



Expert
EXPO

SQL Server 2014

Optimisez l'exploitation
de vos bases de données et tirez parti
des **dernières nouveautés**

Téléchargement
www.editions-eni.fr



Olivier MAITRE

Les éléments à télécharger sont disponibles à l'adresse suivante :
<http://www.editions-eni.fr>
Saisissez la référence de l'ouvrage **EI14SQLOP** dans la zone de recherche et validez. Cliquez sur le titre du livre puis sur le bouton de téléchargement.

Chapitre 1 Introduction

- 1. Les objectifs du livre 15
 - 1.1 Décrire les nouvelles fonctionnalités SQL Server 2014 15
 - 1.2 Décrire d'autres fonctionnalités et combattre les idées reçues 17
- 2. L'organisation du livre 18

Chapitre 2 Les différents composants des moteurs

- 1. Introduction 19
- 2. La configuration réseau du serveur :
la couche communication et les protocoles 20
 - 2.1 La configuration réseau 21
 - 2.1.1 Le masquage d'une instance SQL Server sur le réseau 21
 - 2.1.2 Le cryptage des communications 22
 - 2.2 Les protocoles réseau 23
 - 2.2.1 La mémoire partagée 25
 - 2.2.2 Les canaux nommés 26
 - 2.2.3 TCP/IP 26
- 3. Les différents services 33
 - 3.1 Le service de base de données SQL Server 35
 - 3.1.1 La configuration système du service SQL Server 36
 - 3.1.2 La configuration des fonctionnalités AlwaysON
et Filestream 37
 - 3.1.3 La configuration des options de démarrage 37
 - 3.1.4 La connexion administrateur dédiée 39
 - 3.2 Le service SQL Server Agent 41
 - 3.3 Le service SQL Server Browser 42
 - 3.4 Le service SQL Writer 43

2 **SQL Server 2014**

Optimisez l'exploitation de vos bases de données

3.5	Les services optionnels	43
3.5.1	La recherche de texte intégral	43
3.5.2	Distributed Replay	44
3.6	Un point sur les pare-feu	44
4.	Le SQLOS	45
4.1	Présentation	45
4.2	Les différentes composantes	46
4.3	L'architecture NUMA	47
4.3.1	Le NUMA matériel et le NUMA logiciel	47
4.3.2	Le nœud NUMA et la configuration TCP/IP	50
5.	La mémoire	51
5.1	Présentation	52
5.1.1	Les composants	52
5.1.2	Les différents espaces mémoire	54
5.1.3	L'allocation de mémoire	56
5.2	La configuration	57
5.2.1	La quantité de mémoire allouée	57
5.2.2	AWE	59
5.2.3	Le verrouillage des pages en mémoire	60
5.3	L'extension du pool de mémoires tampons	61
5.3.1	Présentation	61
5.3.2	La configuration de l'extension du pool de mémoires tampons	62
5.4	Le In-memory	64
6.	Les processeurs	64
6.1	Les planificateurs (schedulers) et les workers	64
6.1.1	Les planificateurs	64
6.1.2	Les tâches, les threads et les workers	65
6.1.3	Le Scheduler Monitor	66
6.2	L'hyper-threading	67
6.3	L'affinité de CPU	68
6.3.1	La configuration	69
6.3.2	Le transfert de planificateur	71
6.3.3	L'indicateur de trace 8002	72
6.3.4	Synthèse sur l'affinité de CPU	72
6.4	Le parallélisme	73

- 7. Les entrées-sorties 74
 - 7.1 Les pages et les extensions 75
 - 7.1.1 Le contenu d'une page 75
 - 7.1.2 Les pages système 77
 - 7.2 L'écriture des pages sur disque 79
- 8. La clé principale de service 83
- 9. Conclusion 84

