

Guida del Management Pack di Microsoft System Center per SQL Server 2017+

Microsoft Corporation

Data di pubblicazione: novembre 2017

Il team di Operations Manager invita gli utenti a inviare commenti e suggerimenti sul Management Pack all'indirizzo [sqlmpsfeedback@microsoft.com](mailto:sqlmpsfeedback@microsoft.com).

Copyright

Il documento viene fornito "com'è". Le informazioni e le opinioni espresse nel presente documento, inclusi gli URL e altri riferimenti a siti Web, possono essere soggette a modifiche senza preavviso. L'utente accetta di usarle a proprio rischio.

Alcuni esempi usati in questo documento vengono forniti a scopo puramente illustrativo e sono fittizi. Nessuna associazione reale o connessione è intenzionale o può essere desunta.

Il presente documento non implica la concessione di alcun diritto di proprietà intellettuale relativo ai prodotti Microsoft. È possibile copiare e usare questo documento come riferimento interno. È possibile modificare questo documento per fini di riferimento interno.

© 2017 Microsoft Corporation. Tutti i diritti sono riservati.

Microsoft, Active Directory, Windows e Windows Server sono marchi del gruppo di società Microsoft.

Tutti gli altri nomi di prodotti e società citati nel presente documento sono marchi dei rispettivi proprietari.

Sommario

[Guida del Management Pack di Microsoft System Center per SQL Server 2017+ 4](#_Toc504575605)

[Cronologia delle modifiche 4](#_Toc504575606)

[Introduzione 8](#_Toc504575607)

[Novità 9](#_Toc504575608)

[Configurazioni supportate 9](#_Toc504575609)

[Ambito del Management Pack 10](#_Toc504575610)

[Prerequisiti 10](#_Toc504575611)

[File in questo Management Pack 12](#_Toc504575612)

[Scopo del Management Pack 12](#_Toc504575613)

[Tipi di monitoraggio 12](#_Toc504575614)

[Scenari di monitoraggio 16](#_Toc504575615)

[Rollup dello stato 17](#_Toc504575616)

[Configurare il Management Pack 18](#_Toc504575617)

[Configurazione obbligatoria 18](#_Toc504575618)

[Procedura consigliata: creare un Management Pack per le personalizzazioni 19](#_Toc504575619)

[Come abilitare l'opzione Proxy agente 20](#_Toc504575620)

[Come importare un Management Pack 20](#_Toc504575621)

[Configurazione del monitoraggio 20](#_Toc504575622)

[Configurazione della sicurezza 35](#_Toc504575623)

[Visualizzare informazioni nella console di Operations Manager 60](#_Toc504575624)

[Viste e dashboard (generici) indipendenti dalla versione 60](#_Toc504575625)

[Viste di SQL Server 61](#_Toc504575626)

[SQL Server Reporting 62](#_Toc504575627)

[Appendice: Problemi noti e risoluzione dei problemi 65](#_Toc504575628)

# Guida del Management Pack di Microsoft System Center per SQL Server 2017+

Questa guida è basata sulla versione 7.0.0.0 RTM del Management Pack per Microsoft SQL Server 2017+.

## Cronologia delle modifiche

| **Data di rilascio** | **Modifiche** |
| --- | --- |
| Novembre 2017 (versione 7.0.0.0 RTM) | * Sono stati introdotti vari miglioramenti e correzioni di bug. |
| Ottobre 2017 (versione 6.7.65.0 RC1) | * Il Management Pack è stato nuovamente implementato per abilitare il monitoraggio di SQL Server 2017 e delle versioni future di SQL Server * È stato ridotto il numero di file nel Management Pack * È stata rimossa una dipendenza nel Management Pack per i dashboard di Microsoft SQL Server * È stata introdotta una serie di correzioni e miglioramenti di funzionalità, prestazioni e stringhe di visualizzazione |
| Giugno 2017 (versione 6.7.60.0 RC0) | * È stato implementato il monitoraggio Always On in Windows e Linux * Sono stati implementati flussi di lavoro di latenza del disco * È stata aggiunta la nuova regola di avviso "Accesso non riuscito" per l'evento SQL Server 18456 * È stato aggiunto il supporto per le credenziali di Active Directory nella modalità senza agenti in Windows * Problema risolto: informazioni di percorso file diverse da "sys.master\_files" e "sysfiles" generano un errore quando i file di database secondari del gruppo di disponibilità si trovano in un percorso diverso * Problema risolto: i flussi di lavoro non riescono a connettersi a un'istanza quando è abilitato solo il protocollo Memoria condivisa * Problema risolto: i criteri utente personalizzati eliminati in precedenza da SQL Server in Windows/Linux restano disponibili in System Center Operations Manager * Sono stati introdotti vari miglioramenti al Management Pack |
| Maggio 2017 (versione 6.7.55.0 CTP3) | * Monitoraggio AlwaysOn per Windows: sono stati implementati flussi di lavoro di base simili al Management Pack per SQL Server 2016 * Il cluster SQL ora è supportato in modalità di monitoraggio mista (in precedenza era supportato solo in modalità di monitoraggio senza agenti) * Il Management Pack ora può usare le credenziali di autenticazione di SQL Server nelle modalità di monitoraggio agente/mista (in precedenza era possibile usare le credenziali SQL solo in modalità di monitoraggio senza agenti) * È stata implementata l'esecuzione di attività * È stato implementato il monitoraggio di SQL Server Agent * È stato implementato il monitoraggio dei pool di risorse * Sono stati aggiunti vari monitoraggi e regole delle prestazioni per il monitoraggio delle tabelle ottimizzate per la memoria * È stato implementato il monitoraggio dei criteri utente personalizzati * Sono state migliorate le query SQL per l'individuazione del database * Problema risolto: avvisi "Sostituzione parametro non riuscita durante la creazione dell'avviso per la modifica dello stato del monitoraggio" per i flussi di lavoro dei contenitori tabella ottimizzata per la memoria * Sono stati risolti problemi degli agenti di lettura log * È stato risolto un problema della configurazione SPN * Sono stati aggiornati e corretti gli articoli della Knowledge Base e le stringhe visualizzate |
| Febbraio 2017 (versione 6.7.40.0 CTP2) | * È stato implementato il modulo di mapping per i dati di individuazione; sono state migliorate le query e le origini dati * È stato implementato il supporto per il cookdown completo di tutte le individuazioni in Linux e Windows * È stato implementato il monitoraggio Log shipping * Sono stati implementati nuovi monitoraggi e nuove regole:   + Monitoraggio "Conformità Service Pack"   + Monitoraggio "Servizio Windows SQL Server"   + Monitoraggio "Utilizzo CPU (%)"   + Monitoraggio "Servizio SQL Server(database)"   + Monitoraggio "Criteri di integrità database (Critico)"   + Monitoraggio "Criteri di integrità database (Avviso)"   + Monitoraggio "WMI Health" (Integrità WMI)   + Regola "Memoria usata dalle tabelle (MB)"   + Regola "Memoria usata dagli indici (MB)"   + Regola "MSSQL per Windows: Utilizzo CPU del motore di database (%)"   + Regola "Il motore di database di SQL Server è stato riavviato" * Sono state implementate nuove regole per le prestazioni Spazio database:   + MSSQL: spazio allocato per i database non usato (MB)   + MSSQL: totale spazio disponibile dei database (%)   + MSSQL: spazio disponibile esterno dei database (MB)   + MSSQL: Totale spazio disponibile   + nel log delle transazioni del database (%)   + MSSQL: totale spazio disponibile dei database (MB)   + MSSQL: spazio allocato per i database usato (MB)   + MSSQL: spazio allocato per i database (MB) * Sono state implementate nuove classi:   + Filegroup FILESTREAM di database di SQL Server su <piattaforma>   + Contenitore di dati con ottimizzazione per la memoria del database di SQL Server su <piattaforma>   + Criterio utente personalizzato di SQL Server generico   + Criterio utente personalizzato di SQL Server su <piattaforma>   + Criterio critico database di SQL Server Database su <piattaforma>   + Criterio avviso database di SQL Server Database su <piattaforma>   + Gruppo Pool di risorse di SQL Server su <piattaforma>   + Pool di risorse di SQL Server generico   + Pool di risorse di SQL Server su <piattaforma>   + Pool di risorse interno di SQL Server su <piattaforma>   + Pool di risorse utente di SQL Server su <piattaforma>   + Pool di risorse definite dall'utente di SQL Server su <piattaforma> * Sono stati implementati un nuovo monitoraggio e una nuova regola per gli oggetti FILESTREAM:   + MSSQL in <piattaforma>: Totale spazio disponibile nel filegroup FILESTREAM di database (MB)   + MSSQL in <piattaforma>: Totale spazio disponibile nel filegroup FILESTREAM di database (%) * Sono state implementate nuove regole per le prestazioni per i filegroup di dati ottimizzati per la memoria:   + MSSQL per Windows: Totale spazio disponibile nel filegroup di dati ottimizzati per la memoria del database (MB)   + MSSQL in Windows: Totale spazio disponibile nel filegroup di dati con ottimizzazione per la memoria del database (%) * È stato implementato il modulo "MSSQL-Lettura log" * È stato implementato il monitoraggio Raccolta eventi per Linux e Windows (oltre 400 flussi di lavoro) * Sono state implementate le individuazioni, i rollup e le icone per le nuove classi e sono state aggiornate le icone per Filegroup e per le classi figlio * Sono stati implementati tutti i contatori XTP (oltre 200 flussi di lavoro) * È stato implementato il monitoraggio percentuale bucket vuoti nell'indice hash * È stato implementato il monitoraggio lunghezza media delle catene di righe nei bucket di hash * È stato implementato il servizio "Utilità di avvio del daemon filtri full-text di SQL"; la proprietà "NetworkName" è stata aggiunta al motore di database locale; è stato eseguito il refactoring della struttura di cartelle di monitoraggio Windows * È stata aggiunta la classe "Database locale" in Windows * L'architettura è stata migliorata: le classi "Windows.DBEngine" e "Windows.LocalDBEngine" sono state divise * È stata migliorata la registrazione degli errori * È stata migliorata la gestione degli errori (problemi di connettività) * L'individuazione "LocalDiscoverySeed" è stata reimpostata e ora supporta i nomi estesi e non supporta WoW64 * Aggiunta guidata monitoraggio è stata aggiornata: sono stati risolti problemi del layout, il multithreading e le prestazioni sono state migliorate ed è stato implementato il caricamento in background * Sono stati aggiornati e corretti articoli della Knowledge Base e stringhe visualizzate; è stato unificato il modello di denominazione dei flussi di lavoro * Sono stati corretti gli avvisi per le classi gestiti da un agente locale * Sono stati risolti i problemi di Smart Connect associati ai dati nella cache (connessione WMI) * Sono stati corretti i moduli Linux in modo che ignorino Smart Connect * Problema risolto: la regola "Transazioni totali al secondo" viene eseguita due volte in un intervallo * Problema risolto: SQL Server negli oggetti di database di Windows può essere rilevato più volte * Problema risolto: i filegroup non vengono rilevati in un'istanza SQL Express * Problema risolto: in alcune situazioni Aggiunta guidata monitoraggio non rileva che l'attività di test connessione è stata completata * Problema risolto: gli oggetti di database già rilevati risultano non rilevati se lo stato del database viene convertito in "Offline" |
| Dicembre 2016 (versione 6.7.18.0 CTP1) | Versione originale del Management Pack |

## Introduzione

Contenuto della sezione:

* [Novità](#z875296f2d58e4444bc3f0350fcd3e7ff)
* [Configurazioni supportate](#_Supported_Configurations_1)
* [Ambito del Management Pack](#_Management_Pack_Scope)
* [Prerequisiti](#_Prerequisites)
* [File in questo Management Pack](#z1)

### Novità

Questo Management Pack include le nuove funzionalità seguenti:

* Questo Management Pack è destinato al monitoraggio di SQL Server 2017 e di tutte le versioni successive di SQL Server.
* Funzionamento multipiattaforma: il monitoraggio SQL può essere eseguito nei sistemi operativi Windows e Linux.
* Oltre alla consueta modalità di monitoraggio con agenti ora sono disponibili le modalità di monitoraggio senza agenti e mista. Si noti che il monitoraggio con agenti e il monitoraggio misto sono disponibili solo per SQL Server in Windows.
* È stato implementato un nuovo report per la previsione dello spazio usato dai file di database. Il report include una raccolta di dati riguardanti lo spazio usato dai file di database e la quantità di spazio disponibile. Il report include anche una previsione dello spazio che verrà usato dai file di database. Per altre informazioni, vedere la sezione [SQL Server Reporting](#_SQL_Server_2017).

### Configurazioni supportate

La tabella seguente illustra in dettaglio le configurazioni supportate per il Management Pack:

|  |  |
| --- | --- |
| **Configurazione** | **Supportato** |
| Sistemi operativi | Windows Server 2012  Windows Server 2012 R2  Windows Server 2016  Linux (Ubuntu 16.04 x64) |
| SQL Server | SQL Server 2017 |
| SCOM | System Center Operations Manager 2012 R2  System Center Operations Manager 2016 |
| Server cluster | Sì |
| Monitoraggio con agenti | Solo nel sistema operativo Windows |
| Monitoraggio senza agenti | Sì |
| Ambiente virtuale | Sì |

Nota

Le versioni di SQL Server localizzate (non in lingua inglese) non sono supportate.

L'aggiornamento dalla versione precedente del Management Pack non è supportato. Eseguire un'installazione pulita.

Le condivisioni file SMB sono supportate come opzione di archiviazione. Per altre informazioni, vedere l'articolo [Descrizione del supporto per i file di database di rete in SQL Server](https://support.microsoft.com/en-us/kb/304261).

### Ambito del Management Pack

Il Management Pack per Microsoft SQL Server abilita il monitoraggio delle funzionalità seguenti:

* Motori di database SQL Server (edizioni supportate: Evaluation, Developer, Express)
* Database SQL Server (inclusi filegroup, file di dati e file di registro delle transazioni)
* Gruppi di disponibilità Always On di SQL Server
* Tabelle ottimizzate per la memoria SQL Server (OLTP in memoria di SQL Server)

Importante

Si consiglia di eseguire il monitoraggio di non più di 50 database e 150 file di database per agente System Center Operations Manager, così da evitare picchi di utilizzo della CPU che potrebbero influire sulle prestazioni dei server monitorati.

Nota

Per un elenco completo degli scenari di monitoraggio supportati da questo Management Pack, vedere la sezione "[Scenari di monitoraggio](#_Monitoring_Scenarios)".

Per altre informazioni e istruzioni dettagliate sull'installazione e la configurazione, vedere la sezione "[Configurare il Management Pack](#_Mandatory_Configuration_1)" di questa guida.

### Prerequisiti

In base alla procedura consigliata, è opportuno importare il Management Pack di Windows o Linux Server per il sistema operativo in uso. I Management Pack Server consentono di monitorare gli aspetti del sistema operativo che influiscono sulle prestazioni dei computer che eseguono SQL Server, ad esempio la capacità del disco, le prestazioni del disco, l'uso della memoria, l'uso della scheda di rete e le prestazioni del processore.

Nota

Per questo Management Pack non è necessario un gruppo di gestione di Operations Manager dedicato. È necessaria l'installazione di .NET Framework 4.5 o versione successiva.

Importante

I flussi di lavoro di Linux seguenti sono temporaneamente non disponibili perché non ricevono i dati necessari da SQL Server:

Regole:

* MSSQL in Linux: Totale spazio disponibile nel filegroup di dati ottimizzati per la memoria del database (MB)
* MSSQL in Linux: Totale spazio disponibile nel filegroup di dati ottimizzati per la memoria del database (%)
* MSSQL in Linux: Totale spazio disponibile nel filegroup FILESTREAM di database (%)
* MSSQL in Linux: Totale spazio disponibile nel filegroup FILESTREAM di database (MB)
* MSSQL in Linux: Totale spazio disponibile nel filegroup del database (%)
* MSSQL in Linux: Totale spazio disponibile nel filegroup del database (MB)
* MSSQL in Linux: Spazio disponibile allocato nel filegroup del database (%)
* MSSQL in Linux: Spazio disponibile allocato nel filegroup del database (MB)
* MSSQL in Linux: Spazio disponibile esterno del database (MB)
* MSSQL in Linux: Spazio disponibile allocato del database (MB)
* MSSQL in Linux: Totale spazio disponibile nel log delle transazioni del database (%)
* MSSQL on Linux: Spazio allocato usato del database (MB)
* MSSQL in Linux: Totale spazio disponibile nel database (%)
* MSSQL in Linux: Totale spazio disponibile nel database (MB)
* MSSQL in Linux: Spazio allocato per i database (MB)

Monitoraggi:

* Spazio disponibile nel database
* Modifica percentuale spazio del database
* Spazio disponibile log delle transazioni (%)
* Spazio disponibile filegroup FileStream database

### File in questo Management Pack

Il Management Pack per Microsoft SQL Server include i file seguenti:

* Microsoft.SQLServer.Core.Library.mp
* Microsoft.SQLServer.Core.Views.mp
* Microsoft.SQLServer.Visualization.Library.mpb
* Microsoft.SQLServer.Linux.Views.mp
* Microsoft.SQLServer.Linux.Discovery.mpb
* Microsoft.SQLServer.Linux.Monitoring.mpb
* Microsoft.SQLServer.Windows.Views.mpb
* Microsoft.SQLServer.Windows.Discovery.mpb
* Microsoft.SQLServer.Windows.Monitoring.mpb

**Nota**



Oltre alla presente guida la distribuzione del Management Pack include una guida alla configurazione e personalizzazione dei dashboard SQL Server e un'appendice con informazioni sugli oggetti e i flussi di lavoro del Management Pack.

