**Menjelajahi konsep keamanan di Azure Machine Learning**

Jelajahi dan bereksperimen dengan mengamankan lingkungan pembelajaran mesin untuk memastikan data tetap privat dan model akurat.

**Tujuan pembelajaran**

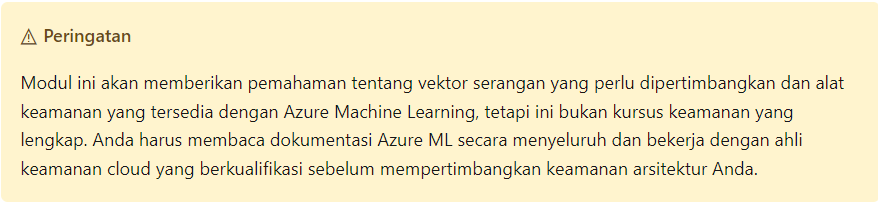
Dalam modul ini, Anda akan:

* Menerapkan dan memahami Kontrol Akses Berbasis Peran dalam Azure Machine Learning
* Menjelaskan bagaimana rahasia dikelola di Azure Machine Learning
* Menggunakan ruang kerja Azure Machine Learning dengan Azure Virtual Network

1. **Pengantar**

Pembelajaran mesin membutuhkan data dalam jumlah besar untuk melatih model yang efektif. Beberapa data ini dapat berisi informasi sensitif individu atau perusahaan yang harus diamankan agar tetap bersifat privat. Tantangan keamanan seputar pembelajaran mesin tidak hanya terbatas pada data, dan penyiapan untuk menciptakan lingkungan kerja yang aman dapat menjadi hal yang menakutkan. Azure Machine Learning (Azure ML) menyediakan beberapa mekanisme yang menawarkan kontrol granular lingkungan jaringan, sumber daya yang digunakan di dalamnya, dan data yang diakses. Tindakan yang tepat dapat melindungi dari penyerang luar dan dari masalah internal seperti kelalaian atau proses yang belum matang.

Banyak serangan pada sistem pembelajaran mesin melibatkan pengaksesan model melalui jaringan yang tidak aman untuk mencuri atau memanipulasi data untuk memengaruhi performa model dan mengakses data sensitif. Dengan membangun penyimpanan data pelatihan yang lebih baik dan lebih aman, mengunci platform pembelajaran mesin, dan mengontrol akses ke input dan output, kami dapat memastikan data tetap terlindungi. Fitur ini berguna untuk ilmuwan data, administrator, dan teknisi operasi yang ingin membuat konfigurasi aman yang sesuai dengan kebijakan perusahaan mereka.



1. **Prasyarat**

* Pemahaman dasar tentang Azure

1. **Tujuan pembelajaran**

Dalam modul ini, Anda akan:

* Menerapkan dan memahami Kontrol Akses Berbasis Peran dalam Azure Machine Learning
* Menjelaskan bagaimana rahasia dikelola di Azure Machine Learning
* Menggunakan ruang kerja Azure Machine Learning dengan Azure Virtual Network

1. **Apa yang dimaksud kontrol akses berbasis peran?**

Kontrol Akses Berbasis Peran Azure (Azure RBAC) adalah sistem otorisasi yang memungkinkan manajemen akses mendetail dari sumber daya Azure Machine Learning. Ini memungkinkan Anda untuk mengelola akses anggota tim ke sumber daya cloud Azure dengan menetapkan peran. Peran ini menentukan aset apa yang dapat digunakan anggota tim di ruang kerja, dan apa yang dapat mereka lakukan dengan sumber daya tersebut. Ini bisa menjadi penting jika tim Anda bekerja dengan data sensitif seperti catatan rumah sakit yang berisi informasi medis pribadi, atau jika Anda ingin membatasi akses ke aset penting untuk anggota tim junior dalam Azure Machine Learning. Dengan menggunakan peran ini, Anda dapat secara realistis mencerminkan struktur organisasi Anda, memastikan tanggung jawab dan aset penting dibagikan kepada individu yang benar.

1. **Peran pengguna**

Peran Azure RBAC dapat ditetapkan untuk individu dan grup. Hak yang ditetapkan kepada setiap grup dialokasikan sebagai sistem berbasis izin, dengan akses dan batasan yang ditetapkan dengan jelas. Kontrol ini diterapkan pada tingkat ruang kerja dan hanya dapat diubah oleh administrator atau pemilik ruang kerja tertentu dalam Azure Machine Learning. Ruang kerja Azure Machine Learning, seperti sumber daya Azure lainnya, hadir dengan tiga peran default saat dibuat. Anda dapat menambahkan pengguna ke ruang kerja dan menetapkan salah satu peran berikut:

* **Pemilik** memiliki akses penuh ke ruang kerja, termasuk kemampuan untuk melihat, membuat, mengedit, atau menghapus aset di ruang kerja. Pemilik juga dapat mengubah penetapan peran.
* **Kontributor** dapat melihat, membuat, mengedit, atau menghapus aset di ruang kerja. Misalnya, kontributor dapat membuat eksperimen, membuat atau melampirkan kluster komputasi, mengirimkan eksekusi, dan menerapkan layanan web.
* **Pembaca** hanya dapat melakukan tindakan baca-saja di ruang kerja. Pembaca dapat membuat daftar dan melihat aset, termasuk kredensial datastore di ruang kerja. Pembaca tidak dapat membuat atau memperbarui aset ini.

1. **Peran kustom**

Jika peran default tidak memenuhi kebutuhan organisasi untuk kontrol akses yang lebih selektif, Anda dapat membuat Peran kustom Anda sendiri. Peran kustom memberi Anda fleksibilitas untuk mengembangkan aturan berbasis izin untuk individu atau grup yang menyediakan akses sambil menentukan ketentuan keamanan Anda sendiri untuk mengamankan data atau sumber daya. Anda dapat membuat peran tersedia di tingkat ruang kerja tertentu, tingkat grup sumber daya tertentu, atau tingkat langganan dengan menentukan cakupan peran kustom Anda, yang dapat kita lihat dalam contoh JSON di bawah ini.

Peran kustom dapat dibuat dengan menentukan kemungkinan tindakan yang diizinkan dan NotAction untuk membatasi aktivitas atau akses tertentu. Anda dapat membuat peran kustom menggunakan portal Azure, Azure PowerShell, Azure CLI, atau REST API. Di bawah ini kita dapat melihat permintaan JSON peran kustom untuk Ilmuwan Data:

{

"Name": "Data Scientist Custom",

"IsCustom": true,

"Description": "Can run experiment but can't create or delete compute or deploy production endpoints.",

"Actions": [

"Microsoft.MachineLearningServices/workspaces/\*/read",

"Microsoft.MachineLearningServices/workspaces/\*/action",

"Microsoft.MachineLearningServices/workspaces/\*/delete",

"Microsoft.MachineLearningServices/workspaces/\*/write"

],

"NotActions": [

"Microsoft.MachineLearningServices/workspaces/delete",

"Microsoft.MachineLearningServices/workspaces/write",

"Microsoft.MachineLearningServices/workspaces/computes/\*/write",

"Microsoft.MachineLearningServices/workspaces/computes/\*/delete",

"Microsoft.Authorization/\*",

"Microsoft.MachineLearningServices/workspaces/computes/listKeys/action",

"Microsoft.MachineLearningServices/workspaces/listKeys/action",

"Microsoft.MachineLearningServices/workspaces/services/aks/write",

"Microsoft.MachineLearningServices/workspaces/services/aks/delete",

"Microsoft.MachineLearningServices/workspaces/endpoints/pipelines/write"

],

"AssignableScopes": [

"/subscriptions/<subscription\_id>/resourceGroups/<resource\_group\_name>/providers/Microsoft.MachineLearningServices/workspaces/<workspace\_name>"

]

}

Perhatikan Action dan NotAction di atas yang menentukan izin untuk peran kustom dan cakupan yang ditetapkan pada tingkat ruang kerja tertentu. Pada contoh ini, tindakan ilmuwan data didefinisikan melalui kartubebas (diwakili oleh tanda \*) yang memperluas izin ke semua yang cocok dengan string tindakan yang Anda berikan. Jadi, dalam contoh di atas, string kartubebas menambahkan semua izin yang terkait dengan pembacaan, penulisan, tindakan, atau penghapusan apa pun di dalam ruang kerja.

