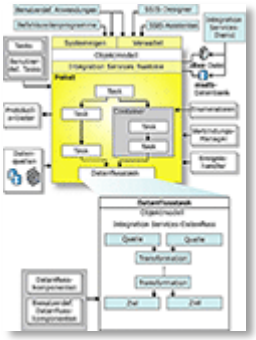
Reporting Services – Dienstarchitektur

Comelio

Reporting Services – Dienstarchitektur

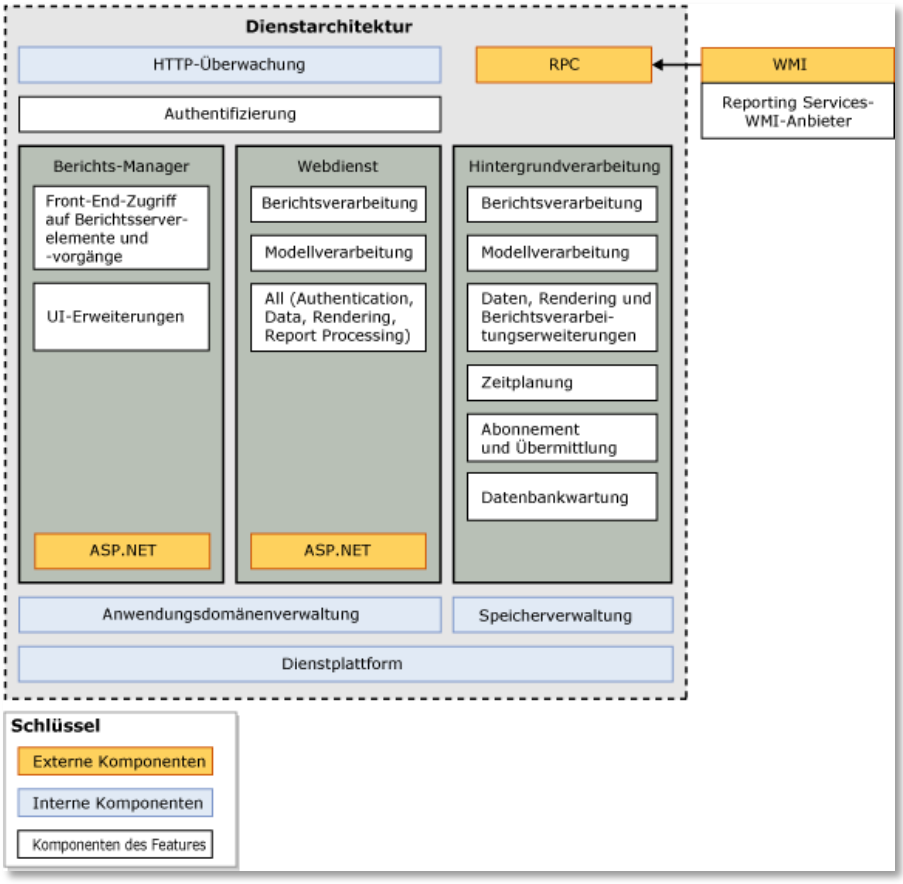


In Reporting Services wird ein Berichtsserver als ein Windows-Dienst implementiert, der aus unterschiedlichen Featurebereichen besteht, die wiederum in separaten Anwendungsdomänen ausgeführt werden. Der Dienst hostet den Berichts-Manager, den Report Server-Webdienst und Hintergrundverarbeitungs-Featurebereiche. In diesem Thema wird die Zusammensetzung des Diensts so beschrieben, dass Sie eine fundierte Entscheidung darüber treffen können, welche Features aktiviert und wie eventuelle Probleme behoben werden sollen.

Dienstarchitektur

Architekturdiagramm

Im folgenden Diagramm wird die Dienstarchitektur in Reporting Services dargestellt.



Nicht alle Berichtsserverfunktionen werden im Architekturdiagramm dargestellt. So sind z.B. die Initialisierung und umkehrbare Verschlüsselung wichtige Servervorgänge, die außerhalb des Bereichs der drei im Diagramm dargestellten Featurebereiche existieren.

Dienst und Infrastruktur

Der Report Server-Windows-Dienst ist ein zusammengefasster Satz Anwendungen, die in einem einzelnen Prozess, unter einem einzelnen Konto, mit Zugriff auf eine einzelne Berichtsserver-Datenbank und einen Satz Konfigurationsdateien ausgeführt werden. Die Konfigurationseinstellungen für den gesamten Dienst werden in ReportServer.config, ReportServerServices.exe.config und der Berichtsserver-Datenbank gespeichert.

Innerhalb des Diensts werden der Berichts-Manager, der Webdienst und die Hintergrundverarbeitung in separaten Anwendungsdomänen ausgeführt. Obwohl alle drei Featurebereiche standardmäßig aktiviert sind, können Sie konfigurieren, welche Teile des Diensts zu einem bestimmten Zeitpunkt verfügbar sind. So können Sie z. B. den Webdienst deaktivieren, wenn Sie keine bedarfsgesteuerte oder interaktive Berichterstellung unterstützen möchten.