## Scopo del Management Pack

Contenuto della sezione:

* [Tipi di monitoraggio](#_Monitoring_Types)
* [Scenari di monitoraggio](#_Monitoring_Scenarios)
* [Rollup dello stato](#_How_Health_Rolls)

Nota

Per informazioni dettagliate sulle individuazioni, le regole e i monitoraggi contenuti nel Management Pack, vedere l'appendice della guida "Microsoft SQL Server Management Pack Objects and Workflows" (Oggetti e flussi di lavoro del Management Pack di Microsoft SQL Server).

### Tipi di monitoraggio

Questo Management Pack offre tre tipi di monitoraggio, descritti di seguito.

#### Monitoraggio con agente locale

Quando viene specificato tramite l'agente SCOM, il monitoraggio viene eseguito in base alla variante standard nota come monitoraggio con agente locale. Non sono necessarie azioni aggiuntive per eseguire il monitoraggio con agente locale; è sufficiente che nel server sia installato Microsoft Monitoring Agent. Se è necessario eseguire il monitoraggio con privilegi limitati, configurare l'ambiente in base alle istruzioni specificate nel corrispondente [articolo](#_Local_Agent_Monitoring) della sezione Ambienti con privilegi limitati.

#### Monitoraggio senza agenti

Il monitoraggio senza agenti viene eseguito da server Management o server gateway mappati sul pool di monitoraggio SQL Server (vedere la sezione [Configurare il pool di monitoraggio di SQL Server](#_Configure_SQL_Server)). Sono supportate sia l'autenticazione di SQL Server sia l'autenticazione di Windows. Per configurare il monitoraggio senza agenti, nella scheda Creazione scegliere il modello Microsoft SQL Server 2017+. Aggiungere le istanze con l'[Aggiunta guidata monitoraggio](#_Configure_Agentless_Monitoring_2). Se è necessario eseguire il monitoraggio con privilegi limitati, configurare l'ambiente in base alle istruzioni specificate nel corrispondente [articolo](#_Agentless_Monitoring) della sezione Ambienti con privilegi limitati.

**Importante**

Le regole seguenti non sono attive se l'istanza di SQL Server su Windows viene monitorata senza agenti:

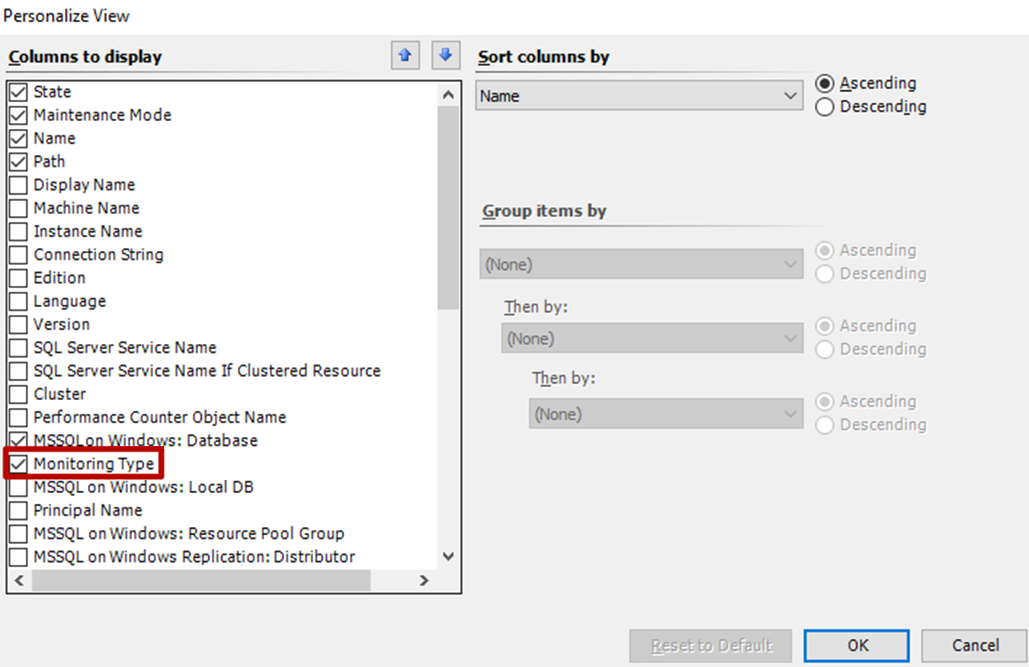
* MSSQL in Windows: il motore degli avvisi è stato arrestato a causa di errori irreversibili del log eventi locale
* MSSQL in Windows: un processo SQL non è stato completato correttamente
* MSSQL in Windows: non è possibile eseguire il passaggio del processo perché il caricamento del sottosistema non è riuscito
* MSSQL in Windows: l'agente è sospetto. Non è stata ricevuta alcuna risposta negli ultimi minuti
* MSSQL in Windows: non è stato possibile avviare SQL Server Agent
* MSSQL in Windows: l'avvio della chiusura automatica di SQL Server Agent è in corso
* MSSQL in Windows: un passaggio di un processo ha causato un'eccezione nel sottosistema
* MSSQL in Windows: SQL Server Agent non riesce a connettersi a SQL Server
* MSSQL in Windows: non è possibile riaprire il log eventi locale

#### Monitoraggio misto

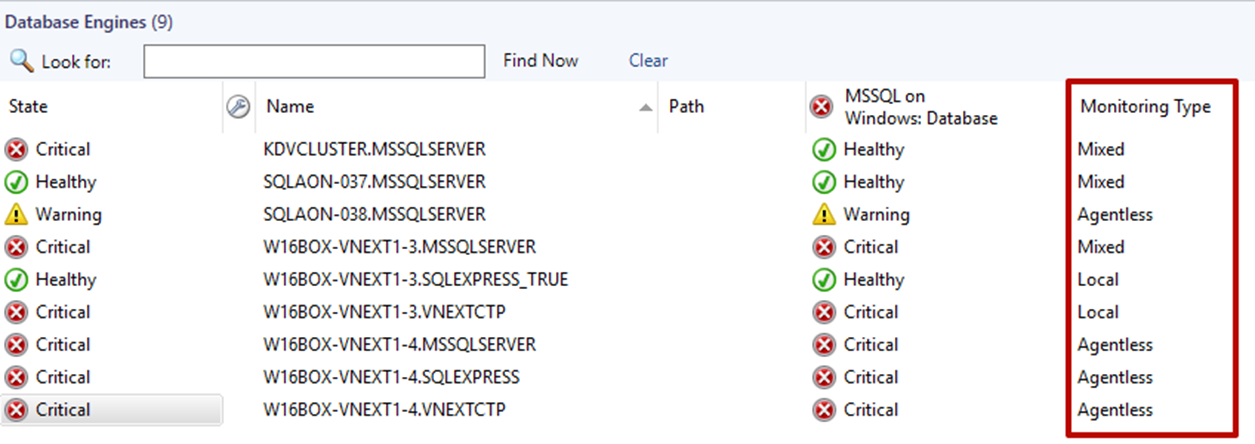
Il monitoraggio misto è destinato ai casi in cui si vuole trasferire il monitoraggio dall'agente a un pool SCOM. Questa modalità di monitoraggio è simile al monitoraggio senza agenti ma non richiede la configurazione manuale delle stringhe di connessione. È possibile abilitare la modalità di monitoraggio mista tramite override (per informazioni dettagliate, vedere la [sezione](#_Enable_Mixed_Monitoring) corrispondente). Quando si abilita il monitoraggio misto l'agente SCOM rileva in locale solo il valore di inizializzazione di SQL Server. Tutti gli altri flussi di lavoro vengono eseguiti dal pool. I dettagli sulla configurazione di individuazione del pool di monitoraggio di SQL Server sono disponibili nella sezione [Configurare il pool di monitoraggio di SQL Server](#_Configure_SQL_Server). Se è necessario eseguire il monitoraggio con privilegi limitati, configurare l'ambiente in base alle istruzioni specificate nel corrispondente [articolo](#_Mixed_Monitoring) della sezione Ambienti con privilegi limitati.

#### Visualizzare i tipi di monitoraggio correnti

Per visualizzare i tipi di monitoraggio attualmente usati in Operations Manager aprire la visualizzazione **Motori di database**, aprire il menu **Personalizza visualizzazione** e abilitare il parametro **Tipo di monitoraggio**:



La visualizzazione **Motori di database** completa ha un aspetto simile al seguente:



#### Casi speciali

Il Management Pack di SQL Server in Windows include varie regole che attivano avvisi quando nel log eventi dell'applicazione di Windows vengono visualizzati gli eventi seguenti:

* MSSQL in Windows: il motore degli avvisi è stato arrestato a causa di errori irreversibili del log eventi locale
* MSSQL in Windows: un processo SQL non è stato completato correttamente
* MSSQL in Windows: non è possibile eseguire il passaggio del processo perché il caricamento del sottosistema non è riuscito
* MSSQL in Windows: l'agente è sospetto. Non è stata ricevuta alcuna risposta negli ultimi minuti
* MSSQL in Windows: non è stato possibile avviare SQL Server Agent
* MSSQL in Windows: l'avvio della chiusura automatica di SQL Server Agent è in corso
* MSSQL in Windows: un passaggio di un processo ha causato un'eccezione nel sottosistema
* MSSQL in Windows: SQL Server Agent non riesce a connettersi a SQL Server
* MSSQL in Windows: non è possibile riaprire il log eventi locale

Per impostazione predefinita queste regole funzionano in modalità locale, ma non in modalità mista. Operations Manager non segnala o raccoglie eventi relativi a un agente nel registro eventi se questi vengono prodotti in un computer diverso dal computer locale. Se tuttavia si esegue l'override del parametro "AllowProxying" per queste regole la segnalazione viene abilitata.

**Nota:** l'abilitazione di questa opzione può causare l'esecuzione di codice remoto. Pertanto questo flag viene considerato come potenzialmente dannoso. Se non si è certi che il computer sia protetto, è consigliabile non eseguire l'override del parametro "AllowProxying".

### Scenari di monitoraggio

#### Individuazione di istanze del motore di database di SQL Server

Se si usa la modalità di monitoraggio con agente o mista il Management Pack individua automaticamente istanze autonome e cluster di SQL Server in tutti i sistemi gestiti che eseguono il servizio agente System Center Operations Manager.

#### Individuazione di database e monitoraggio dello stato

Per ogni motore di database gestito, i database vengono individuati e monitorati tramite una serie di regole e monitoraggi. Per l'elenco completo delle regole e dei monitoraggi specifici per i database, vedere l'appendice "Microsoft SQL Server Management Pack Objects and Workflows" (Oggetti e flussi di lavoro del Management Pack di Microsoft SQL Server).

È possibile applicare override all'individuazione per specificare un parametro "Exclude List" (in formato delimitato da virgole) per i nomi di database che devono essere ignorati dall'individuazione.

#### Monitoraggio dello spazio dei file di dati e dei file di log delle transazioni

Il Management Pack raccoglie un set di metriche per abilitare il monitoraggio dello spazio al livello di file, filegroup e database. È possibile usare i report per esaminare queste informazioni per più database e per intervalli di tempo lunghi.

Questa funzionalità supporta i tipi di supporto seguenti:

* Archiviazione locale (lettere delle unità e punti di montaggio)
* Volumi condivisi del cluster
* Condivisioni SMB
* BLOB di Azure

Per impostazione predefinita, il monitoraggio dello spazio è abilitato per tutti i livelli. Pertanto viene registrato un avviso solo quando tutti i file del filegroup risultano non integri. Se l'ambiente in uso è sensibile a qualsiasi carico supplementare, è possibile disabilitare il monitoraggio a livello di file e di filegroup.

#### Molti database nella stessa unità

Il monitoraggio dello spazio offerto da questo Management Pack può causare disturbo negli ambienti in cui numerosi database condividono lo stesso supporto ed è abilitata l'impostazione **Aumento automatico** per le dimensioni dei database. In questi casi viene generato un avviso per ogni database quando la quantità di spazio disponibile sul disco rigido raggiunga la soglia. Per ridurre il disturbo, disattivare i monitoraggi dello spazio per i file di dati e i file di log delle transazioni e usare il Management Pack del sistema operativo per monitorare lo spazio sul disco rigido.

#### Monitoraggio della latenza di archiviazione del database

Questo Management Pack raccoglie le metriche delle prestazioni "latenza lettura disco database (ms)" e "latenza scrittura disco database (ms)" per ogni database. Il Management Pack definisce anche due monitoraggi associati che registrano gli avvisi in caso di un peggioramento significativo delle prestazioni. Questi monitoraggi sono disabilitati per impostazione predefinita. Abilitare questi monitoraggi solo per database specifici e solo se necessario.

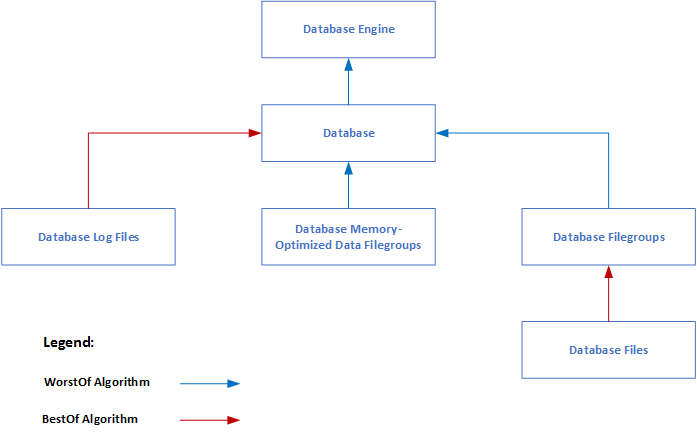
#### Sessioni bloccate

Il Management Pack definisce il monitoraggio "**Sessioni di blocco**" che consente di eseguire una query in ogni database di una sessione se questa viene bloccata per un periodo di tempo prolungato. Se viene rilevato un blocco che supera la soglia specificata, lo stato viene modificato e viene generato un avviso.

È possibile applicare una sostituzione per modificare il parametro **WaitMinutes**, che determina se il tempo di blocco della sessione bloccata va considerato o meno come eccessivo. Il valore predefinito di questo parametro è **un minuto**.

### Rollup dello stato

Nel diagramma riportato di seguito viene illustrato come gli stati di integrità degli oggetti vengano sottoposti a rollup in questo Management Pack.



## Configurare il Management Pack

In questa sezione vengono fornite le istruzioni per la configurazione e l'ottimizzazione del Management Pack.

Contenuto della sezione:

* [Configurazione obbligatoria](#_Mandatory_Configuration_2)
* [Procedura consigliata: creare un Management Pack per le personalizzazioni](#z2)
* [Come abilitare l'opzione Proxy agente](#z3)
* [Come importare un Management Pack](#_How_to_Import_1)
* [Configurazione della sicurezza](#_Monitoring_Configuration)
* [Configurazione del monitoraggio](#_Monitoring_Configuration_1)

### Configurazione obbligatoria

Per configurare il Management Pack per Microsoft SQL Server seguire questa procedura:

* Vedere la sezione "[Configurare il Management Pack](#_Mandatory_Configuration_1)" di questa guida.
* Concedere le autorizzazioni necessarie come descritto nella sezione "[Configurazione della sicurezza](#_Security_Configuration)" di questa guida.
* Abilitare l'opzione Proxy agente in tutti gli agenti installati nei server appartenenti al cluster. Non è necessario abilitare questa opzione per i server autonomi. Per altre informazioni sull'abilitazione dell'opzione Proxy agente, vedere la sezione "[Come abilitare l'opzione Proxy agente](#_How_to_Enable)" di questa guida.
* Importare il Management Pack.
* Associare i profili RunAs di SQL Server ad account che dispongono delle autorizzazioni appropriate. Per altre informazioni sulla configurazione di profili RunAs, vedere la sezione "[Come configurare i profili RunAs](#_How_to_configure_1)" di questa guida.
* Per garantire il corretto funzionamento del Management Pack verificare che le istanze di SQL Server consentano le connessioni tramite il protocollo TCP/IP e che il servizio SQL Server Browser venga sempre eseguito nel server host. Il protocollo TCP/IP è supportato per tutti gli scenari di monitoraggio. Si noti che il protocollo "Memoria condivisa" è supportato solo per gli scenari di monitoraggio con agente locale. Il protocollo "Named Pipes" non è supportato.

