

Capítulo 2

Administración basada en directivas

Al finalizar el capítulo, el alumno podrá:

- Identificar los componentes de una directiva de SQL Server.
- Configurar las directivas de administración en SQL Server.
- Monitorear el cumplimiento de las directivas de SQL Server.

Temas

1. Introducción al Declarative Management Framework
2. Implementación de administración basada en directivas
3. Forzar el cumplimiento de una directiva
4. Monitorear el cumplimiento de una directiva
5. Best Practice Analyzer basado en directivas

1. Introducción al Declarative Management Framework

Introducción al Declarative Management Framework

Facilita la escalabilidad:

- Distribución a través de múltiples servidores.
- Ayuda a definir directivas consistentes, a través de la empresa.

Control de Configuración:


- Ofrece una vista lógica de la configuración de los sistemas.
- Define la configuración de los servicios de datos.

Monitoreo de Desempeño:

- Gestión de operación de múltiples servidores.
- Optimiza la ejecución de los servicios de datos.

2 - 6

Copyright © Todos los Derechos Reservados - Cibertec Perú S.A.C.



El Declarative Management Framework (DMF) permite a los administradores de bases de datos, crear y aplicar directivas que regulan la configuración y operación de un servidor o servidores SQL Server. Si, por ejemplo, los servidores administrados requieren el uso de la funcionalidad de expiración de contraseñas, con DMF, se puede crear una directiva que refuerce el cumplimiento de este requerimiento en todos los servidores SQL Server de la compañía y de esta manera evitar, e incluso auditar intentos de transgresión, situaciones que pongan en riesgo la seguridad de los servidores.

El (DMF) se basa en la administración de multiservidores para poder ejecutar las directivas, a través de toda la organización.

2. Implementación de administración basada en directivas

Implementación de administración basada en directivas

Permite definir qué se puede hacer y qué no se puede hacer en el servidor.

Componentes de Administración Basada en directivas

Objetivos (Targets)

- Entidades que son administradas.

Directiva

- Una condición que define el comportamiento deseado.

Condiciones


- Una expresión Boolean que especifica el estado deseado.

Facetas

- Propiedades sobre las cuales se define la directiva.

3 - 6

Copyright © Todos los Derechos Reservados - Cibertec Perú S.A.C.



Para comprender mejor su funcionamiento, se definen algunos de los conceptos utilizados y a continuación, se presentan ejemplos de su uso.

Objetivos

Aquellas entidades que podrán ser afectadas por las directivas son denominadas objetivos. Se organizan de forma jerárquica comenzando a nivel de instancia, base de datos y finalmente, por tipo de objetos (tablas, vistas, etc.). Ejemplos de objetivos: base de datos, tablas, índices, procedimientos almacenados, etc.

Directiva

Una directiva configura el cumplimiento de una condición indicando además a qué objetivos de la jerarquía se deben aplicar. También se indica de qué forma se desea hacer la directiva efectiva. Se puede elegir entre:

- No forzar la aplicación de esta. En este caso, lanzar manualmente la comprobación.
- Forzar su aplicación. En este caso, utilizar disparadores (triggers) DDL para evaluarla en el acto.
- Comprobarla instantáneamente. Se notificará con un evento en el log cuando se infringe la directiva.
- Comprobación programada. Mediante un trabajo (job) del Agente de SQL Server se comprobará con una frecuencia configurable.

Condiciones

Las condiciones representan expresiones generadas a partir de las propiedades de las facetas aplicables al objetivo en cuestión. Por ejemplo, se podría tener una expresión que controlara que el nombre de los procedimientos almacenados comience por **pa_** como una buena práctica de nomenclatura. Para ello, se crearía una expresión donde se valida que la propiedad **name** de la faceta **StoredProcedure Facet** cumpla la condición **LIKE 'pa_%'**.