Obwohl die Serverfeaturebereiche in getrennte Anwendungsdomänen isoliert werden, werden die Speicherverwaltung und die Prozesssicherheit für den Dienst insgesamt verwaltet. Arbeitsspeicherschwellenwerte werden für den Dienst in seiner Gesamtheit konfiguriert. Der Berichtsserver verarbeitet Wiederverwendungsaktionen als interne Vorgänge. Sie können bei Bedarf keine einzelnen Teile des Diensts wiederverwenden. Aber Sie können Konfigurationseinstellungen angeben, die festlegen, wie lange permanente Verbindungen geöffnet gehalten werden.

Falls Sie die Featurebereiche eines Diensts zwischen mehreren Instanzen segmentieren (z.B. den Berichts-Manager in einer ersten, den Webdienst in einer zweiten und die Hintergrundverarbeitung in einer dritten Instanz aktivieren), beziehen sich die Speicher- und Konfigurationseinstellungen auf die Anwendungen, die in dieser speziellen Instanz ausgeführt werden. Beachten Sie, dass selbst beim Segmentieren der Featurebereiche des Diensts gegenseitige Abhängigkeiten bestehen. Eine vollständige Berichtsserverinstallation verwendet in der Regel alle drei Instanzen.

HTTP-Überwachung

Reporting Services bietet einen HTTP-Listener, der eingehende Anforderungen überwacht, die an HTTP.SYS an einem bestimmten Port auf dem lokalen Computer geleitet werden. Der Hostname und der Port werden während einer URL-Reservierung angegeben, wenn Sie den Server konfigurieren. Je nach verwendetem Betriebssystem kann der angegebene Port für andere Anwendungen freigegeben werden.
Der HTTP-Listener implementiert das HTTP 1.1-Protokoll. Er verwendet die im Betriebssystem integrierten HTTP.SYS-Funktionen. Daher sind für Reporting Services Betriebssysteme erforderlich, die HTTP.SYS als interne Komponente einschließen.Wenn der HTTP-Listener eine Anforderung verarbeitet, wird sie zur Überprüfung der Benutzeridentität an die Authentifizierungsebene weitergeleitet. Der Report Server-Webdienst wird aufgerufen, nachdem die Anforderung authentifiziert wurde.
Der HTTP-Listener verwendet Version 1.0 der HTTP-Server-API.

Authentifizierungsebene

Reporting Services schließt eine Authentifizierungsebene ein, welche die Identität des Benutzers oder der Anwendung überprüft, von dem bzw. von der die Anforderung gestellt wird. Die folgenden Authentifizierungstypen werden unterstützt: integrierte Sicherheit von Windows, NTLM-Authentifizierung, Standardauthentifizierung, Formulare oder benutzerdefinierte Authentifizierung und anonymer Zugriff. Reporting Services verwendet standardmäßig die integrierte Sicherheit von Windows und die NTLM-Authentifizierung. Sie können jedoch in den Konfigurationsdateien einen anderen Authentifizierungstyp festlegen. Jede Berichtsserverinstanz kann genau für einen Authentifizierungstyp konfiguriert werden. Wenn Sie eine Bereitstellungskonfiguration für horizontales Skalieren verwenden, muss jeder Knoten der Umgebung den gleichen Authentifizierungstyp aufweisen.
Die Berichtsserverauthentifizierung operiert innerhalb des Kontexts der Netzwerk-Sicherheitseinstellungen und der Clientanwendungen. Die erfolgreiche Verwendung eines besonderen Authentifizierungstyps richtet sich nach den Browser- und Netzwerk-Sicherheitsfeatures. Für die Verwendung der integrierten Windows-Sicherheit ist es z. B. erforderlich, dass Sie Internet Explorer verwenden, über die Kerberos-Netzwerkauthentifizierung verfügen und dass der Identitätswechsel aktiviert ist. Falls Sie überdies die integrierte Sicherheit für Berichtsdatenquellen-Verbindungen verwenden möchten, muss auch die Delegierung aktiviert sein, um nachfolgende Verbindungen mit Remotedatenquellen zuzulassen.

Berichts-Manager

Der Berichts-Manager ist ein Client ohne Speicherbedarf, der einen Web-Front-End-Zugriff auf den Report Server-Webdienst bietet. Er ist das im Lieferumfang enthaltene Tool zum Anzeigen und Verwalten von Berichtsserverinhalt und -vorgängen.

Standardmäßig stellt er den Front-End-Zugriff auf den Webdienst bereit, der in der gleichen Serverinstanz ausgeführt wird. Falls der Webdienst nicht in der Serverinstanz aktiviert ist, können Sie mit dem Berichts-Manager auf einen Report Server-Webdienst in einer anderen Instanz oder auf einem anderen Computer verweisen, indem Sie eine URL in den Konfigurationsdateien festlegen.