### Procedura consigliata: creare un Management Pack per le personalizzazioni

Il Management Pack per Microsoft SQL Server è bloccato per impedire la modifica delle impostazioni originali del file. Tuttavia è possibile creare personalizzazioni, ad esempio sostituzioni o nuovi oggetti di monitoraggio, e salvarle in un Management Pack diverso. Per impostazione predefinita, Operations Manager salva tutte le personalizzazioni nel Management Pack predefinito. È invece consigliabile creare un Management Pack separato per ogni Management Pack bloccato da personalizzare.

La creazione di un nuovo Management Pack per l'archiviazione delle sostituzioni presenta i seguenti vantaggi:

* Quando si crea un Management Pack per archiviare impostazioni personalizzate per un Management Pack bloccato, è utile basare il nome del nuovo Management Pack sul nome del Management Pack da personalizzare, ad esempio "Override di Microsoft SQL Server".
* La creazione di un nuovo Management Pack per l'archiviazione delle personalizzazioni di ogni Management Pack bloccato semplifica l'esportazione delle personalizzazioni da un ambiente di test a un ambiente di produzione. Semplifica anche l'eliminazione di un Management Pack, poiché è necessario eliminare eventuali dipendenze prima di eliminare un Management Pack. Se le personalizzazioni per tutti i Management Pack vengono salvate nel Management Pack predefinito ed è necessario eliminare un singolo Management Pack, sarà prima di tutto necessario eliminare il Management Pack predefinito, in modo da eliminare anche le personalizzazioni ad altri Management Pack.

Per altre informazioni sui Management Pack bloccati e non bloccati, vedere l'articolo [Management Pack Formats](http://go.microsoft.com/fwlink/?LinkId=108355) (Formati dei Management Pack). Per altre informazioni sulle personalizzazioni dei Management Pack e sul Management Pack predefinito, vedere l'articolo [About Management Packs](http://go.microsoft.com/fwlink/?LinkId=108356) (Informazioni sui Management Pack).

Come creare un nuovo Management Pack per le personalizzazioni

|  |
| --- |
| 1. Aprire la Console operatore e fare clic sul pulsante Amministrazione.  2. Fare clic con il pulsante destro del mouse su Management Pack, quindi scegliere Crea nuovo Management Pack.  3. Immettere un nome, ad esempio Personalizzazioni SQLMP, quindi fare clic su Avanti.  4. Fare clic su Crea. |

### Come abilitare l'opzione Proxy agente

Per abilitare l'**opzione Proxy agente** seguire questa procedura:

1. Aprire la Console operatore e fare clic sul pulsante **Amministrazione**.

2. Nel riquadro Amministratore fare clic su Gestito tramite agente.

3. Fare doppio clic su un agente nell'elenco.

4. Nella scheda Sicurezza selezionare Consenti a questo agente di funzionare come proxy e individuare oggetti gestiti sugli altri computer.

### Come importare un Management Pack

Per informazioni dettagliate sull'importazione di un Management Pack, vedere l'articolo [Come importare un Management Pack](#z3).

### Configurazione del monitoraggio

Questo Management Pack dispone di tre modalità di monitoraggio: con agente locale, senza agenti e misto. Questa sezione illustra come configurare il monitoraggio con questo Management Pack:

* [Configurare il monitoraggio di istanze cluster di SQL Server](#_Configure_Monitoring_of)
* [Configurare il monitoraggio senza agenti tramite Aggiunta guidata monitoraggio](#_Configure_Agentless_Monitoring_2)
* [Abilitare il monitoraggio misto per SQL Server in Windows tramite override](#_Configure_Agentless_Monitoring_1)
* [Configurare il pool di monitoraggio di SQL Server](#_Configure_SQL_Server)

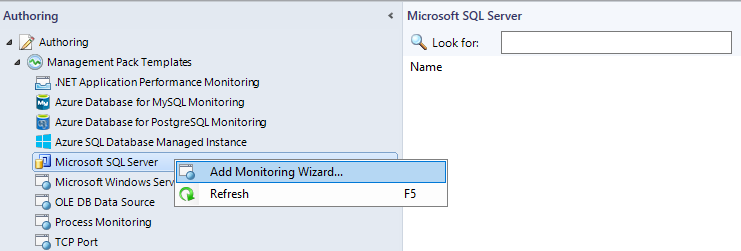
#### Configurare il monitoraggio di istanze cluster di SQL Server

Il Management Pack esegue il monitoraggio delle istanze cluster di SQL Server attivando flussi di lavoro dal pool di monitoraggio di SQL Server. Questo significa che il monitoraggio dei cluster di SQL Server non richiede nessuna configurazione particolare se si usa la modalità di monitoraggio senza agenti o mista. Quando invece si configura il monitoraggio locale assicurarsi che l'account azione dei server di gestione con mapping sul pool di monitoraggio di SQL Server disponga di autorizzazioni sufficienti per monitorare le istanze cluster. Per fare ciò seguire la procedura descritta nella [sezione](#_How_to_configure_1) corrispondente.

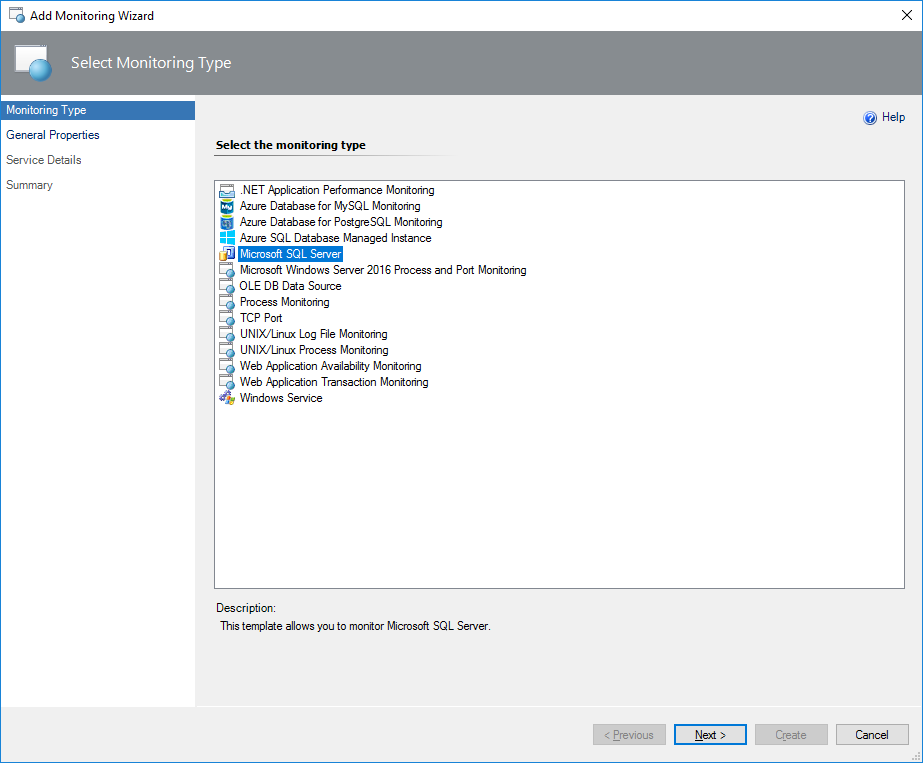
#### Configurare il monitoraggio senza agenti tramite Aggiunta guidata monitoraggio

Per iniziare il monitoraggio senza agenti di istanze di SQL Server seguire questa procedura:

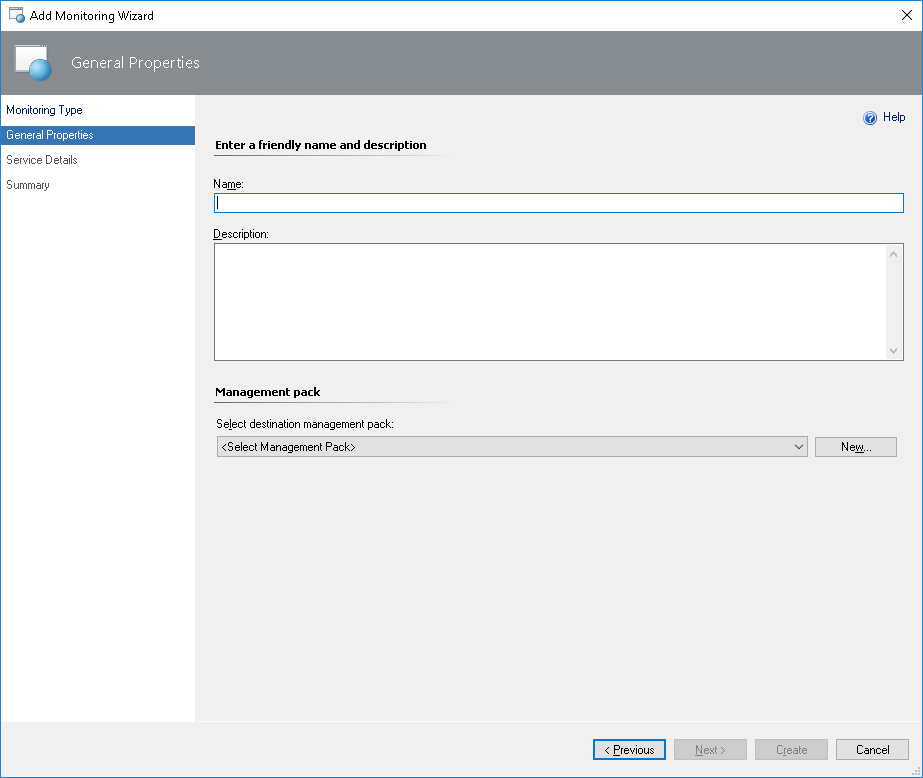
In Operations Manager passare a **Creazione e modifica** | **Modelli Management Pack**, fare clic con il pulsante destro del mouse su **Microsoft SQL Server** e scegliere **Aggiunta guidata monitoraggio**.

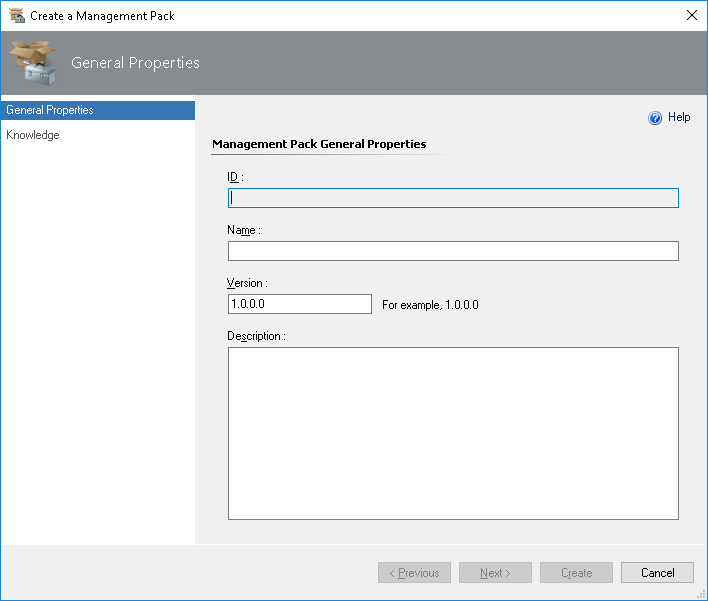


Nella finestra **Tipo di monitoraggio** selezionare **Microsoft SQL Server** e fare clic sul pulsante **Avanti**.

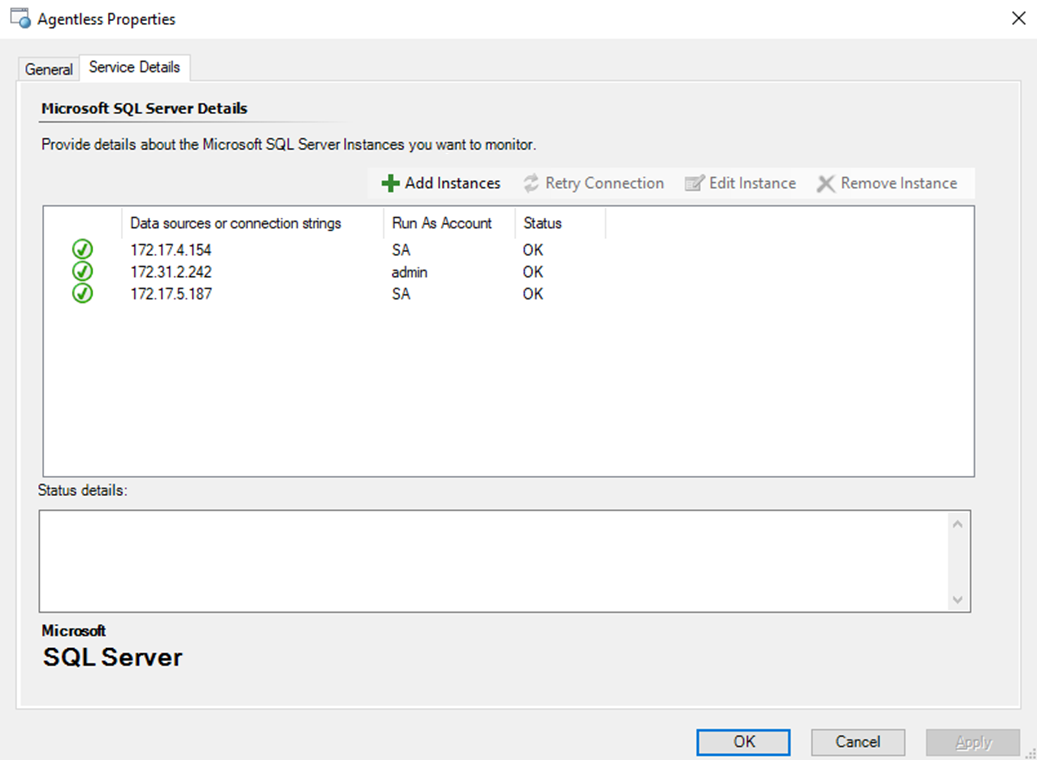


Nella finestra **Proprietà generali** immettere **Nome** e **Descrizione** del modello, quindi in **Seleziona Management Pack di destinazione** specificare dove verrà archiviato il modello.

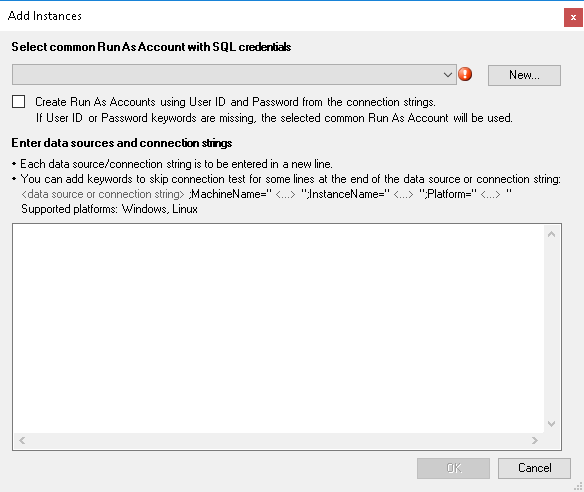


È anche possibile creare un nuovo Management Pack di destinazione facendo clic su **Nuovo**.  
  


Nella finestra **Dettagli servizio** specificare i dettagli delle istanze da monitorare.



Fare clic sul pulsante **Aggiungi istanza** per aggiungere le singole istanze da monitorare.



In questa finestra selezionare l'account RunAs comune creato in Operations Manager con le credenziali SQL appropriate. Quindi immettere le origini dati e/o le stringhe di connessione. Seguire le istruzioni specificate in questa finestra per evitare errori e test eccessivi della connessione.