Facetas

Representa una agrupación lógica de las propiedades comunes de diferentes objetivos. Por ejemplo, la faceta "Index Facet" agrupa propiedades como **IsClustered**, **SpaceUsed**, **FillFactor**, etc. Sobre estas propiedades, se pueden crear condiciones a validar y estas serán dependientes de cada tipo de objetivo. Algunas facetas pueden ser comunes para diferentes tipos de objetos.

La administración basada en directivas sería útil para resolver los problemas presentados en los escenarios siguientes:

- Una directiva de la compañía prohíbe habilitar correo electrónico de base de datos o SQL Mail. Una directiva se crea para comprobar el estado del servidor de esas dos características. Un administrador compara el estado del servidor con la directiva. Si el estado del servidor indica que es incompatible, el administrador elige el modo Configurar y la directiva pone el estado del servidor como compatible.
- Las bases de datos de producción tienen una convención de nomenclatura que requiere que todos los nombres de los procedimientos almacenados comiencen con las letras **usp**. Se crea una directiva para aplicar esta convención. Un administrador prueba esta directiva y recibe una lista de procedimientos almacenados que no la cumplen. Si los procedimientos almacenados futuros no obedecen esta convención de nomenclatura, se produce un error en las instrucciones de creación de los procedimientos almacenados.

En otro escenario que podríamos presentar es un caso en el cual se decide reforzar la directiva de contraseñas seguras en una instancia SQL Server llamada **SQL01**, en este caso, se puede decir que:

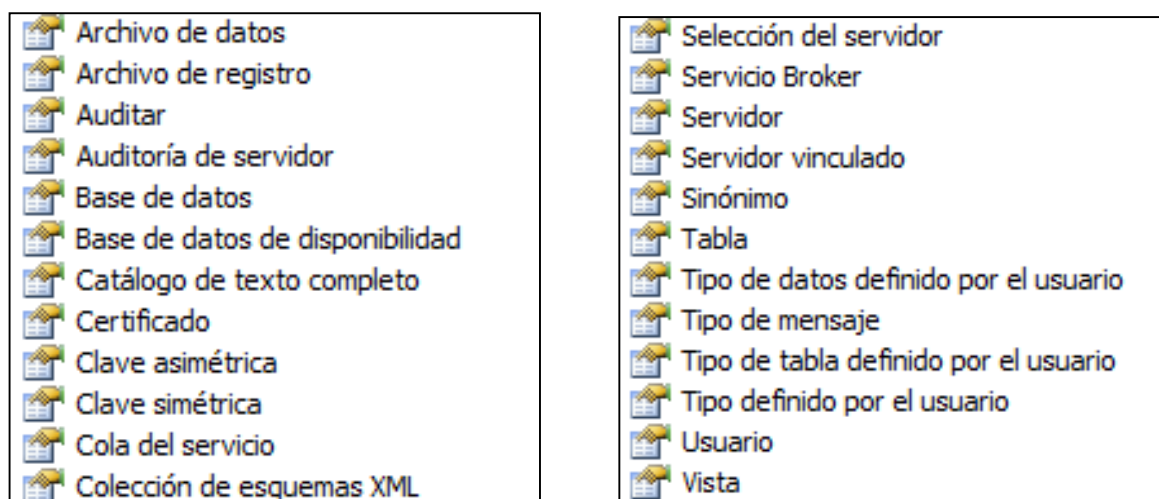
- El objetivo de la directiva es la instancia de SQL Server llamada **SQL01**.
- La faceta involucrada son los Inicios de sesión que contiene todas las propiedades relacionadas a los inicios de sesión (Login) SQL Server.
- La condición a crear, en base al facet **logins**, contendría una sola cláusula que exija que el campo **@Password ExpirationEnabled** tenga un valor de **True**.
- Finalmente, se debería crear la directiva que refuerce esta condición contra el target **SQL01**.

2.1 Implementación de una directiva

Los pasos para implementar una directiva son los siguientes:

1. **Seleccionar la faceta que contiene la propiedad a controlar**

Lo primero en determinar es qué faceta es la que se desea controlar. Como se ha visto anteriormente, una faceta es un agrupador de propiedades. La agrupación es por objetos, componentes del servidor o base de datos. A continuación, se muestran algunos ejemplos de facetas con las que se puede trabajar.



