Acesso ao Analysis Services via HTTP/HTTPS: Arquitecturas, Configurações e Mecanismos de Autenticação e Controlo de Acesso

Carlos Rui Gouveia Carvalhal

Resumo: **O Analysis Services disponibiliza três Mecanismos de Acesso: Acesso Directo, Acesso HTTP/HTTPS e Acesso XMLA. De entre estes, o Mecanismo de Acesso Directo é aquele que garante o melhor desempenho em termos de tempo de resposta e segurança, características que o tornam no Mecanismo de Acesso de uso preferencial. No entanto, este mecanismo só pode ser usado nos acessos intra-domínio, devido às limitações do Mecanismo de Autenticação que utiliza, a Integrated Windows Authentication. Nas situações em que o Cliente e o Analysis Services não partilham o mesmo domínio, ou quando se pretende que o acesso seja feito via Internet, pode ser usado o Mecanismo de Acesso via HTTP/HTTPS. No entanto, a utilização deste mecanismo de acesso não é trivial, apresentado algumas peculiaridades, pelo facto do Analysis Services não suportar acessos directos via HTTP/HTTPS, sendo necessário recorrer ao Servidor Web IIS.**

Neste artigo será analisado o Modelo Lógico e os Modelos Físicos de acesso ao Analysis Services via HTTP/HTTPS e descritas as configurações que têm de ser aplicadas ao IIS para este conseguir servir Acessos HTTP/HTTPS ao Analysis Server. Serão, ainda, analisados os Mecanismos de Segurança e Controlo de Acesso utilizados pelo Analysis Services, quer em termos de Autenticação dos Utilizadores, quer em termos de Definição de Security Roles.

Abstract: Analysis Services disposes three Access Mechanisms: Direct Access, HTTP/HTTPS Access and XMLA Access. From among these mechanisms, the Direct Access is that one that guarantees the lowest response time and the strongest security, characteristics that turn it the mechanism of preferential use. But this mechanism can be used only in intra-domain accesses, by imposition of the Authentication Mechanism that it uses, the Integrated Windows Authentication. When the Client and the Analysis Services doesn't share the same domain, or when the access must be made by Internet, can be used the HTTP/HTTPS Access Mechanism. However, the use of this mechanism is not trivial, presenting some peculiarities; a consequence of Analysis Services doesn't to support, by him self, HTTP/HTTPS Accesses. In fact, HTTP/HTTPS Access to Analysis Services is provided by the IIS Web Server.

In this paper, the Logical Model and the Physical Models, used by Analysis Services, to provide HTTP/HTTPS access thought the IIS Web Server, will be analyzed, and will be explained the steps required to setting it up. The Mechanisms of Security and Access Control, used by Analysis Services, will be analyzed too, being covered both Users Authentication and Security Roles Definition.

Palavras Chave: **OLAP, Aplicações Cliente OLAP, MS SQL Server Analysis Services, Mecanismos de Comunicação com o Analysis Services, Mecanismo de Acesso Directo, Mecanismo de Acesso via HTTP/HTTPS, Mecanismo de Acesso via XMLA, Mecanismos de Segurança e Controlo de Acessos ao Analysis Services, Mecanismos de Autenticação de Utilizadores, Definição de Security Roles no Analysis Services, Database Roles, Cube Roles, Mining Model Roles, Mecanismo de Memória Partilhada, Mecanismo de Named Pipes, Biblioteca Data Pump, PivotTable Services.**

I. INTRODUCÃO

Antes de iniciar a análise dos Mecanismos de Comunicação com o Analysis Services, é importante esclarecer que, a versão do Analysis Services na qual se baseia este documento é a que acompanha o MS SQL Server 2000, frequentemente designada MS SQL Server Analysis Services 2000, ou, duma forma mais compacta Analysis Services 2000 (AS2000). Este é um aspecto importante, pois, ao contrário do Analysis Services 2005 (abreviadamente AS2005, a versão que acompanha o MS SQL Server 2005), cujo Mecanismo de Comunicação nativo é o XMLA (de XML for Analysis, uma API XML, baseada no SOAP –Simple Object Access Protocol–, desenvolvida pela Microsoft com o objectivo de fornecer acesso aos dados, e funcionalidades, do Analysis Services às aplicações Cliente Web, sem ser necessário instalar do lado do Cliente nenhum software específico, nomeadamente o PivotTable Services –imposição que é apontada, frequentemente, como um obstáculo ao desenvolvimento de Aplicações Cliente OLAP baseadas no Analysis Services), os Mecanismos de Comunicação do AS2000 baseiam-se no PivotTable Services, i.e., todos os acessos ao Analysis Services têm de ser processados por uma instância do PivotTable Services. Apesar deste suportar, de forma não nativa, acessos via XMLA, esta funcionalidade requer a instalação, do lado o Servidor Web IIS, de uma Internet Server API (ISAPI), fornecida, pela Microsoft, sob a forma de um Software Development Kit (designado XML for Analysis SDK), que processa os pedidos XMLA e os transforma num formato

"consumível" pelo AS2000. (Notar que o acesso, ao AS2000, via XMLA não será analisado neste documento, mas sim num outro artigo.) E ainda, os acessos via HTTP/HTTPS, além de requererem a utilização do PivotTable Services do lado do Cliente, exigem configurações e procedimentos especiais do lado do Servidor Web, os quais serão analisados, detalhadamente, ao longo deste artigo.

Conforme já foi referido, o acesso ao AS2000, doravante designado Analysis Services, requer a instalação, do lado do Cliente, do PivotTable Services, mais precisamente do PivotTable Services 8.0, que implementa o OLE DB Provider for OLAP Services 8.0 (e também o ADO MD Provider) e requer a instalação do MDAC 2.6 (de MS Data Access Components, é a componente que contém as Core Data Access Components, tais como o OLE DB Provider, o ADO Provider e o driver ODBC) [9]. O ficheiro que instala ambas as componentes é o ptsfull.exe (existe também um ficheiro, o ptslite.exe, que instala somente o PivotTable Services 8.0, o que pressupõe que a máquina Cliente já tem instalado o MDAC 2.6), localizado no directório MSOLAP\Install\PTS do CD do MS SQL Server 2000 [9]. A Figura 1 apresenta a Arquitectura Cliente do Analysis Services, onde é possível verificar quais as componentes envolvidas na interacção entre as Aplicação Cliente e o PivotTable Services.

O Analysis Services suporta um Mecanismo de Acesso Directo, implementado através do protocolo SQL Analysis Services Protocol, um protocolo de rede da família TCP/IP que utiliza, por defeito, a Porta TCP 2725. Como não envolve nenhuma outra componente, este mecanismo de acesso garante uma taxa de transferência de dados elevada e um tempo de resposta reduzido, aspectos essenciais nas soluções OLAP. No entanto, o Mecanismo de Acesso Directo utiliza o Mecanismo de Autenticação Integrated Windows Authentication, que requer que os utilizadores estejam no mesmo domínio que o Analysis Server, o que inviabiliza a sua utilização nos acessos inter-domínios ou via Internet. Adicionalmente, a utilização da Porta TCP 2725 é outro condicionante à sua utilização nestas situações, pois, por razões de segurança, esta Porta está, normalmente, fechada nos Firewalls, não sendo, na maior parte dos casos, recomendável/desejável a sua abertura. A Figura 2 apresenta o modelo lógico (e também uma possível arquitectura física) usado por este mecanismo de acesso.

A Connection String usada nos Acessos Directos ao Analysis Services apresenta o formato "Provider=MSOLAP; Data Source=<OLAPServerName>; Initial Catalog= <OLAPDatabaseName>; [User ID=UserName; Password= UserPassword;]", onde <OLAPServerName> é a identificação do Analysis Server que se pretende aceder e <OLAPDatabaseName> é a BD OLAP que se pretende aceder. Apesar desta Connection String suportar a introdução de credencias, estes dados não serão utilizados, pelo Analysis Services, na autenticação do utilizador. No seu lugar, o Analysis Services, utilizará a credencial Windows do Utilizador, a qual (por imposição do Mecanismo de Autenticação usado, o Integrated Windows Authentication) terá de corresponder a uma Conta de Domínio, no Domínio no qual o Analysis Server (e a máquina Cliente) está instalado, e ter permissões de acesso ao Analysis Services.

