Describe configuring relational data services

6 minutes

After you've provisioned a resource, you'll often need to configure it to meet the needs of your applications and environment. For example, you might need to set up network access, or open a firewall port to enable your applications to connect to the resource.

In this unit, you'll learn how to enable network access to your resources, and how you can prevent accidental exposure of your resources to third parties. You'll see how to use authentication and access control to protect the data managed by your resources.

Configure connectivity and firewalls

The default connectivity for Azure relational data services is to disable access to the world.

Configure connectivity to virtual networks and on-premises computers

To enable connectivity, use the **Firewalls and virtual networks** page for a service. To enable connectivity, choose **Selected networks**. Three further sections will appear, labeled **Virtual network**, **Firewall**, and **Exceptions**.

> **Note**
>
> An Azure Virtual Network is a representation of your own network in the cloud. A virtual network enables you to connect virtual machines and Azure services together, in much the same way that you might use a physical network on-premises. Azure ensures that each virtual network is isolated from other virtual networks created by other users, and from the Internet. Azure enables you to specify which machines (real and virtual), and services, are allowed to access resources on the virtual network, and which ports they can use.

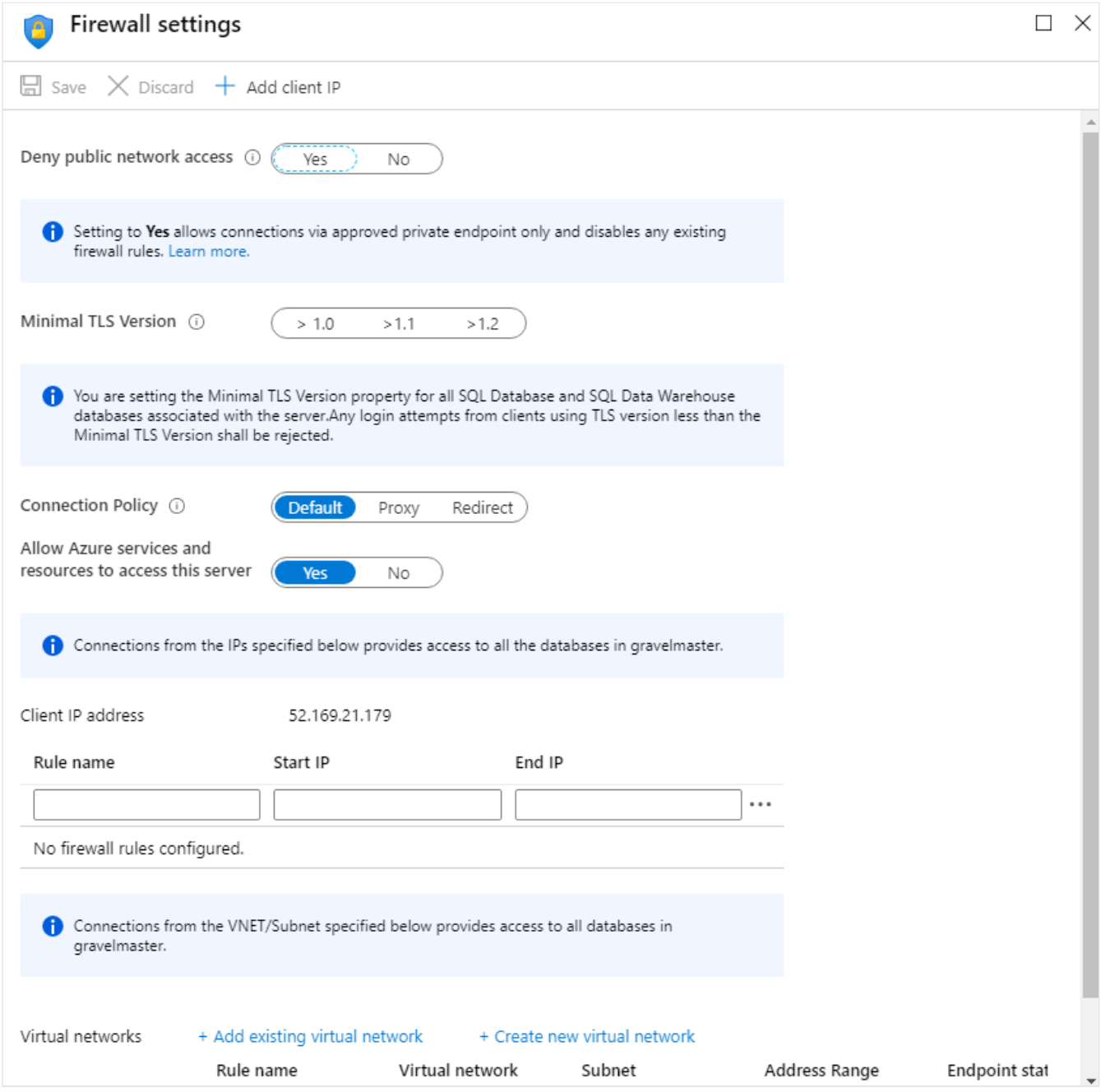
In the **Virtual networks** section, you can specify which virtual networks are allowed to route traffic to the service. When you create items such as web applications and virtual machines, you can add them to a virtual network. If these applications and virtual machines require