2. **Definir la condición que se debe cumplir**

La condición es una expresión booleana, es decir, su aplicación debe retornar un valor de verdadero o falso.

La expresión de la condición se construye en base a las propiedades de la faceta seleccionada. La condición es la que va a definir si la directiva se cumple o no, en función al valor de retorno. Si la expresión retorna falso, la directiva no se cumple. Asimismo, si la expresión retorna verdadero, la directiva sí se cumple.

La expresión puede ser simple, con una sola comparación de valores o puede ser compuesta utilizando varias propiedades enlazadas mediante operadores lógicos, tal como se muestra en la figura.

Nombre: ConfiguraciónBD

Faceta: Base de datos

Expresión:

	Y/O	Campo		Operado	Valor	
		@AutoClose	...	=	False	...
	AND	@AutoCreateStatisticsEn...	...	=	True	...
	AND	@AutoShrink	...	=	False	...
▶	AND	@AutoUpdateStatisticsEn...	...	=	True	...

3. Definir la directiva que contiene los objetivos y filtros

Una vez determinada la faceta y la condición, se debe crear la directiva que se va a validar.

En las directivas se pueden especificar un destino u objetivos. Como se ha visto anteriormente, un objetivo es aquella entidad que podrá ser afectada por las directivas, es decir, la directiva no se tiene necesariamente que aplicar a todos los servidores o bases de datos, si no que puede establecer condiciones para acotar o limitar el ámbito de alcance de la directiva.

Nombre: ValidaConfiguraciónBD

☐ Habilitado

Condición de comprobación: ConfiguraciónBD

Para destinos:

☒ Todas Database ←

Modo de evaluación: A petición

Restricción de Server: Ninguna ←

Un ejemplo de esto es que, si se implementa una directiva que usa una faceta de base de datos, se puede especificar mediante una condición que la directiva debe ser evaluada, únicamente, en bases de datos que se llamen de una manera particular.

Campo		Operado	Valor	
@Name	...	LIKE	'AdventureWorks%'	...

Condición de comprobación: CondNombreTabla


Para destinos:

☒ Toda Table
en bdAW Database

Modo de evaluación: A petición

Restricción de Server: CondServProd

Campo		Operado	Valor	
@NetName	...	LIKE	'%PROD%'	...



Del mismo modo, si se va a desplegar la directiva a través de varios servidores, se puede especificar mediante una condición que la directiva debe ser evaluada, únicamente, en servidores que cumplen determinada característica.

4. Verificar si SQL Server cumple con la directiva

Existen diferentes formas de verificar si una directiva se cumple o no. Los modos de evaluación permiten definir cómo se hará. Puede ser una directiva de monitoreo a demanda, programada o una directiva de cumplimiento forzado que limita las acciones de los usuarios.

También, hay distintos modos de registros de la acción, para que quede una huella de lo sucedido y se tenga información histórica para revisar, inclusive, en caso de una auditoría.

3. Forzar el cumplimiento de una directiva


Forzar el cumplimiento de una directiva

Modos de evaluación de una directiva:

- **A petición.**- Evalúa la directiva cuando lo requiera el usuario.
- **Al cambiar: impedir.**- Impide que una acción se cumpla si viola la directiva.
- **Al cambiar: solo registrar.**- Utiliza la notificación de eventos para evaluar una directiva.
- **Al programar.**- Utiliza un trabajo del Agente SQL Server para evaluar una directiva periódicamente.

2 - 19

Copyright © Todos los Derechos Reservados - Cibertec Perú S.A.C.



Para aplicar una directiva, se debe definir el modo de evaluación, que define cómo y en qué momento se va a llevar a cabo una evaluación.