No entanto, quando as máquinas em que correm a Aplicação Cliente e o Analysis Services não partilham o mesmo Domínio, não pode ser usado o Mecanismo de Acesso Directo, devendo ser usado o acesso via HTTP/HTTPS ou o acesso via XML. Ao longo deste

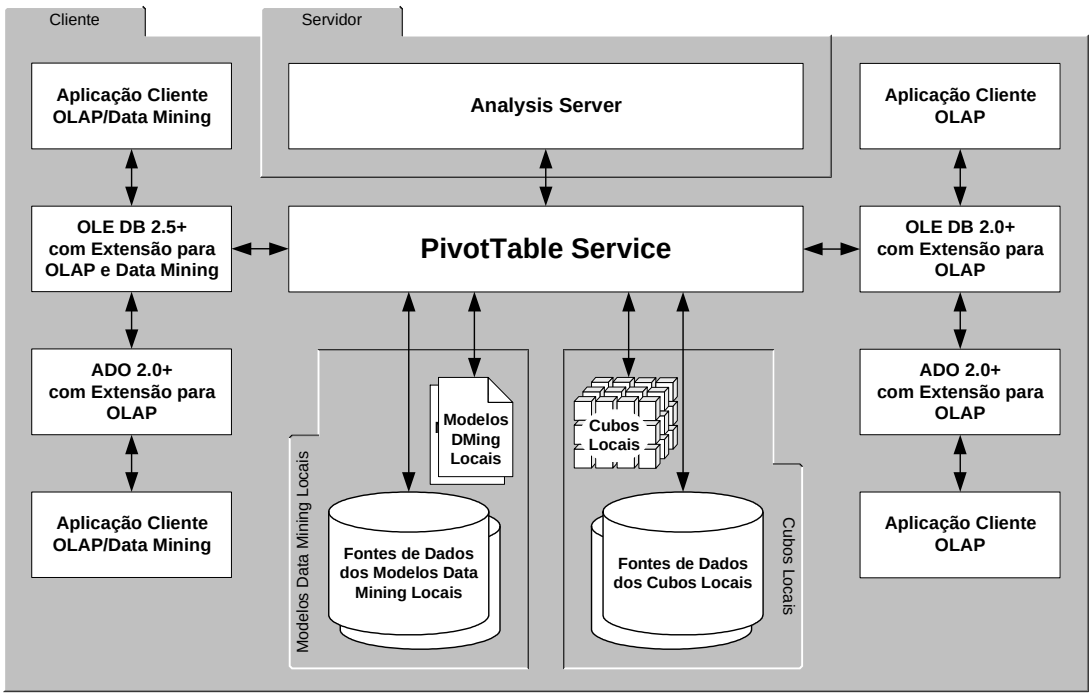

Figura 1: Arquitectura Cliente do Analysis Services. (Adaptado de [12])

artigo analisar-se-á o Mecanismo de Acesso via HTTP/HTTPS, sendo o Mecanismo de Acesso via XML coberto noutro artigo.

Convém salientar que o Mecanismo de Acesso via HTTP/HTTPS tem alguns inconvenientes, devendo, por este motivo, ser usado, somente, nas situações em que o Mecanismo de Acesso Directo não pode ser usado. Por um lado, os acessos ao Analysis Services via HTTP/HTTPS são mais lentos do que os acessos directos, pelo facto do Servidor Web IIS ter de processar os pedidos que chegam do PivotTable Services e as respostas dadas pelo Analysis Server. Por outro lado, a utilização do HTTP/HTTPS introduz vulnerabilidades na segurança do sistema.

II. ARQUITECTURA LÓGICA

Os Acessos via HTTP/HTTPS regem-se pelo modelo lógico representado na Figura 3, apresentando a Connection String o formato "Provider=MSOLAP; Data Source={http|https}://<IISOLAPServerName>/[<Path to msolap.asp>/]; Initial Catalog=<OLAPDatabaseName>; [User ID=UserName; Password=UserPassword;]", que difere da usada no Acesso Directo na forma como é identificada a fonte de dados OLAP (i.e., o Analysis Server). Nesta Connecion String o Analysis Server é identificado através do URL do Directório Virtual, do Servidor Web IIS, que contém a "aplicação" responsável pelo acesso ao Analysis Server. Quando o PivotTable Services recebe uma Connection String com este formato, utiliza o URL nela indicado (adicionando-lhe previamente a string "/msolap.asp") para aceder a uma Página Web ASP, específica e especial, designada msolap.asp, localizada no Web Site/Directório Virtual indicado pelo URL fornecido. (Apesar do ficheiro msolap.asp poder ser colocado no Directório Virtual Raiz, do Servidor Web, recomenda-se, por razões de segurança, a utilização de outro Directório Virtual.) Esta Página Web ASP permite aceder ao Objecto Data Pump, PUPump, implementado pela Biblioteca Data Pump, msmdpump.dll. Objecto este que comunica directamente com o Analysis Server, servindo-se da Página Web ASP para retornar, ao PivotTable Services, os dados e metadados resultantes. [2, 3]

No entanto, é de notar que a conectividade/acessibilidade via HTTP/HTTPS só está disponível na versão Enterprise do Analysis Services (MS Analysis Services Enterprise Edition), aquela que acompanha o MS SQL Server 2000 Enterprise Edition. [9, 8]

A Figura 3 descreve a arquitectura e fluxo de dados do processo de comunicação entre uma instância do PivotTable Services (a pedido de uma Aplicação Cliente) e o Analysis Server, via HTTP/HTTPS, usando o Objecto Data Pump. Sobre este diagrama estão identificados uma série de pontos, numerados de 1 a 9, que serão descritos a seguir [2]:

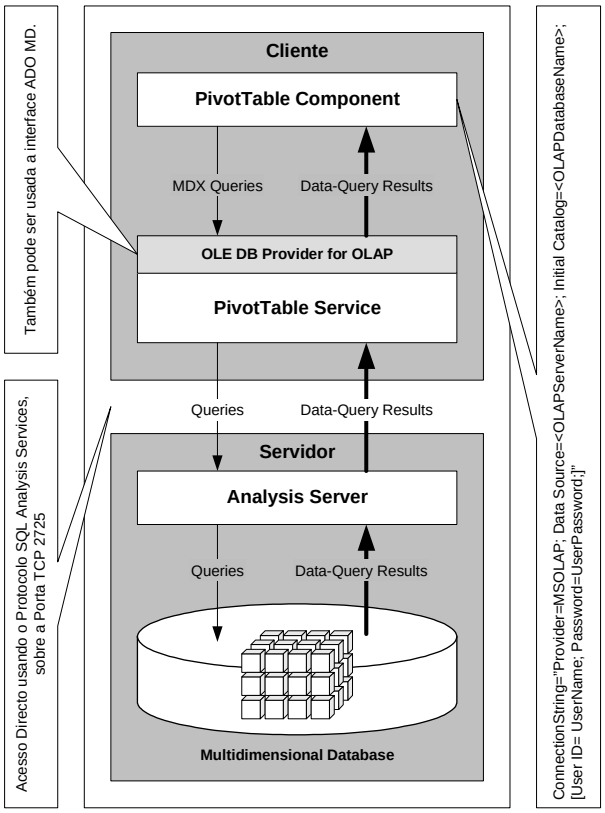

Figura 2: Arquitectura Lógica usada pelo Mecanismo de Acesso Directo ao Analysis Services.

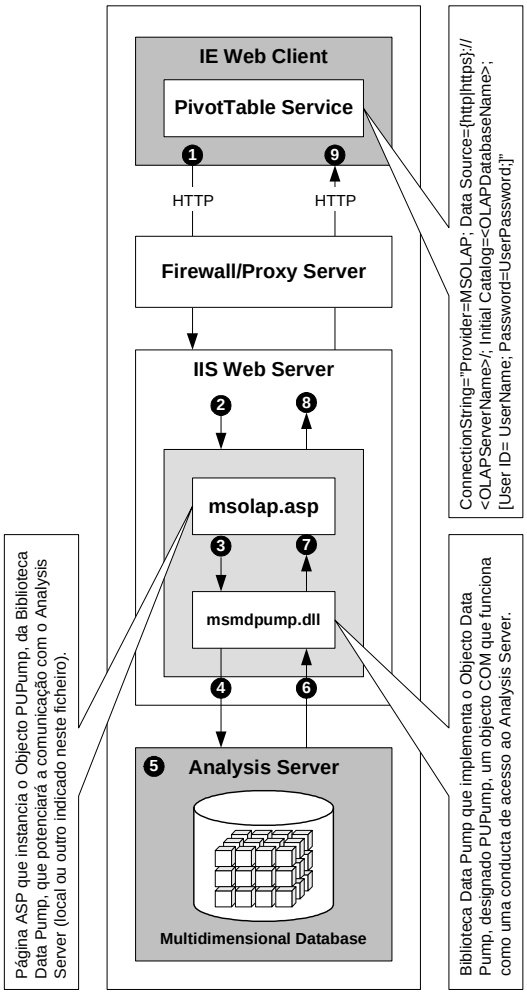

Figura 3: Arquitectura Lógica usada pelo Mecanismo de Acesso ao Analysis Services via HTTP/HTTPS. (Adaptado de [2].)