Chapitre 3
Le In-Memory

- 1. Introduction 85
 - 1.1 Comment Hekaton accélère-t-il les traitements ? 86
 - 1.2 Les prérequis 87
 - 1.3 L'intégration dans SQL Server 87
- 2. La durabilité : un point sur le stockage 88
 - 2.1 La création d'un groupe de fichiers 88
 - 2.2 Les fichiers de données 91
 - 2.2.1 Les data files 91
 - 2.2.2 Les delta files 92
 - 2.2.3 Les accès aux fichiers 92
 - 2.3 Considérations sur le sous-système disque 94
- 3. Les tables optimisées en mémoire 95
 - 3.1 La création d'une table en mémoire 95
 - 3.2 La structure d'un enregistrement 100
 - 3.3 Les index 101
 - 3.3.1 Les index de hachage 101
 - 3.3.2 Les range index 105
 - 3.4 Les statistiques de distribution 107
 - 3.4.1 La création et la mise à jour manuelles 108
 - 3.4.2 Les statistiques et les plans d'exécution
des procédures stockées compilées 108
 - 3.5 La gestion de la mémoire 111

4 **SQL Server 2014**

Optimisez l'exploitation de vos bases de données

4.	La gestion des transactions	112
4.1	Les modes d'isolation	113
4.1.1	Les modes d'isolation compatibles	113
4.1.2	L'option MEMORY_OPTIMIZED_ELEVATE_ TO_SNAPSHOT	114
4.2	Le journal des transactions	116
4.3	Les instructions DML et la durée de vie de l'enregistrement	120
4.3.1	L'ajout de données	120
4.3.2	La suppression de données	121
4.3.3	La validation	122
5.	Les procédures stockées compilées	122
5.1	Le cycle de vie	123
5.1.1	La création	123
5.1.2	La modification	126
5.1.3	La suppression	126
5.2	Le plan d'exécution	126
5.3	Quelques limitations	127
6.	L'aide à la migration	129
6.1	La collecte des données	130
6.1.1	Le jeu d'éléments de collecte de performances de transaction	130
6.1.2	Les rapports	131
6.2	Le Conseiller d'optimisation de la mémoire	135
6.3	Le Conseiller compilation native de procédure stockée	139
7.	Conclusion	143

Chapitre 4 **Les outils clients**

1.	Introduction	145
2.	Management Studio	146
2.1	L'installation	147
2.2	L'Explorateur d'objets	148
2.2.1	L'inscription d'une instance de l'explorateur d'objets	148
2.2.2	Le volet Détails de l'Explorateur d'objets	149
2.3	L'éditeur de texte et de requête	150

- 2.4 La personnalisation de l'environnement 152
 - 2.4.1 Les raccourcis-clavier 152
 - 2.4.2 Le codage couleur de la barre d'état 153
 - 2.4.3 Le contrôle de l'exécution de la requête 154
- 2.5 L'Explorateur de solutions 155
- 3. Le gestionnaire de configuration SQL Server 156
 - 3.1 La configuration et la gestion des services SQL Server 156
 - 3.2 La configuration des protocoles réseau 157
- 4. Le Profiler 158
 - 4.1 L'identification de problèmes de performances 158
 - 4.1.1 La mise à jour automatique des statistiques de distribution 158
 - 4.1.2 Les recompilations 159
 - 4.1.3 Les locks et les deadlocks 159
 - 4.2 Le profiler et DTA 160
 - 4.3 Les traces Replay 162
 - 4.3.1 La capture de la trace sur l'instance source 162
 - 4.3.2 La relecture de la trace 162
 - 4.4 Les procédures stockées système 164
- 5. Les événements étendus 167
 - 5.1 La liste des objets 167
 - 5.2 Les cibles des informations de collecte 168
 - 5.2.1 La cible Histogram 169
 - 5.2.2 La cible de type ring_buffer 171
 - 5.2.3 La cible event_file 172
 - 5.3 Le paramétrage de la session 175
- 6. La collecte de données 178
 - 6.1 L'implémentation 178
 - 6.1.1 La mise en place de la base centrale 178
 - 6.1.2 La mise en place des compteurs de collecte 179
 - 6.2 Le fonctionnement 182
 - 6.3 Les rapports 183
- 7. Les outils natifs en ligne de commande 184
 - 7.1 SQLCMD 184
 - 7.1.1 La connexion à une instance 185
 - 7.1.2 La connexion avec une connexion administrateur dédiée 185
 - 7.1.3 Le lancement de commandes T-SQL 186

