertificate##	sa	CONTROL SERVER	Grant
##MS_PolicySigningCertificate##	sa	VIEW ANY DEFINITION	Grant
##MS_SmoExtendedSigningCertificate##	sa	VIEW ANY DEFINITION	Grant
##MS_PolicyEventProcessingLogin##	sa	CONNECT SQL	Grant
##MS_PolicyTsqlExecutionLogin##	sa	CONNECT SQL	Grant
##MS_PolicyTsqlExecutionLogin##	sa	VIEW ANY DEFINITION	Grant
##MS_PolicyTsqlExecutionLogin##	sa	VIEW SERVER STATE	Grant
##MS_AgentSigningCertificate##	sa	CONNECT SQL	Grant
TEST2019\sysadmin	sa	CONNECT SQL	Grant
NT SERVICE\SQLWriter	sa	CONNECT SQL	Grant
NT SERVICE\Winmgmt	sa	CONNECT SQL	Grant
NT Service\MSSQLSERVER	sa	CONNECT SQL	Grant
NT AUTHORITY\SYSTEM	sa	ALTER ANY AVAILABILITY GROUP	Grant
NT AUTHORITY\SYSTEM	sa	CONNECT SQL	Grant
NT AUTHORITY\SYSTEM	sa	VIEW SERVER STATE	Grant
NT SERVICE\SQLSERVERAGENT	sa	CONNECT SQL	Grant
NT SERVICE\SQLTELEMETRY	sa	ALTER ANY EVENT SESSION	Grant
NT SERVICE\SQLTELEMETRY	sa	CONNECT ANY DATABASE	Grant
NT SERVICE\SQLTELEMETRY	sa	CONNECT SQL	Grant
NT SERVICE\SQLTELEMETRY	sa	VIEW ANY DEFINITION	Grant
NT SERVICE\SQLTELEMETRY	sa	VIEW SERVER STATE	Grant
Demonstration login	sa	CONNECT SQL	Grant

Processors

This section provides information about the processors settings assigned to the instance.

Processors

Automatically Set Processor Affinity Mask	True
Automatically Set I/O Affinity Mask	True
Maximum Worker Threads	0

4 CPUs

Name	NUMA Node	Processor Affinity	I/O Affinity
CPU0	NumaNode0	False	False
CPU1	NumaNode0	False	False
CPU2	NumaNode0	False	False
CPU3	NumaNode0	False	False

Security

This section provides information about the security settings assigned to the instance.

Security	
Login Mode	Windows Authentication Mode
Login Auditing	Failed Logins Only
Proxy Account Enabled	False

Options	
Common Criteria Compliance Enabled	False
Enable C2 Audit Tracing	False
Cross Database Ownership Chaining	False

Surface Area Configuration

Surface area configuration allows administrators to selectively enable or disable features thereby minimizing those features that can be attacked by a malicious user.

Surface Area Configuration	
Ad Hoc Remote Queries Enabled	False
CLR Integration Enabled	False
Database Mail Enabled	True
OLE Automation Enabled	False
Remote DAC Enabled	False
Service Broker Endpoint Active	False
SOAP Endpoint Active	False
SQL Mail Enabled	False
XPCmdShell Enabled	False

SQL Server Agent

The SQL Server Agent is a Microsoft Windows service that executes scheduled administrative tasks.

General Settings

Service Account	NT Service\SQLSERVERAGENT
Service Start Mode	Automatic
Automatically Restart SQL Server Agent	True
Automatically Restart SQL Server	True
Error Log File	C:\Program Files\Microsoft SQL Server\MSSQL15.MSSQLSERVER\MSSQL\Log\SQLAGENT.OUT
Write OEM File	False

Alerts

SQL Server Agent alerts are automated responses to events such as SQL Server events, performance conditions, and Windows Management Instrumentation (WMI) events.

1 Alerts

Name	Type	Enabled
Demonstration alert	SQL Server Event Alert	True

Demonstration alert

SQL Server Agent alerts are automated responses to events such as SQL Server events, performance conditions, and Windows Management Instrumentation (WMI) events.

General Settings

Alert Type	SQL Server Event Alert
Enabled	True

Alert Definition

Database Name	<all databases>
Severity	1
Raise Alert When Message Contains	Demonstration message text

Response

Job Name	Demonstration Maintenance Plan.Subplan_1
Email Notifications	Demonstration operator
Net Send Notifications	
Pager Notifications	

Options

Include Alert Error Text	E-mail
Additional Notification Message	Additional demonstation notification message.
Delay Between Responses (Seconds)	300

Jobs

You can use SQL Server Agent jobs to automate routine administrative tasks and run them on a recurring basis, making administration more efficient.

2 Jobs

Name	Owner	Category	Enabled
Demonstration Maintenance Plan.Subplan_1	TEST2019\sysadmin	Database Maintenance	True
syspolicy_purge_history	sa	[Uncategorized (Local)]	True

Demonstration Maintenance Plan.Subplan_1

You can use SQL Server Agent jobs to automate routine administrative tasks and run them on a recurring basis, making administration more efficient.

General Settings

Owner	TEST2019\sysadmin
Category	Database Maintenance
Description	No description available.
Enabled	True
Date Created	10/09/2020 14:03:31
Date Last Modified	10/09/2020 14:03:32

1 Steps

Step	Name	Type	On Success	On Failure
1	Subplan_1	SQL Server Integration Services Package	Quit the job reporting success	Quit the job reporting failure

Alerts

Alerts	Demonstration alert

Schedules

There are no scheduled defined for this job.