1. Uma Aplicação Cliente tenta aceder ao Analysis Services usando o PivotTable Services. Se for especificada uma URL na propriedade Data Source da Connection String, passada ao PivotTable Services, este adicionará a string "/msolap.asp" ao URL e utilizará o protocolo HTTP/HTTPS para enviar uma Mensagem-Pedido HTTP POST à página msolap.asp, incluindo a Connection String e outros dados e metadados na parte binária da mensagem.
2. O Servidor IIS recebe a Mensagem-Pedido HTTP POST e, se o pedido for validado com sucesso, instanciará a página msolap.asp. Como parte do processo de validação, o IIS estabelece o contexto de segurança no qual esta página vai ser executada. Se for utilizada a Basic Authentication o PivotTable Services trocará Mensagens HTTP Header com o IIS, passando-lhe as credenciais do utilizador (Username e Password). Do lado do Servidor Web, o IIS impersonalizará estes dados.
3. A página msolap.asp instancia o Objecto PUPump da Biblioteca Data Pump (msmdpump.dll).
4. O Objecto PUPump lê os dados da HTTP Stream, enviada pelo PivotTable Services como parte da Mensagem-Pedido HTTP POST, num buffer SAFEARRAY (usando o método BinaryRead do Objecto ASP Request) e envia este buffer para o Analysis Server especificado, não examinando de forma alguma o conteúdo da HTTP Stream.
5. O Analysis Server processa o pedido feito pelo Objecto PUPump, acedendo, para tal à BD OLAP.
6. O Analysis Server responde ao Objecto PUPump, com uma mensagem que contém dados e metadados.
7. O Objecto PUPump introduz (formatando convenientemente) estes dados e metadados num Buffer SAFEARRAY.
8. O Objecto PUPump escreve o conteúdo do Buffer SAFEARRAY numa HTTP Stream (usando o método BinaryWrite do Objecto ASP Response) e envia estes dados, para o IIS, como parte de uma Mensagem-Resposta HTTP POST.
9. O IIS envia o Stream HTTP para o PivotTable Services para o seu processamento.

III. ARQUITECTURA FÍSICA

Originalmente, a acessibilidade via HTTP/HTTPS ao Analysis Server requeria que o Analysis Services e o IIS partilhassem o mesmo Servidor Windows, pois a Biblioteca Data Pump usava, exclusivamente, o Mecanismo de Memória Partilhada na comunicação com o Analysis Server. No entanto, com o lançamento do Service Pack 3 (SP3) do MS SQL Server 2000 Analysis Services, a Biblioteca Data Pump passou a poder usar também o Mecanismo Named Pipes na troca de informação com o Analysis Server. O que permitiu ultrapassar a limitação inicial, pois, a utilização de Named Pipes permite instalar a Biblioteca Data Pump e o IIS, numa máquina distinta daquela em que está instalado o Analysis Services, incrementando, assim, a segurança e estabilidade do IIS e do Analysis Services. [2]

Dessa forma, a Biblioteca Data Pump pode ser configurada para usar um de dois mecanismos de transporte de dados na comunicação com o Analysis Server [2]:

- ***Mecanismo de Memória Partilhada:*** Originalmente a Biblioteca Data Pump usava o mecanismo de transporte de dados baseado em Ficheiros de Memória Partilhada para comunicar com o Analysis Server. Um Ficheiro de Memória Partilhada permite a partilha de memória entre duas ou mais aplicações recorrendo ao mapeamento de uma secção da memória virtual para um ficheiro, recorrendo, para tal, a um Objecto File-Mapping e ao uso de File Views para manipular o Ficheiro de Memória Partilhada. No caso do Analysis Services, o System Pagefile desempenha o papel de Ficheiro de Memória Partilhada, sendo usado na passagem de informação entre a Biblioteca Data Pump e o Analysis Server. Este mecanismo de transporte de dados é altamente recomendado nas arquitecturas físicas baseadas na Configuração de Computador Único (descrita mais adiante nesta secção), por razões de segurança e desempenho, não podendo ser usado, de forma alguma, com a Configuração Multi-Computador (também descrita mais adiante nesta secção) pois, a Biblioteca Data Pump e o Analysis Services têm de partilhar a mesma máquina.
- ***Mecanismo de Named Pipes:*** Conforme já foi referido atrás, a partir do SP3 do MS SQL Server 2000 Analysis Services, a Biblioteca Data Pump passou a dispor de mais um mecanismo de transporte de dados na comunicação com o Analysis Server, um mecanismo baseado em Named Pipes. Sendo usada, para tal a Named Pipe \\<ServerName>\pipe\PlatoNamedPipe. Este mecanismo de transporte de dados é recomendado nas arquitecturas físicas baseadas na Configuração Multi-Computador. Apesar de também poder ser usado com a Configuração de Computador Único, tal não é recomendado, por não ser tão eficiente (para esta configuração) quanto o Mecanismo de Memória Partilhada.

Conforme já foi referido, a Figura 3 descreve somente a Arquitectura Lógica do acesso ao Analysis Server via HTTP/HTTPS. Em termos físicos, existe uma multiplicidade de arquitecturas, que podem ser agrupadas em duas categorias [2]:

- ***Configuração de Computador Único:*** Nesta configuração o IIS (que contém a Biblioteca Data Pump, responsável pela conectividade HTTP/HTTPS ao Analysis Server) e o Analysis Services residem na mesma máquina. Esta configuração caracteriza-se pela facilidade no acesso à rede e na conectividade HTTP/HTTPS. Nesta configuração, o IIS comunica directamente com o Analysis Server usando o Mecanismo de Memória Partilhada. A Figura 4 apresenta um exemplo típico de uma arquitectura física baseada nesta configuração.
- ***Configuração Multi-Computador:*** Nesta configuração o IIS (que contém a Biblioteca Data Pump, responsável pela conectividade HTTP/HTTPS ao Analysis Server) e o Analysis Services residem em máquinas distintas, podendo, a arquitectura, envolver firewalls e servidores adicionais. Esta configuração fornece maior segurança e estabilidade no acesso à rede e na conectividade HTTP/HTTPS. Nesta configuração, o IIS (que contém a Biblioteca Data Pump) pode comunicar directamente com o Analysis Server ou através de outro servidor IIS e/ou firewalls. A Figura 5 apresenta três exemplos de arquitecturas físicas baseadas nesta configuração.

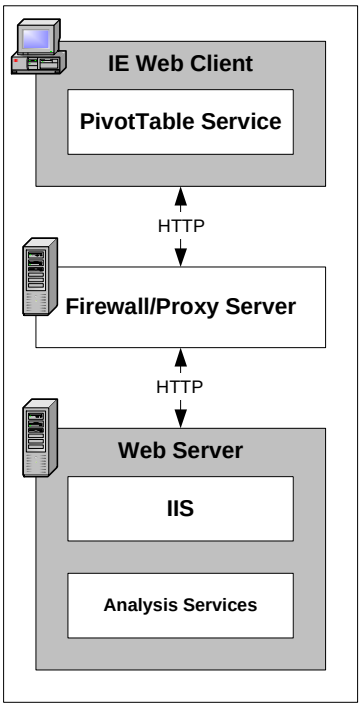

Figura 4: Arquitectura Física de acesso ao Analysis Services via HTTP/HTTPS com o IIS e o Analysis Services instalados na mesma máquina (Configuração de Computador Único). (Adaptado de [2].)

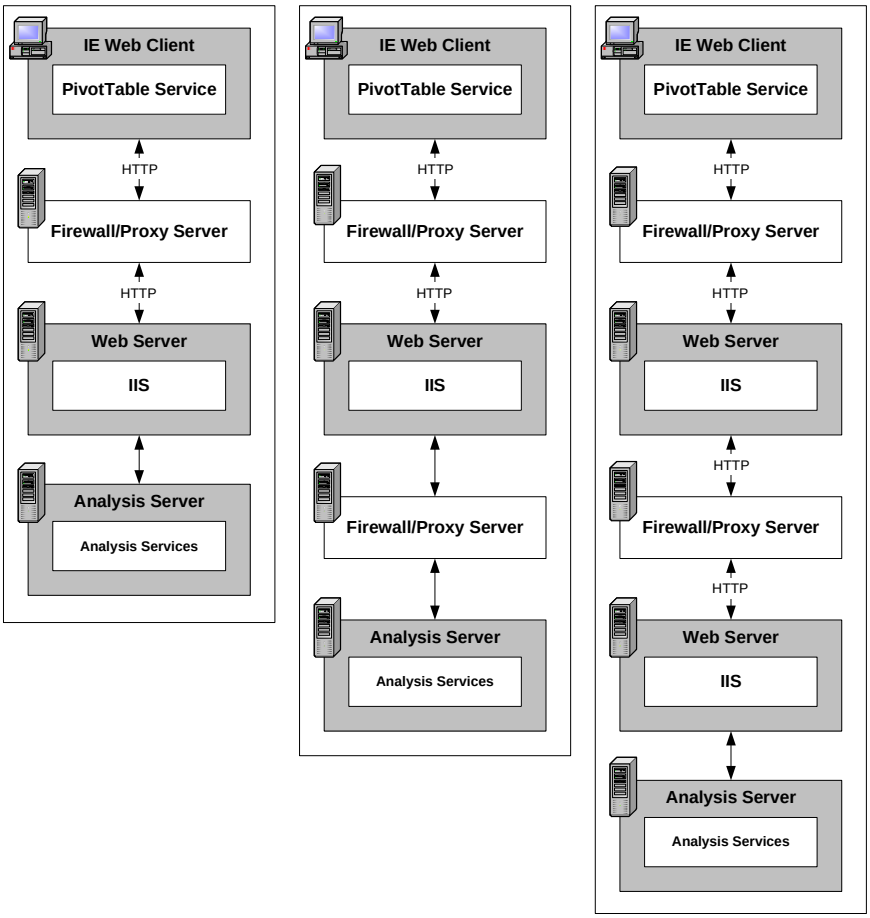

Figura 5: Exemplos de Arquitecturas Físicas de acesso ao Analysis Services via HTTP/HTTPS com o IIS e o Analysis Services instalados em múltiplas máquinas (Configurações Multi-Computador). (Adaptado de [2].)