access to your resource, add the virtual network containing these items to the list of allowed networks.

If you need to connect to the service from an on-premises computer, in the **Firewall** section, add the IP address of the computer. This setting creates a firewall rule that allows traffic from that address to reach the service.

The **Exceptions** setting allows you to enable access to any other services that cannot be uniquely isolated through virtual network or IP address rules.

The image below shows the **Firewalls and virtual networks** page for an Azure SQL database. MySQL and PostgreSQL have a similar page.



> **Note**

Azure SQL Database communicates over port 1433. If you're trying to connect from within a corporate network, outbound traffic over port 1433 might not be allowed by your network's firewall. If so, you can't connect to your Azure SQL Database server unless your IT department opens port 1433.

ⓘ Important

A firewall rule of 0.0.0.0 enables all Azure services to pass through the server-level firewall rule and attempt to connect to a single or pooled database through the server.

Configure connectivity from private endpoints.

Azure Private Endpoint is a network interface that connects you privately and securely to a service powered by Azure Private Link. Private Endpoint uses a private IP address from your virtual network, effectively bringing the service into your virtual network. The service could be an Azure service such as Azure App Service, or your own Private Link Service. For detailed information, read What is Azure Private Endpoint?.

The **Private endpoint connections** page for a service allows you to specify which private endpoints, if any, are permitted access to your service. You can use the settings on this page, together with the **Firewalls and virtual networks** page, to completely lock down users and applications from accessing public endpoints to connect to your Azure SQL Database account.

Configure authentication

With Azure Active Directory (AD) authentication, you can centrally manage the identities of database users and other Microsoft services in one central location. Central ID management provides a single place to manage database users and simplifies permission management.

You can use these identities and configure access to your relational data services.

For detailed information on using Azure AD with Azure SQL database, visit the page What is Azure Active Directory authentication for SQL database on the Microsoft website. You can also authenticate users connecting to Azure Database for PostgreSQL and Azure Database for MySQL with AD.

Configure access control

Azure AD enables you to specify who, or what, can access your resources. Access control defines what a user or application can do with your resources once they've been

authenticated.

Access management for cloud resources is a critical function for any organization that is using the cloud. Azure role-based access control (Azure RBAC) helps you manage who has access to Azure resources, and what they can do with those resources. For example, using RBAC you could:

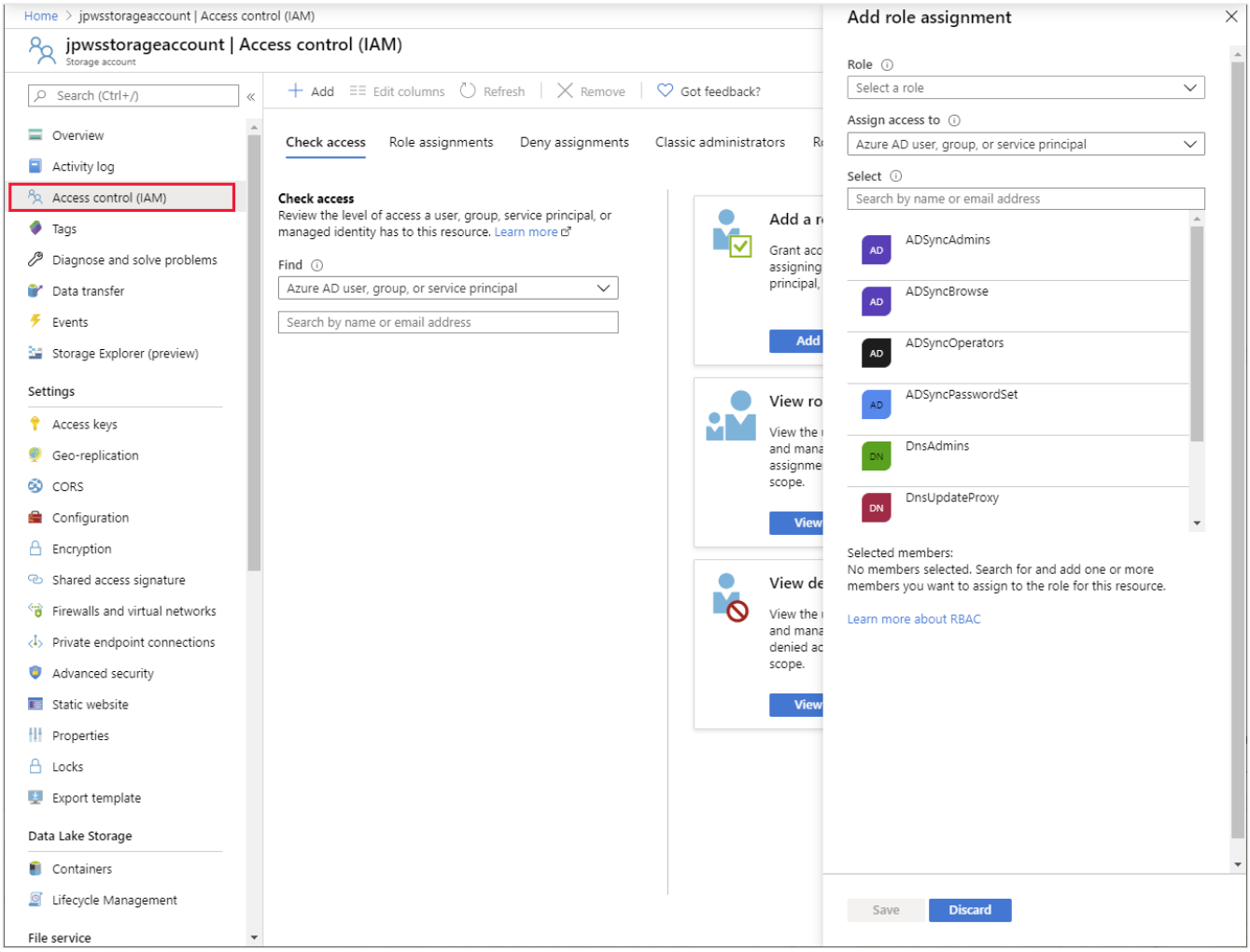
- Allow one user to manage virtual machines in a subscription and another user to manage virtual networks.
- Allow a database administrator group to manage SQL databases in a subscription.
- Allow a user to manage all resources in a resource group, such as virtual machines, websites, and subnets.
- Allow an application to access all resources in a resource group.

You control access to resources using Azure RBAC to create role assignments. A role assignment consists of three elements: a security principal, a role definition, and a scope.

- A **security principal** is an object that represents a user, group, service principal, or managed identity that is requesting access to Azure resources.
- A **role definition**, often abbreviated to *role*, is a collection of permissions. A role definition lists the operations that can be performed, such as read, write, and delete. Roles can be given high-level names, like owner, or specific names, like virtual machine reader. Azure includes several built-in roles that you can use, including:
  - **Owner** - Has full access to all resources including the right to delegate access to others.
  - **Contributor** - Can create and manage all types of Azure resources but can't grant access to others.
  - **Reader**- Can view existing Azure resources.
  - **User Access Administrator** - Lets you manage user access to Azure resources.