6 **SQL Server 2014**

Optimisez l'exploitation de vos bases de données

7.2	PowerShell	186
7.2.1	Avantages de PowerShell	186
7.2.2	PowerShell et SQL Server : les méthodes	187
8.	L'assistant Paramétrage du moteur de base de données	187
8.1	La charge de travail	188
8.2	La relecture de la charge de travail	188
8.3	L'analyse du résultat et l'application des recommandations	191
8.3.1	L'analyse du résultat	191
8.3.2	L'application des recommandations	192
8.4	L'utilitaire DTA	193
8.5	L'impact sur les performances	193
8.5.1	La fonctionnalité serveur de test/serveur de production	193
8.5.2	Les index hypothétiques	194
9.	La boîte à outils	194
9.1	L'analyseur de performances	195
9.1.1	Présentation	195
9.1.2	La collecte temps réel	196
9.1.3	Les ensembles de collecteurs de données	198
9.1.4	Les rapports	199
9.2	Le Best Practices Analyzer	200
9.2.1	L'installation et le lancement	201
9.2.2	La configuration et l'analyse du scan	202
9.3	SQLDIAG	203
9.3.1	Le fichier de configuration	204
9.3.2	La collecte	206
9.3.3	L'analyse des résultats	208
9.4	SQLIO	211
9.4.1	La configuration et les paramètres	211
9.4.2	L'exploitation des résultats	213
9.4.3	Les tests de performances et la comparaison	214
10.	Conclusion	215

Chapitre 5
Les bases de données

- 1. Introduction 217
- 2. Les bases de données système 217
 - 2.1 La base de données Master 218
 - 2.2 La base de données Resource 218
 - 2.3 La base de données Tempdb 219
 - 2.4 La base de données msdb 222
 - 2.4.1 L'accès aux informations 223
 - 2.4.2 La gestion des historiques 223
 - 2.5 La base de données model 226
- 3. Les bases de données utilisateurs 226
 - 3.1 Les fichiers et les groupes de fichiers 226
 - 3.1.1 Les groupes de fichiers de données 227
 - 3.1.2 Les groupes de fichiers spéciaux 229
 - 3.1.3 Les fichiers de données 230
 - 3.1.4 Le journal des transactions 232
 - 3.2 La configuration des fichiers 239
 - 3.2.1 Les propriétés des fichiers 239
 - 3.2.2 La taille des fichiers : l'augmentation et la réduction 240
 - 3.3 Les bases de données à relation contenant-contenu 247
 - 3.3.1 Présentation 247
 - 3.3.2 Zoom sur le classement 248
 - 3.4 Les modes de récupération 250
 - 3.4.1 Le processus de recouvrement 253
 - 3.4.2 L'option FAST RECOVERY 255
 - 3.5 Les options de base de données 255
 - 3.5.1 Les options de statistiques 255
 - 3.5.2 La réduction automatique de la base de données 256
 - 3.5.3 Les modes de récupération 256
 - 3.5.4 Les options de récupération 256
 - 3.5.5 La durabilité retardée 257
- 4. Conclusion 258

Chapitre 6 **La sécurité**

1. Introduction	259
2. La sécurité des accès	259
2.1 Les modes d'authentification	260
2.1.1 L'authentification Windows	260
2.1.2 L'authentification mixte	262
2.2 Les rôles et les privilèges	263
2.2.1 Le niveau serveur	263
2.2.2 Le niveau base de données	267
2.3 La sécurité des bases de données à relation contenant-contenu	268
2.3.1 Les utilisateurs de base de données à relation contenant-contenu	268
2.3.2 Le cryptage des bases de données à relation contenant-contenu	270
2.4 La surface d'exposition	270
2.4.1 La configuration de la surface d'exposition	271
2.4.2 L'option Trustworthy	272
3. La sécurité des données	275
3.1 Les solutions de cryptage proposées par Windows	275
3.1.1 EFS	275
3.1.2 BitLocker	276
3.2 L'implémentation du cryptage par SQL Server	276
3.2.1 Les différents outils	276
3.2.2 La hiérarchie dans SQL Server	280
3.3 La protection des données	286
3.3.1 Les procédures stockées, les fonctions et les vues	286
3.3.2 Le niveau colonne	287
3.3.3 Le niveau base : TDE	296
3.4 La protection des fichiers de sauvegarde	301
4. Conclusion	303