3.1 Modos de evaluación de directivas

El DMF de SQL Server brinda cuatro modos de evaluación de directivas:

- **A petición**
No realiza un chequeo automático de la directiva, sino que permite hacerlo a discreción y de manera manual.
- **Al programar**
Permite programar la ejecución automática de la directiva usando el agente SQL Server, asimismo, se crea un registro cada vez que la directiva se ejecuta y encuentra una ocurrencia de no cumplimiento de esta.
- **Al cambiar: solo registrar**
Crea un registro cada vez que se encuentra una ocurrencia de no cumplimiento de una directiva.
- **Al cambiar: prevenir**
Cada vez que se encuentra una acción que no cumpla una directiva, será impedida de ejecutarse.

Cabe recordar que las políticas y condiciones DMF son almacenadas en la base de datos **msdb**, por lo que es conveniente realizar una copia de seguridad de manera frecuente de esta base de datos.

Es importante notar que una política se creará, por defecto, deshabilitada, por lo que se marca la opción **Habilitar al momento de crear la directiva**. Cuando la directiva está deshabilitada, solo se puede ejecutar a petición.

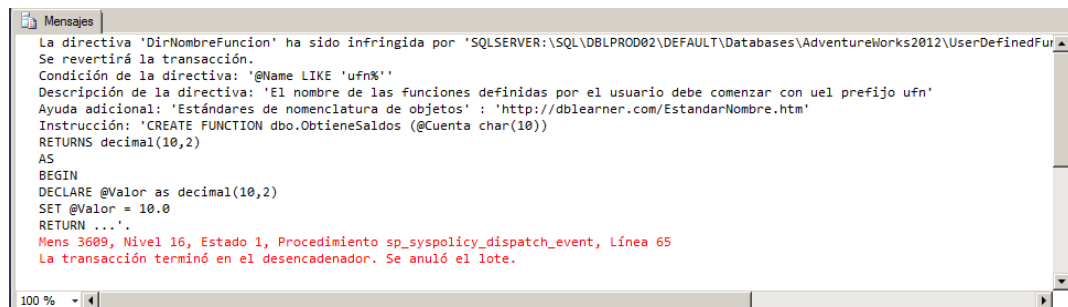
3.2 Forzar el cumplimiento de una directiva

El DMF ofrece la posibilidad de forzar el cumplimiento de una directiva, obligando que la condición de la directiva se cumpla, evaluando la acción del usuario en el momento que la realiza.

Solo son ciertas facetas que tienen propiedades que permiten forzar el cumplimiento de la directiva en tiempo de ejecución. Para que esto se cumpla, al momento de diseñar la directiva se debe seleccionar el modo de evaluación **Al cambiar: impedir**.

Este modo de evaluación, evalúa la directiva en tiempo de ejecución e impide ejecutar alguna acción o comando si este va en contra a lo especificado en la condición de la directiva.

Esta acción puede ser ejecutada por un usuario o por una aplicación. En caso fuera ejecutado por una aplicación, se debe implementar el control de errores adecuado para manejar el rechazo de la acción, por parte de la directiva como una excepción.



Este modo de evaluación, que permite forzar el cumplimiento de la directiva, garantiza que se cumplan los estándares definidos por los administradores de bases de datos. Este tipo de directivas se pueden desplegar a todos los servidores para garantizar uniformidad de estándares en toda la organización.

Operativamente, este tipo de directivas utiliza desencadenadores DDL para evaluar y de esta forma, evitar cualquier infracción de las directivas.

**Nota**

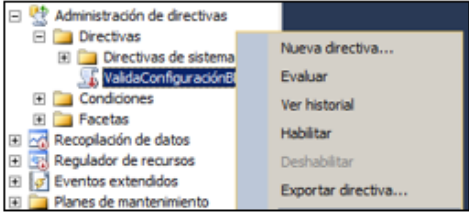
Las directivas con modo de evaluación **Al cambiar: impedir**, tienen que estar habilitadas para ser evaluadas.

4. Monitorear el cumplimiento de una directiva

Monitorear el cumplimiento de una directiva

Ejecución a demanda a través de diferentes opciones.