Namun, jika kita melihat NotActions di atas, kita dapat melihat pembatasan, antara lain pada penghapusan atau pembuatan ruang kerja atau sumber daya komputasi baru. Pembatasan ini lebih diutamakan daripada tindakan yang diizinkan secara eksplisit.

1. **Sistem**

Tantangan umum bagi pengembang adalah manajemen rahasia dan info masuk yang digunakan untuk mengamankan komunikasi antara komponen yang berbeda. Azure Machine Learning mengandalkan **Azure Active Directory (Azure AD)** untuk autentikasi dan/atau komunikasi antara sumber daya cloud Azure lainnya. Azure AD adalah layanan manajemen akses dan identitas berbasis cloud yang membantu karyawan Anda masuk dan mengakses sumber daya cloud di Azure.

1. **Autentikasi dengan Azure AD**

Secara umum, ada tiga alur kerja autentikasi yang dapat Anda gunakan saat menyambungkan ke ruang kerja:

**Interaktif**: Anda menggunakan akun Anda di Azure Active Directory untuk mengautentikasi secara manual atau mendapatkan token autentikasi. Autentikasi interaktif digunakan selama **eksperimen dan pengembangan berulang**. Autentikasi interaktif memungkinkan Anda untuk mengontrol akses ke sumber daya (seperti layanan web) pada basis per pengguna.

**Perwakilan layanan:** Anda membuat akun perwakilan layanan di Azure Active Directory, dan menggunakannya untuk mengautentikasi atau mendapatkan token autentikasi. Perwakilan layanan digunakan saat Anda memerlukan proses otomatis untuk mengautentikasi ke layanan. Misalnya, integrasi berkelanjutan dan skrip penyebaran yang melatih dan menguji model setiap kali perubahan kode pelatihan memerlukan akses berkelanjutan dan akan mendapat manfaat dari akun utama layanan.

**Sesi Azure CLI**: Anda menggunakan sesi Azure CLI aktif untuk mengautentikasi. Autentikasi Azure CLI digunakan selama **eksperimen dan pengembangan berulang**, atau saat Anda memerlukan **proses otomatis untuk mengautentikasi** ke layanan menggunakan sesi pra-autentikasi. Anda dapat masuk ke Azure melalui Azure CLI di stasiun kerja lokal Anda, tanpa menyimpan info masuk dalam kode atau meminta pengguna untuk mengautentikasi.

**Identitas terkelola:** Saat menggunakan SDK Azure Machine Learning di Azure Machine Learning, Anda dapat menggunakan identitas terkelola untuk Azure. Alur kerja ini memungkinkan VM tersambung ke ruang kerja menggunakan identitas terkelola, tanpa menyimpan info masuk dalam kode atau meminta pengguna untuk mengautentikasi. Kluster komputasi Azure Machine Learning juga dapat dikonfigurasi untuk menggunakan identitas terkelola guna mengakses ruang kerja saat melatih model.

1. **Identitas Terkelola**

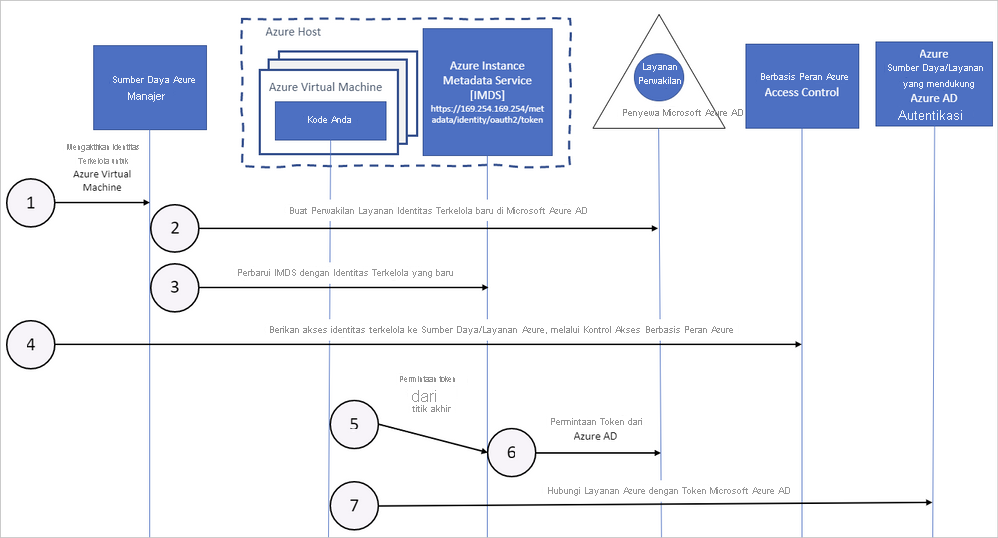
Saat mengonfigurasi ruang kerja Azure Machine Learning dengan cara yang dapat dipercaya, sangat penting untuk memastikan bahwa berbagai layanan cloud yang terkait dengan ruang kerja memiliki tingkat akses yang benar. Identitas terkelola memungkinkan Anda mengautentikasi layanan dengan memberikan identitas yang dikelola secara otomatis untuk aplikasi atau layanan yang akan digunakan saat menyambungkan ke layanan cloud Azure. Identitas terkelola bekerja dengan layanan apa pun yang mendukung autentikasi Azure AD, dan menyediakan log aktivitas sehingga admin dapat melihat aktivitas pengguna seperti waktu masuk, kapan operasi dimulai, dan oleh siapa.

Ada dua jenis identitas terkelola:

* **Ditetapkan sistem**: Beberapa layanan Azure memungkinkan Anda mengaktifkan identitas terkelola secara langsung pada instans layanan. Saat Anda mengaktifkan identitas terkelola yang ditetapkan sistem, identitas dibuat di Azure AD yang terkait dengan siklus hidup instans layanan tersebut. Secara desain, hanya sumber daya Azure yang dapat menggunakan identitas ini untuk meminta token dari Azure AD, dan ketika sumber daya dihapus, Azure secara otomatis menghapus identitas untuk Anda.
* **Ditetapkan pengguna**: Anda juga dapat membuat identitas terkelola sebagai sumber daya Azure mandiri. Anda dapat membuat identitas terkelola yang ditetapkan pengguna dan menetapkannya ke satu atau beberapa instans layanan Azure. Identitas dikelola secara terpisah dari sumber daya yang menggunakannya dan akan tetap ada jika sumber daya yang menggunakannya dihapus. Untuk mempermudah, sebaiknya gunakan peran yang ditetapkan sistem kecuali Anda memerlukan solusi akses kustom.

Setelah Anda memiliki identitas terkelola, Anda dapat meminta token melalui titik akhir token pada sumber daya seperti komputer virtual. Token ini kemudian bekerja dengan otorisasi pengguna yang ada dari Azure RBAC untuk mengizinkan mereka melakukan tindakan, seperti menarik kunci dari Azure Key Vault atau rahasia lainnya. Demikian pula, anggaplah pengguna memiliki peran Azure RBAC yang mengizinkan penggunaan solusi penyimpanan Azure. Dalam hal ini, token tersebut dapat digunakan untuk mengautentikasi dan membaca atau mendorong data ke penyimpanan tanpa kredensial apa pun dalam kodenya. Operasi pada identitas terkelola dapat dilakukan dengan menggunakan templat Azure Resource Manager (ARM), portal Azure, Azure CLI, PowerShell, dan REST API.