Chapitre 7**L'audit et les changements de données**

1. Introduction	305
2. SQL Server Audit	305
2.1 La mise en place	306
2.2 L'objet d'audit	307
2.3 Les actions et les groupes d'actions	316
2.4 L'association entre les objets d'audit et une base de données	319
2.5 La sécurisation du système d'audit	321
2.6 Un point sur les performances	325
3. La capture de données modifiées	325
3.1 La mise en place	326
3.2 Les tables de changements	328
3.3 Les fonctions d'exploitation des changements	329
3.4 Les travaux de collecte et de nettoyage	329
3.4.1 Le travail de capture	329
3.4.2 Le travail de purge	330
3.5 La capture	330
3.5.1 Le journal des transactions	330
3.5.2 Le paramétrage de la capture	331
3.5.3 Le fonctionnement de la capture	332
3.6 La purge des changements	332
3.6.1 Le paramétrage du nettoyage	332
3.6.2 Le fonctionnement du nettoyage	333
3.7 Les performances	333
4. Change Tracking	334
4.1 La mise en place	335
4.2 Les tables système	336
4.3 La purge	338
4.4 La restitution des données	339
4.4.1 Les fonctions système	339
4.4.2 Le mode d'isolation SNAPSHOT	340
5. Conclusion	341

Chapitre 8**La maintenance des bases de données**

1. Introduction	343
2. Les sauvegardes et les restaurations	344
2.1 Les sauvegardes complètes, différentielles et du journal de transactions	344
2.1.1 Les sauvegardes complètes.	344
2.1.2 Les sauvegardes différentielles.	346
2.1.3 Les sauvegardes du journal de transactions	347
2.2 Les sauvegardes et les restaurations partielles (fichiers et groupes de fichiers).	348
2.2.1 Les différences entre le mode simple et le mode complet	348
2.2.2 La répartition des données.	349
2.2.3 La sauvegarde en mode simple	350
2.2.4 La restauration en mode simple	352
2.2.5 La sauvegarde en mode complet	354
2.2.6 La restauration en mode complet	354
3. Les index	362
3.1 Les différents types d'index	363
3.1.1 Les index cluster et les index non cluster	363
3.1.2 Les index filtrés	366
3.1.3 Les index en ligne	366
3.1.4 L'index columnstore.	373
3.2 La fragmentation.	374
3.2.1 La détection	377
3.2.2 La correction.	379
3.3 Les DMV : des aides à la création.	381
4. Les statistiques de distribution	383
4.1 La composition	384
4.1.1 L'échantillon et l'histogramme	385
4.1.2 La fréquence, la densité et la sélectivité	385
4.2 Les différents types de statistiques	386
4.2.1 Les statistiques filtrées.	386
4.2.2 Les statistiques de résumé de chaîne.	387
4.2.3 Les statistiques sur les colonnes calculées	387
4.2.4 Les statistiques et les objets temporaires	388

- 4.3 La consultation 391
 - 4.3.1 DBCC SHOW_STATISTICS 391
 - 4.3.2 sys.stats 393
 - 4.3.3 STATS_DATE() 394
 - 4.3.4 sys.dm_db_stats_properties() 394
- 4.4 La création 394
 - 4.4.1 La création implicite 395
 - 4.4.2 La création automatique 396
 - 4.4.3 La création manuelle 396
- 4.5 La maintenance 397
 - 4.5.1 La maintenance automatique 398
 - 4.5.2 La maintenance manuelle 402
- 4.6 Les optimisations 405
 - 4.6.1 Les indicateurs de trace 405
 - 4.6.2 Les statistiques incrémentales 407
- 5. L'intégrité de la base 408
 - 5.1 Les types de corruptions 409
 - 5.2 L'option CHECKSUM de la commande de sauvegarde 410
 - 5.3 La commande DBCC CHECKDB :
la vérification de l'intégrité de la base de données 411
 - 5.3.1 Description du processus 412
 - 5.3.2 L'espace disque nécessaire 415
 - 5.3.3 L'interprétation de la sortie 416
 - 5.3.4 Les options de réparation 417
 - 5.4 L'autocorrection des pages dans les sessions
de mise en miroir et AlwaysON 418
- 6. Conclusion 418