- Individualmente: Opción Evaluar en el menú contextual de cada directiva.



2 - 18 Copyright © Todos los Derechos Reservados - Cibertec Perú S.A.C.

Existen otros modos que pueden ser utilizados, de acuerdo a las necesidades de los administradores.

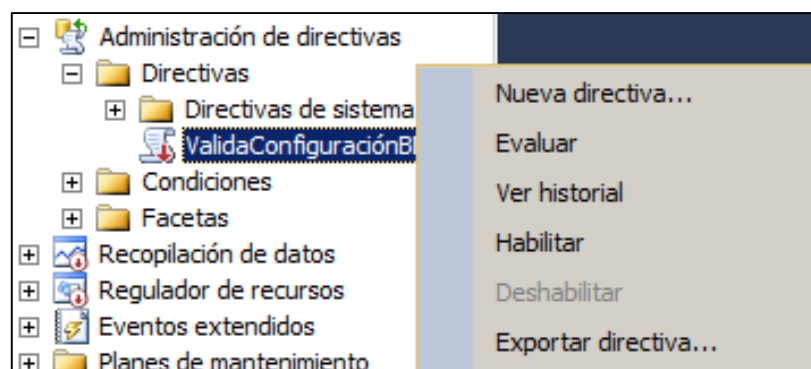
4.1 Ejecución a demanda

Este tipo de ejecución permite al usuario decidir en qué momento va a evaluar la directiva. Se utiliza para directivas de uso ocasional o directivas específicas que se utilizan una sola vez.

Hay varias formas en las que los administradores pueden ejecutar las directivas a demanda.

Evaluación individual

Una de ellas es individualmente por cada directiva. Para ello, se puede utilizar SQL Server Management Studio y en la carpeta **Directivas**, que forma parte del nodo Administración, ubicar la directiva que se desea evaluar, invocar el menú contextual haciendo clic derecho y seleccionar la opción **Evaluar**.