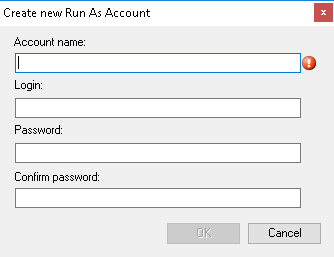
I dati devono essere immessi con il formato indicato negli esempi seguenti:

*172.31.2.133;MachineName="W12BOX-839";InstanceName="MSSQLSERVER";Platform="Windows"*

*172.31.2.133,50626;MachineName="W12BOX-839";InstanceName="SQLEXPRESS";Platform="Windows"*

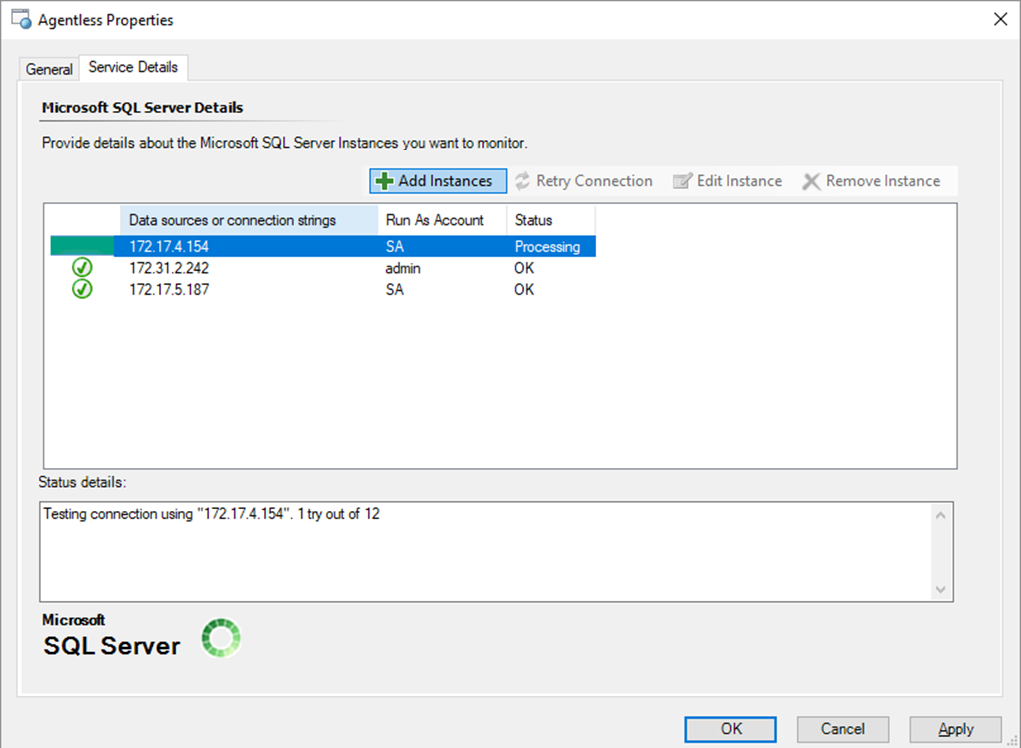
*172.17.5.115;MachineName="ubuntu";InstanceName="MSSQLSERVER";Platform="Linux"*

È anche possibile creare un nuovo account RunAs facendo clic sul pulsante **Nuovo**.



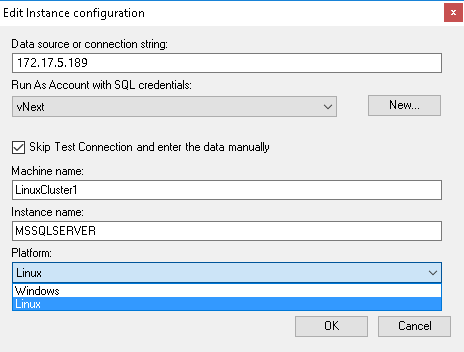
Nella finestra corrispondente immettere il nome del nuovo account RunAs e le credenziali del server SQL da sottoporre a monitoraggio.

Fare clic su **OK** nella finestra **Aggiungi istanza** per inviare i dati immessi.

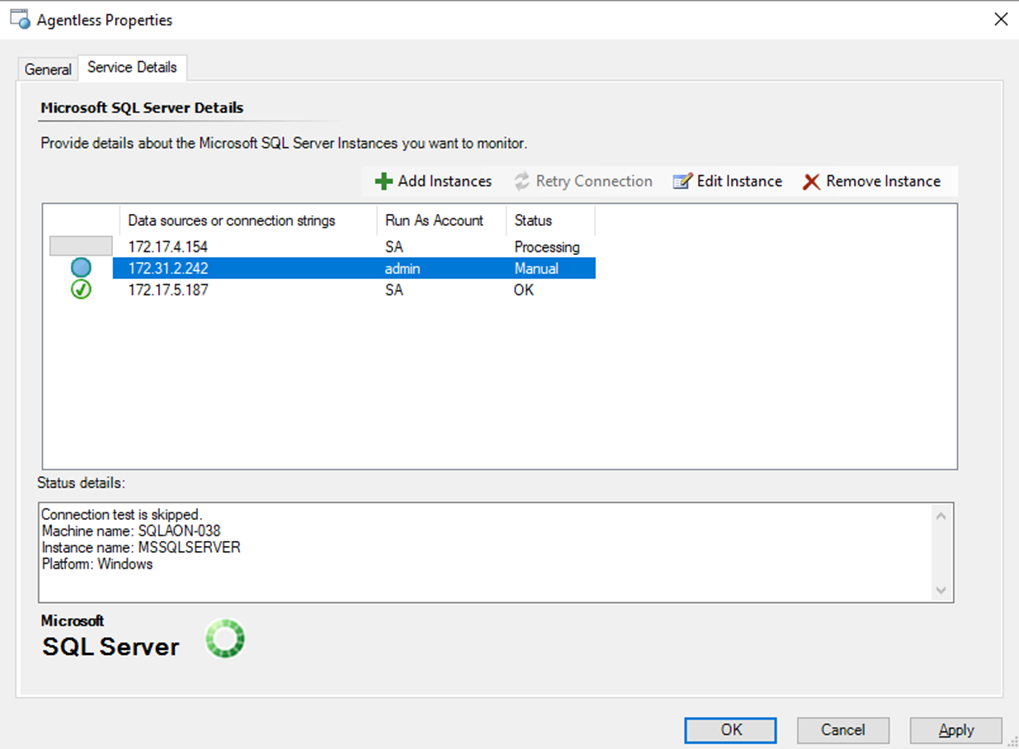


**Nota:** quando si aggiunge un'istanza basata su Linux il test della connessione non riesce se si specifica come stringa di connessione un indirizzo IP e il tipo di autenticazione è "Windows AD credentials" (Credenziali di Windows Active Directory). In questo caso specificare come stringa di connessione il nome del computer.

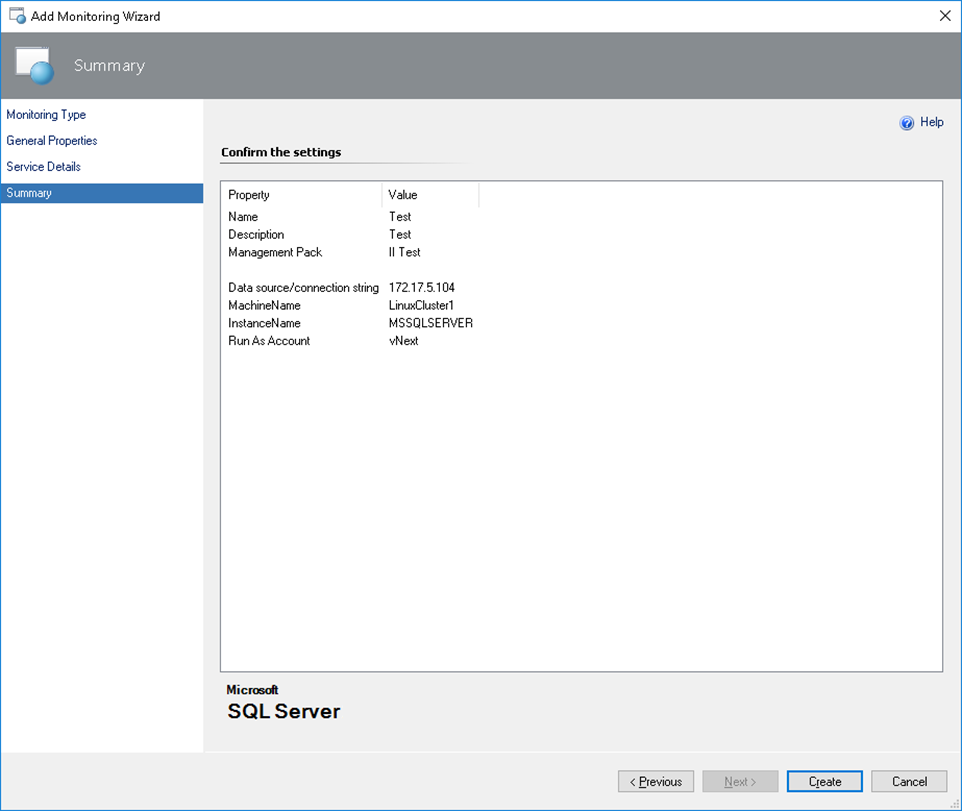
Quando viene completato il test della connessione è possibile visualizzare e modificare le proprietà dell'istanza aggiunta. Per farlo selezionare l'istanza e fare clic sul pulsante **Edit Instance** (Modifica istanza).



Per ignorare il test della connessione e immettere i dati manualmente selezionare la casella corrispondente in questa finestra. In questo caso lo stato dell'istanza verrà impostato su manuale.



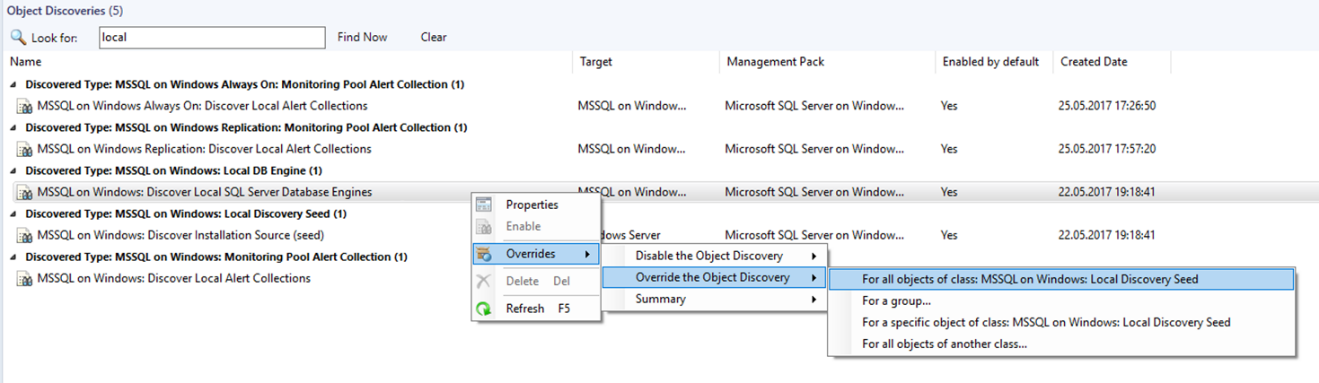
Nella finestra **Riepilogo** è possibile visualizzare le impostazioni di monitoraggio e confermarle facendo clic sul pulsante **Crea**.



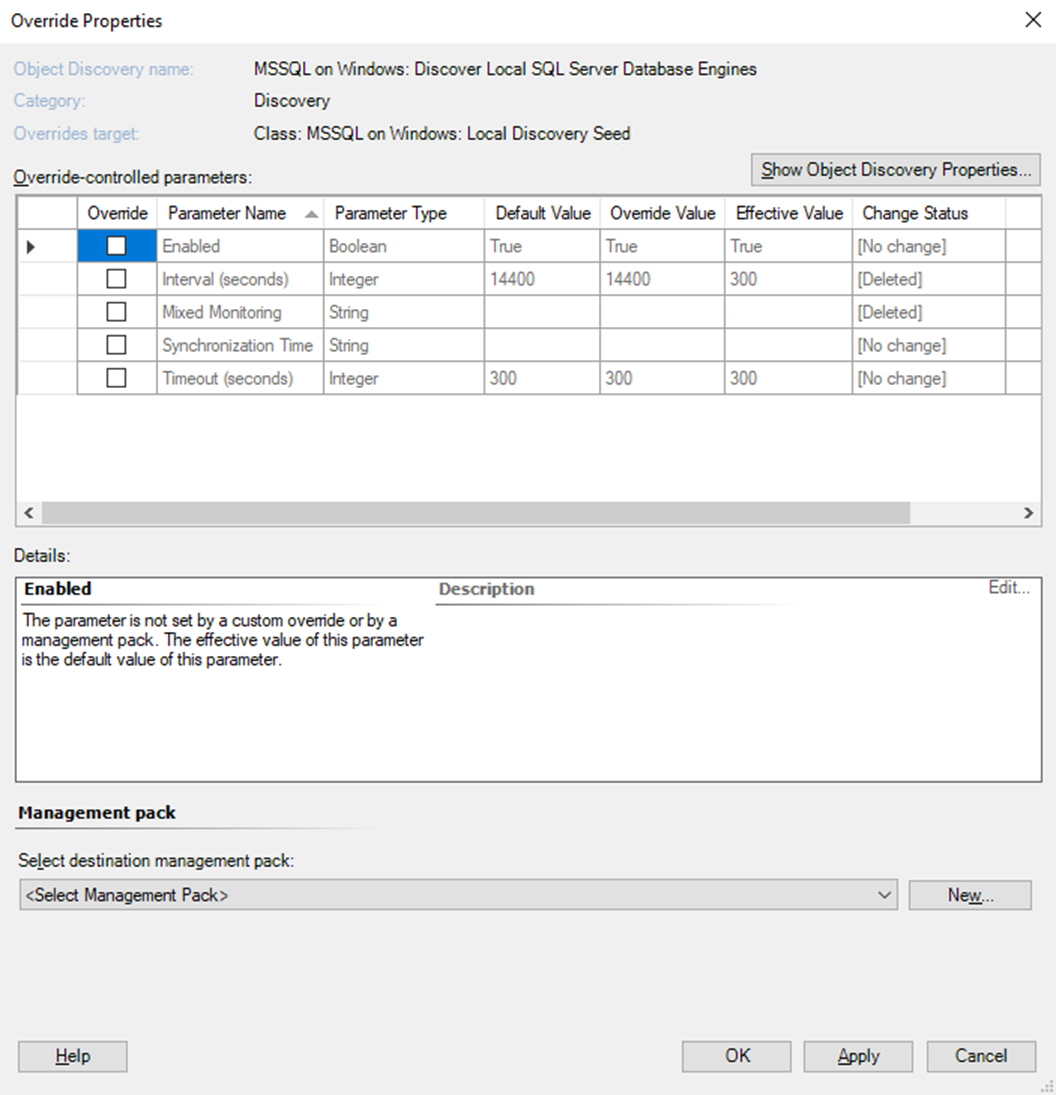
Dopo questa operazione viene creato il modello di monitoraggio.

#### Abilitare il monitoraggio misto per SQL Server in Windows tramite override

Per avviare il monitoraggio di istanze di SQL Server in modalità mista, in Operations Manager passare a **Creazione e modifica** | **Oggetti Management Pack**, selezionare **Individuazioni oggetti** e visualizzare l'individuazione oggetto **MSSQL: Discover Local SQL Database Engines on Windows (MSSQL: Individua motori di database SQL locali in Windows)**. Fare clic con il pulsante destro del mouse su questa individuazione e selezionare l'azione seguente: **Sostituzioni** > **Override the Object Discovery (Sostituisci individuazione utente)** > **Tutti gli oggetti della classe: MSSQL on Windows (MSSQL in Windows): Local Discovery Seed (Valore di inizializzazione individuazione locale)**.

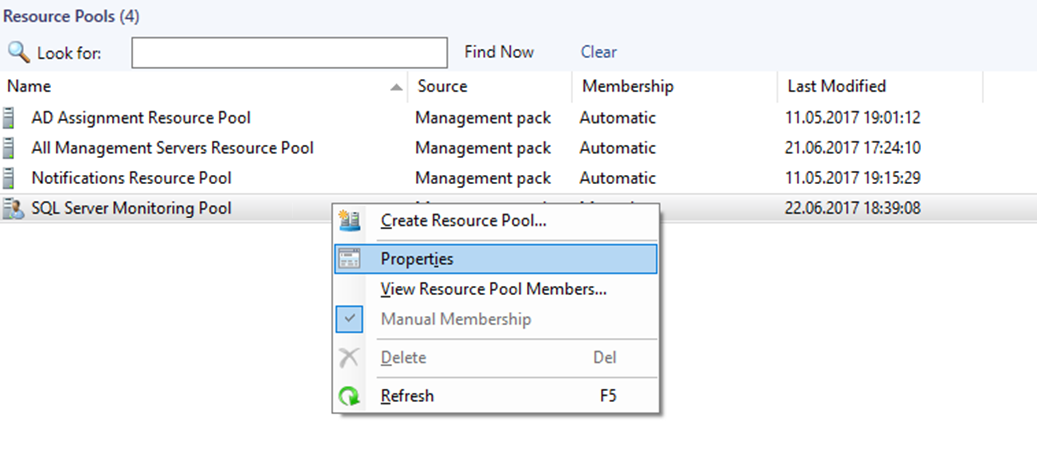


Viene visualizzata la finestra **Proprietà di sostituzione**. Abilitare la sostituzione per il parametro **Monitoraggio misto** e immettere nel campo **Valore di sostituzione** i nomi delle istanze per le quali impostare il monitoraggio senza agenti. I nomi delle istanze devono essere separati da virgole. Per aggiungere tutte le istanze immettere il carattere asterisco (\*) nel campo. Di conseguenza tutte le istanze, incluse quelle con lo stesso nome in server diversi, vengono monitorate nel pool in modalità mista.