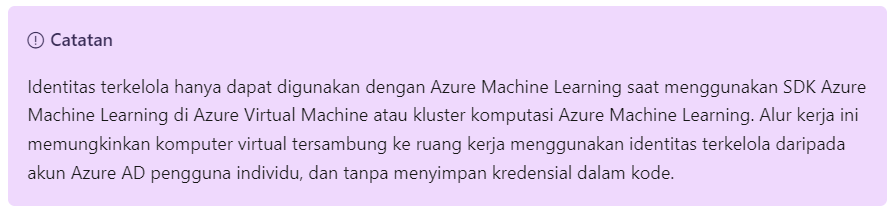
Di bawah ini kita dapat melihat alur kerja khas untuk identitas terkelola dalam komputer virtual:



1. **Identitas dengan kluster komputasi**

Kluster komputasi Azure Machine Learning dapat menggunakan identitas terkelola untuk mengautentikasi akses ke sumber daya Azure dalam Azure Machine Learning tanpa menyertakan kredensial dalam kode Anda. Ini berguna untuk secara cepat memberikan izin minimum yang diperlukan untuk mengakses sumber daya sambil mengamankan sumber daya penting lainnya. Misalnya, selama alur kerja pembelajaran mesin, ruang kerja memerlukan akses ke Azure Container Registry untuk gambar Docker, dan akun penyimpanan untuk data pelatihan. Secara default, identitas yang ditetapkan sistem diaktifkan langsung di kluster komputasi Azure Machine Learning dan semua sumber daya ini akan tersedia untuk digunakan. Setelah kluster komputasi dihapus, Azure akan secara otomatis membersihkan kredensial dan identitas di Azure Active Directory. Kluster komputasi juga dapat mendukung identitas yang ditetapkan pengguna kustom yang ditetapkan untuk beberapa sumber daya dan akan tetap ada setelah sumber daya dihapus.

Selama pembuatan kluster atau saat mengedit detail kluster komputasi, di Pengaturan tingkat lanjut, alihkan Tetapkan identitas terkelola dan tentukan identitas yang ditetapkan sistem atau identitas yang ditetapkan pengguna. Perhatikan bahwa kluster komputasi Azure Machine Learning hanya mendukung satu identitas yang ditetapkan sistem atau beberapa identitas yang ditetapkan pengguna, tidak keduanya secara bersamaan.



**3. Latihan – Menyiapkan Azure Machine Learning dengan peran kustom**

Ruang Kerja Machine Learning mungkin merupakan salah satu sumber daya paling menarik bagi Ilmuwan Data dan Teknisi ML.

Ruang Kerja Machine Learning adalah sumber daya tingkat tinggi tempat Anda bekerja dengan artefak yang diperlukan dalam Azure Machine Learning, seperti himpunan data, model, dan peran pengguna.

Dalam latihan ini, kami akan menyiapkan Ruang Kerja Azure Machine Learning, yang akan digunakan dalam latihan dan modul berikut.

1. **Prasyarat**

* Akun Azure dan Langganan

Jika Anda belum memiliki langganan Azure, ikuti petunjuk pada tautan di bawah ini:

Buat langganan di portal Azure.

1. **Masuk ke Azure**

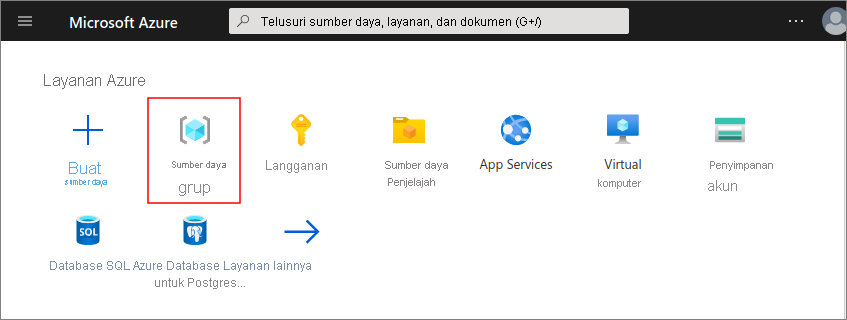
Masuk ke portal Azure.

1. **Buat Grup Sumber Daya**

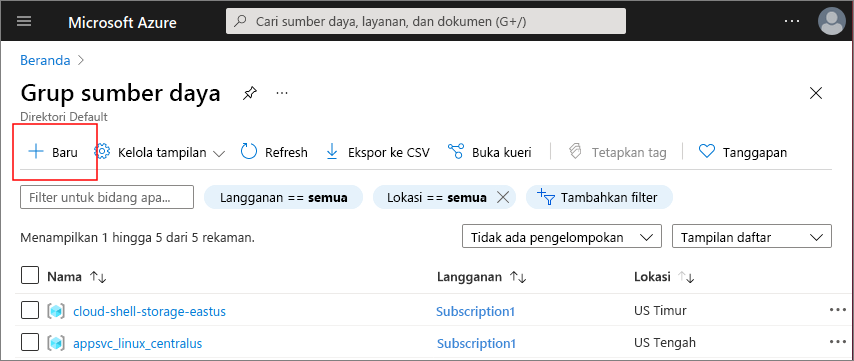
Grup Sumber Daya adalah tempat administrator dapat membuat grup logis sumber daya, seperti volume penyimpanan, komputer virtual, dan ruang kerja ML, sehingga mereka dapat lebih mudah melacak biaya, menerapkan kontrol akses, dan memantau aktivitas.

Mari buat Grup Sumber Daya untuk latihan ini:

1. Di portal Azure, pilih **Grup Sumber Daya:**

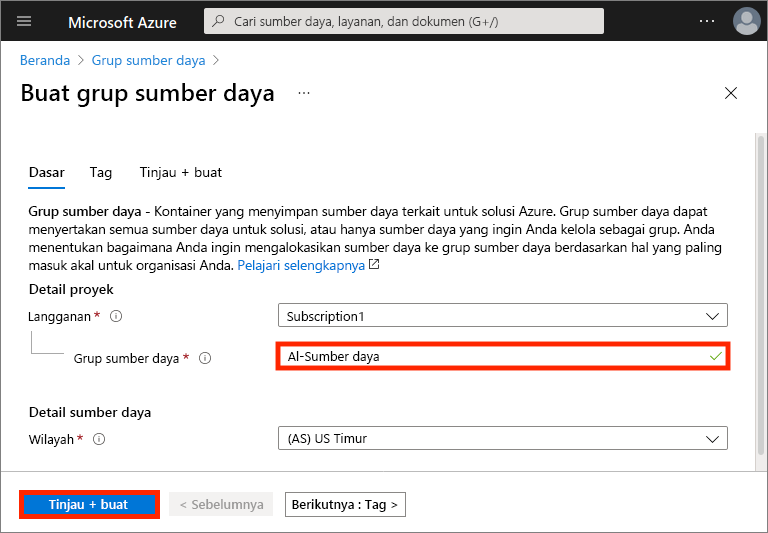


1. Pilih **Baru** atau **Buat** dalam daftar grup sumber daya:



1. Mengisi formulir untuk menambahkan Grup Sumber Daya baru

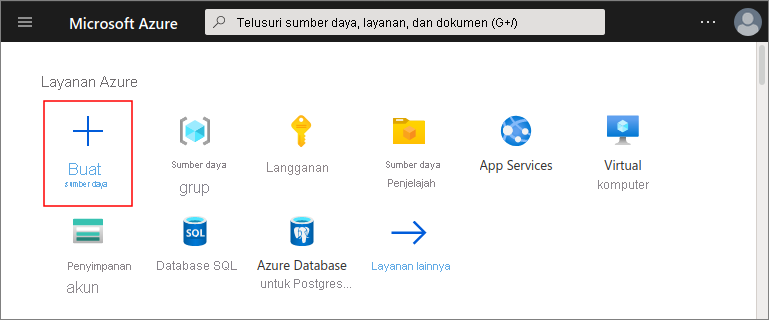
* Pilih langganan yang Anda buat sebelumnya.
* Gunakan AI-Resource sebagai nama grup Sumber Daya.
* Pilih wilayah pilihan Anda.
* Pilih Tinjau dan buat, lalu pilih Buat.