Chapitre 9
Les very large databases (VLDB)

- 1. Introduction 421
- 2. Le partitionnement 422
 - 2.1 L'implémentation 423
 - 2.1.1 La clé de partitionnement 423
 - 2.1.2 La fonction de partition 424

2.1.3	Le schéma de partition.	426
2.1.4	La création d'une table partitionnée	427
2.2	Les index partitionnés.	428
2.3	Les opérations sur les partitions.	430
2.3.1	SPLIT	431
2.3.2	MERGE.	434
2.3.3	SWITCH.	437
2.3.4	Les performances	440
3.	La compression.	442
3.1	Les différents modes	442
3.1.1	Le mode ROW	442
3.1.2	Le mode PAGE	443
3.2	Le choix des données à compresser	443
3.2.1	L'impact sur les performances	443
3.2.2	Les gains attendus	445
3.2.3	L'implémentation.	445
3.2.4	La modification des données d'une table compressée	451
4.	L'index columnstore.	452
4.1	Le stockage en colonne	452
4.1.1	Présentation	452
4.1.2	La structure de l'index columnstore	454
4.1.3	La construction	455
4.2	La gestion des données	457
4.2.1	L'insertion de données	457
4.2.2	La suppression de données.	461
4.3	Un point sur les performances	461
4.3.1	La compression de données	461
4.3.2	L'élimination de segments	462
4.3.3	Le mode batch	465
5.	La vérification des corruptions	468
6.	Conclusion	469

Chapitre 10

Les performances

1. Introduction	471
2. Les principales sources de contentions	472
2.1 La CPU et les planificateurs	472
2.1.1 Le parallélisme	472
2.1.2 La compilation ou la recompilation	474
2.1.3 Les spinlocks	476
2.2 La mémoire	477
2.2.1 La surveillance de la quantité de mémoire totale utilisée	478
2.2.2 La mémoire et les requêtes	478
2.2.3 La surveillance de l'allocation mémoire pour les requêtes : l'identification des contentions	481
2.3 La base tempDB	482
2.3.1 Une source de contentions	482
2.3.2 Les optimisations	483
2.4 La concurrence d'accès	489
2.4.1 La problématique des lectures incorrectes, répétées et fantômes	489
2.4.2 La gestion des conflits	490
2.4.3 Les verrous	491
2.4.4 Les modes d'isolation	493
2.5 Le journal des transactions	504
2.5.1 Les limites du log manager	505
2.5.2 La détection des contentions	505
2.5.3 Les transactions à durabilité différée	507
3. Le plan d'exécution des requêtes	510
3.1 La génération du plan d'exécution	511
3.1.1 Les passerelles de compilation	511
3.1.2 Les niveaux d'optimisation	512
3.2 La mise en cache et la réutilisation du plan	513
3.3 La capture du plan d'exécution	517
3.3.1 Les plans estimés et les plans réels	517
3.3.2 La récupération du plan d'exécution réel	518

14 _____ SQL Server 2014

Optimisez l'exploitation de vos bases de données

3.4	La réutilisation du plan : le parameter sniffing.....	519
3.4.1	Le problème	519
3.4.2	Les solutions.....	520
4.	Le nouvel estimateur de cardinalité	521
4.1	L'ancien estimateur vs le nouvel estimateur	522
4.2	L'utilisation du nouvel estimateur	523
4.2.1	La configuration.....	523
4.2.2	La détection de l'utilisation du nouvel estimateur.....	525
4.3	L'impact sur les performances	526
4.3.1	L'estimation des filtres.....	527
4.3.2	La high value.....	528
5.	Conclusion	530
	Index	531

Chapitre 6

La sécurité

1. Introduction

La sécurité des données est un enjeu capital. Une base de données peut être amenée à stocker des données très sensibles, confidentielles.