#### Configurare il pool di monitoraggio di SQL Server

Il pool di monitoraggio è disponibile per la configurazione in Operations Manager. Per configurare il pool di monitoraggio selezionare **Amministrazione | Pool di risorse**, fare clic con il pulsante destro del mouse su **SQL Server Monitoring Pool** (Pool di monitoraggio SQL Server) nell'elenco Pool di risorse e selezionare l'opzione **Adesione manuale**. Selezionare **Proprietà**.



Viene visualizzata la finestra **SQL Server Monitoring Pool Properties** (Proprietà pool di monitoraggio SQL Server). In questa finestra selezionare la scheda **Appartenenza al pool**. Nella scheda fare clic sul pulsante **Aggiungi** per popolare il pool di monitoraggio.



È possibile configurare manualmente il pool di monitoraggio SQL Server aggiungendo gateway o server di gestione personalizzati.

### Configurazione della sicurezza

Questa sezione illustra come configurare la sicurezza per questo Management Pack.

Contenuto della sezione:

* [Profili RunAs](#_Run_As_Profiles)
* [Ambienti con privilegi limitati](#_Low-privilege_environments)

#### Profili RunAs

L'elenco dei profili RunAs è il seguente:

* Profilo RunAs Microsoft SQL Server Discovery: questo profilo è associato a tutte le individuazioni.
* Profilo RunAs Microsoft SQL Server Monitoring: questo profilo è associato a tutti i monitoraggi e le regole.
* Profilo RunAs Microsoft SQL Server: questo profilo è associato a tutte le attività.
* Profilo RunAs Microsoft SQL Server SQL Credentials: questo profilo viene usato per l'autenticazione nelle istanze di Microsoft SQL Server tramite le credenziali SQL.

Quando si usano le modalità di monitoraggio locale o mista, per impostazione predefinita tutte le individuazioni, i monitoraggi e le attività definiti nei Management Pack di SQL Server usano gli account definiti nel profilo RunAs "Account azione predefinito". Se l'account azione predefinito di un sistema specificato non ha le autorizzazioni necessarie per individuare o monitorare l'istanza di SQL Server, tale sistema può essere associato a credenziali più specifiche nei profili RunAs "Microsoft SQL Server…" che dispongono dell'accesso.

##### Come configurare i profili RunAs nelle modalità di monitoraggio locale e mista

Per configurare i profili RunAs, seguire uno degli scenari descritti di seguito:

1. L'account azione predefinito di SCOM è mappato all'account di sistema locale o a qualsiasi account utente di dominio, incluso nel gruppo Administrators locale nel sistema operativo dei computer monitorati. Si noti che l'account usato deve essere concesso con diritti di amministratore di sistema nelle istanze di SQL Server monitorate. A tal fine è necessario concedere i diritti di amministratore di sistema al gruppo locale BUILTIN\Administrators nell'elenco di accesso di sicurezza di SQL Server. In questo caso, il monitoraggio delle istanze di SQL Server verrà eseguito per impostazione predefinita, fatta eccezione per alcune configurazioni descritte di seguito. Seguire questa procedura per assicurarsi che tutti i requisiti siano soddisfatti: se si archiviano database di SQL Server in una condivisione file SMB, verificare che l'account azione predefinito disponga dei diritti descritti nella sezione [Ambienti con privilegi limitati](#_Low-privilege_environments) corrispondente.
2. L'account azione predefinito di SCOM è mappato all'account di sistema locale o all'account utente di dominio come nello scenario precedente, ma non è possibile concedere i diritti di amministratore di sistema a tale account, finché i criteri di sicurezza impediscono la concessione di tali diritti all'account azione predefinito di SCOM. Se i criteri di sicurezza consentono di concedere diritti di amministratore di sistema per un account utente di dominio separato, che verrà usato solo per l'avvio dei flussi di lavoro del Management Pack di SQL Server, eseguire i passaggi seguenti:
3. Creare un nuovo account utente di dominio e aggiungere l'account al gruppo Administrators locale su ogni server monitorato.
4. Concedere i diritti di amministratore di sistema a questo account in SQL Server.
5. Creare un nuovo account azione in SCOM ed eseguirne il mapping all'account utente di dominio creato in precedenza.
6. Eseguire il mapping del nuovo account azione a tutti i profili RunAs del Management Pack di SQL Server.
7. Se si archiviano database di SQL Server in una condivisione file SMB, verificare che l'account utente di dominio disponga dei diritti descritti nella sezione [Ambienti con privilegi limitati](#_Low-privilege_environments) corrispondente.
8. L'account azione predefinito SCOM è associato all'account di sistema locale ma non può avere i diritti SA se i criteri di sicurezza impediscono la concessione dei diritti di accesso a SQL Server al sistema locale. È possibile concedere diritti SA o con privilegi limitati a SCOM HealthService usando il relativo ID di sicurezza del servizio. Per altri dettagli, vedere gli articoli [SQL Server uses a service SID to provide service isolation](https://support.microsoft.com/en-us/help/2620201/sql-server-uses-a-service-sid-to-provide-service-isolation) (SQL Server usa un SID del servizio per impostare l'isolamento del servizio) e [How to configure SQL Server 2012 to allow for System Center Advisor monitoring](https://support.microsoft.com/en-us/help/2667175/how-to-configure-sql-server-2012-to-allow-for-system-center-advisor-mo) (Come configurare SQL Server 2012 per consentire il monitoraggio di System Center Advisor). Il processo di configurazione è descritto nella sezione [Come configurare il monitoraggio mediante un ID di sicurezza del servizio](#_How_to_Configure_3). Si noti che questo metodo è destinato solo alla modalità di monitoraggio locale.
9. Per concedere i diritti minimi necessari per i flussi di lavoro del Management Pack SQL, seguire le istruzioni riportate nella sezione [Ambienti con privilegi limitati](#_Low-privilege_environments).

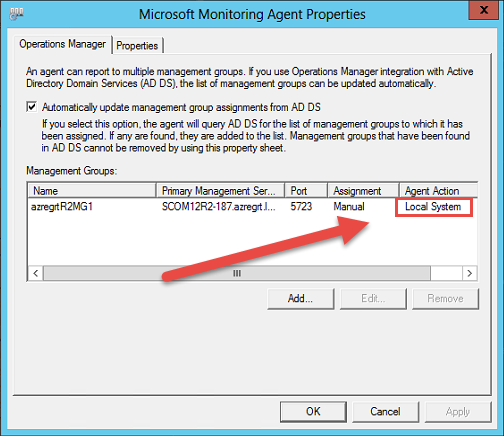
##### Come configurare i profili RunAs in modalità di monitoraggio senza agenti

Creare un account di accesso in SQL Server a scopo di monitoraggio e concedere all'account i diritti di amministratore di sistema o un set di autorizzazioni con privilegi limitati. Per l'accesso è possibile usare l'autenticazione di SQL Server o l'autenticazione di Windows. Quindi usare questo accesso nell'Aggiunta guidata monitoraggio durante l'aggiunta di un'istanza di SQL Server da monitorare. Vedere la sezione [Configurare il monitoraggio senza agenti tramite Aggiunta guidata monitoraggio](#_Configure_Agentless_Monitoring_2) per informazioni sull'aggiunta di un'istanza di SQL Server da monitorare senza agenti e la sezione [Configurare il monitoraggio senza agenti con privilegi limitati tramite Aggiunta guidata monitoraggio](#_Configure_Low-Privilege_Agentless) per informazioni su come configurare il monitoraggio con privilegi limitati in modalità senza agenti.

#### Come configurare il monitoraggio mediante un ID di sicurezza del servizio

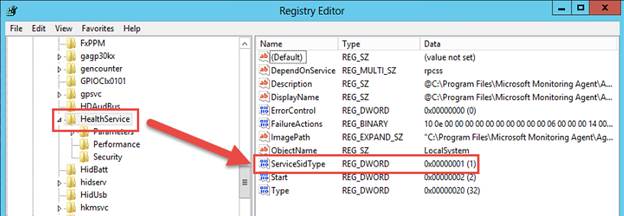
La procedura seguente consente di configurare il monitoraggio tramite ID di sicurezza del servizio per SQL Server 2017 con monitoraggio tramite agente in un'istanza di Windows Server.

1. L'agente di monitoraggio SCOM deve usare l'account "Sistema locale" (come nel caso illustrato di seguito) o qualsiasi altro account di dominio senza diritti di amministratore.

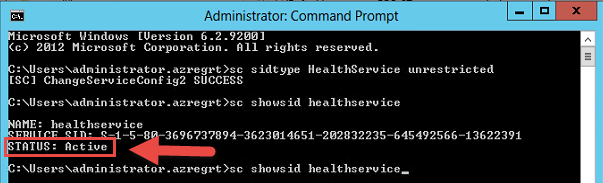


1. Nel computer gestito con l'agente SCOM aprire l'editor del Registro di sistema. Aggiungere la chiave REG\_DWORD "*ServiceSidType*" con il valore "1" in "*HKEY\_LOCAL\_MACHINE\SYSTEM\CurrentControlSet\Services\HealthService*".

Questo passaggio è necessario per attivare un ID di sicurezza per il Servizio integrità.



1. Aprire il prompt dei comandi come amministratore ed eseguire la query "*sc sidtype HealthService unrestricted*", quindi riavviare "Servizio integrità".
2. Aprire il prompt dei comandi come amministratore ed eseguire la query successiva: "*sc showsid HealthService*". Il valore "STATUS" del servizio deve essere "Active":



1. Aprire SQL Server Management Studio e connettersi a SQL Server 2017 sull'istanza di Windows, che deve essere monitorata usando l'ID di sicurezza del Servizio integrità.
2. In SSMS eseguire la query riportata di seguito:

SET NOCOUNT ON;

DECLARE @accountname nvarchar(**128**);

DECLARE @command1 nvarchar(MAX);

DECLARE @command2 nvarchar(MAX);

DECLARE @command3 nvarchar(MAX);

SET @accountname = 'NT SERVICE\HealthService';

SET @command1 = 'USE [master];

CREATE LOGIN ['+@accountname+']

FROM WINDOWS WITH DEFAULT\_DATABASE=[master];';

SET @command2 = '';

SELECT @command2 = @command2 + 'USE ['+db.name+'];

CREATE USER ['+@accountname+']

FOR LOGIN ['+@accountname+'];'

FROM sys.databases db

left join sys.dm\_hadr\_availability\_replica\_states hadrstate

on db.replica\_id = hadrstate.replica\_id

WHERE db.database\_id <> **2**

AND db.user\_access = **0**

AND db.state = **0**

AND db.is\_read\_only = **0**

AND (hadrstate.role = **1** or hadrstate.role is null);

SET @command3 = 'USE [master];

GRANT VIEW ANY DATABASE TO ['+@accountname+'];

GRANT VIEW ANY DEFINITION TO ['+@accountname+'];

GRANT VIEW SERVER STATE TO ['+@accountname+'];

GRANT SELECT on sys.database\_mirroring\_witnesses to ['+@accountname+'];

USE [msdb];

EXEC sp\_addrolemember @rolename=''PolicyAdministratorRole'', @membername='''+@accountname+''';

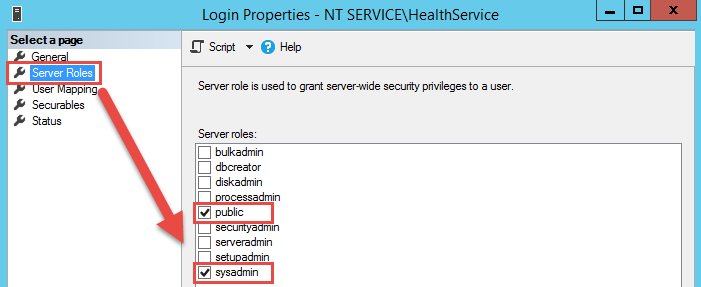
EXEC sp\_addrolemember @rolename=''SQLAgentReaderRole'', @membername='''+@accountname+''';';

EXECUTE sp\_executesql @command1;

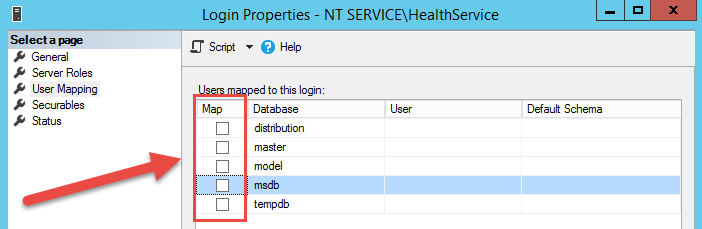
EXECUTE sp\_executesql @command2;

EXECUTE sp\_executesql @command3;

1. Concedere i ruoli del server "public" e "sysadmin" all'accesso "NT SERVICE\HealthService":



1. Deselezionare le caselle di controllo "Mapping" per tutti i database nella scheda "Mapping utenti"



#### Ambienti con privilegi limitati

Questa sezione descrive come configurare il Management Pack per Microsoft SQL Server per l'accesso con privilegi limitati. Tutti i flussi di lavoro, vale a dire individuazioni, regole, monitoraggi e azioni in questo Management Pack sono associati ai profili RunAs descritti nella sezione "[Profili RunAs](#_Run_As_Profiles)". Per abilitare il monitoraggio con privilegi limitati, è necessario concedere le autorizzazioni appropriate agli account RunAs e associare gli account ai profili RunAs corrispondenti. Le sottosezioni seguenti descrivono come concedere le autorizzazioni a livello di sistema operativo e a livello di SQL Server per tutti i [tipi di monitoraggio](#_Monitoring_Options).

Nota

Per la descrizione dettagliata dei profili RunAs definiti nel Management Pack per Microsoft SQL Server, vedere la sezione "[Profili RunAs](#_Run_As_Profiles)".

**Nota**

Per altre informazioni sulla configurazione di profili RunAs, vedere la sezione "[Come configurare i profili RunAs](#_How_to_configure_1)" di questa guida.

##### Monitoraggio con agente locale

Per configurare gli ambienti con privilegi limitati per il monitoraggio con agente locale, seguire questa procedura.

###### Configurare un ambiente con privilegi limitati in Active Directory

1. In Active Directory creare tre utenti di dominio da utilizzare comunemente per l'accesso con privilegi limitati a tutte le istanze di destinazione di SQL Server:

a. SQLTaskAction

b. SQLDiscovery

c. SQLMonitor

1. Creare un gruppo di dominio denominato SQLMPLowPriv e aggiungere gli utenti di dominio seguenti:

a. SQLDiscovery

b. SQLMonitor

1. Concedere un'autorizzazione speciale: Controller di dominio di sola lettura - "Autorizzazioni di lettura" a **SQLMPLowPriv**

###### Configurare un ambiente con privilegi limitati nel computer agente

1. Concedere le autorizzazioni di lettura nel percorso del Registro di sistema "**HKLM:\Software\Microsoft\Microsoft SQL Server**" per SQLTaskAction e **SQLMPLowPriv**.
2. Aggiungere gli utenti di dominio SQLTaskAction e SQLMonitor al gruppo locale "EventLogReaders".
3. Configurare l'impostazione dei criteri di sicurezza locali "Consenti accesso locale" per consentire all'utente di dominio SQLTaskAction e agli utenti del gruppo di dominio SQLMPLowPriv di accedere localmente.
4. Concedere le autorizzazioni "Esegui metodi", "Abilita account", "Abilita remoto" e "Sicurezza lettura" a SQLTaskAction e **SQLMPLowPriv** per gli spazi dei nomi WMI seguenti:
   1. **root**
   2. **root\cimv2**
   3. **root\default**
   4. **root\Microsoft\SqlServer\ComputerManagement14**
5. Concedere le autorizzazioni di lettura nel percorso del Registro di sistema "**HKLM:\Software\Microsoft\Microsoft SQL Server\*[InstanceID]*\MSSQLServer\Parameters**" per **SQLMPLowPriv** per ogni istanza monitorata.