Notifications

Email Notification	Never
Pager Notification	Never
Write Windows Application Event Log Event	When the job fails
Delete Action	Never

Targets

Target Servers	CLUSTER-2K19-2

Subplan_1

A job step is an action that the job takes on a database or a server. Every job must have at least one job step.

General Settings

Type	SQL Server Integration Services Package
Run As	SQL Server Agent Service Account
Command	/Server "$(ESCAPE_NONE(SRVR))" /SQL "Maintenance Plans\Demonstration Maintenance Plan" /set "\Package\Subplan_1.Disable;false"

Advanced

On Success Action	Quit the job reporting success
Retry Attempts	0
Retry Interval (Minutes)	0
On Failure Action	Quit the job reporting failure
Output File	
Log To Table	False
Include Step Output In Job History	False

syspolicy_purge_history

You can use SQL Server Agent jobs to automate routine administrative tasks and run them on a recurring basis, making administration more efficient.

General Settings

Owner	sa
Category	[Uncategorized (Local)]
Description	No description available.
Enabled	True
Date Created	09/09/2020 11:29:40
Date Last Modified	09/09/2020 11:29:41

3 Steps

Step	Name	Type	On Success	On Failure
1	Verify that automation is enabled.	Transact-SQL Script (T-SQL)	Go to the next step	Quit the job reporting success
2	Purge history.	Transact-SQL Script (T-SQL)	Go to the next step	Quit the job reporting failure
3	Erase Phantom System Health Records.	PowerShell	Quit the job reporting success	Quit the job reporting failure

Alerts

There are no alerts assigned to this job.

1 Schedules

Name	Enabled	Summary
syspolicy_purge_history_schedule	True	Occurs every 1 days at 02:00:00. Schedule will be used starting on 01 January 2008.

Notifications

Email Notification	Never
Pager Notification	Never
Write Windows Application Event Log Event	Never
Delete Action	Never

Targets

Target Servers	CLUSTER-2K19-2

Verify that automation is enabled.

A job step is an action that the job takes on a database or a server. Every job must have at least one job step.

General Settings

Type	Transact-SQL Script (T-SQL)
Run As	SQL Server Agent Service Account

Command	IF (msdb.dbo.fn_syspolicy_is_automation_enabled() != 1)
	BEGIN
	RAISERROR(34022, 16, 1)
	END

Database	master

Advanced

On Success Action	Go to the next step
Retry Attempts	0
Retry Interval (Minutes)	0
On Failure Action	Quit the job reporting success
Output File	
Log To Table	False
Include Step Output In Job History	False

Purge history.

A job step is an action that the job takes on a database or a server. Every job must have at least one job step.

General Settings

Type	Transact-SQL Script (T-SQL)
Run As	SQL Server Agent Service Account
Command	EXEC msdb.dbo.sp_syspolicy_purge_history
Database	master

Advanced

On Success Action	Go to the next step
Retry Attempts	0
Retry Interval (Minutes)	0
On Failure Action	Quit the job reporting failure
Output File	
Log To Table	False
Include Step Output In Job History	False

Erase Phantom System Health Records.

A job step is an action that the job takes on a database or a server. Every job must have at least one job step.

General Settings

Type	PowerShell
Run As	SQL Server Agent Service Account
Command	if ('$(ESCAPE_SQUOTE(INST))' -eq 'MSSQLSERVER') {$a = '\DEFAULT'} ELSE {$a = ''}; (Get-Item SQLSERVER:\SQLPolicy\$(ESCAPE_NONE(SRVR))$a).EraseSystemHealthPhantomRecords()
Database	master

Advanced

On Success Action	Quit the job reporting success
Retry Attempts	0
Retry Interval (Minutes)	0
On Failure Action	Quit the job reporting failure
Output File	
Log To Table	False
Include Step Output In Job History	False

Operators

Operators are aliases for people or groups that can receive electronic notification when jobs have completed or alerts have been raised. The SQL Server Agent service supports the notification of administrators through operators. Operators enable notification and monitoring capabilities of SQL Server Agent.

1 Operators

Name	E-mail Address	Enabled	Pager	Pager Days
Demonstration operator	demonstration@email.com	True		None

Proxies

A SQL Server Agent proxy account defines a security context in which a job step can run. Each proxy corresponds to a security credential. To set permissions for a particular job step, create a proxy that has the required permissions for a SQL Server Agent subsystem, and then assign that proxy to the job step.

1 Proxies

Name	Subsystems	Description
Demonstration proxy name	PowerShell	This is a demonstration proxy.

Demonstration proxy name

A SQL Server Agent proxy account defines a security context in which a job step can run. Each proxy corresponds to a security credential. To set permissions for a particular job step, create a proxy that has the required permissions for a SQL Server Agent subsystem, and then assign that proxy to the job step.

General Settings

Credential Name	Demonstration credential
Credential Identity	TEST2019\Administrator
Description	This is a demonstration proxy.
Enabled	True
Subsystems	PowerShell

Principals

Database Roles	
Logins	Demonstration login
Server Roles	

Version History

The version history displays the changes that have been made to the documentation of this item over time - either automatically when a change has been detected, or manually by users of the system.

4 versions

Version	Username	Date	Time	Description
1.03	DEMO2012R2\sysadmin	02 November 2020	12:12	Updated by XIA Configuration Client Data
1.02	DEMO2012R2\sysadmin	02 November 2020	11:30	Added Primary Owner.
1.01	DEMO2012R2\sysadmin	02 November 2020	10:42	Updated by XIA Configuration Client Data
1.00	DEMO2012R2\sysadmin	02 November 2020	10:42	Item created.