L'implémentation de la sécurité des données au sein d'une base se décline à deux niveaux. Tout d'abord le premier niveau consiste à sécuriser les accès en définissant quels utilisateurs accèdent à quelles données, tout en contrôlant le type d'accès. C'est la mise en place des comptes utilisateurs et des autorisations.

Puis le second niveau consiste à sécuriser les données elles-mêmes afin de se prémunir contre toutes intrusions : c'est le cryptage.

Ce chapitre ne reprend pas les fondamentaux de l'implémentation des différents aspects de la sécurité sous SQL Server mais propose plutôt un focus sur certains enjeux critiques de la sécurité et sur les nouveautés introduites dans ce domaine par la version 2014 du moteur.

2. La sécurité des accès

La sécurité des accès consiste à définir d'une part la population disposant de l'autorisation de se connecter à l'instance et aux bases de données, et d'autre part les droits et donc les actions permises pour chaque utilisateur connecté. La première étape concerne donc également l'authentification. Une personne qui se connecte à une instance doit être authentifiée par l'instance. Cette section commence par faire un rappel des méthodes d'authentification proposées par le moteur avant de mettre en avant les nouvelles autorisations apportées par la version 2014.

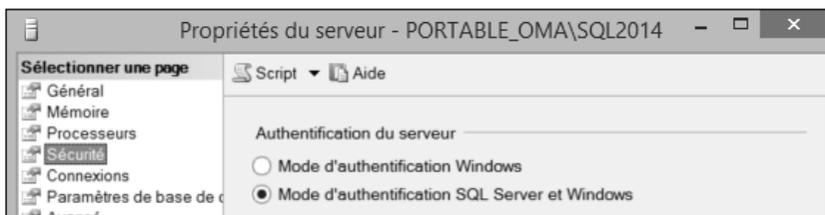
La sécurité des bases de données à relation contenant contenu et enfin la configuration de la surface d'exposition sont ensuite traitées.

2.1 Les modes d'authentification

Le moteur SQL Server propose deux modes d'authentification : le mode mixte, qui autorise les comptes SQL Server et les comptes Windows à se connecter à l'instance, et le mode Windows seulement qui comme son nom l'indique ne permet les connexions que par le biais de comptes Windows.

Le choix du mode d'authentification se fait durant l'installation du moteur et peut être changé par la suite.

► Pour changer le mode d'authentification d'une instance, depuis Management Studio, faites un clic droit sur l'instance et sélectionnez **Propriétés** puis choisissez le nœud **Sécurité** dans la fenêtre **Propriétés du serveur**. Choisissez le mode d'authentification souhaité puis cliquez sur **OK**. Un message vous avertit que l'instance doit être redémarrée pour que le changement soit effectif.



Changement du mode d'authentification d'une instance

2.1.1 L'authentification Windows

L'authentification Windows est une authentification intégrée qui récupère les informations du compte Windows de l'utilisateur pour se connecter, en s'appuyant sur l'architecture de domaine Active Directory. Il est impossible dans ce mode d'authentification de spécifier explicitement un compte et un mot de passe Windows. C'est forcément le compte de l'utilisateur courant qui est utilisé. C'est pour cela qu'on lui donne également le nom d'authentification intégrée.

Lorsque l'on choisit le mode d'authentification Windows, la connexion à l'instance via un compte SQL Server est impossible. Pendant l'installation, le compte "sa" (login SQL Server disposant de tous les droits, automatiquement créé lors de l'installation d'une instance) est désactivé et un mot de passe lui est attribué par le programme d'installation afin de sécuriser le compte.