Der Berichts-Manager wird innerhalb einer Browsersitzung auf dem Clientcomputer ausgeführt. Es gibt keine Anwendungsdateien oder Einstellungen, die auf dem Client gespeichert werden. Der Sitzungszustand wird beibehalten, solange das Browserfenster geöffnet ist. Die benutzerspezifischen Einstellungen werden in der Berichtsserver-Datenbank gespeichert und wiederverwendet, wenn der Benutzer eine Verbindung mit dem Berichts-Manager herstellt.

Der Berichts-Manager kann auf den Abonnementdefinitionsseiten benutzerdefinierte Erweiterungseinstellungen für die Übermittlung aufnehmen. Falls Sie benutzerdefinierte Übermittlungserweiterungen erstellen und bereitstellen, kann der Berichts-Manager Optionen und Text für diese Erweiterung dynamisch anzeigen.

Um den Berichts-Manager zu verwenden, müssen Sie für die Anwendung eine URL definieren. Sie können den Berichts-Manager wirksam deaktivieren, indem Sie die URL erst gar nicht erstellen. Falls Sie in der Standardkonfiguration Reporting Services installiert haben, ist die URL bereits erstellt. Sie müssen diese dann löschen, wenn Sie die Anwendung deaktivieren möchten.

Wenn Sie den Berichtsserver so konfigurieren, dass er im integrierten SharePoint-Modus ausgeführt wird, wird der Berichts-Manager deaktiviert. Sie können den Berichts-Manager nicht auf einem Berichtsserver verwenden, der im integrierten SharePoint-Modus ausgeführt wird, selbst wenn Sie die URL zuvor konfiguriert haben.

Report Server-Webdienst

Der Report Server-Webdienst ist das Hauptmodul für alle bedarfsgesteuerten Berichts- und Modellverarbeitungsanforderungen, die von einem Benutzer oder einer Anwendung in Echtzeit initiiert werden, einschließlich der meisten Anforderungen, die an den und vom Berichts-Manager geleitet werden.

Der Report Server-Webdienst führt eine End-To-End-Verarbeitung von Berichten aus, die bei Bedarf ausgeführt werden. Zur Unterstützung der interaktiven Verarbeitung authentifiziert der Webdienst den Benutzer und prüft die Autorisierungsregeln vor der Verarbeitung einer Anforderung. Der Webdienst unterstützt die Standardsicherheitserweiterung von Windows sowie benutzerdefinierte Authentifizierungserweiterungen.

Der Webdienst ist auch die primäre programmgesteuerte Schnittstelle für benutzerdefinierte Anwendungen, die mit dem Berichtsserver integriert werden. Wenn Sie eine benutzerdefinierte Benutzeroberfläche bereitstellen, können Sie den Webdienst ohne Berichts-Manager verwenden.

Hintergrundverarbeitung

Die Hintergrundverarbeitung verweist auf Vorgänge, die im Hintergrund ausgeführt und vom Berichtsserver initiiert werden. Die Hintergrundverarbeitung besteht meist aus der geplanten Berichtsverarbeitung und der Abonnementverarbeitung. Sie umfasst aber auch die Verwaltungsaufgaben der Berichtsserver-Datenbank.

Die Hintergrundverarbeitung für Planung, Abonnement und Bereitstellung kann konfiguriert und über das Facet der Oberflächenkonfiguration für Reporting Services der richtlinienbasierten Verwaltung in Management Studio deaktiviert werden. Wenn Sie diese Vorgänge deaktivieren, steht die geplante Berichts- oder Modellverarbeitung in der aktuellen Dienstinstanz nicht zur Verfügung. Die Datenbankverwaltung ist eine wesentliche Aufgabe, die nicht deaktiviert werden kann, da der Server im Betriebszustand bleibt.

Die Hintergrundverarbeitungsvorgänge benötigen eine Front-End-Anwendung oder den Webdienst für eine Definition. Zeitpläne und Abonnements werden auf den Anwendungsseiten des Berichts-Managers oder auf einer SharePoint-Website erstellt, falls der Berichtsserver für die SharePoint-Integration konfiguriert ist. Anschließend werden sie an den Webdienst weitergeleitet, der die Definitionen in der Berichtsserver-Datenbank erstellt und speichert.

Wie im Diagramm der Dienstarchitektur dargestellt, werden sowohl die Authentifizierung als auch die Speicherverwaltung von der Hintergrundverarbeitung anders durchgeführt als vom Berichts-Manager und dem Webdienst. Hintergrundprozesse überprüfen mithilfe von Authz.dll, ob das Benutzerkonto, das zum Erstellen des Abonnements verwendet wurde, noch über die erforderlichen Berechtigungen zum Anzeigen des Berichts verfügt. Durch diese Prüfung wird gewährleistet, dass der Benutzer, der den Bericht erhalten soll, ein gültiger Windows-Benutzer in der Domäne ist. Alle anderen Berichts- und Modellverarbeitungsvorgänge, die als Hintergrundprozess ausgeführt werden, werden unter der Identität des Kontos für die unbeaufsichtigte Ausführung angefordert.