Bài học sắp tới sẽ tập trung vào việc cấu hình và quản lý kết nối, tường lửa, xác thực, và quản lý truy cập cho các tài nguyên được triển khai trong Microsoft Azure. Dưới đây là một tổng quan về nội dung của bài học:

1. **Cấu hình Kết nối và Tường lửa**: Bạn sẽ học cách kích hoạt quyền truy cập mạng đến các tài nguyên của bạn và làm thế nào để ngăn chặn sự phơi bày vô tình của tài nguyên của bạn cho bên thứ ba. Bạn sẽ thấy cách sử dụng xác thực và kiểm soát truy cập để bảo vệ dữ liệu được quản lý bởi các tài nguyên của bạn.
2. **Xác thực và Kiểm soát Truy cập**: Bạn sẽ được giới thiệu về cách sử dụng xác thực thông qua Azure Active Directory để quản lý các danh tính người dùng cơ sở dữ liệu và các dịch vụ Microsoft khác tại một vị trí tập trung. Bạn cũng sẽ học cách xác định ai hoặc cái gì có thể truy cập vào các tài nguyên của bạn và xác định những gì họ có thể làm sau khi được xác thực.
3. **Quản lý Truy cập dựa trên Vai trò (RBAC)**: Bạn sẽ tìm hiểu về Azure Role-Based Access Control (RBAC), giúp bạn quản lý ai có quyền truy cập vào các tài nguyên Azure của bạn và họ có thể thực hiện những hành động gì với các tài nguyên đó. Bạn sẽ được hướng dẫn về cách gán các vai trò và xác định phạm vi của chúng.
4. **Bảo mật Dữ liệu Tiên tiến**: Cuối cùng, bạn sẽ tìm hiểu về các tính năng bảo mật dữ liệu tiên tiến trong Azure, bao gồm bảo vệ và đánh giá mối đe dọa. Bạn sẽ biết cách sử dụng các tính năng này để giám sát và phát hiện các hoạt động bất thường có thể gây hại hoặc đe dọa dữ liệu được quản lý bởi dịch vụ của bạn.

Trong bài học này, bạn sẽ hiểu được cách cấu hình và quản lý các khía cạnh quan trọng của bảo mật và quản lý tài nguyên trong môi trường điện toán đám mây của Microsoft Azure.