NTLM vs Kerberos

Deux protocoles d'authentification peuvent être utilisés pour se connecter à une instance SQL Server : NTLM et Kerberos. NTLM est le protocole historique, basé sur un compte utilisateur et un mot de passe et utilisant un mécanisme de stimulation/réponse (challenge-response). Kerberos est plus sécurisé mais nécessite néanmoins certains prérequis. Si l'un des prérequis suivants n'est pas respecté, l'authentification Kerberos échoue et c'est NTLM qui est utilisé :

- Le client doit choisir le mode d'authentification Windows.
- Le client et le serveur SQL Server doivent se trouver dans le même domaine ou dans des domaines approuvés.
- Le SPN du service doit être créé sur le compte de démarrage du service SQL Server (voir le chapitre Les différents composants des moteurs - Les différents services pour en savoir plus sur les SPN). Lorsque le client demande à se connecter à un serveur SQL Server, il s'adresse au contrôleur de domaine et demande un accès au service SQL en l'identifiant par son SPN. Le contrôleur interroge alors le catalogue Active Directory pour récupérer le compte qui contient ce SPN, c'est-à-dire le compte de démarrage du service SQL Server. Et s'il n'en trouve pas, il renvoie le compte machine du serveur. Le client se présente alors avec un ticket d'authentification au service SQL. Ce dernier ne peut pas déchiffrer lorsqu'il démarre avec un compte autre que le compte machine (compte système local). Et dans ce cas l'authentification Kerberos échoue.
- Le serveur SQL doit être correctement enregistré dans le DNS car c'est le nom complet du serveur (FQDN) qui est utilisé dans le SPN.

■ Remarque

Le choix du protocole se fait automatiquement. Si les prérequis nécessaires à Kerberos sont respectés, c'est ce protocole qui est utilisé, sinon c'est NTLM sous certaines conditions.

Les groupes Windows

Dans la pratique, plutôt que d'ajouter directement les comptes Windows des utilisateurs dans l'instance SQL Server afin de leur donner les accès, il est préférable d'ajouter des groupes Windows, apportant une souplesse à l'utilisation. Ainsi, les droits peuvent être attribués à des groupes plutôt qu'à des utilisateurs individuels. En outre, pour autoriser un nouvel utilisateur ou supprimer les droits d'un utilisateur existant, il suffit de l'ajouter dans le bon groupe Windows, sans avoir à intervenir au niveau de l'instance SQL Server.

■ Remarque

Et depuis SQL Server 2012, il est (enfin !) possible d'affecter un schéma par défaut à un groupe Windows.

2.1.2 L'authentification mixte

L'authentification mixte comprend l'authentification Windows, en permettant en plus l'authentification SQL Server, c'est-à-dire l'authentification par le biais de comptes et mots de passe SQL Server. Lorsque l'on choisit ce mode d'authentification, la première chose à faire est de définir un mot de passe fort pour le compte "sa", le compte administrateur par défaut.

■ Remarque

Le compte "sa" est le compte historique de l'administrateur par défaut de toutes les instances SQL Server, quelle que soit la version. Bien connu, il est recommandé de lui affecter un mot de passe fort et de changer ce mot de passe régulièrement pour sécuriser le compte au maximum, voire de le désactiver.

Lorsque l'on se connecte dans ce mode d'authentification, il faut préciser le compte SQL Server et son mot de passe dans la chaîne de connexion, ce qui peut poser problème dans des scripts ou batchs qui contiennent alors ces informations de connexion en clair. Par ailleurs, ces informations par défaut transitent en clair sur les réseaux, et nécessitent dans certains cas la mise en place du cryptage des communications (voir le chapitre Les différents composants des moteurs - Les différents services).

Moins sécurisée que l'authentification Windows et donc non recommandée, l'authentification SQL Server reste néanmoins très utilisée car elle apporte les avantages suivants :

- La connexion Windows entre domaines non approuvés est impossible. La connexion SQL Server peut être utilisée dans ce cas.
- L'authentification Windows permet également la connexion à une instance SQL Server à partir de clients installés sur des plateformes non Windows, pour lesquelles l'utilisation de compte Windows est impossible (client Linux par exemple).
- Elle permet enfin la prise en charge d'applications ne supportant pas l'authentification Windows.

2.2 Les rôles et les privilèges

Les droits sont donnés aux utilisateurs par le biais de rôles et de privilèges déclinés au niveau serveur (instance) ou base de données. Voyons les nouveautés dans ce domaine apportées par la version 2014 du moteur SQL Server.