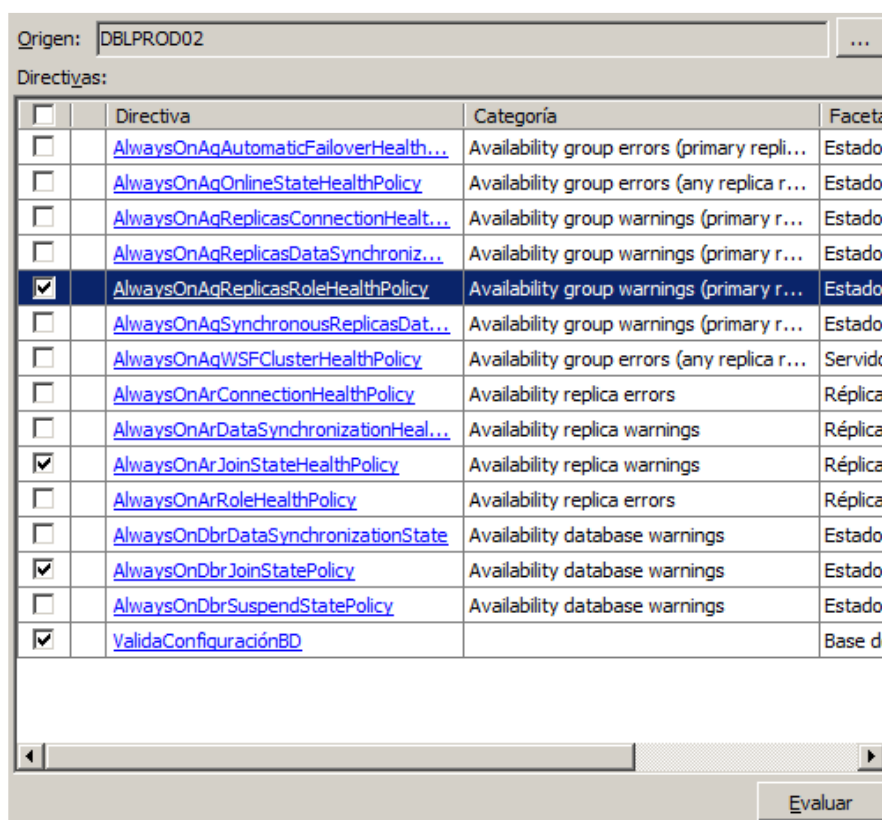


Nótese que la directiva está deshabilitada, lo cual no representa inconvenientes para este modo de evaluación. Además, que en el menú contextual cuenta con la opción **Ver historial**, el cual permite ver toda la historia de ejecuciones de la directiva, para analizar los cambios en el tiempo o para revisiones de auditoría.

Evaluación masiva

Otra forma en la que los administradores pueden ejecutar las directivas a demanda; es de forma masiva.

Para ello, se utiliza **SQL Server Management Studio** y en la carpeta de Directivas que forma parte del nodo administración, invocar el menú contextual haciendo clic derecho y seleccionar la opción **Evaluar**.



En este caso, aparecen en una ventana todas las directivas, de usuario y del sistema, agrupadas por categoría. En el lado izquierdo, se cuenta con cajas de chequeo por cada directiva, las cuales pueden ser seleccionadas por el administrador de base de datos.

Esto permite a los administradores, ejecutar varias directivas a la vez, facilitando la evaluación de las mismas.

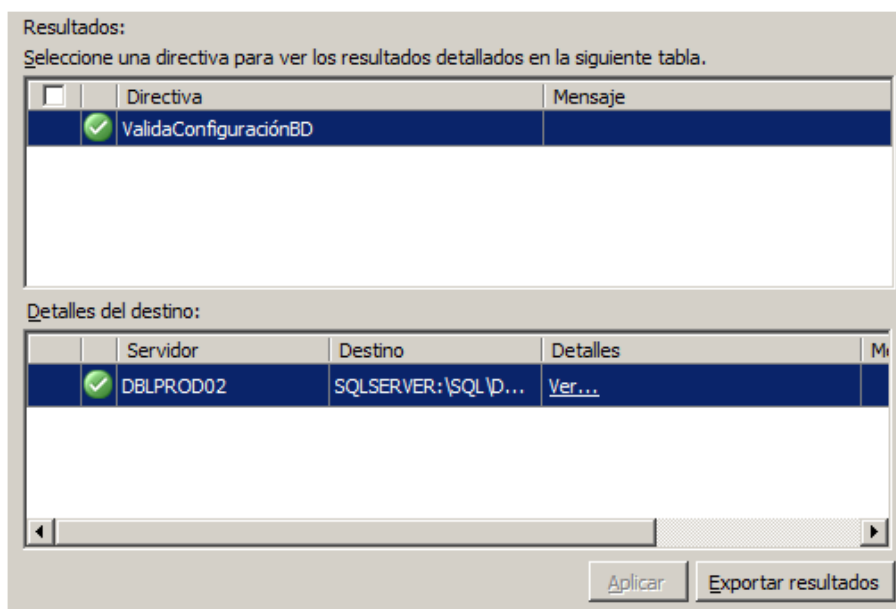
Análisis de resultados

Cuando se evalúa una directiva, el sistema muestra el resultado de dos maneras:

- El resultado general explica en la primera sección si la directiva se ha cumplido. Si esto es así, el sistema muestra un ícono circular de color verde con el símbolo de check.
- Si la política no se ha cumplido el sistema muestra un ícono circular de color rojo con una X.

Para que una directiva se cumpla, todas las evaluaciones a nivel de detalle se deben haber cumplido. El detalle muestra la evaluación en todos los destinos definidos.

Un destino puede ser un objeto, una base de datos o un servidor. Basta que una evaluación, a nivel de detalle de destino, no se cumpla para que toda la política no se cumpla.



Por esto último, es que el sistema también muestra el detalle de los destinos y si la directiva se cumplió o no en dicho destino, mostrando los íconos explicados anteriormente.