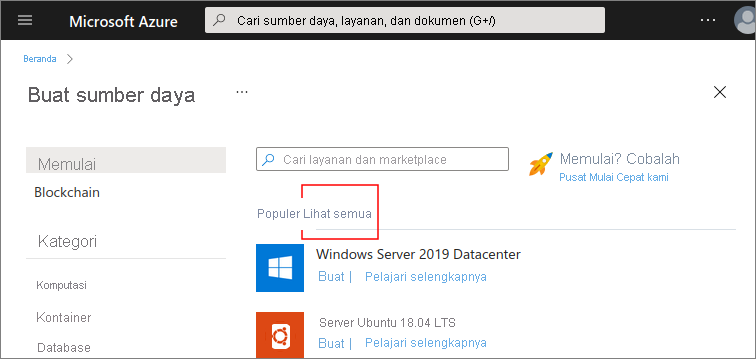
1. **Membuat Ruang Kerja ML**

Untuk membuat Ruang Kerja ML, ikuti langkah-langkah berikut:

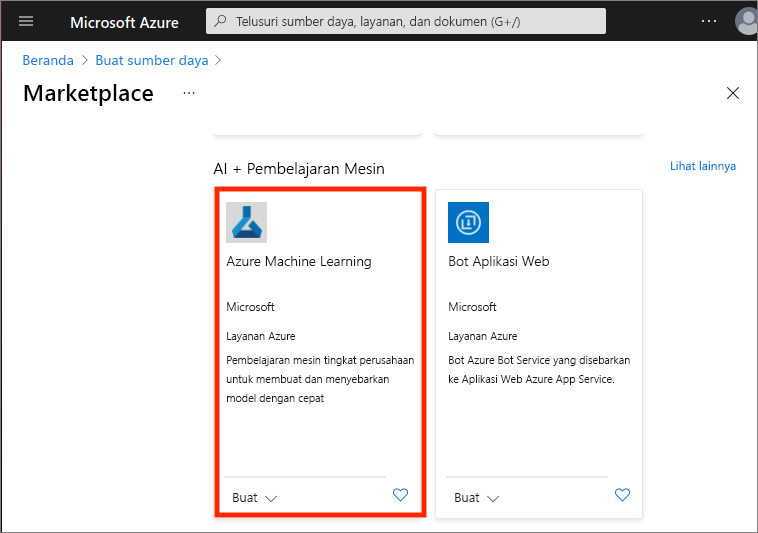
1. Pilih **Beranda** untuk kembali ke beranda
2. Pilih **Buat sumber daya** di portal Azure:



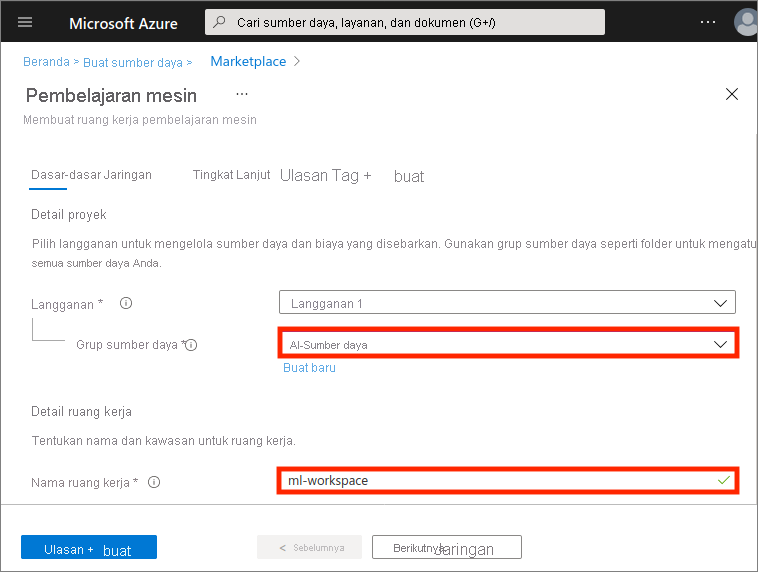
1. Pilih **Lihat semua.**



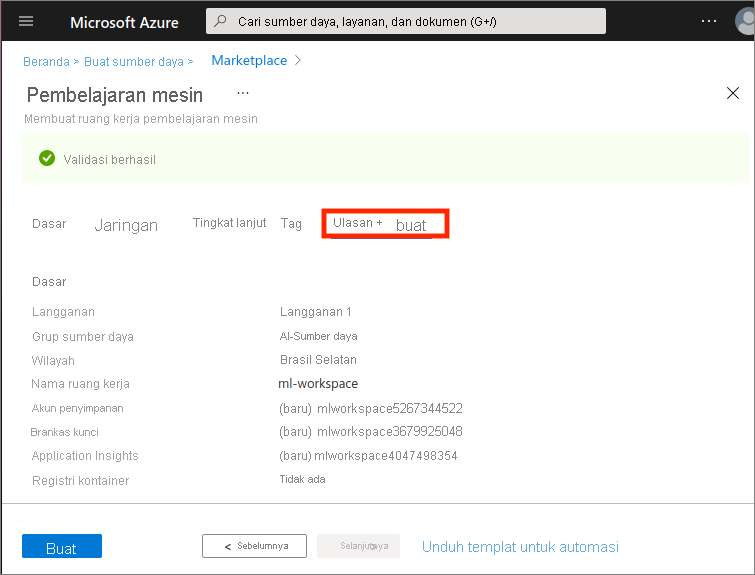
1. Gulir ke bawah hingga opsi **AI + Pembelajaran Mesin** terlihat dan pilih **buat**.



1. Isi formulir, pilih langganan Anda saat ini dan grup sumber daya yang telah kami buat sebelumnya **(AI-Resource**). Gunakan **ml-workspace** sebagai nama ruang kerja:



1. Pilih tombol **Tinjau + buat** untuk memuat layar konfirmasi tinjauan:



1. Pilih **Buat** untuk mulai menyebarkan ruang kerja baru (ini mungkin memerlukan waktu beberapa menit).

**Penting**

Perhatikan bahwa penyebaran di atas menciptakan sumber daya lain:

* Akun penyimpanan digunakan untuk menyimpan file yang digunakan oleh Ruang Kerja beserta data untuk eksperimen dan pelatihan model

**Link** : <https://azure.microsoft.com/en-us/products/category/storage/>

* Instans Application Insights, digunakan untuk memantau layanan prediktif di Ruang Kerja.

**Link** : <https://azure.microsoft.com/en-us/products/monitor/>

* Instans Azure Key Vault, digunakan untuk mengelola rahasia seperti kunci autentikasi dan kredensial yang digunakan oleh Ruang Kerja.

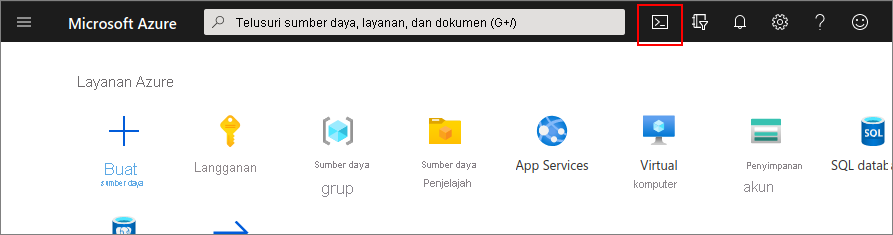
**Link :** <https://azure.microsoft.com/en-us/products/key-vault/>

* Sebuah registri kontainer, dibuat sesuai kebutuhan untuk mengelola kontainer untuk model yang disebarkan.