###### Configurare un ambiente con privilegi limitati nell'istanza del motore di database di SQL Server

1. Aprire SQL Server Management Studio e connettersi all'istanza del motore di database di SQL Server.
2. In SQL Server Management Studio creare un account di accesso per "SQLMPLowPriv" per ogni istanza del motore di database di SQL Server in esecuzione in un server monitorato e concedere le autorizzazioni seguenti:
   1. VIEW SERVER STATE
   2. VIEW ANY DATABASE
   3. VIEW ANY DEFINITION
   4. EXECUTE ON xp\_readerrorlog

use master

GO

GRANT VIEW server state to [SQLMPLowPriv]

GRANT VIEW any definition to [SQLMPLowPriv]

GRANT VIEW any database to [SQLMPLowPriv]

GRANT EXECUTE ON xp\_readerrorlog TO [SQLMPLowPriv]

1. Creare un utente SQLMPLowPriv in ogni database utente, master, msdb e modello. Collegare gli utenti SQLMPLowPriv all'account di accesso SQLMPLowPriv. Se si aggiunge l'utente nel database modello, verrà creato automaticamente un utente SQLMPLowPriv in ogni database futuro creato dall'utente. Sarà necessario specificare manualmente l'utente per tutti i database che verranno collegati o ripristinati in futuro.

use master

GO

CREATE USER [SQLMPLowPriv] FOR LOGIN [SQLMPLowPriv]

1. Per il database msdb concedere a un utente SQLMPLowPriv le autorizzazioni seguenti:
   1. EXECUTE ON msdb.dbo.sp\_help\_job
   2. EXECUTE ON msdb.dbo.sp\_help\_jobactivity
   3. SELECT ON sysjobs\_view
   4. SELECT ON sysschedules
   5. SELECT ON sysjobschedules
   6. SELECT ON log\_shipping\_monitor\_history\_detail
   7. SELECT ON log\_shipping\_monitor\_secondary
   8. SELECT ON log\_shipping\_secondary\_databases
   9. SELECT ON log\_shipping\_monitor\_primary
   10. SELECT ON log\_shipping\_primary\_databases

use master

GO

grant EXECUTE ON msdb.dbo.sp\_help\_job to [SQLMPLowPriv]

grant EXECUTE ON msdb.dbo.sp\_help\_jobactivity to [SQLMPLowPriv]

grant SELECT ON sysjobs\_view to [SQLMPLowPriv]

grant SELECT ON sysschedules to [SQLMPLowPriv]

grant SELECT ON sysjobschedules to [SQLMPLowPriv]

grant SELECT ON log\_shipping\_monitor\_history\_detail to [SQLMPLowPriv]

grant SELECT ON log\_shipping\_monitor\_secondary to [SQLMPLowPriv]

grant SELECT ON log\_shipping\_secondary\_databases to [SQLMPLowPriv]

grant SELECT ON log\_shipping\_monitor\_primary to [SQLMPLowPriv]

grant SELECT ON log\_shipping\_primary\_databases to [SQLMPLowPriv]

1. Per il database msdb: aggiungere l'utente SQLMPLowPriv al ruolo del database **SQLAgentReaderRole**.

use master

GO

ALTER ROLE [SQLAgentReaderRole] ADD MEMBER [SQLMPLowPriv]

1. Per il database msdb: aggiungere l'utente **SQLMPLowPriv** al ruolo del database **PolicyAdministratorRole**.

use master

GO

ALTER ROLE [PolicyAdministratorRole] ADD MEMBER [SQLMPLowPriv]

###### Configurare un ambiente con privilegi limitati nel server che ospita una condivisione SMB usata dal motore di database di SQL Server

1. Concedere le autorizzazioni di condivisione aprendo la finestra di dialogo delle proprietà della condivisione che ospita i file di dati o i file di log delle transazioni di SQL Server.
2. Concedere le autorizzazioni di lettura a SQLMPLowPriv.
3. Concedere le autorizzazioni NTFS aprendo la finestra di dialogo delle proprietà per la cartella condivisa e passare alla scheda "Sicurezza".
4. Concedere le autorizzazioni di lettura a SQLMPLowPriv.

###### Configurare l'account azione dell'attività con privilegi limitati nell'istanza del motore di database di SQL Server

1. Aprire SQL Server Management Studio e connettersi all'istanza del motore di database di SQL Server.
2. In SQL Server Management Studio creare un account di accesso per SQLTaskAction per ogni istanza del motore di database di SQL Server in esecuzione in un server monitorato.
3. Creare un utente SQLTaskAction in ogni database utente, master, msdb e modello. Collegare gli utenti SQLTaskAction all'account di accesso SQLTaskAction. Se si aggiunge l'utente nel database modello viene creato automaticamente un utente SQLTaskAction in ogni database futuro creato dall'utente. Sarà necessario specificare manualmente l'utente per tutti i database che verranno collegati o ripristinati in futuro.

use master

GO

CREATE USER [SQLTaskAction] FOR LOGIN [SQLTaskAction]

###### Abilitare l'esecuzione delle attività di System Center Operations Manager per un oggetto di database

Per alcune attività opzionali di System Center Operations Manager è richiesto un privilegio superiore per il computer agente e/o un database per consentire l'esecuzione dell'attività.

I seguenti passaggi di provisioning devono essere eseguiti nel computer agente o nel database solo se si vuole consentire all'operatore della console System Center Operations Manager di eseguire interventi di correzione nella destinazione.

1. Se l'attività è correlata all'avvio o all'arresto di un servizio NT (ad esempio il servizio Motore di database, il servizio SQL Server Agent, il servizio di ricerca full-text SQL o Integration Services), nel computer agente concedere l'autorizzazione utente SQLTaskAction per avviare o arrestare un servizio NT. Ciò comporta l'impostazione del descrittore di sicurezza di un servizio. Per ulteriori informazioni, vedere la pagina Web relativa a [sc sdset](http://go.microsoft.com/fwlink/?LinkId=193876).

Leggere i privilegi esistenti per un servizio specifico (usando **sc sdshow**) e concedere privilegi aggiuntivi all'utente SQLTaskAction per il server.

Ad esempio, si supponga che i risultati del comando **SC sdshow** per il servizio SQL Server siano i seguenti:

D:(A;;CCLCSWRPWPDTLOCRRC;;;SY)(A;;CCDCLCSWRPWPDTLOCRSDRCWDWO;;;BA)(A;;CCLCSWLOCRRC;;;IU)(A;;CCLCSWLOCRRC;;;SU)S:(AU;FA;CCDCLCSWRPWPDTLOCRSDRCWDWO;;;WD)

In questo caso la riga di comando seguente concede accesso sufficiente a SQLTaskAction per avviare e arrestare il servizio SQL Server. Sostituire le stringhe a colori con i valori appropriati e mantenere ogni elemento in un'unica riga di testo:

sc sdset SQLServerServiceName D:(A;;GRRPWP;;;SID for SQLTaskAction)(A;;CCLCSWRPWPDTLOCRRC;;;SY)(A;;CCDCLCSWRPWPDTLOCRSDRCWDWO;;;BA)(A;;CCLCSWLOCRRC;;;IU)(A;;CCLCSWLOCRRC;;;SU)S:(AU;FA;CCDCLCSWRPWPDTLOCRSDRCWDWO;;;WD)

1. In SQL Server Management Studio aggiungere SQLTaskAction al ruolo del database db\_owner per ogni database, se l'attività è correlata all'esecuzione di controlli del database:

a. "Controllo catalogo (DBCC)"

b. "Controllo database (DBCC)"

c. "Controllo disco (DBCC)" (richiama DBCC CHECKALLOC)

use master

GO

ALTER ROLE [db\_owner] ADD MEMBER [SQLTaskAction]

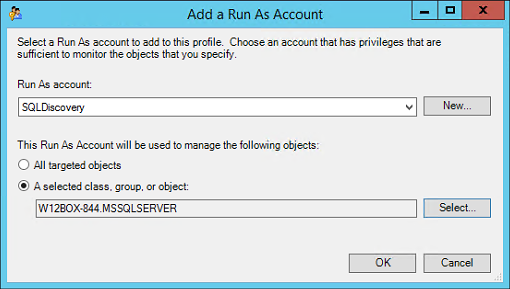
1. Concedere il privilegio ALTER ANY DATABASE all'account di accesso SQLTaskAction per eseguire l'attività, se è relativa alla modifica dello stato del database:

a. "Impostazione database offline"

b. "Impostazione database su stato di emergenza"

c. "Impostazione database su stato online"

###### Configurare System Center Operations Manager

1. Importare il Management Pack di SQL Server se tale operazione non è ancora stata effettuata.
2. Creare un account RunAs SQLTaskAction, SQLDiscovery e SQLMonitor con il tipo di account "Windows". Per ulteriori informazioni su come creare un account RunAs, vedere [Come creare un account RunAs in Operations Manager 2007](http://go.microsoft.com/fwlink/?LinkId=193877) o [Come creare un account RunAs in Operations Manager 2012](http://go.microsoft.com/fwlink/?LinkId=717832). Per ulteriori informazioni sui vari tipi di account RunAs, vedere [Profili RunAs e Account RunAs in Operations Manager 2007](http://go.microsoft.com/fwlink/?LinkId=193879) o [Gestione di account e profili RunAs in Operations Manager 2012](http://go.microsoft.com/fwlink/?LinkId=717833).
3. Nella console System Center Operations Manager, configurare i profili RunAs per il Management Pack di SQL Server come riportato di seguito:
   1. Impostare il profilo RunAs "Microsoft SQL Server Task" per l'uso dell'account RunAs SQLTaskAction.
   2. Impostare il profilo RunAs "Microsoft SQL Server Discovery" per l'uso dell'account RunAs SQLDiscovery.
   3. Impostare il profilo RunAs "Microsoft SQL Server Monitoring" per l'uso dell'account RunAs SQLMonitor.
4. Per evitare problemi con il monitoraggio di SQL Server usare gli account RunAs SQLTaskAction, SQLDiscovery e SQLMonitor per la gestione delle istanze del motore di database di SQL Server:

##### Monitoraggio senza agenti

Per configurare gli ambienti con privilegi limitati per il monitoraggio senza agenti, seguire questa procedura.

**Nota**

La procedura seguente è adatta per SQL Server su entrambe le piattaforme: Windows e Linux.

###### Configurare un ambiente con privilegi limitati nell'istanza del motore di database di SQL Server

1. Aprire SQL Server Management Studio e connettersi all'istanza del motore di database di SQL Server.
2. In SQL Server Management Studio, per ogni istanza del motore di database di SQL Server in esecuzione in un server monitorato creare un account di accesso SQL per il monitoraggio e concedere le autorizzazioni seguenti:

use master

GO

GRANT VIEW server state to [SQLMPLowPriv]

GRANT VIEW any definition to [SQLMPLowPriv]

GRANT VIEW any database to [SQLMPLowPriv]

Passare a Mapping utenti nell'impostazione per l'account di accesso SQL creato e aggiungere il ruolo **db\_datareader** per il database master:

use master

GO

ALTER ROLE [db\_datareader] ADD MEMBER [SQLMPLowPriv]

GO

e concedere le autorizzazioni seguenti:

use master

GO

GRANT EXECUTE ON xp\_readerrorlog to [SQLMPLowPriv]

1. Creare un utente in ogni database utente, master, msdb e modello. Collegare gli utenti creati all'account di accesso. Se si aggiunge un utente nel database modello, verrà creato automaticamente un utente in ogni database futuro creato dall'utente. Sarà necessario specificare manualmente l'utente per tutti i database che verranno collegati o ripristinati in futuro:

use [yourdatabase]

GO

CREATE USER [SQLMPLowPriv] FOR LOGIN [SQLMPLowPriv]

GO

use [master]

GO

CREATE USER [SQLMPLowPriv] FOR LOGIN [SQLMPLowPriv]

GO

use [msdb]

GO

CREATE USER [SQLMPLowPriv] FOR LOGIN [SQLMPLowPriv]

GO

use [model]

GO

CREATE USER [SQLMPLowPriv] FOR LOGIN [SQLMPLowPriv]

GO

1. Per il database msdb concedere all'utente le autorizzazioni seguenti:

use msdb

GO

GRANT EXECUTE ON msdb.dbo.sp\_help\_job to [SQLMPLowPriv]

GRANT EXECUTE ON msdb.dbo.sp\_help\_jobactivity to [SQLMPLowPriv]

GRANT SELECT ON sysjobs\_view to [SQLMPLowPriv]

GRANT SELECT ON sysschedules to [SQLMPLowPriv]

GRANT SELECT ON sysjobschedules to [SQLMPLowPriv]

GRANT SELECT ON log\_shipping\_monitor\_history\_detail to [SQLMPLowPriv]

GRANT SELECT ON log\_shipping\_monitor\_secondary to [SQLMPLowPriv]

GRANT SELECT ON log\_shipping\_secondary\_databases to [SQLMPLowPriv]

GRANT SELECT ON log\_shipping\_monitor\_primary to [SQLMPLowPriv]

GRANT SELECT ON log\_shipping\_primary\_databases to [SQLMPLowPriv]

###### Abilitare l'esecuzione delle attività di System Center Operations Manager per un oggetto di database

Per alcune attività opzionali di System Center Operations Manager è richiesto un privilegio superiore per il computer agente e/o un database per consentire l'esecuzione dell'attività.

I seguenti passaggi di provisioning devono essere eseguiti nel database solo se si vuole consentire all'operatore della console System Center Operations Manager di eseguire interventi di correzione nella destinazione.

1. In SQL Server Management Studio aggiungere un account di accesso SQL (SQLMPLowPriv) al ruolo del database **db\_owner** per ogni database se l'attività è associata all'esecuzione di controlli del database:
   1. "Controllo catalogo (DBCC)"
   2. "Controllo database (DBCC)"
   3. "Controllo disco (DBCC)" (richiama DBCC CHECKALLOC)

use [yourdatabase]

GO

ALTER ROLE [db\_owner] ADD MEMBER [SQLMPLowPriv]

GO

1. Concedere il privilegio ALTER ANY DATABASE all'account di accesso SQL (SQLMPLowPriv) per eseguire attività del database:
   1. "Impostazione database su stato online"
   2. "Impostazione database offline"
   3. "Impostazione database sullo stato di emergenza"

use master

GO

GRANT ALTER ANY DATABASE to [SQLMPLowPriv]

1. Per il database msdb: aggiungere l'utente SQLMPLowPrivai ruoli del database **SQLAgentReaderRole** e **PolicyAdministratorRole**:

use [msdb]

GO

ALTER ROLE [PolicyAdministratorRole] ADD MEMBER [SQLMPLowPriv]

GO

use [msdb]

GO

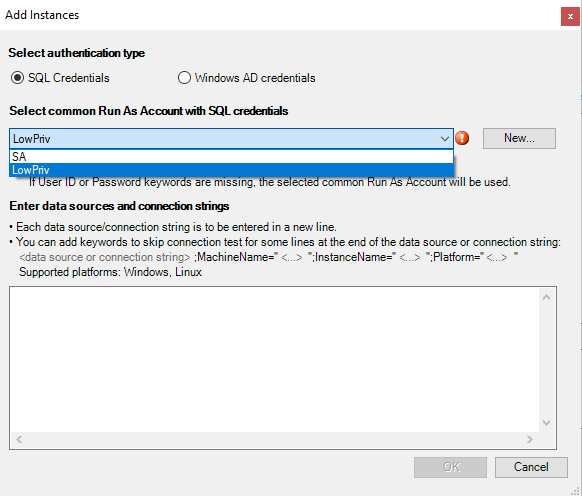
ALTER ROLE [SQLAgentReaderRole] ADD MEMBER [SQLMPLowPriv]

GO

###### Configurare il monitoraggio senza agenti con privilegi limitati tramite Aggiunta guidata monitoraggio

Eseguire le azioni specificate nella procedura della sezione ["Configurare il monitoraggio senza agenti tramite Aggiunta guidata monitoraggio"](#_Configure_Agentless_Monitoring_2) con alcune modifiche indicate di seguito:

Fare clic sul pulsante **Aggiungi istanza** per aggiungere le singole istanze da monitorare.



In questa finestra selezionare un account RunAs comune con l'accesso SQL con privilegi limitati appropriato. Quindi immettere le origini dati e/o le stringhe di connessione. Seguire le istruzioni specificate in questa finestra per evitare errori.

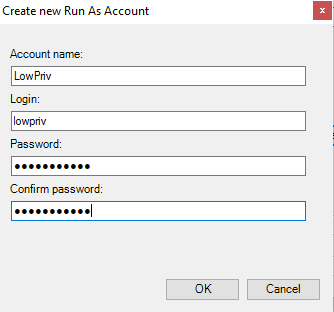
I dati devono essere immessi con il formato indicato negli esempi seguenti:

*172.31.2.133;MachineName="W12BOX-839";InstanceName="MSSQLSERVER";Platform="Windows"*

*172.31.2.133,50626;MachineName="W12BOX-839";InstanceName="SQLEXPRESS";Platform="Windows"*

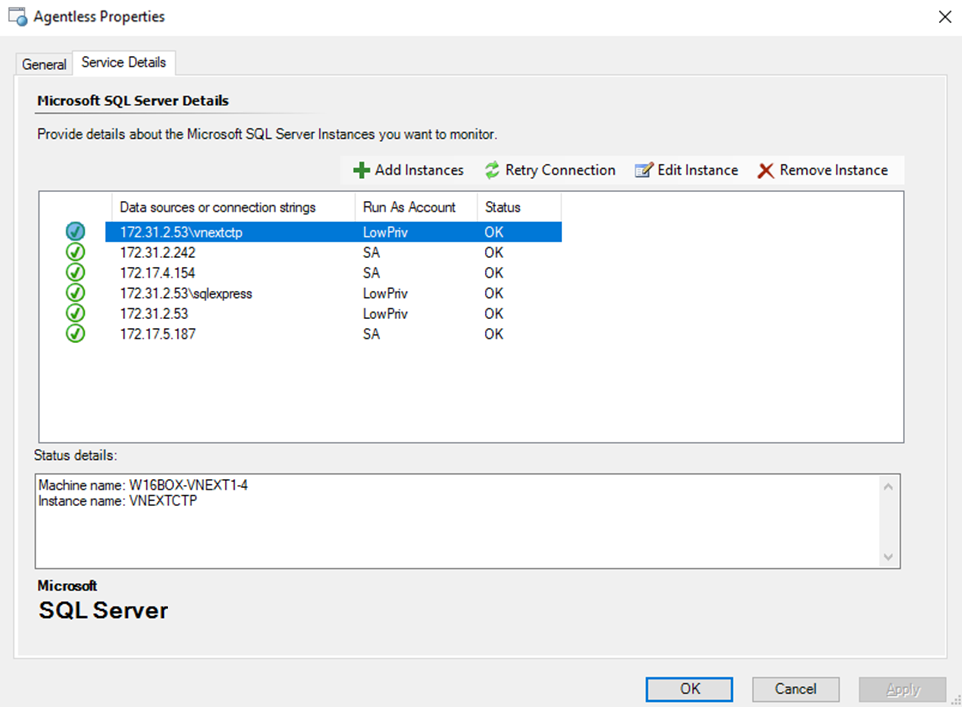
*172.17.5.115;MachineName="ubuntu";InstanceName="MSSQLSERVER";Platform="Linux"*

È anche possibile creare un nuovo account RunAs facendo clic sul pulsante **Nuovo**.