Cada vez que se evalúa una directiva, los resultados se van almacenando en la base de datos **msdb** y se pueden revisar a través del historial de la directiva.

Adicionalmente, por cada destino evaluado, el sistema muestra un detalle de las condiciones de las directivas que han sido utilizadas para la evaluación. Como se observa en la figura de resultados, en la sección de detalles del destino, por cada destino evaluado se muestra un enlace en la columna detalles. Cuando se invoca este enlace se muestran las condiciones y si se cumplieron o no.

	Y/O	Resultado	Campo	Operado	Valor esperado	Valor real
✓		✓	@AutoCreateStatisticsEna...	=	True	True
	AND	✓	@AutoShrink	=	False	False
	AND	✓	@AutoUpdateStatisticsEna...	=	True	True

Nótese que para cada condición, se muestran los íconos de conformidad o no conformidad. Basta que una condición no se cumpla para que la directiva no sea conforme.

Esta ventana muestra, detalladamente, el campo o propiedad de la faceta, el operador y el valor esperado. Al lado muestra el valor real para que en caso de que la condición no se cumpla, poder determinar el por qué.

Esta opción también permite hacer cambios en la configuración del destino de modo que se adecúe a la directiva y quede en estado conforme.

4.2 Ejecución programada

Con el objetivo de poder programar la evaluación de directivas, se cuenta con el modo de **evaluación al programar**, este modo permite establecer un plan de ejecución periódica.

La ejecución del modo de **evaluación al programar** está soportada por el agente de SQL Server. Los programas son los mismos utilizados para programar un trabajo del agente de SQL Server.

Se pueden establecer periodicidades diarias, semanales, mensuales, etc., así como, el horario de ejecución, pudiendo evaluar una directiva más de una vez al día.

Como la ejecución se realiza de forma desatendida, el resultado de la evaluación no se puede revisar en tiempo de ejecución. En este caso el resultado de la directiva es almacenada en el historial, desde el cual los administradores pueden analizar posteriormente el resultado de la evaluación.

5. Best Practice Analyzer basado en directivas

Best Practice Analyzer basado en directivas

Microsoft SQL Server BPA es una herramienta de diagnóstico que realiza lo siguiente:

- Obtiene información sobre el servidor y sobre instancias de SQL Server desde la versión 2012.
- Determina si las configuraciones están definidas, de acuerdo a las mejores prácticas recomendadas.
- Reportes sobre configuraciones, indicando definiciones que difieren de la recomendación.
- Indica potenciales problemas en las instancias instaladas de SQL Server.
- Recomienda soluciones a potenciales problemas.
- Requiere Microsoft Baseline Configuration Analyzer 2.0.

2 - 23

Copyright © Todos los Derechos Reservados - Cibertec Perú SAC.



Best Practice Analyzer (BPA) es una herramienta de análisis que permite validar las configuraciones de SQL Server, para las versiones 2012, 2014 y 2016.

Con esta herramienta se podrá obtener información sobre el estado y configuración del servidor y sobre sus instancias de SQL Server. A través del análisis, se podrá determinar si las configuraciones del servidor o bases de datos están definidas, de acuerdo a las mejores prácticas recomendadas por el equipo de SQL Server de Microsoft.