**Link** : <https://azure.microsoft.com/en-us/products/container-registry/>

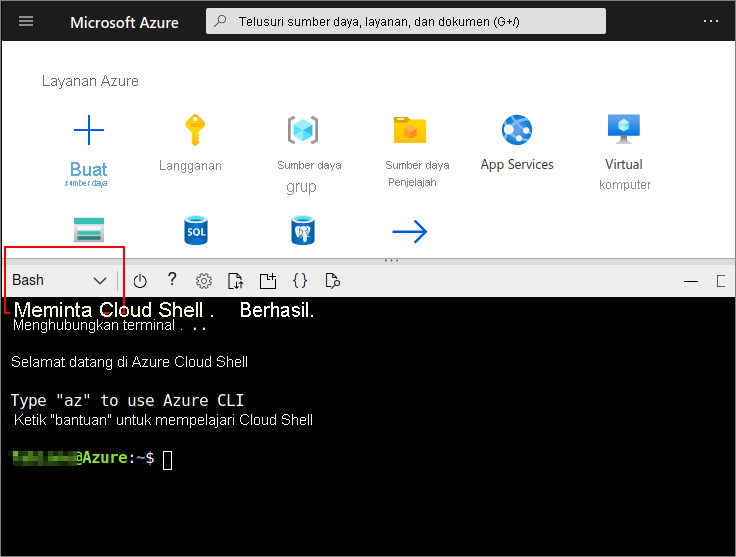
1. **Buat Peran Kustom dan Tetapkan ke Ruang Kerja**
2. Pilih Beranda untuk kembali ke beranda
3. Buka Azure Cloud Shell

* Pilih Ikon Cloud Shell:



* atau gunakan URL langsung di browser Anda: <https://shell.azure.com.>

1. Pilih **Bash** atau **PowerShell** (kami akan menggunakan bash):



1. **Tentukan Peran Kustom:**
2. Menggunakan editor teks pilihan Anda, buat file bernama **data\_scientist\_custom\_role.json**, ganti informasi di bawah ini:



1. Unggah file definisi peran:

* Pilih ikon **unggah/Unduh file**
* Pilih **Unggah**
* Pilih file **data\_scientist\_custom\_role.json** yang Anda buat di atas:

{

"Name": "Data Scientist Custom",

"IsCustom": true,

"Description": "Can run experiment but can't create or delete compute.",

"Actions": ["\*"],

"NotActions": [

"Microsoft.MachineLearningServices/workspaces/\*/delete",

"Microsoft.MachineLearningServices/workspaces/write",

"Microsoft.MachineLearningServices/workspaces/computes/\*/write",

"Microsoft.MachineLearningServices/workspaces/computes/\*/delete",

"Microsoft.Authorization/\*/write"

],

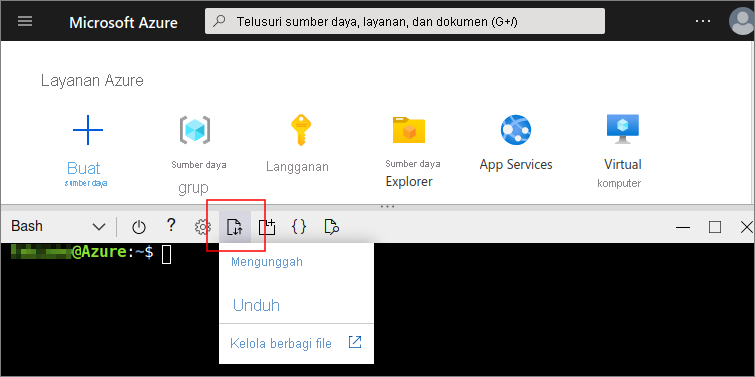
"AssignableScopes": [

"/subscriptions/<subscription\_id>/resourceGroups/<resource\_group\_name>/providers/Microsoft.MachineLearningServices/workspaces/<workspace\_name>"

]

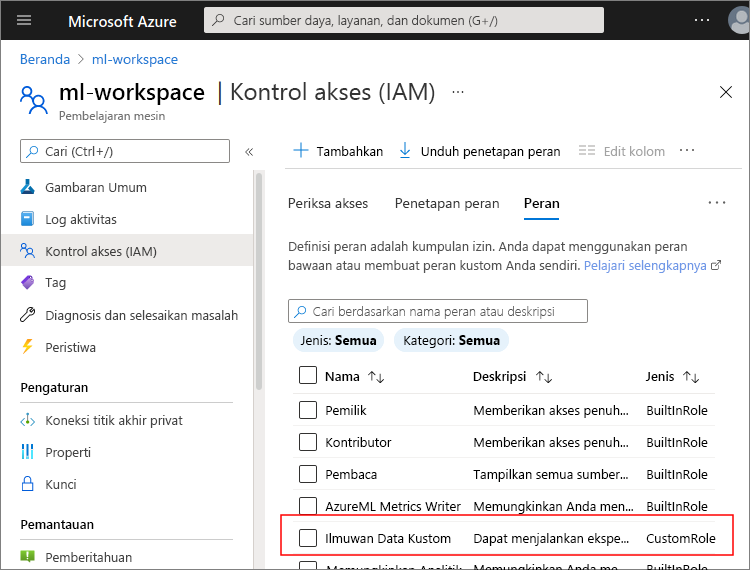
}

1. Buat definisi peran menggunakan perintah CLI az role definition create (perhatikan bahwa argumen terakhir adalah file yang baru saja kita unggah):



Ini menambahkan peran "Kustom Ilmuwan Data", yang terbatas pada menjalankan eksperimen di **ml-workspace.**

Untuk memverifikasi dan mencantumkan peran yang ada menggunakan portal Azure, pilih opsi **Kontrol Akses (IAM)** di ml-workspace Anda, lalu pilih tab **Peran**:



1. **Ringkasan**

Selamat!

Di unit ini Anda telah membahas topik berikut:

* Membuat grup Sumber Daya
* Membuat Ruang Kerja Machine Learning
* Menggunakan Cloud Shell untuk menjalankan perintah dan mengunggah file ke akun Anda
* Mendefinisikan Peran Kustom untuk Machine Learning dengan akses ke ruang kerja Anda

1. **Sumber daya lainnya**

Untuk membaca selengkapnya tentang Ruang Kerja dan Peran Kustom, kunjungi:

* Apa itu ruang kerja Azure Machine Learning?

Link : <https://learn.microsoft.com/id-id/azure/machine-learning/concept-workspace>

* Kelola grup sumber daya Azure Resource Manager dengan menggunakan portal Microsoft Azure

Link : <https://learn.microsoft.com/id-id/azure/azure-resource-manager/management/manage-resource-groups-portal#what-is-a-resource-group>

* Kelola akses ke ruang kerja Azure Machine Learning

Link : <https://learn.microsoft.com/id-id/azure/machine-learning/how-to-assign-roles?tabs=labeler>

**4. Kunci dan rahasia dengan Azure Key Vault**

Sebagian besar aplikasi jaringan perlu bekerja dengan rahasia, seperti kata sandi atau string koneksi database. Ketika melakukan pembelajaran mesin di Azure, kita biasanya menggunakan rahasia untuk mengakses data pelatihan atau melihat hasilnya. Khususnya ketika bekerja dengan data pribadi, penting untuk memastikan bahwa rahasia dikelola dengan benar.

1. **Jangan simpan rahasia dalam kode sumber**

Menyimpan rahasia dalam kode sumber tidak praktis dan anti-pola keamanan. Ini hadir untuk beberapa alasan:

* Mengubah kata sandi berarti memperbarui kode sumber, yang mungkin berarti membangun kembali dan menerbitkan ulang aplikasi.
* Rahasia berkode keras membuatnya canggung untuk bekerja dengan lingkungan yang berbeda, seperti lingkungan pementasan dan produksi. Ini juga meningkatkan risiko modifikasi yang tidak disengaja atau penghancuran data lingkungan produksi selama pengembangan.
* Semua orang dengan akses ke kode sumber mendapatkan akses ke semua rahasia. Hal ini membuat hampir tidak mungkin untuk memastikan bahwa hanya anggota tim senior yang memiliki akses ke sumber daya yang sensitif. Ini juga berarti bahwa setiap pembagian, atau kebocoran, kode sumber Anda juga memberikan kunci keamanan Anda kepada pihak luar.
* Kontrol sumber, seperti git, biasanya akan menyimpan kata sandi lama dalam riwayat. Ini berarti anggota tim masa depan mendapatkan akses ke semua kata sandi historis.