2.2.1 Le niveau serveur

Trois nouvelles autorisations de niveau serveur apparaissent avec SQL Server 2014.

SELECT ALL USER SECURABLES

Cette autorisation permet au compte qui en bénéficie d'accéder à l'ensemble des données des bases de données qui lui sont accessibles. Jusqu'à présent, il fallait explicitement attribuer les droits de lecture à l'utilisateur (user) associé au compte (login) dans chacune des bases pour lui en donner l'accès. Il suffit dorénavant de donner le privilège **SELECT ALL USER SECURABLES** au login.

Mais ce nouveau privilège offre également une possibilité qui était attendue de longue date. Considéré non plus comme une autorisation mais comme une restriction, et associé à l'autorisation **CONTROL SERVER**, ce privilège peut donner la possibilité de créer des comptes d'administrateur de bases de données ayant tous les droits, sauf celui de visualiser les données elles-mêmes. Les données les plus confidentielles ou sensibles sont alors soumises à un meilleur contrôle : même les administrateurs de bases de données n'y ont pas accès.

► Pour créer un compte ayant tous les droits sauf celui de consulter les données, créez tout d'abord un login (Windows ou SQL Server) au niveau de l'instance en utilisant la commande suivante :

```
CREATE LOGIN test_dba WITH PASSWORD = 'T35t_db#';
```

Puis mettez en place les droits sur le login en vous appuyant sur les privilèges **CONTROL SERVER** et **SELECT ALL USER SECURABLES** :

```
GRANT CONTROL SERVER TO test_dba;  
GO  
DENY SELECT ALL USER SECURABLES TO test_dba;  
GO
```

Ainsi, il est dorénavant possible de créer un rôle de serveur fixe disposant des droits mentionnés précédemment, puis de peupler ce rôle avec les comptes des administrateurs de bases de données. On a donc la possibilité de créer ainsi le rôle DBA, capable de toutes les actions d'administration mais ne pouvant pas accéder aux données elles-mêmes.

Attention néanmoins dans ce dernier cas : le compte d'administrateur dispose effectivement de tous les droits d'administration, y compris celui... de donner les droits de lecture des données à un autre compte ou rôle que lui-même ! Rien ne l'empêche en effet d'octroyer le droit **SELECT ALL USER SECURABLE** au rôle dont il fait partie, ce qu'il ne peut pas faire sur son propre compte.

Ce levier est donc un moyen d'éviter que l'administrateur de bases de données n'accède à des données sensibles de manière intempestive, mais ne l'interdit pas dans l'absolu. Un système d'audit des accès ou des changements de privilèges viendra donc compléter l'implémentation de ces droits dans ce contexte (voir le chapitre L'audit et les changements de données).

Créez deux comptes SQL Server dba1 et dba2 ainsi qu'un rôle de serveur fixe db_admins. Dans un cas, vous allez donner les autorisations directement sur le compte dba1, dans le deuxième cas, vous affecterez les autorisations au rôle db_admins et ajouterez le compte dba2 en tant que membre de ce rôle :

```
Use master
GO
--Création du premier utilisateur dba1 et mise en place des droits
CREATE LOGIN dba1 WITH PASSWORD = 'dba', CHECK_POLICY=OFF;
GO
GRANT CONTROL SERVER TO dba1;
GO
DENY SELECT ALL USER SECURABLES TO dba1;
GO

--Création d'un rôle de serveur fixe et affectation des droits
CREATE SERVER ROLE db_admins;
GO
GRANT CONTROL SERVER TO db_admins;
GO
DENY SELECT ALL USER SECURABLES TO db_admins;
GO

--Création du deuxième utilisateur et ajout dans le rôle
CREATE LOGIN dba2 WITH PASSWORD = 'dba', CHECK_POLICY=OFF;
GO
ALTER SERVER ROLE db_admins ADD MEMBER dba2
GO
```

00 % < <

Résultats

Commande(s) réussie(s).

Création d'un login et d'un rôle type administrateur de bases de données