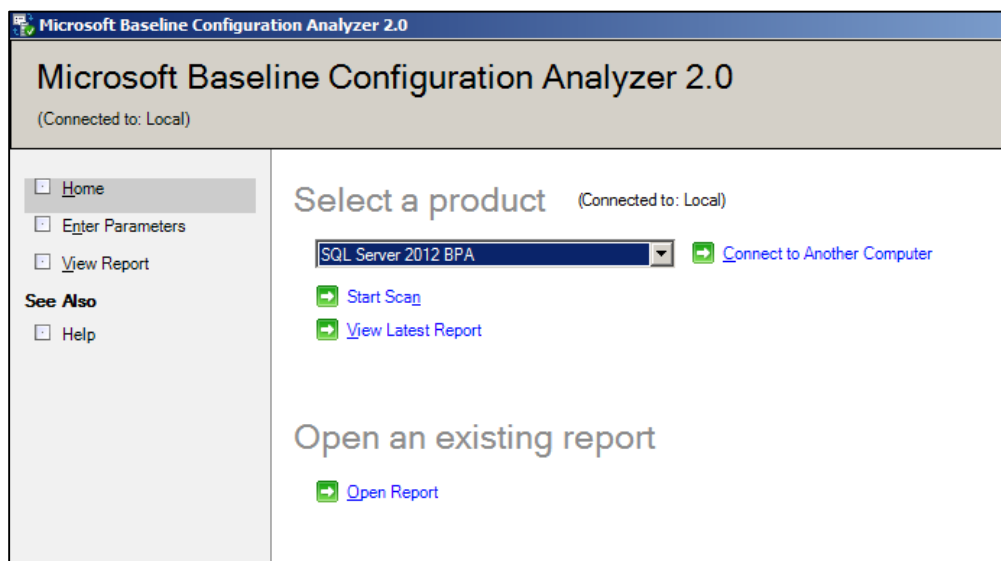
Como resultado de la ejecución de la herramienta se emiten reportes sobre las configuraciones, acompañado de indicaciones con las definiciones que difieren de la recomendación de mejor práctica.

Estos reportes indican cuáles son los potenciales problemas en las instancias instaladas de SQL Server y para cada indicación, sugiere o recomienda soluciones a los potenciales problemas detectados. BPA no resuelve los problemas automáticamente. Ese trabajo debe ser llevado a cabo por los administradores de los servidores.

La ejecución de BPA puede ser contra la instancia o instancias locales, así como, instancias remotas, permitiendo administrar la ejecución desde un solo computador.

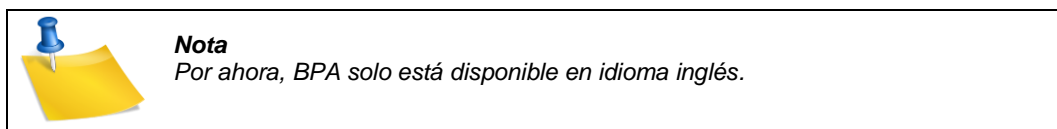
Para poder instalar y ejecutar BPA se requiere instalar previamente, la herramienta Microsoft Baseline Configuration Analyzer 2.0, el cual sirve de base para el funcionamiento de BPA.

Otro requisito de BPA es **PowerShell 2.0**.



El uso de esta herramienta se basa en la necesidad de una correcta configuración de servidores SQL Server, considerada una tarea importante dentro de la administración de equipos. La apropiada configuración de los servidores y bases de datos dará a un servidor, mayor velocidad de respuesta, estabilidad en la operación y mayores niveles de seguridad.

Si no se tuviera disponible la herramienta BPA, realizar este trabajo podría resultar complejo y tedioso, sobre todo cuando las alternativas de configuración, varían de acuerdo a cada equipo e incluso se modifican a través del tiempo.



5.1. Ejecución de BPA

Para ejecutar BPA se deben seleccionar los ámbitos de aplicación. BPA provee los siguientes ámbitos de aplicación:

- **Engine:** motor de base de datos.
- **Replication:** replicación de bases de datos.
- **Setup:** configuraciones de servidor.
- **Analysis Services:** servicios de análisis.
- **Integration Services:** servicios de integración.
- **Reporting Services:** servicios de reportes.

Cuando un administrador ejecuta BPA puede seleccionar cualquier combinación de los ámbitos, según se requiera.

Una vez seleccionados los ámbitos de aplicación se debe hacer clic en la opción de inicio del análisis.

Luego de ejecutar BPA, se obtienen los siguientes resultados:

- Conformidad/no-conformidad: los resultados de conformidad se dan cuando se cumple la condición de una regla de mejor práctica. La no conformidad se da cuando la condición no se cumple.
- Impacto de la no-conformidad.
- Recomendaciones.
- Links a información, detallado sobre la regla.