Salah satu alternatif terbaik untuk menyimpan rahasia dalam kode sumber adalah dengan membuatnya tersedia di lingkungan aplikasi. Dalam pola ini, aplikasi Anda meminta rahasia dari lingkungan lalu menggunakannya untuk tersambung ke sumber daya yang diperlukan. Kelemahan penyimpanan rahasia yang disebutkan di atas dalam kode sumber dihilangkan, selama setiap lingkungan memiliki nilai rahasia yang berbeda, seperti kata sandi yang berbeda untuk mengakses sumber daya tertentu.

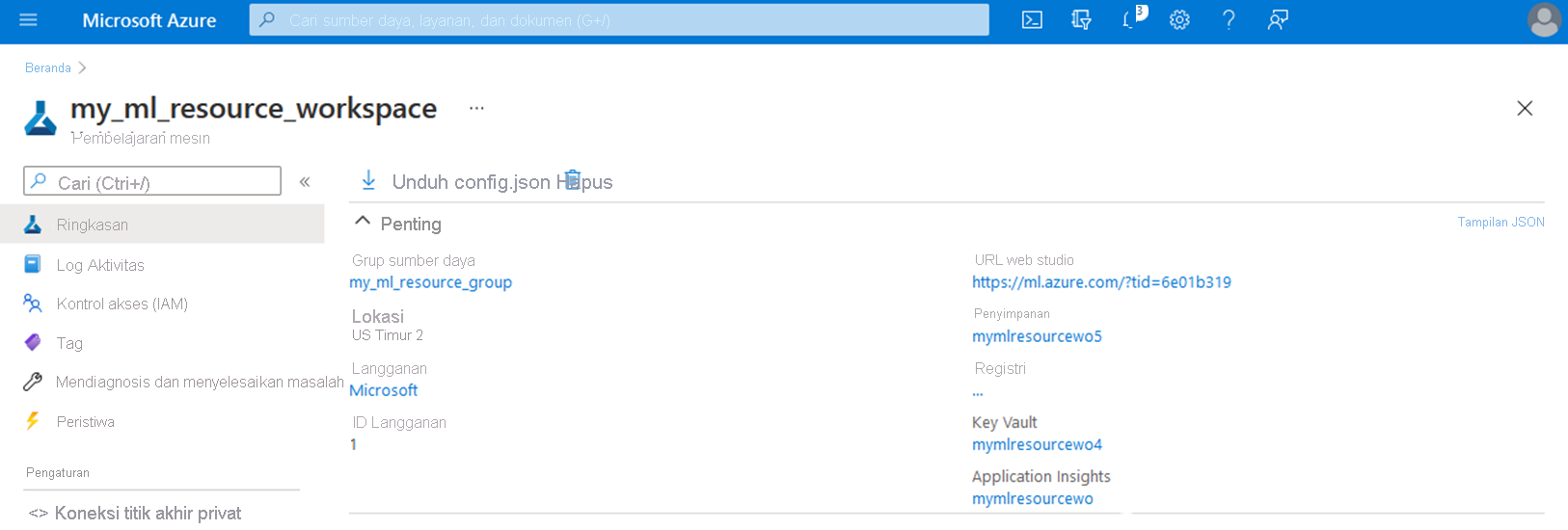
1. **Azure Key Vault**

Azure Key Vault menyediakan penyimpanan rahasia umum yang aman untuk aplikasi di lingkungan yang dihosting Azure. Semua jenis rahasia dapat disimpan, selama nilainya tidak lebih besar dari 25kb dan dapat dibaca dan dikembalikan sebagai string. Rahasia diberi nama, dan jenis kontennya (seperti kata sandi atau sertifikat) secara opsional dapat disimpan di samping nilai untuk memberikan petunjuk yang membantu interpretasinya saat diambil.

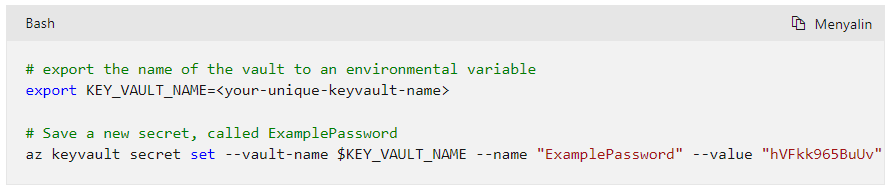
Rahasia yang disimpan di Azure Key Vault dienkripsi, secara opsional di tingkat perangkat keras. Rahasia ditangani secara transparan, dan tidak memerlukan tindakan dari pengguna atau aplikasi yang meminta rahasia. Mereka juga dapat dinonaktifkan sementara, dan secara otomatis aktif atau kedaluwarsa pada tanggal tertentu.

1. **Cara kerja Key Vault dengan Azure Machine Learning**

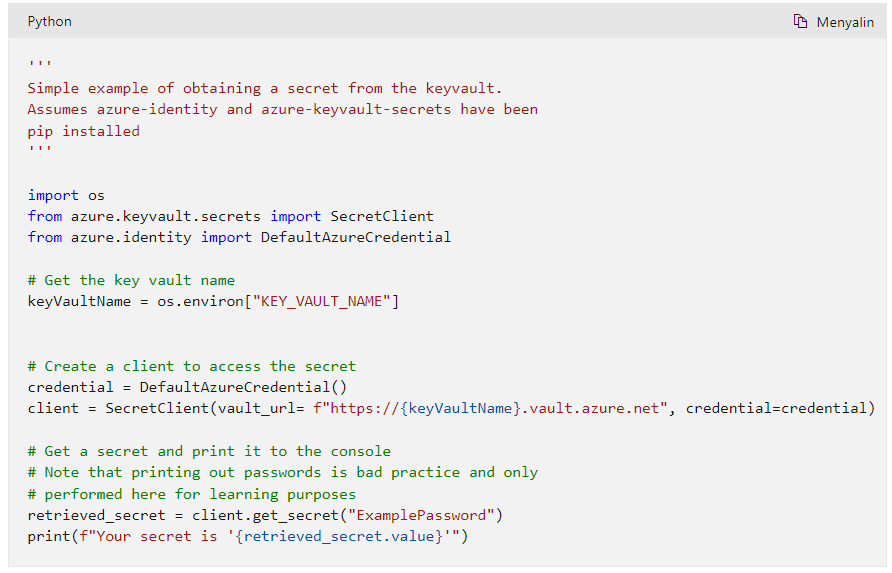
Saat Anda membuat ruang kerja Azure Machine Learning, ini secara otomatis membuat Key Vault. Untuk melihat Azure Key Vault yang terkait dengan ruang kerja Anda, buka tab Gambaran Umum ruang kerja. Key vault muncul di sisi kanan.