IV. Instalação da Biblioteca Data Pump

Se se pretende correr o IIS e o Analysis Services na mesma máquina e usar a Memória Partilhada como mecanismo de comunicação entre o Analysis Server e a Biblioteca Data Pump, basta construir e configurar o Web Site que vai fornecer a conectividade HTTP/HTTPS, conforme indicado na secção seguinte, pois o programa de instalação do Analysis Services instala e regista automaticamente a Biblioteca Data Pump. [2]

No entanto, para usar a Biblioteca Data Pump num Servidor IIS instalado numa outra máquina que não aquela onde está instalado o Analysis Services, é necessário instalar e registar a Biblioteca Data Pump antes de construir o Web Site, no IIS, que vai fornecer a conectividade HTTP/HTTPS ao Analysis Services. Os passos seguintes descrevem como instalar e registar a biblioteca msmdpump.dll num Servidor IIS [2]:

- Copiar o ficheiro msmdpump.dll, localizado no directório \bin do Analysis Services, por defeito C:\Program Files\Microsoft Analysis Services\bin, para um subdirectório do Servidor IIS. (Este passo não é bem necessário, pois, uma vez registado, o ficheiro msmdpump.dll pode estar localizado em qualquer directório do Servidor Windows.)
- Registar o ficheiro msmdpump.dll no Servidor IIS, executando a instrução regsvr32 msmdpump.dll, numa janela Command Prompt do Windows e sobre o directório do Servidor IIS que contém o ficheiro msmdpump.dll.

V. Configuração do IIS para a utilização da Biblioteca Data Pump

Independentemente da Arquitectura e do Mecanismo de Transporte de Dados utilizado, para poder usar a Biblioteca Data Pump, vai ser necessário construir e configurar/preparar (para utilização da Biblioteca Data Pump) um Web Site ou Directório Virtual no IIS, a partir do qual vai ser fornecida a conectividade HTTP/HTTPS ao Analysis Services. Para tal, deverá proceder-se conforme indicado a seguir [2]:

- Por questões de segurança, recomenda-se que o Servidor Web IIS, que vai ser usado para fornecer a conectividade HTTP/HTTPS ao Analysis Services, seja usado exclusivamente para este efeito, devendo disponibilizar, desta forma, somente o Web Site de acesso ao Analysis Services, o qual deverá ser acedido por HTTPS, e não por HTTP, usando um Certificado SSL (Secure Sockets Layer) para o Analysis Services Server, que terá de ser adquirido e instalado. Adicionalmente, vai ser necessário abrir a porta 443 do Firewall, que vai ser usada no acesso via HTTPS e, visto que o Servidor IIS já não fornecerá acesso via HTTP, deverá ser fechada a porta 80.
- Criar um subdirectório no Servidor IIS e copiar o ficheiro msolap.asp (localizado no directório \bin do Analysis Services, por defeito C:\Program Files\Microsoft Analysis Services\bin) para este directório. Nos passos seguintes este directório será referenciado como Data Pump Folder. Notar que, por razões de segurança, é recomendável que este directório seja exterior ao directório do Default Web Site (\inetpub\wwwroot\).
- Usando o IIS Manager, criar um novo Web Site. Se se pretender usar o protocolo HTTPS, em vez do protocolo HTTP, será necessário configurar este novo Web Site para ser acedido por HTTPS, usando o Certificado SSL, para o Analysis Services Server, previamente instalado.
- Fazer do Data Pump Folder o Web Site Home Directory do novo Web Site.
- No IIS Manager, seleccionar a Check Box Read de modo a que as Permissões do Servidor Web referentes ao Web Site Home Directory permita aos utilizadores visualizar o seu conteúdo.
- No IIS Manager, seleccionar Script Only na List Box Execute Permition, para que o ficheiro msolap.asp possa ser executado a partir do Web Site Home Directory.
- Para efectuar alterações futuras, escolher a opção Properties do menu contextual associado ao novo Directório Virtual (invocado accionando o botão direito do rato).

Deve-se alterar as configurações de segurança definidas, pelo IIS Manager, durante o processo de criação do novo Web Site ou Directório Virtual. Pois, por defeito, o IIS Manager acciona os mecanismos de autenticação Anonymous Access, Digest Authentication e Integrated Windows Authentication. E, visto que, este Web Site ou Directório Virtual destina-se, exclusivamente, ao acesso, via PivotTable Services, ao Analysis Server, só se deve disponibilizar o mecanismo de autenticação apropriado à implementação pretendida, desactivando todos os restantes. [2]

VI. Configuração da Biblioteca Data Pump

Para se utilizar a Biblioteca Data Pump numa Configuração Multi-Computador (ignorar esta secção se for usado o mecanismo de transporte de dados de Memória Partilhada numa Configuração de Computador Único) é necessário editar o ficheiro msolap.asp de modo a redireccionar o Data Pump para o Analysis Server correspondente. No entanto, isso só deve ser feito depois de construído e configurado, conforme descrito na secção anterior, o Web Site IIS que vai fornecer conectividade HTTP/HTTPS ao Analysis Services. [2]

Para alterar o ficheiro msolap.asp proceder da forma seguinte [2]:

- Abrir o ficheiro msolap.asp no Notepad, por exemplo. Este ficheiro encontra-se no Data Pump Folder, referido na secção anterior.
- Editar o ficheiro msolap.asp de modo à propriedade ServerName do Objecto Pump referencie o Analysis

Server apropriado. A Figura 6 apresenta a Bold as alterações que é necessário efectuar.

- Salvar as alterações efectuadas e fechar o ficheiro msolap.asp.

Para efeitos de teste, pode-se forçar o mecanismo de transporte Named Pipe numa Configuração de Computador Único. (Conforme já foi referido atrás, na prática, não se deve usar o mecanismo de transporte Named Pipe numa Configuração de Computador Único, por ser ineficiente.) Para fazê-lo basta substituir "<server_name>" por "localhost" no exemplo da Figura 6. Para restaurar a utilização do mecanismo de transporte de Memória Partilhada numa Configuração de Computador Único, basta remover as instruções apresentadas a Bold no exemplo da Figura 6, ou atribuir o valor "" (string vazia) à propriedade ServerName do Objecto Pump. [2]

VII. Mecanismos de Segurança e Autenticação/Controlo de Acesso

Ao comparar-se a arquitectura do MS SQL Server 2000 Analysis Services com a arquitectura de um SGBD Relacional, tal como o MS SQL Server 2000, nota-se a ausência de uma peça importante na camada de segurança do Analysis Services: o Analysis Services não tem o seu próprio Mecanismo de Autenticação. Ao contrário do SQL Server, o Analysis Services usa exclusivamente o Mecanismos de Autenticação do Windows para validar e verificar as permissões dos utilizadores, e as definições das Security Roles do Analysis Services baseiam-se nos

```
<%@ LANGUAGE="VBSCRIPT"%>
<%' ************** Do not change this file ***************
   ' Changing of this file can bring unexpected results
   ' NEVER add any HTML tags. Places that are allowed to
   ' change will be specified explicitly in the comments.
   ' ******************************************************
%>
<%Response.Expires = 0%>
<%Response.Buffer=FALSE%>
<%Server.ScriptTimeout=3600%>
<HTML><%
    On Error Resume Next
    Call ReadData
    ' This is error handling code and should not be modified
    ' This code will take care of the potentional errors in
    ' this asp page.
    if ( Err.Number <> 0 ) Then
        errstr = "<Error>" + CStr(-8) + "</Error>"
        errstr = errstr + "<SysError>" + CStr(err.Number) +
                 "</SysError>"
        errstr = errstr + "<Note>" + err.Description + "</Note>"
        Response.AddHeader "Pump-Error", errstr
        Response.Flush
        Response.End
    End if
    Function ReadData
        ' You can modify code of this function, but we don't
        ' recommend doing it.
        if (isEmpty(Session("StoredPump"))) Then
            Set pump = Server.CreateObject("PUPump.PUPump.1")
            Set Session("StoredPump") = pump
        else
            Set pump = Session("StoredPump")
        End if
        ' Replace <server_name> with the name
        ' of the destination Analysis server.
        pump.ServerName = "<server_name>"
        ' This value can be changed.
        pump.Timeout=60
        pump.ReadData
        Response.Flush
        Response.End
    End Function
%>
```

Figura 6: Conteúdo do ficheiro msolap.asp. Estão representadas a Bold as instruções que têm de ser alteradas de modo a configurar a Biblioteca Data Pump para utilizar o Analysis Server apropriado.