  You can also create your own custom roles. For detailed information, see Create or update Azure custom roles using the Azure portal on the Microsoft website.
- A **scope** lists the set of resources that the access applies to. When you assign a role, you can further limit the actions allowed by defining a scope. This is helpful if, for example, you want to make someone a Website Contributor, but only for one resource group.

You add role assignments to a resource in the Azure portal using the **Access control (IAM)** page. The **Role assignments** tab enables you to associate a role with a security principal, defining the level of access the role has to the resource. For further information, read Add or remove Azure role assignments using the Azure portal.

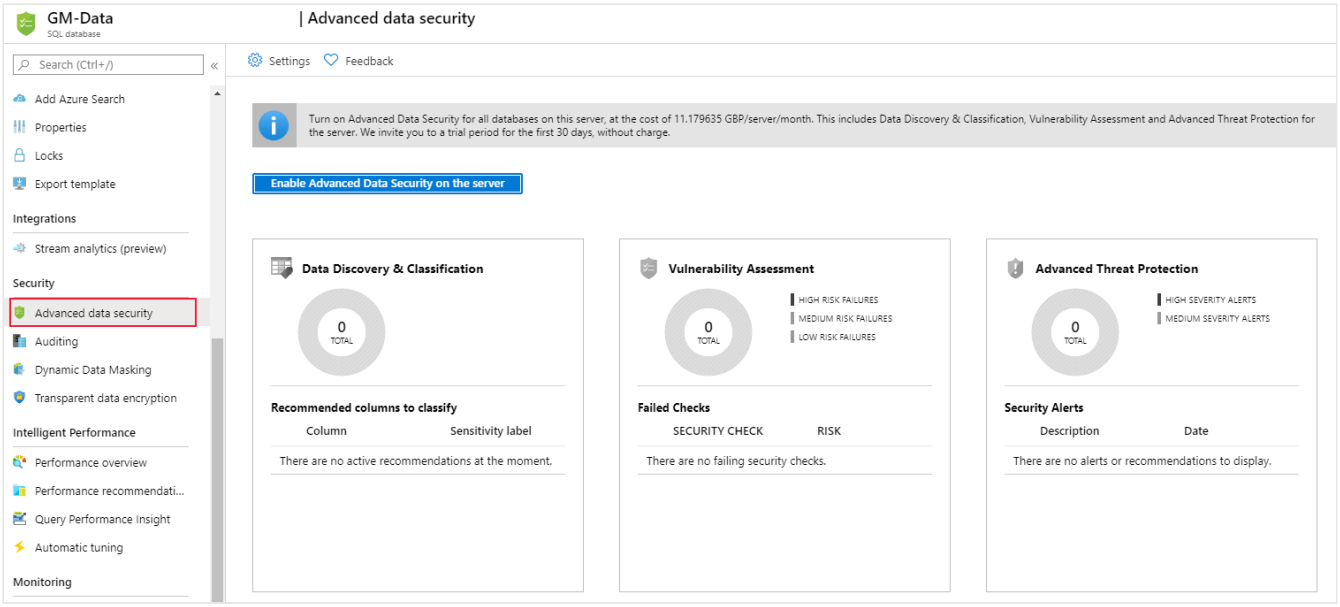


Configure advanced data security

Apart from authentication and authorization, many services provide additional protection through advanced data security.

Advanced data security implements threat protection and assessment. Threat protection adds security intelligence to your service. This intelligence monitors the service and detects unusual patterns of activity that could be harmful, or compromise the data managed by the service. Assessment identifies potential security vulnerabilities and recommends actions to mitigate them.

The image below shows the **Advanced data security** page for SQL database. The corresponding pages for MySQL and PostgreSQL are similar.



Next unit: Describe configuring Azure SQL Database, Azure Database for PostgreSQL, and Azure Database for MySQL

Continue >