Saat Anda pertama kali membuat ruang kerja, Key Vault Anda akan dibuat secara otomatis. Key Vault dapat diakses melalui aplikasi Anda. Misalnya, Anda dapat menggunakan Azure Shell untuk mengatur variabel lingkungan yang menyimpan nama Penyimpanan Kunci, dan menyimpan kata sandi ke penyimpanan kunci tersebut seperti:



Kata sandi ini disimpan dengan aman dan dienkripsi. Sebagai contoh, aplikasi Python yang menggunakan SDK Azure Machine Learning dapat mengakses kunci ini sebagai berikut:



Outputnya adalah kata sandi asli yang kami simpan:



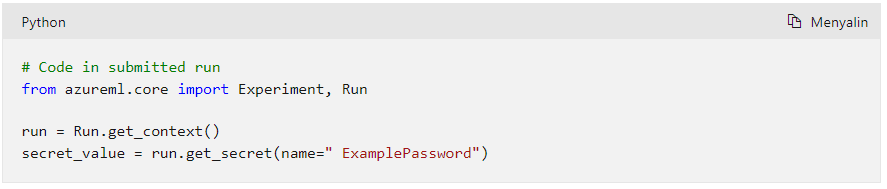
1. **Bekerja dengan eksekusi jarak jauh**

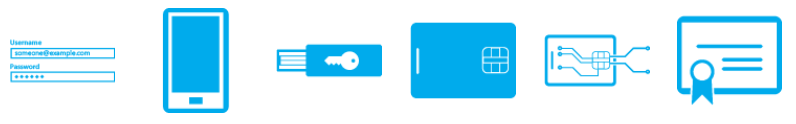
Fitur di atas memberikan solusi umum untuk menggunakan Key Vault. Biasanya, dengan Azure Machine Learning, Anda akan mengeksekusi kode melalui eksekusi jarak jauh.

Alur standar untuk menggunakan rahasia dalam konteks ini adalah:

* Masuk ke Azure dan sambungkan ke ruang kerja Anda,
* Atur rahasia di Key Vault Ruang Kerja,
* Mengirim eksekusi jarak jauh, lalu
* Dalam eksekusi jarak jauh, dapatkan rahasia dari Key Vault dan gunakan.

Saat menggunakan SDK Python dan menjalankannya, rahasia dapat dengan mudah diakses secara langsung. Ini karena proses yang dikirimkan sadar akan ruang kerjanya. Contohnya:





1. **Baca selengkapnya**

Untuk informasi selengkapnya tentang menggunakan rahasia untuk mengamankan dan mengakses data Anda, kami merekomendasikan sumber daya berikut:

* Azure Key Vault

**Link** : <https://learn.microsoft.com/id-id/azure/key-vault/>

* Kelas Keyvault di Python SDK

**Link** : <https://learn.microsoft.com/id-id/python/api/azureml-core/azureml.core.keyvault.keyvault?view=azure-ml-py&viewFallbackFrom=azure-ml-py%22&preserve-view=true>

* Menggunakan Rahasia Dalam Eksekusi dengan Python

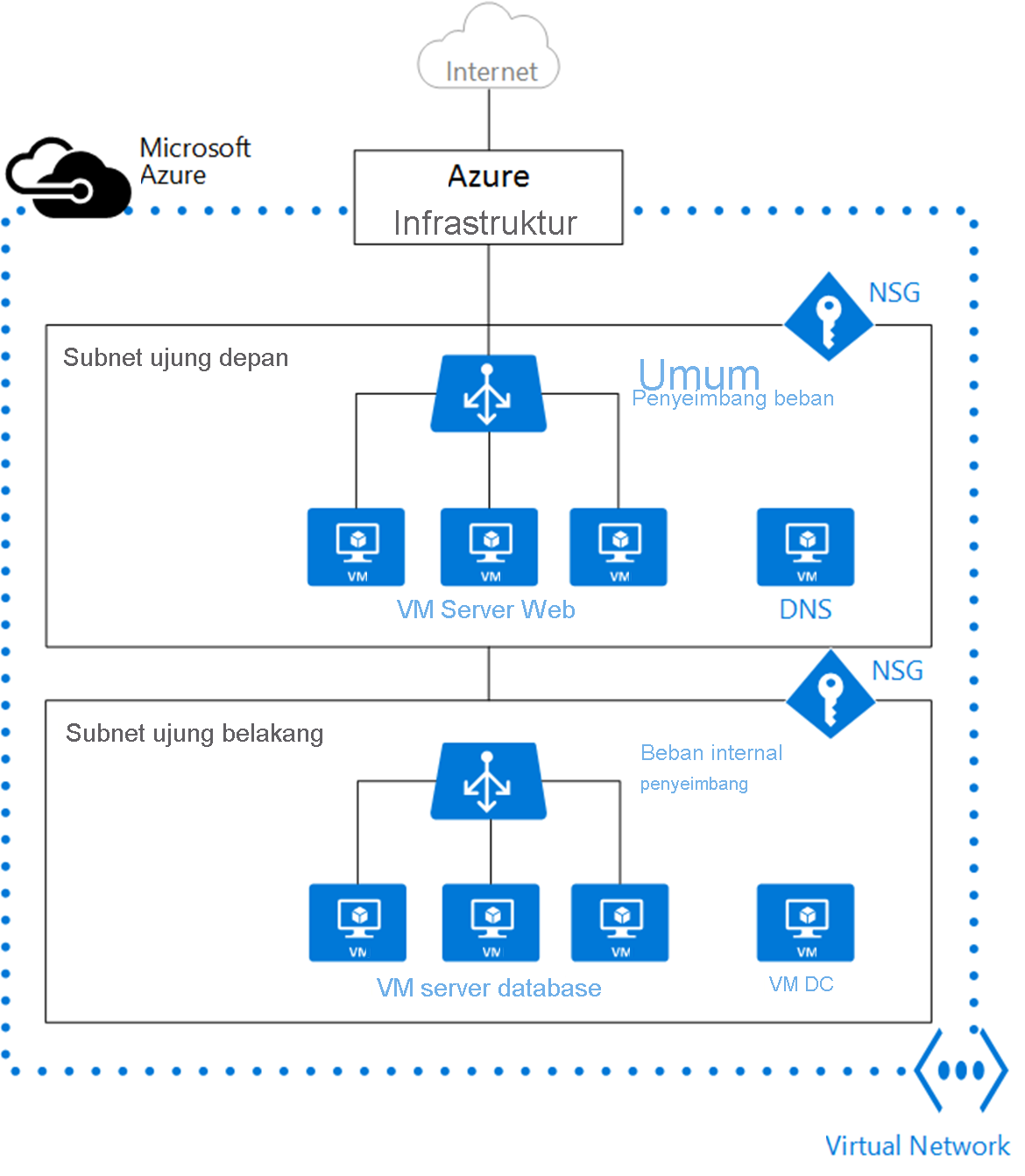
**Link** : <https://learn.microsoft.com/id-id/azure/machine-learning/how-to-use-secrets-in-runs>

**5. Mengamankan jaringan Azure Machine Learning Anda**

Sebelum Anda memulai model pelatihan, penting untuk mengamankan jaringan Azure Machine Learning Anda dari gangguan luar. Tanpa mengamankan jaringan terlebih dahulu, Anda dapat membiarkan data dan model Anda terpapar ke pelaku yang berpotensi berbahaya dan menyebabkan pencurian atau serangan data yang dapat mengubah perilaku model secara negatif. Perubahan ini sering kali sulit dikenali karena sifat kumpulan data atau parameter yang sering besar dan memengaruhi perilaku model. Kami akan mulai dengan memisahkan pelatihan model Anda dari jaringan yang lebih luas ke jaringan virtualnya sendiri untuk menghindari masalah ini.

1. **Jaringan virtual dan grup keamanan**

Untuk mengamankan ruang kerja Azure Machine Learning dan sumber daya komputasi, kami akan menggunakan jaringan virtual (VNet). Azure VNet adalah blok bangunan dasar untuk jaringan privat Anda di Azure. VNet memungkinkan sumber daya Azure, seperti Azure Blob Storage dan Azure Container Registry, untuk berkomunikasi secara aman dengan satu sama lain, dengan internet, dan dengan jaringan lokal. VNet mirip dengan jaringan tradisional yang akan Anda operasikan di pusat data Anda sendiri, tetapi membawa manfaat tambahan dari infrastruktur Azure seperti skala, ketersediaan, dan isolasi. Dengan VNet, Anda dapat meningkatkan keamanan antara sumber daya Azure dan memfilter lalu lintas jaringan untuk memastikan hanya pengguna tepercaya yang memiliki akses ke jaringan.