Utilizadores e Grupos do Windows (ao longo desta secção quando se refere ao Windows como Sistema Operativo está-se a referir a um dos três Sistemas Operativos seguintes: MS Windows NT4, MS Windows 2000 e MS Windows 2003). Quando projectou o Analysis Services, a Microsoft tinha boas razões para não desenvolver um modelo de autenticação semelhante ao do SQL Server 2000. De facto, os Mecanismos de Segurança do Windows disponibilizam funcionalidades difíceis de duplicar, tais como: validação segura, encriptação de Passwords, definição de grupos de utilizadores, administração de utilizadores e auditoria. No próprio SQL Server 2000, a Microsoft desencoraja a Autenticação SQL Server e recomenda a utilização da Autenticação Windows. No entanto, é preciso ter presente que a Autenticação SQL Server fornece algumas funcionalidades que a Autenticação Windows não duplica, como é o caso do suporte HTTP nos acessos ao Servidor por parte dos Cliente. No caso do Analysis Services, o acesso HTTP/HTTPS é garantido pelo IIS, baseando-se, para tal, nos Mecanismos de Autenticação do Windows. [11]

Neste contexto, a segurança no acesso ao Analysis Services, via HTTP/HTTPS, por parte dos seus utilizadores finais, é assegurada/controlada através da [7]:

- ***Autenticação dos utilizadores durante o processo de conexão ao Analysis Server:*** Função delegada nos Mecanismos de Autenticação do Windows/IIS, pois o Analysis Server não tem o seu próprio mecanismo de autenticação de utilizadores. Este processo determina quais os utilizadores ou grupo de utilizadores que podem conectarem-se ao Analysis Server a partir das aplicações Cliente. [7, 9]
- ***Definição de Security Roles ao nível da Base de Dados, do Cubo/Modelo Mining, dos Membros das Dimensões e da Célula:*** Estas Security Roles, definidas no Analysis Manager, determinam, para o seu nível de detalhe, quais os utilizadores ou grupos de utilizadores que podem aceder aos dados e o seu tipo de acesso (só leitura ou de leitura e escrita). A sua definição assenta sobre a estrutura de Utilizadores e Grupos do Windows, e a sua aplicação pressupõe uma autenticação prévia e bem sucedida dos utilizadores (recorrendo aos Mecanismos de Autenticação do Windows/IIS) durante o processo de conexão. [7, 7.1]

A.- Autenticação dos Utilizadores no Acesso ao Analysis Server

Conforme já foi referido, quem fornece a conectividade HTTP/HTTPS ao Analysis Server é o IIS, o qual, por sua vez, também é o responsável pela autenticação e verificação de permissões de acesso dos utilizadores. (Notar que controlar quem pode aceder ao Analysis Server, via HTTP/HTTPS, ressume-se a controlar quem pode executar o ficheiro msolap.asp, responsável pela conectividade HTTP/HTTPS ao Analysis Server.) Por este

motivo os mecanismos de autenticação de utilizadores no acesso ao Analysis Server, via HTTP/HTTPS, serão aqueles que forem disponibilizados pelo IIS, mais precisamente pelo IIS Directory Security, os quais, por sua vez, assentam sobre os Mecanismos de Autenticação do Windows.

Neste contexto, o IIS Directory Security disponibiliza quatro Mecanismos de Autenticação/Controlo de Acesso ao Analysis Services (dependendo da versão do IIS, podem ser mais do que quatro, no entanto, os aqui apresentados são os mais utilizados): Anonymous Authentication, Integrated Windows Authentication, Basic Authentication e Digest Authentication. [4, 10, 2, 9]

A.1.- Anonymous Authentication

Este mecanismo permite o acesso ao Analysis Services por parte de qualquer utilizador sem se proceder a qualquer tipo de autenticação. Quando é usado este mecanismo de controlo de acesso, o IIS atribui, por defeito, ao utilizador uma conta especial com o identificador IUSER_<NomeMáquinaAcesso> (uma Conta Windows do servidor sobre o qual o IIS está instalado, utilizada por este último para fornecer acesso Anonymous aos Directórios Virtuais), onde NomeMáquinaAcesso é a identificação da máquina a partir da qual o utilizador está a conectar-se. Esta conta vai ser passada ao Analysis Services, como credencial de acesso do utilizador, pelo que terá de ser adicionada às Security Roles que se pretende que o utilizador Anonymous tenha acesso. No entanto, se não se quiser usar a conta IUSER como conta de acesso do utilizador Anonymous, pode-se indicar (no IIS Manager) o nome de uma outra conta mais apropriada. De facto, recomenda-se a criação de uma conta genérica com o único propósito de ser usada no acesso dos utilizadores Anonymous ao Analysis Services. Isto vai permitir que estes utilizadores cheguem ao Analysis Services usando uma conta convenientemente configurada para o efeito, em vez da conta multi-usos IUSER, o que aumenta ligeiramente o controlo sobre a segurança. Nesta situação, a conta que terá de ser adicionada às Security Roles do Analysis Services será a nova conta, criada para o efeito, e não a conta IUSER. [4, 10, 2]

Quando os Servidores IIS e Analysis Server não partilham a mesma máquina (Configuração Multi-Computador) é mesmo necessário modificar a conta Windows que o IIS usa no acesso Anonymous. Em vez da conta IUSER_<NomeMáquinaAcesso>, uma conta local sem acesso à rede, tem de ser usada uma Conta de Domínio comum a ambos os servidores (Servidor IIS e Analysis Server). Se não puder ser criada uma Conta de Domínio comum aos dois servidores (por não existir nenhuma Trust Relationship entre ambos os servidores ou entre os seus domínios) podem-se criar contas locais em cada um dos servidores, com credenciais idênticas (UserName e Password) e fazer-se a correspondência entre elas. No entanto, este artifício tem encargos administrativos, pois obriga os administradores de ambas as máquinas a manterem estas contas sincronizadas. [4, 10, 2]

A.2.- Integrated Windows Authentication

Este mecanismo de controlo de acessos (formalmente chamado NTLM Protocol e também conhecido como Windows NT Challenge/Response Authentication) só pode ser usado se houverem acessos Intranet controlados ou acessos Internet baseados em VPN (Virtual Private Network) (entre a máquina cliente e a rede na qual reside o Servidor IIS). O utilizador tem de ter, e estar a usar na máquina cliente, uma Conta de Domínio, válida para o domínio em que se insere a máquina onde corre o Servidor IIS (que fornece o acesso HTTP/HTTPS ao Analysis Services) para que o acesso seja concretizado. Sendo as credenciais de acesso (que incluem, além do UserName e Password, o Domain Name), obtidas pelo IIS usando a funcionalidade Single Sign-On (SSO), aquelas com as quais o utilizador fez o login, no ambiente Windows, da máquina cliente, não sendo necessário nenhum processamento especial por parte do IIS. No entanto, se o processo de autenticação inicial falhar (por as credenciais de acesso armazenadas na máquina do cliente não concederem acesso ao recurso pretendido), o Browser Web pedirá ao utilizador para introduzir outra credencial de acesso (UserName e Password), tendo o utilizador três oportunidades para fornecer uma credencial válida, após o que o processo abortará. As credenciais do utilizador são transmitidas (entre a máquina cliente e o Servidor IIS) codificadas usando uma técnica de Hashing (podendo também ser transmitida usando um Kerberos Ticket quando é usado o Kerberos). Este mecanismo, apesar de ser o mais recomendável, tem a limitação de não poder atravessar Servidores Proxy ou Firewalls, a menos que haja uma ligação PPTP entre a máquina cliente e a rede na qual reside o Servidor IIS, recorrendo, por exemplo, a VPNs. [4, 10, 2]

Se não for possível definir Contas de Domínio entre a máquina cliente e o Servidor IIS, pode ser usado o artifício descrito na secção Anonymous Authentication. No entanto, devido à carga administrativa associada à manutenção do sincronismo entre o "par de contas correspondentes", esta aproximação só é praticável para um reduzido número de contas. [4, 10, 2]