Nella finestra corrispondente immettere il nome del nuovo account RunAs e le credenziali del server SQL da sottoporre a monitoraggio.

Dopo la selezione di **OK** nella finestra **Aggiungi istanza** viene eseguito il test della connessione all'istanza selezionata.



Quando viene completato il test della connessione è possibile visualizzare e modificare le proprietà dell'istanza aggiunta. Per farlo selezionare l'istanza e fare clic sul pulsante **Edit Instance** (Modifica istanza).

Dopo questa operazione viene creato il modello di monitoraggio.

##### Monitoraggio misto

Per configurare gli ambienti con privilegi limitati per il monitoraggio misto seguire la procedura descritta nella sezione [Monitoraggio con agente locale](#_Local_Agent_Monitoring) e quindi seguire questa procedura:

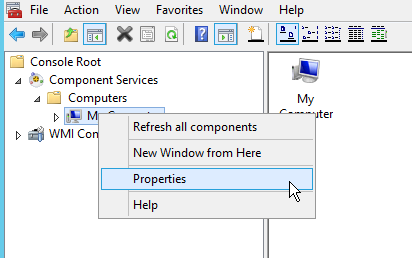
###### Gestire l'accesso remoto a WMI

La procedura seguente configura la sicurezza per le configurazioni con account con privilegi limitati. In ogni server di monitoraggio con modalità mista seguire questa procedura:

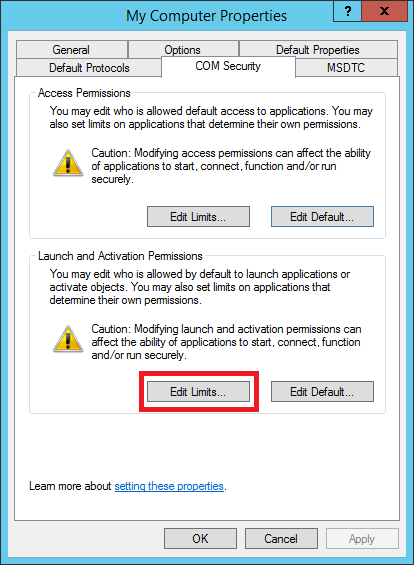
1. Avviare mmc.exe e aggiungere due snap-in:

* **Servizi componenti**
* **Controllo WMI** (per il computer locale)

1. Espandere **Servizi componenti**, fare clic con il pulsante destro del mouse su **Risorse del computer** e scegliere **Proprietà**. Viene visualizzata la finestra di dialogo corrispondente:

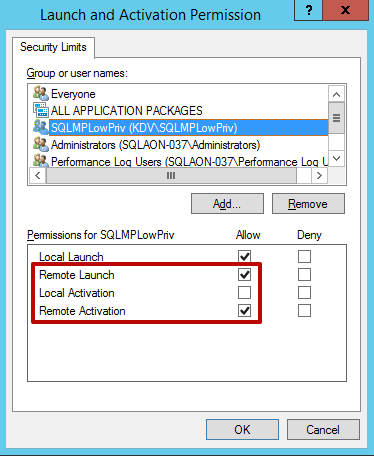


1. Nella finestra di dialogo passare alla scheda **Sicurezza**.
2. Fare clic sul pulsante **Modifica limiti** nella sezione **Autorizzazioni di esecuzione e attivazione**. Viene visualizzata la finestra di dialogo corrispondente:



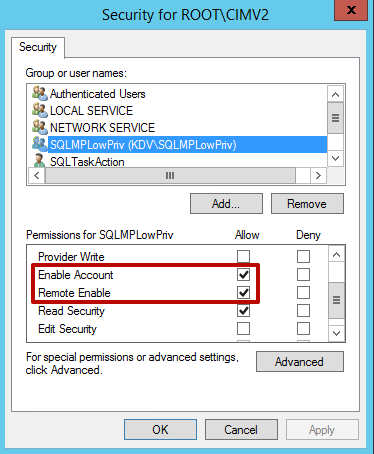
1. Nella finestra di dialogo impostare le autorizzazioni seguenti per l'account del computer remoto:

* **Avvio remoto**
* **Attivazione remota**



1. Passare allo snap-in **Controllo WMI** e chiamare le relative proprietà. Verrà visualizzata la finestra di dialogo corrispondente.
2. Nella finestra di dialogo passare alla scheda **Sicurezza**, selezionare gli spazi dei nomi **Root\CIMV2** e **Root\Microsoft\SqlServer** e fare clic sul pulsante **Sicurezza**.
3. Aggiungere le autorizzazioni seguenti per il computer di destinazione:

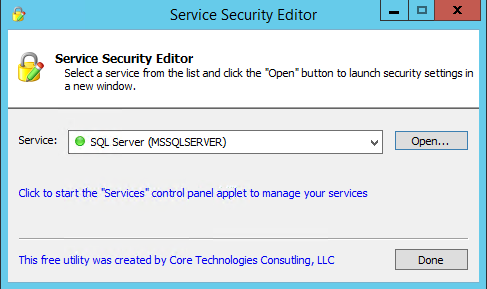
* **Abilita account**
* **Abilita remoto**

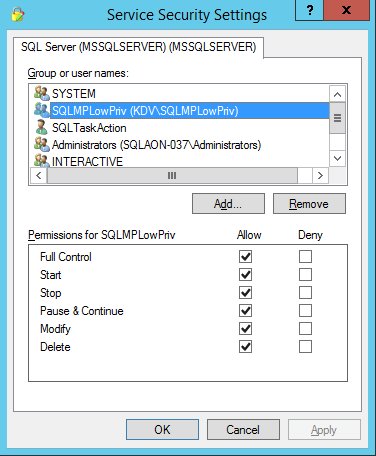


1. Fare clic sul pulsante **Avanzate**. Verrà visualizzata la finestra di dialogo corrispondente.
2. Nella finestra di dialogo selezionare l'account di destinazione e fare clic sul pulsante **Modifica**.
3. Nella finestra di dialogo seguente verificare che il parametro **Si applica a** sia impostato sul valore **Solo questo spazio dei nomi** e che siano impostate le autorizzazioni seguenti:

* **Abilita account**
* **Abilita remoto**

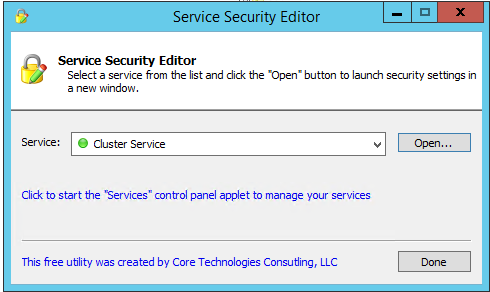
1. Impostare i diritti per i servizi SQL Server, SQL Agent e Utilità di avvio del daemon filtri full-text di SQL mediante [Service Security Editor (strumento per la GUI)](https://www.coretechnologies.com/products/ServiceSecurityEditor/). Eseguire l'utilità, trovare il servizio e aprire Service Security Settings (Impostazioni Service Security):

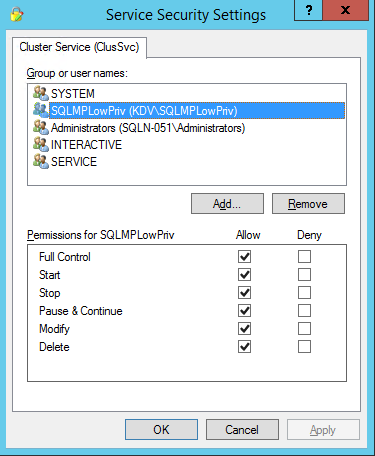




Aggiungere il gruppo **SQLMPLowPriv** e il nome utente **SQLTaskAction**,impostare le autorizzazioni "Controllo completo" e applicare il risultato. Eseguire questa procedura per tutti i servizi SQL Server: **SQL Server, SQL Agent** e **Utilità di avvio del daemon filtri full-text di SQL**.

1. Impostare i diritti per ClusSvc (Servizio cluster) usando [Service Security Editor (strumento per la GUI)](https://www.coretechnologies.com/products/ServiceSecurityEditor/). Eseguire l'utilità, trovare il servizio e aprire Service Security Settings (Impostazioni Service Security):





Aggiungere il gruppo **SQLMPLowPriv** e le autorizzazioni "Controllo completo" e applicare il risultato.

###### Concedere autorizzazioni per ottenere informazioni sui servizi

1. Recuperare il SID dell'utente.

Al prompt dei comandi di Windows digitare **PowerShell** e premere INVIO per aprire PowerShell.

Eseguire il comando seguente per recuperare il SID utente di *Spotlight User* (Utente Spotlight). Sostituire ***domainName***e ***userName***con il nome dominio e il nome utente dell'account ***Spotlight User*** (Utente Spotlight):

[wmi]"win32\_group.domain='***domainName***',name='***userName***'" | select –ExpandProperty SID

1. Recuperare il SDDL corrente per Gestione controllo servizi.

Al prompt dei comandi di Windows eseguire il comando seguente per recuperare il SDDL corrente di Gestione controllo servizi. Il SDDL viene salvato nel file con nome *file.txt*.

sc sdshow scmanager > *file.txt*

Il SDDL è simile al seguente. Per altre informazioni, vedere [Microsoft KB914392](http://support.microsoft.com/kb/914392).

D:(A;;CC;;;AU)(A;;CCLCRPRC;;;IU)(A;;CCLCRPRC;;;SU)(A;;CCLCRPWPRC;;;SY)(A;;KA;;;BA)S:(AU;FA;KA;;;WD)(AU;OIIOFA;GA;;;WD)

1. Modificare il SDDL.

Copiare la sezione del SDDL che termina con IU (Interactive Users, utenti interattivi). Questa sezione è una clausola tra parentesi completa, ovvero (A;;CCLCRPRC;;;IU). Incollare questa clausola subito dopo la clausola copiata.

Nel nuovo testo sostituire *IU* con il SID utente di *Spotlight User* (Utente Spotlight).

Il nuovo SDDL è simile al seguente:

D:(A;;CC;;;AU)(A;;CCLCRPRC;;;IU) (A;;CCLCRPRC;;;**S-1-5-21-214A909598-1293495619-13Z157935-75714**)(A;;CCLCRPRC;;;SU)(A;;CCLCRPWPRC;;;SY)(A;;KA;;;BA) S:(AU;FA;KA;;;WD)(AU;OIIOFA;GA;;;WD)

1. Impostare le credenziali di sicurezza per l'accesso a Gestione controllo servizi.

Il comando sdset in sc imposta le credenziali di sicurezza per l'accesso a Gestione controllo servizi (scmanager). Si noti che le autorizzazioni in scmanager vengono sostituite. L'impostazione delle credenziali di sicurezza non è additiva. Per questo motivo è necessario copiare le autorizzazioni esistenti.

sc sdset scmanager "D:(A;;CC;;;AU)(A;;CCLCRPRC;;;IU)(A;;CCLCRPRC;;;SU)(A;;CCLCRPWPRC;;;SY)(A;;KA;;;BA)(A;;CCLCRPRC;;;**S-1-5-21-214A909598-1293495619-13Z157935-75714**)S:(AU;FA;KA;;;WD)(AU;OIIOFA;GA;;;WD)"

###### Usare una chiave del Registro di sistema per gestire l'accesso remoto al Registro di sistema

Creare una chiave del Registro di sistema per gestire l'accesso remoto al Registro di sistema. Se è necessario creare la chiave per limitare l'accesso al Registro di sistema, seguire questa procedura:

1. Avviare l'editor del Registro di sistema (Regedt32.exe) e trovare la chiave seguente:  
   HKEY\_LOCAL\_MACHINE\SYSTEM\CurrentControlSet\Control
2. Nel menu Modifica fare clic su Aggiungi chiave e immettere i valori seguenti:  
   Nome chiave: SecurePipeServers  
   Classe: REG\_SZ
3. Individuare la chiave seguente:  
   HKEY\_LOCAL\_MACHINE\SYSTEM\CurrentControlSet\Control\ SecurePipeServers
4. Nel menu Modifica fare clic su Aggiungi chiave e immettere i valori seguenti:  
   Nome chiave: winreg  
   Classe: REG\_SZ
5. Individuare la chiave seguente:  
   HKEY\_LOCAL\_MACHINE\SYSTEM\CurrentControlSet\Control\ SecurePipeServers\winreg
6. Nel menu Modifica fare clic su Aggiungi valore e quindi immettere i valori seguenti:  
   Nome valore: Description  
   Tipo di dati: REG\_SZ  
   Stringa: Registry Server
7. Individuare la chiave seguente:  
   HKEY\_LOCAL\_MACHINE\SYSTEM\CurrentControlSet\Control\ SecurePipeServers\winreg
8. Fare clic con il pulsante destro del mouse su winreg, scegliere Autorizzazioni e modificare le autorizzazioni correnti o aggiungere gli utenti o i gruppi ai quali si vuole concedere l'accesso.
9. Chiudere l'editor del Registro di sistema e riavviare Windows.

## Visualizzare informazioni nella console di Operations Manager

### Viste e dashboard (generici) indipendenti dalla versione

Questo Management Pack Microsoft introduce una struttura di cartelle comune, che verrà usata nelle versioni future dei Management Pack per componenti di SQL Server diversi. Le viste e i dashboard seguenti sono indipendenti dalla versione e visualizzano informazioni su tutte le versioni di SQL Server:

 SQL Server 2017+

Avvisi attivi



Ruoli di SQL Server

Riepilogo

Stato attività



 Motori di database SQL

Avvisi attivi

 Tutti i dati sulle prestazioni

Riepilogo

Stato attività



 Disponibilità elevata AlwaysOn

Motori di database



 Motori di database

 Database

 Filegroup

Motori di database in Linux



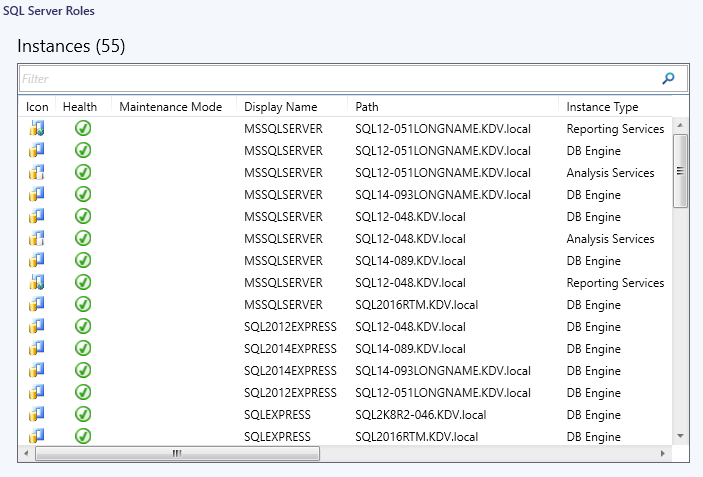
Motori di database in Windows



 Dati ottimizzati per la memoria

 SQL Agent

Il dashboard "Ruoli di SQL Server" offre informazioni su tutte le istanze del motore di database di SQL Server, di SQL Server Reporting Services, di SQL Server Analysis Services e di SQL Server Integration Services:



Per altre informazioni, vedere la guida dei dashboard di Microsoft SQL Server.