No entanto, quando o Servidor IIS e o Analysis Services não partilham a mesma máquina, deixa de pode ser usada a Integrated Windows Authentication (ou pelo menos passa a ser muito complicado fazê-lo), pois este mecanismo de autenticação só permite um Hop de transferência de credenciais. Dessa forma a credencial transferida durante o Hop entre a máquina cliente e o Servidor IIS não pode ser reutilizada no acesso ao Analysis Services. Esta restrição não é exclusiva do Analysis Services, pois aplica-se também ao SQL Server e ao Exchange. Apesar de ser tecnicamente possível suportar múltiplos Hops, fazê-lo requer a utilização de

Kerberos Authentication, o que exige uma Arquitectura de Domínio muito mais elaborada. [4, 10, 2]

A.3.- Basic Authentication

Este mecanismo de autenticação requer acessos Internet controlados, i.e., que os utilizadores tenham contas individuais de acesso, no Servidor Windows sobre o qual corre o Servidor IIS, não sendo utilizadas as credenciais dos utilizadores nas máquinas Clientes (ao contrário do que acontece na Integrated Windows Authentication). A credencial da conta de acesso pode ou não ser incluída na Connection String de acesso ao Analysis Services, através dos atributos User ID e Password. Se estes atributos forem deixados em branco, o utilizador será inquerido, pelo Cliente Web no sentido de fornecer estes dados, sendo-lhe concedidas três tentativas para introduzir uma credencial válida. Notar que, no entanto, não é seguro incluir a credencial de acesso na Connection String pois, esta poderá vir a ser visualizada por outros, se for incluída numa Página HTML e for visualizado o código fonte desta página. [4, 10, 2]

Uma vantagem da Basic Authentication é o facto desta estar contemplada na especificação HTTP, sendo, dessa forma, suportada pela maior parte dos Clientes Web. No entanto, quando é usada, a credencial do utilizador circula entre a máquina cliente e o Servidor IIS sem nenhum tipo de codificação/encriptação, podendo, dessa forma, ser facilmente interceptada e reutilizada por Network Sniffers. Por este motivo, este mecanismo de autenticação deve ser usado sobre ligações seguras, que garantam a encriptação dos dados que circulam na rede, como é o caso das ligações baseadas nos protocolos SSL e HTTPS. [4, 10, 2]

Notar que o protocolo de autenticação preferencial, e de mais fácil implementação, do Analysis Services é o NTLM/Integrated Windows Authentication (os outros protocolos de autenticação suportados são Kerberos e Negotiate), o qual só permite um Hop de transferência de credenciais. No entanto, como o login do utilizador é feito do lado do Servidor IIS e não do lado da máquina cliente, a transferência da credencial do utilizador para o Analysis Server só necessita de um único Hop, independentemente de estar a ser usada uma Configuração de Computador Único ou Multi-Computador, pelo que esta limitação do protocolo NTLM não impõe constrangimentos à utilização da Basic Authentication. [4, 10, 2]

Quando for utilizada uma Configuração Multi-Computador as contas dos utilizadores devem ser Contas de Domínio. Se não for possível definir Contas de Domínio entre os dois sistemas deve ser usado o artifício descrito na secção Anonymous Authentication. Tal como acontecia com a Integrated Windows Authentication, esta aproximação é impraticável para mais do que uma pequena quantidade de contas. [4, 10, 2]

A.4.- Digest Authentication

Este mecanismo de autenticação é semelhante à Basic Authentication, diferindo desta somente no facto da Digest Authentication criptografar a credencial do utilizador, utilizando o algoritmo de Hash MD5 (Message Digest Algorithm 5), antes de enviá-la pela rede. Dessa forma, a credencial do utilizador viaja pela rede como uma sequência de dígitos de 128 Bits praticamente indecifrável. Apesar de mais seguro na transmissão das credenciais dos utilizadores, este mecanismo obriga ao armazenamento, no Controlador de Domínio, de uma versão "legível" (é usada encriptação reversível) das credenciais do utilizador, o que obriga a um reforço das medidas de segurança sobre esta máquina. (No entanto, esta fragilidade pode ser ultrapassada se for utilizado o mecanismo de autenticação Advanced Digest Authentication, só suportado pelo IIS 6.0 e o Windows Server 2003, no qual as credenciais dos utilizadores são armazenadas no Controlador de Domínio criptografadas em MD5.) Adicionalmente, este mecanismo de autenticação tem alguns requisitos particulares, entre os quais pode-se salientar o facto de só ser suportado pelo IE 5.0 e pelo IIS 5.0, ou por versões mais recentes destes produtos, e, pelo Windows 2000 Server ou Windows Server 2003, em termos de SO do Controlador de Domínio e do Servidor IIS. É ainda necessário que o Utilizador e o Servidor IIS sejam membros do mesmo domínio, e que a Conta Windows do Utilizador seja armazenada em Active Directory no Controlador do Domínio e configurada com encriptação reversível. [4, 10, 2]

B.- Definição de Security Roles no Analysis Services

As Security Roles determinam o tipo (só de leitura ou de leitura/escrita) e a abrangência (BD, Cubo/Modelo Mining, Membro da Dimensão e Célula) do acesso que os Utilizadores ou Grupos de Utilizadores têm sobre os objectos do Analysis Services. Na sua definição começa-se por especificar quais os Utilizadores que têm acesso aos objectos controlados pela Security Role e, seguidamente, dependendo do tipo de Security Role, especifica-se a lista dos Objectos controlados pela Role e as Políticas, Permissões e Regras, que implementam a Segurança do Objecto ao Nível da Dimensão e da Célula, conforme descrito mais adiante nesta secção. [5, 7]

Notar que, conforme já foi referido, o Analysis Services não tem o seu próprio Sistema de Contas de Utilizadores, utilizando exclusivamente as Contas e Grupos de Utilizadores do Windows. Por este motivo, antes de definir a estrutura de Security Roles que controlará o acesso às BD Multidimensionais e Modelos Mining geridos pelo Analysis Services, será necessário projectar e implementar, no Windows, a estrutura de Contas e Grupos de Utilizadores que vai ser usada pelo Analysis Services. [5, 7]

Um Utilizador pode ser incluído em múltiplas Roles de um Analysis Server, tendo, neste caso, o acesso resultante da combinação destas Roles. Se alguma destas Roles concede, ao Utilizador, acesso a um Objecto, o utilizador terá acesso a este Objecto. Exceptuam-se os acessos controlados por Regras do tipo Custom usadas na definição da Segurança ao Nível das Dimensões, pois, nem todas as combinações destas Regras podem ser resolvidas. [7.1]

O Analysis Services define três categorias de Security Roles: Database Role, Cube Role e Mining Model Role.

B.1.- Database Role

Estas Security Roles, definidas ao nível da BD, e mantidas no Database Role Manager, representam o nível hierárquico mais elevado na definição de Security Roles. As restantes categorias de Security Roles são sempre definidas a partir de uma Database Role, herdando desta o seu nome, a lista de Utilizadores e, no caso das Cube Roles, os valores por defeito para as Permissões de acesso às Dimensões dos Cubos, aos quais a Database Role dá acesso. As alterações efectuadas, sobre a lista de Utilizadores, nas Security Roles Descendentes de uma Database Role, são as únicas que afectam a Database Role. [5.1, 6.1, 7.1]

Sempre que for adicionado um objecto, à lista de objectos controlados pela Database Role, será criada uma Security Role Descendente desta, com o mesmo nome da Database Role e do tipo correspondente ao objecto. Desta forma, quando for adicionado um Cubo será criada, ao nível do Cubo, uma Cube Role, com o mesmo nome da Database Role, e quando for adicionado um Modelo Mining será criada, ao nível do Modelo Mining, uma Mining Model Role, com o mesmo nome da Database Role. Existem, no entanto, outras metodologias de criação de Cube Roles e Mining Model Roles recorrendo, respectivamente, ao Cube Role Manager e Mining Model Role Manager, sendo, no entanto, também criada, caso ainda não exista, uma Database Role com o mesmo nome da Cube Role ou Mining Model Role. [5.1, 6.1, 7.1]

Nas Database Roles é possível controlar o acesso às Dimensões da BD por parte dos Utilizadores da Role, implementando a Segurança ao Nível da Dimensão, através da especificação dos Níveis/Membros das Dimensões que os Utilizadores da Role podem visualizar quando exploram os Cubos, ou ainda através da concessão de acessos de leitura/escrita às Dimensões editáveis e da especificação dos Membros destas que podem ser alterados. (No entanto, esse acesso só se tornará efectivo após a inclusão, na Database Role, dos Cubos, que utilizam estas Dimensões.) Isto é feito no Database Role Manager, indicando qual é a Regra que rege a aplicação de cada uma das Permissões a cada uma das Dimensões. A Tabela 1 descreve as Permissões e Regras usadas nas Definições de Segurança ao Nível da Dimensão. Notar que estas definições de segurança são herdadas por todos os Cubos incluídos na Database Role e podem ser alteradas ao nível de cada um dos Cubos (editando a Cube Role respectiva). [5.1, 5.4, 6.1, 6.4, 7.2, 7.2.1]

B.2.- Cube Role

Estas Security Roles, definidas ao nível do Cubo, e mantidas no Cube Role Manager, controlam o acesso dos Utilizadores a um determinado Cubo da BD (um único Cubo), permitindo alterar/refinar a implementação de Segurança ao Nível da Dimensão, herdada da Database Role que lhe precede, e implementando a Segurança ao Nível da Célula. Adicionalmente, permite controlar o acesso dos seus Utilizadores até aos dados fonte das células (Drillthrough). No entanto, essa funcionalidade requer que o Cubo esteja configurado para tal. Em termos de Segurança ao Nível da Célula as Cube Roles permitem limitar as Células que os Utilizadores da Role podem visualizar quando exploram os Cubos, assim como também permitem conceder acessos de leitura/escrita aos Cubos editáveis e limitar as Células destes que podem ser

Tabela 1: Permissões e Regras usadas nas Definições de Segurança ao Nível da Dimensão. (Adaptado de [6.1, 6.2, 6.4, 6.5, 7.2, 7.2.1].)

PERMISSÃO	REGRA
Read: Determina quais os Membros que são visíveis, afectando, assim, o tamanho do "Cubo Visível".	***Unrestricted:*** Os Utilizadores podem ver todos os Membros. Esta é a Regra por defeito.
	Fully Restricted: Os Utilizadores não podem ver os Membros. Quando explorarem um Cubo que inclua esta Dimensão não a visualizarão.
	Custom: Só serão visualizados os Níveis e/ou Membros que forem especificados. Na especificação por Níveis indica-se o Top Level e/ou o Bottom Level. Na especificação por Membros estes podem ser indicados utilizando as opções Allow Only, Denny Only e Allow and Deny. Estes dois métodos podem ser utilizados de forma combinada.
Read/Write: Determina quais os Membros que são editáveis. Esta Permissão só está disponível para as Dimensões editáveis. Se à posteriori a Dimensão deixar de ser editável esta Permissão será desactivada.	***Unrestricted:*** Os Utilizadores podem alterar todos os Membros. Esta Regra só está disponível se a Regra da Permissão Read for Unrestricted.
	Fully Restricted: Os Utilizadores não podem alterar os Membros. Esta é a Regra por defeito e só está disponível se a Regra da Permissão Read for Unrestricted ou Fully Restricted.
	Custom: Os Utilizadores só podem alterar os Níveis e/ou Membros que forem especificados. Na especificação por Níveis indica-se o Top Level e/ou o Bottom Level. Na especificação por Membros estes podem ser indicados utilizando as opções Allow Only, Denny Only e Allow and Deny. Estes dois métodos podem ser utilizados de forma combinada. Esta Regra só está disponível se a Regra da Permissão Read for Unrestricted ou Custom.

editadas. Isso é feito seleccionando a Política que rege o acesso às Células do Cubo, e, para a Política Advanced, indicando, para cada uma das Permissões, a Regra que a rege. Se uma Política ou Regra permitir alterar o valor de uma Célula, esta será alterada se for atómica, se não o for, a alteração estará condicionada à capacidade da aplicação cliente em dispersar a alteração pelas suas Células atómicas subordinadas. A Tabela 2 descreve cada uma das Políticas, Permissões e Regras usadas nas Definições de Segurança ao Nível da Célula. As alterações nas Definições de Segurança do Nível da Dimensão processam-se tal como nas Database Roles, baseando-se, também, nas Permissões e Regras descritas na Tabela 1. [5.2, 5.5, 6.2, 6.5, 6.6, 7.3, 7.3.1]

O Capítulo 11 de [1] descreve detalhadamente, recorrendo a capturas de ecrã, os procedimentos a seguir na criação de Security Roles das categorias Database Role e Cube Role, começando pela criação dos Utilizadores e Grupos de Utilizadores, e terminando nas Definições de Segurança ao Nível da Dimensão e da Célula.

B.3.- Mining Model Role

Estas Security Roles, definidas ao nível do Modelo Mining, e mantidas no Mining Model Role Manager, controlam o acesso dos Utilizadores a um determinado Modelo Mining da BD (um único modelo). Além de potenciar a criação de Mining Model Roles, o Mining Model Role Manager só permite alterar a lista de Utilizadores da Mining Model Role. Notar que, tal como acontece com as Cube Role, estas alterações propagam-se para a Database Role e as Mining Model Roles com o mesmo nome da Mining Model Role. [5.3, 6.3, 7.1]

VIII. CONCLUSÕES

O Mecanismo de Acesso Directo ao Analysis Services é aquele que garante os menores tempos de resposta e as taxas de transferência de dados mais elevadas por não haver nenhum intermediário entre o PivotTable Services e o Analysis Server, o que não acontece com o Mecanismo de Acesso via HTTP/HTTPS, onde a intermediação do Servidor Web IIS (e da aplicação que faz de ponte entre este e o Analysis Server) deteriora significativamente o tempo de resposta. No entanto, o facto do Mecanismo de Acesso Directo utilizar, exclusivamente, o Mecanismo de Autenticação Integrated Windows Authentication e a Porta TCP 2725 (Protocolo SQL Analysis Services) condiciona a sua utilização inter-domínio e sobre a Internet. Por um lado, a Integrated Windows Authentication requer que os utilizadores se encontrem no mesmo domínio que o Analysis Services, e por outro lado, a existência de Firewalls levanta dificuldades à utilização da Porta TCP 2725. Nestas situações é necessário utilizar outro mecanismo de acesso, nomeadamente o Mecanismo de Acesso via HTTP/HTTPS, que só está disponível na

Tabela 2: Políticas, Permissões e Regras usadas nas Definições de Segurança ao Nível da Célula. (Adaptado de [6.2, 6.6, 7.3, 7.3.1].)

POLÍTICA	
Unrestricted Read: Os Utilizadores podem visualizar o valor de todas as Células. Esta é a Política por defeito.	
Unrestricted Read/Write: Os Utilizadores podem visualizar e alterar o valor de todas as Células	
Advanced: Os Utilizadores podem visualizar e alterar somente as Células que forem especificadas nas Permissões e Regras.	
PERMISSÃO *(só para a Política Advanced)*	**REGRA** *(só para a Política Advanced)*
Read: Determina quais as Células que podem ser visualizadas. As Células especificadas nesta permissão são visualizáveis independentemente de terem sido derivadas de Células não visualizáveis.	***Unrestricted:*** Os Utilizadores podem ver todas as Células. Esta é a Regra por defeito.
	Fully Restricted: Os Utilizadores só podem visualizar os valores das Células especificadas na Permissão Read/Write ou na Permissão Read Contingent (as Células incluídas nesta Permissão estão sujeitas às limitações por ela impostas).
	Custom: Só serão visualizadas as Células que forem aqui especificadas. Esta especificação pode ser feita através de uma expressão MDX, que identifique as Células cujos valores podem ser ou não ser visualizados.
Read Contingent: Determina quais as Células que podem ser visualizadas. No entanto, as Células Derivadas especificadas nesta Permissão só são visualizáveis se as Células das quais derivam também forem visualizáveis (i.e., estejam incluídas numa Permissão Read ou numa Permissão Read Contingent sem, no entanto, ser derivada). As Células não Derivadas incluídas nesta Permissão são visualizáveis.	***Unrestricted:*** Os Utilizadores podem visualizar o valor de todas as Células não Derivadas. As Células Derivadas só serão visualizáveis se as Células das quais derivam estiverem incluídas nas Permissões Read ou Read/Write.
	Fully Restricted: Os Utilizadores só podem visualizar os valores das Células especificadas nas Permissões Read ou Read/Write. Esta é a Regra por defeito.
	Custom: Só serão visualizadas as Células que forem aqui especificadas, as quais estão, no entanto, sujeitas às limitações Read Contingent. Pode-se utilizar uma expressão MDX para identificar as Células cujos valores podem ser visualizados e aquelas cujos valores não podem ser visualizados.
Read/Write: Determina quais as Células que podem ser alteradas. Esta Permissão só pode ser usada nos Cubos editáveis. Se à posteriori o Cubo deixar de ser editável esta Permissão será desactivada. As Células aqui especificadas passam a ser visualizadas nos moldes da Permissão Read (e não nos moldes da Permissão Read Contingent).	***Unrestricted:*** Os Utilizadores podem alterar o valor de todas as Células.
	Fully Restricted: Os Utilizadores não podem alterar os valores das Células.
	Custom: Os Utilizadores só podem alterar as Células especificadas. A especificação pode recorrer a uma expressão MDX para identificar as Células cujos valores podem ser ou não ser visualizados.

versão Enterprise do Analysis Services, aquela que acompanha o MS SQL Server 2000 Enterprise Edition. (A outra opção, que não é explorada neste artigo, é o Mecanismo de Acesso via XMLA, com desempenho semelhante, mas que não requer a utilização do PivotTable Services, do lado do Cliente.)