### Viste di SQL Server

Il Management Pack per Microsoft SQL Server introduce un set completo di viste relative allo stato, alle prestazioni e agli avvisi disponibili nella cartella dedicata:

Monitoraggio

Microsoft SQL Server 2017+

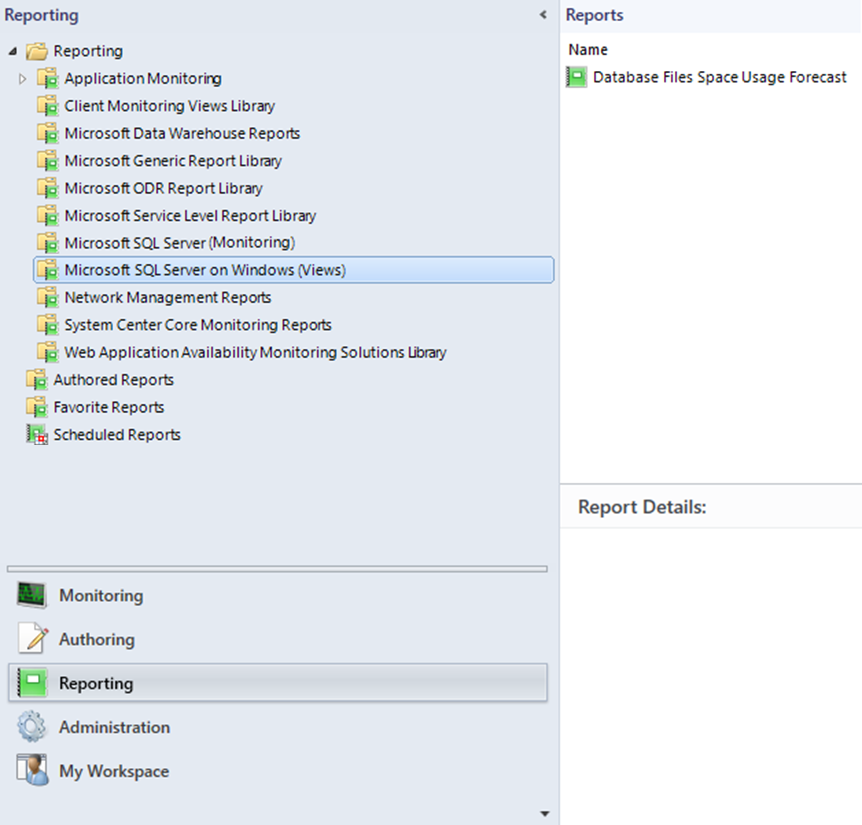
Motori di database di SQL Server

Nota

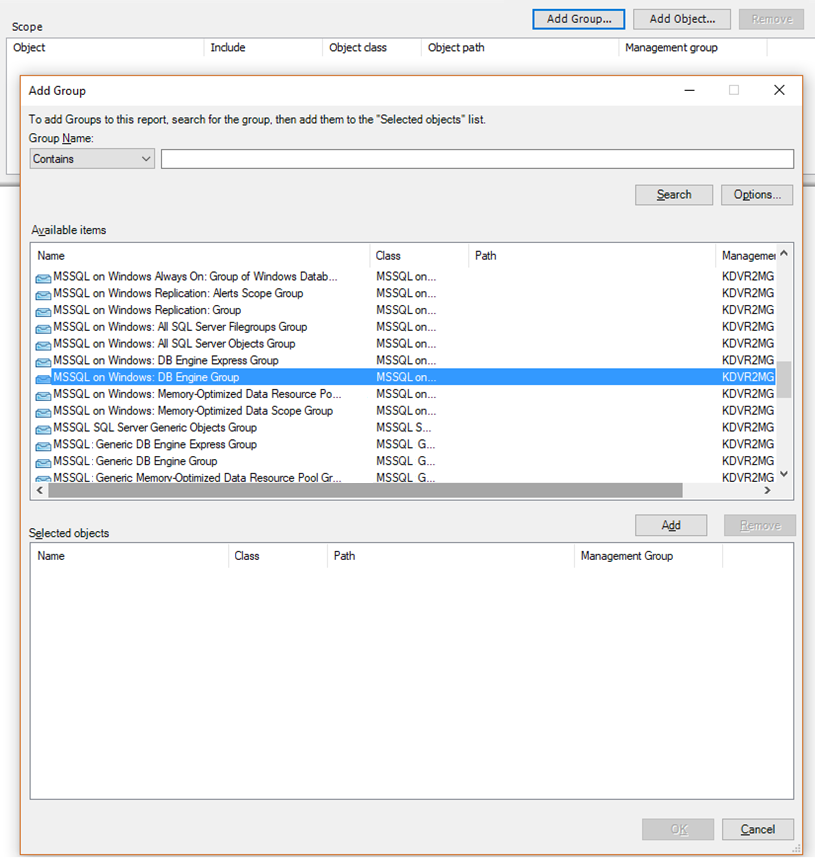
Alcune viste possono contenere un elenco molto lungo di oggetti o metriche. Per trovare un oggetto o un gruppo di oggetti specifico, è possibile usare i pulsanti Ambito, Cerca e Trova sulla barra degli strumenti di Operations Manager. Per altre informazioni, vedere l'articolo "[Ricerca di dati e oggetti nelle console di Operations Manager](http://go.microsoft.com/fwlink/?LinkId=717834)" nella Guida di Operations Manager.

### SQL Server Reporting

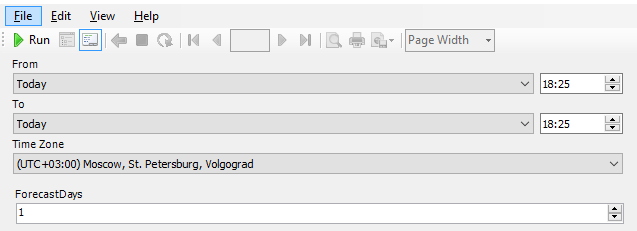
Il Management Pack per Microsoft SQL Server ora include il reportDatabase Files Space Usage Forecast (Previsione spazio usato da file di database) nella sezione corrispondente di System Center Operations Manager:



Per aprire il menu del report fare doppio clic sul report. In questo menu è necessario aggiungere un oggetto (o un gruppo di oggetti) al report:



Selezionare quindi il periodo e il fuso orario corrispondente per il report e il numero di giorni per la previsione d'uso dello spazio file:



Fare clic su pulsante Esegui per creare il report. Il report visualizza diversi grafici con i seguenti elementi di prestazioni:

• Spazio file usato all'inizio (GB)

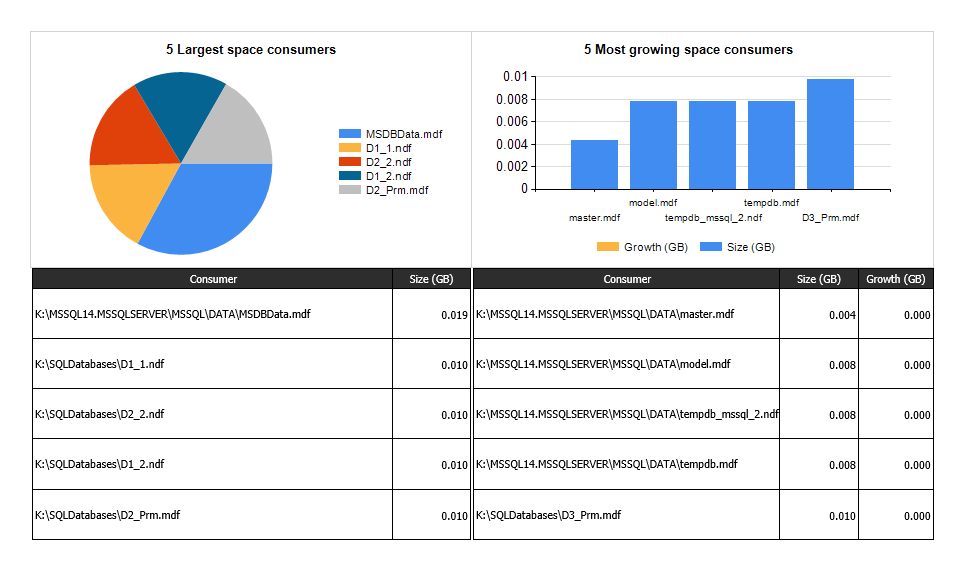
• Spazio file usato alla fine (GB)

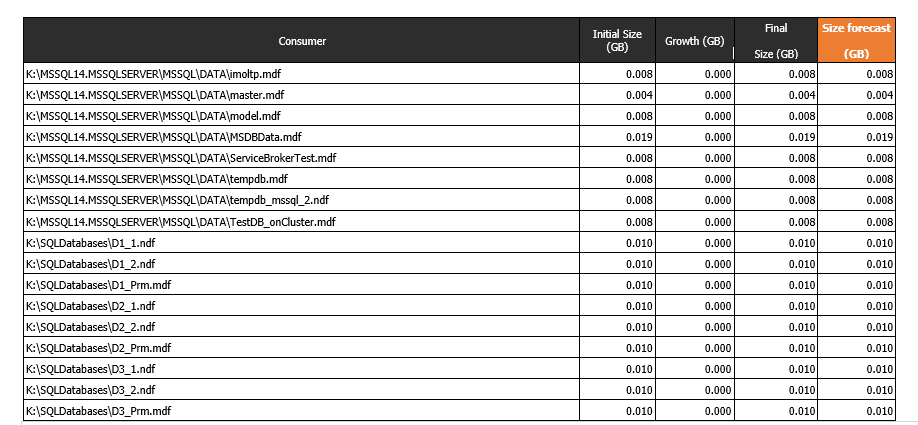
• Media spazio file libero all'inizio (%)

• Media spazio file libero alla fine (%)

• Previsione uso spazio file (GB)

Il report visualizza un grafico separato per ogni oggetto o gruppo di oggetti selezionato.



È possibile visualizzare la previsione d'uso dello spazio corrispondente in una tabella separata:  


Si noti che il report funziona solo con oggetti Windows.

## Appendice: Problemi noti e risoluzione dei problemi

**Le regole e i monitoraggi possono restituire dati errati se i valori dell'intervallo di sostituzione predefinito vengono modificati**

**Problema:** se il parametro sostituibile Intervallo (secondi) viene impostato su un valore inferiore al valore predefinito, le regole e i monitoraggi possono restituire dati errati.

**Soluzione:** assicurarsi che il parametro sostituibile Intervallo (secondi) sia impostato su un valore non inferiore al valore predefinito.

**L'individuazione valore di inizializzazione di un pacchetto piattaforma eliminato potrebbe essere ancora in esecuzione nei nodi del pool**

**Problema:** se dopo l'eliminazione di un pacchetto piattaforma l'individuazione valore di inizializzazione corrispondente resta in esecuzione nei nodi del pool può verificarsi un errore.

**Soluzione:** quando si elimina un pacchetto piattaforma, eliminare manualmente l'individuazione valore di inizializzazione corrispondente.

**Lo stato del monitor "Stato del database" cambia in continuazione**

**Problema:** se il parametro "Chiusura automatica" per il database è "True", lo stato del monitor "Stato del database" cambia continuamente da "Integro" a "Recupero/ripristino del database" e viceversa a seconda del timeout impostato nei parametri di sostituzione.

**Soluzione:** in base alle specifiche dell'operazione di monitoraggio non è necessaria alcuna soluzione.

**Se si abilita il parametro di database "Chiusura automatica" la raccolta della metrica delle prestazioni si blocca**

**Problema:** se il parametro di database "Chiusura automatica" è impostato su "True" tutte le regole per le prestazioni restituiscono valori vuoti.

**Soluzione:** impostare di nuovo il parametro di database "Chiusura automatica" su "False".

**Se un computer che contiene un'istanza monitorata senza agenti non è disponibile si verificano vari errori nel registro eventi del nodo Watcher**

**Problema:** se un computer che contiene un'istanza monitorata senza agenti non è disponibile si verificano vari errori di monitoraggio e rilevamento del Management Pack SQL Server Windows nel registro eventi del nodo Watcher. Gli errori si ripetono fino a quando il computer non torna disponibile.

**Soluzione:** nessuna soluzione disponibile.

**Possono verificarsi problemi durante l'installazione del Management Pack**

**Problema:** è possibile che l'agente di lettura log avvii la scansione dell'intero log di SQL Server, con conseguente attivazione di tutti gli avvisi rilevati. È anche possibile che la proprietà RepeatCount contenga un numero di eventi eccessivo.

**Soluzione:** nessuna soluzione disponibile.

**Le virgolette doppie in un nome di database possono causare errori nelle attività della console del database**

**Problema:** le attività della console Database usano i nomi di database racchiusi tra virgolette doppie come argomenti. Un nome di database può contenere qualsiasi simbolo, incluse le virgolette doppie. In tal caso le attività della console per il database non funzionano.

**Soluzione:** nessuna soluzione.

**Quando un'istanza non è disponibile il registro eventi riceve l'eccezione Module.Monitoring.Performance.MSSQLLogReaderEventTrigger**

**Problema:** quando un'istanza non è disponibile il registro eventi riceve l'eccezione Module.Monitoring.Performance.MSSQLLogReaderEventTrigger. L'eccezione viene ricevuta fino a quando l'istanza non torna disponibile. L'intervallo di ricezione dell'eccezione è uguale all'intervallo più breve impostato per le regole di avviso.

**Soluzione:** nessuna soluzione.

**Quando un'istanza non è disponibile il registro eventi riceve l'eccezione Module.Monitoring.Performance.SqlOsPerfCounterReaderHelper**

**Problema:** quando un'istanza non è disponibile il registro eventi riceve l'eccezione Module.Monitoring.Performance.SqlOsPerfCounterReaderHelper. L'eccezione viene ricevuta fino a quando l'istanza non torna disponibile. L'intervallo di ricezione dell'eccezione è uguale all'intervallo più breve delle regole per le prestazioni.

**Soluzione:** nessuna soluzione.

**Comportamenti anomali degli stati operativi dei monitoraggi**

**Problema:** se il pool di risorse contiene più di un server di gestione, gli stati operativi di tutti i monitoraggi cambiano a seconda delle impostazioni di failover del pool di risorse.

**Soluzione:** nessuna soluzione.

**SQL Server in Docker: dopo il riavvio di Docker si verificano vari errori**

**Problema:** dopo il riavvio di SQL Server in Docker si verificano vari errori perché la voce Docker-ID (MachineName) è stata modificata dopo il riavvio.

**Risoluzione:** in SCOM passare alle proprietà del modello di monitoraggio, aprire la scheda Dettagli servizio e fare clic su "Ripeti connessione".

**È possibile che si verifichino gli errori 40 e 121**

**Problema:** in rari casi è possibile che si verifichino gli errori di monitoraggio 40 e 121 nel registro eventi.

**Soluzione:** nessuna soluzione.

**Intervalli di ricerca prolungati**

**Problema:** se si usa un pool di risorse con più nodi Watcher, gli intervalli di individuazione possono risultare notevolmente più lunghi.

**Soluzione:** nessuna soluzione.

**Nessuna regola di evento funziona sui motori di database SQL localizzati**

**Problema:** nessuna regola di evento funziona sui motori di database SQL localizzati. Nell'implementazione corrente queste regole funzionano solo con la versione in lingua inglese.

**Soluzione:** nessuna soluzione.

**La modalità di manutenzione delle istanze cluster non è disponibile**

**Problema:** nell'implementazione corrente la modalità di manutenzione non funziona per le istanze cluster 2017.

**Soluzione:** nessuna soluzione.

**I criteri eliminati vengono visualizzati in Operations Manager.**

**Problema:** i criteri di SQL Server in Windows/Linux eliminati in SQL Server Management Studio sono ancora visualizzati in Operations Manager.

**Soluzione:** nessuna soluzione.

**Le attività della console per gli oggetti gruppo di disponibilità con nomi contenenti il carattere virgolette doppie non funzionano**

**Problema:** il carattere virgolette doppie non può essere usato nei nomi di gruppo di disponibilità e database del gruppo di disponibilità (per Always On). Le attività della console per oggetti con nomi di questo tipo non funzionano.

**Soluzione:** nessuna soluzione.

**La connessione non riesce quando viene specificato un indirizzo IP come stringa di connessione per un'istanza basata su Linux.**

**Problema:** quando si aggiunge un'istanza basata su Linux (passaggio "Aggiungi istanza" dell'Aggiunta guidata monitoraggio), il test della connessione non riesce se si specifica come stringa di connessione un indirizzo IP e il tipo di autenticazione è "Windows AD credentials" (Credenziali di Windows Active Directory).

**Soluzione:** specificare come stringa di connessione il nome del computer e usare il tipo di autenticazione corretto.

**Problema di SCOM: il servizio di configurazione può risultare bloccato dopo la reinstallazione del Management Pack.**

**Problema:** il servizio di configurazione può risultare bloccato dopo la reinstallazione del Management Pack. In apparenza si tratta di un problema di SCOM.

**Soluzione:** nessuna soluzione.

**Lo stato del monitoraggio "Database Critical Policies Availability" (Disponibilità di criteri critici del database) non diventa "Critico".**

**Problema:** lo stato del monitoraggio "Database Critical Policies Availability" (Disponibilità di criteri critici del database) non diventa "Critico" quando si verifica un problema legato alla disponibilità dei Criteri di criticità database ospitati in questo database.

**Soluzione:** nessuna soluzione.