No entanto, a utilização deste mecanismo de acesso não é trivial, apresentado algumas peculiaridades, pelo facto do Analysis Services não suportar acessos directos via HTTP/HTTPS. Estes acessos serão fornecidos pelo Servidor Web IIS, recorrendo ao Objecto Data Pump PUPump (responsável pela comunicação com o Analysis Services) que é implementado pela Biblioteca Data Pump msmdpump.dll. O acesso a este objecto é feito através da Página Web ASP msolap.asp.

Originalmente, a acessibilidade via HTTP/HTTPS ao Analysis Server requeria que o Analysis Services e o Servidor Web IIS partilhassem o mesmo Servidor Windows, pois a Biblioteca Data Pump usava, exclusivamente, o Mecanismo de Memória Partilhada na comunicação com o Analysis Server. No entanto, com o lançamento do SQL Server 2000 Service Pack 3, a Biblioteca Data Pump passou a poder usar também o Mecanismo Named Pipes na troca de informação com o Analysis Server. Esta alteração permitiu ultrapassar a limitação inicial, pois, a utilização de Named Pipes permite instalar a Biblioteca Data Pump e o Servidor Web IIS, num Servidor Windows distinto daquele em que está instalado o Analysis Services.

O Analysis Services não tem o seu próprio Mecanismo de Autenticação, usando exclusivamente os Mecanismos de Autenticação do Windows, para validar e verificar as permissões de acesso dos utilizadores, e recorrendo aos Utilizadores e Grupos do Windows na definição das suas Security Roles. São estas Security Roles que determinam, para o seu nível de detalhe (BD, Dimensão/Membro de Dimensão e Célula, ou ainda Modelo Mining), quais os Utilizadores, ou Grupos de Utilizadores, que podem aceder aos dados e o seu tipo de acesso (só de leitura ou de leitura e escrita).

REFERÊNCIAS

[1]: Jacobson R. *The Microsoft SQL Server 2000 Analysis Services Step by Step*. Microsoft Press. September 2000.

[2]: Kennedy D., Wickert D. "Improved Web Connectivity in Microsoft SQL Server 2000 Analysis Services". *MSDN Library. SQL Server 2000.* May 2003. http://msdn.microsoft.com/library/default.asp?url=/library/en-us/dnsql2k/html/sql_datapump.asp (22 July 2005).

[3]: Melomed E. "Configuring HTTP Access to SQL Server 2005 Analysis Services on Microsoft Windows Server 2003". *Microsoft TechNet. Microsoft SQL Server TechCenter. SQL Server 2005.* August 2005. http://www.microsoft.com/technet/prodtechnol/sql/2005/httpasws.mspx (20 September 2005).

[4]: Morey J. "IIS 4.0 and 5.0 Authentication Methods Chart". *Microsoft TechNet. Windows 2000 Server. IIS5.0*. July 1999. http://www.microsoft.com/technet/prodtechnol/windows2000serv/technologies/iis/maintain/featusability/authmeth.mspx (22 July 2005).

[5]: "Creating Security Roles". *MSDN Library. SQL Server 2000. Administering Analysis Services. Administrative Tasks*. http://msdn.microsoft.com/library/en-us/olapdmad/agsecurityroles_0t2r.asp (30/11/2005).

[5.1]: "Creating Database Roles". *[5]. Creating Security Roles.* http://msdn.microsoft.com/library/en-us/olapdmad/agsecurityroles_3n77.asp (30/11/2005).

[5.2]: "Creating Cube Roles". *[5]. Creating Security Roles.* http://msdn.microsoft.com/library/en-us/olapdmad/agsecurityroles_7ohf.asp (30/11/2005).

[5.3]: "Creating Mining Model Roles". *[5]. Creating Security Roles.* http://msdn.microsoft.com/library/en-us/olapdmad/agsecurityroles_7uib.asp (30/11/2005).

[5.4]: "Defining Custom Rules for Dimension Security". *[5]. Creating Security Roles.* http://msdn.microsoft.com/library/en-us/olapdmad/agsecurityroles_2sxl.asp (30/11/2005).

[5.5]: "Defining Custom Rules for Cell Security". *[5]. Creating Security Roles.* http://msdn.microsoft.com/library/en-us/olapdmad/agsecurityroles_2e7t.asp (30/11/2005).

[6]: "Creating Security Roles". *MSDN Library. SQL Server 2000. How To.* http://msdn.microsoft.com/library/en-us/olapdmad/aghtroles_2myb.asp (30/11/2005).

[6.1]: "How to Create a Database Role". *[6]. Creating Security Roles.* http://msdn.microsoft.com/library/en-us/olapdmad/aghtroles_52hx.asp (30/11/2005).

[6.2]: "How to Create a Cube Role, Change its Defaults Values, and Specify Cell Security". *[6]. Creating Security Roles.* http://msdn.microsoft.com/library/en-us/olapdmad/aghtroles_76ux.asp (30/11/2005).

[6.3]: "How to Create a Mining Model Role and Change its Defaults Values". *[6]. Creating Security Roles.* http://msdn.microsoft.com/library/en-us/olapdmad/aghtroles_5tf7.asp (30/11/2005).

[6.4]: "How to Create a Custom Rule for Dimension Security in a Database Role". *[6]. Creating Security Roles.* http://msdn.microsoft.com/library/en-us/olapdmad/aghtroles_7i05.asp (30/11/2005).

[6.5]: "How to Create a Custom Rule for Dimension Security in a Cube Role". *[6]. Creating Security Roles.* http://msdn.microsoft.com/library/en-us/olapdmad/aghtroles_806d.asp (30/11/2005).

[6.6]: "How to Create a Custom Rule for Cell Security". *[6]. Creating Security Roles.* http://msdn.microsoft.com/library/en-us/olapdmad/aghtroles_6tq1.asp (30/11/2005).

[7]: "Security and Authentication". *MSDN Library. SQL Server 2000. Analysis Services Architecture.* http://msdn.microsoft.com/library/en-us/olapdmad/agsecurity_7309.asp (30/11/2005).

[7.1]: "Database, Cube, and Mining Model Roles". *[7]. Security and Authentication. End-User Security*. http://msdn.microsoft.com/library/en-us/olapdmad/agsecurity_93g3.asp (30/11/2005).

[7.2]: "Dimension Security". *[7]. Security and Authentication. End-User Security*. http://msdn.microsoft.com/library/en-us/olapdmad/ agsecurity_3xbt.asp (30/11/2005).

[7.2.1]: "Custom Rules in Dimension Security". *[7.2]. Dimension Security*. http://msdn.microsoft.com/library/en-us/olapdmad/agsecurity_2b95.asp (30/11/2005).

[7.3]: "Cell Security". *[7]. Security and Authentication. End-User Security*. http://msdn.microsoft.com/library/en-us/olapdmad/agsecurity_0321.asp (30/11/2005).

[7.3.1]: "Custom Rules in Cell Security". *[7.3]. Cell Security*. http://msdn.microsoft.com/library/en-us/olapdmad/agsecurity_4mbd.asp (30/11/2005).

[8]: "INF: How To connect to Analysis Server 2000 by Using HTTP Connection". *Microsoft Support Centre*. Article ID: 279489. Revision: 1.0. 22 April 2003. http://support.microsoft.com/default.aspx?scid=KB;EN-US;q279489 (12 April 2005).

[9]: "MS Support WebCast: Microsoft SQL Server 2000 Analysis Services: How to Connect to Analysis Services over the Internet". *Microsoft Help and Support*. Article ID: 324961. Revision: 1.0. Last Review: 9 August 2004. http://support.microsoft.com/default.aspx?scid=kb;en-us;324961 (22 July 2005).

[10]: "Authentication Methods Supported in IIS 6.0". *Microsoft TechNet. MS Windows Server 2003 TechCenter. IIS 6.0 Technical Reference.* http://www.microsoft.com/technet/prodtechnol/WindowsServer2003/Library/IIS/36ea667e-c578-43b5-87fa-a2f174efb27a.mspx (22 July 2005)

[11]: Whitney R., Ramey T. "Analysis Services and HTTP". *SQL Server Magazine.* InstantDoc #40909. January 2004. http://www.windowsitpro.com/SQLServer/Article/ArticleID/40909/40909.html (12 April 2005).

[12]: "Analysis Services Client Architecture". *MSDN Library. SQL Server 2000. Analysis Services Architecture. Server and Client Architecture.* http://msdn.microsoft.com/library/en-us/olapdmad/agarchitecture_8mp1.asp (September 30, 2005).