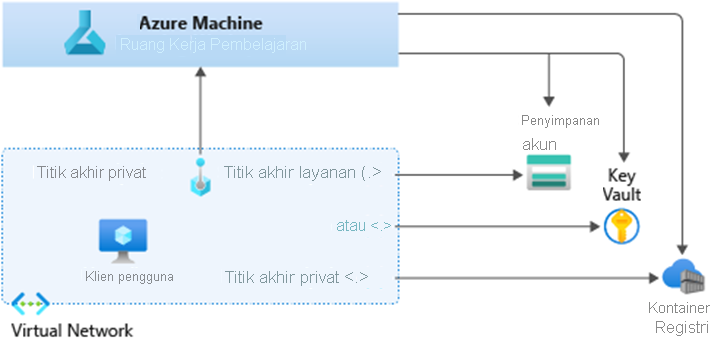
Pada gambar di atas, kita dapat melihat struktur khas untuk Virtual Network (VNet) yang terdiri dari:

* **Ruang alamat IP**: Saat membuat VNet, Anda harus menentukan ruang alamat IP privat kustom menggunakan alamat publik dan privat (RFC 1918).
* **Subnet**: Ditampilkan di atas sebagai komputer virtual (VM) terpisah, subnet memungkinkan Anda untuk mengelompokkan jaringan virtual menjadi satu atau beberapa sub-jaringan dan mengalokasikan sebagian dari ruang alamat jaringan virtual ke setiap subnet, meningkatkan keamanan dan performa.
* **Antarmuka jaringan (NIC**) adalah interkoneksi antara VM dan jaringan virtual (VNet). Saat membuat VM di portal Azure, antarmuka jaringan secara otomatis dibuat untuk Anda.
* **Grup keamanan jaringan (NSG)** dapat berisi beberapa aturan keamanan masuk dan keluar yang memungkinkan Anda memfilter lalu lintas ke dan dari sumber daya menurut alamat IP sumber dan tujuan, port, dan protokol.
* **Penyeimbang beba**n dapat dikonfigurasi untuk menangani lalu lintas masuk dan keluar ke VM dan VNet secara efisien, sekaligus menawarkan metrik untuk memantau kesehatan VM.

1. **Jalur menuju VNet**

Mengintegrasikan layanan Azure ke jaringan virtual Azure memungkinkan akses pribadi ke layanan dari mesin virtual atau sumber daya komputasi di jaringan virtual. Anda dapat mengintegrasikan layanan Azure di jaringan virtual Anda dengan opsi berikut:

* **Titik akhir layanan** memberikan identitas jaringan virtual Anda ke layanan Azure. Setelah mengaktifkan titik akhir layanan di jaringan virtual, Anda dapat menambahkan aturan jaringan virtual untuk mengamankan sumber daya layanan Azure ke jaringan virtual Anda. Titik akhir layanan menggunakan alamat IP publik.
* **Titik akhir privat** adalah antarmuka jaringan yang menghubungkan Anda dengan aman ke layanan yang didukung oleh Azure Private Link. Titik akhir privat menggunakan alamat IP privat dari VNet Anda, secara efektif membawa layanan Azure ke VNet Anda.



Anda dapat menyambungkan komputer dan jaringan lokal Anda ke VNet melalui jaringan privat maya (VPN) dengan beberapa cara. **VPN titik-ke-situs** adalah sambungan antara jaringan virtual dan komputer tunggal di jaringan Anda. Komunikasi dikirim dengan terowongan terenkripsi melalui internet. Setiap komputer yang ingin membuat konektivitas dengan VNet harus mengonfigurasi koneksinya, jadi sebaiknya digunakan jika Anda hanya memiliki beberapa pengguna yang perlu tersambung ke VNet. Jenis koneksi ini sangat bagus jika Anda baru memulai karena memerlukan sedikit atau tidak ada perubahan pada jaringan yang ada.

Meskipun **VPN Situs-ke-situs** dapat dibuat antara perangkat VPN lokal dan Azure VPN Gateway yang disebarkan di jaringan virtual. Tipe sambungan ini memungkinkan sumber daya lokal mana pun yang Anda otorisasi untuk mengakses jaringan virtual. Komunikasi antara perangkat VPN lokal Anda dan gateway VPN Azure dikirim melalui terowongan terenkripsi melalui internet.

**ExpressRoute** dapat digunakan sebagai pengganti VPN jika Anda ingin mempercepat pembuatan koneksi privat ke layanan Azure. Layanan ini memungkinkan Anda membuat koneksi privat antara pusat data Microsoft dan infrastruktur di lokal Anda atau di fasilitas lain. Koneksi ExpressRoute terpisah dari internet publik dan menawarkan keamanan, keandalan, dan kecepatan tinggi dengan latensi lebih rendah daripada koneksi biasa melalui internet. ExpressRoute memiliki berbagai pilihan harga tergantung pada perkiraan kebutuhan bandwidth Anda.

1. **Mengamankan ruang kerja dan sumber daya**

Untuk mulai mengamankan jaringan Anda, Anda harus tersambung ke ruang kerja Anda melalui titik akhir privat (IP privat), yang akan kita bahas dalam latihan berikutnya. Titik akhir privat dapat ditambahkan ke ruang kerja melalui Azure Machine Learning Python SDK, Azure CLI, atau dalam tab Jaringan portal Azure. Dari sana, Anda kemudian dapat membatasi akses ke ruang kerja Anda hanya terjadi melalui alamat IP privat.

Namun, ini saja tidak akan memastikan keamanan ujung-ke-ujung dengan sendirinya, jadi pastikan layanan Azure lain yang Anda ajak berkomunikasi juga berada di belakang VNet. Karena komunikasi ke ruang kerja kemudian diatur agar hanya diizinkan dari VNet, lingkungan pengembangan apa pun yang menggunakan ruang kerja harus menjadi anggota VNet kecuali Anda telah mengonfigurasi jaringan untuk mengizinkan koneksi IP publik.

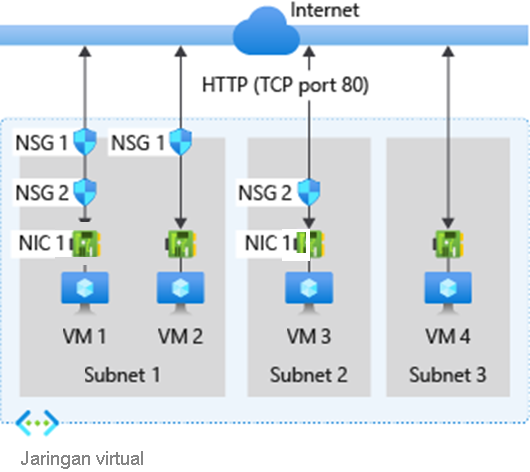
Metode berikut dapat digunakan untuk menyambung ke ruang kerja aman:

* **Gateway VPN Azure** - Menghubungkan jaringan lokal ke VNet melalui koneksi privat. Koneksi dibuat melalui internet publik. Ada dua jenis gateway VPN yang mungkin Anda gunakan:
  + Titik-ke-situs: Setiap komputer klien menggunakan klien VPN untuk tersambung ke VNet.
  + Situs-ke-situs: Perangkat VPN menyambungkan VNet ke jaringan lokal Anda.
* **ExpressRoute** - Menyambungkan jaringan lokal ke cloud melalui koneksi privat. Koneksi dibuat menggunakan penyedia konektivitas.
* **Azure Bastion** - Dalam skenario ini, Anda membuat Azure Virtual Machine (kadang-kadang disebut jump box) di dalam VNet. Lalu Anda menghubungkan ke VM menggunakan Azure Bastion. Bastion memungkinkan Anda untuk terhubung ke VM menggunakan sesi RDP atau SSH dari browser web lokal Anda. Anda kemudian menggunakan jump box sebagai lingkungan pengembangan Anda. Karena berada di dalam VNet, jump box dapat langsung mengakses ruang kerja.

1. **Grup keamanan dan lalu lintas**

Anda dapat menggunakan grup keamanan jaringan (NSG) Azure untuk memfilter lalu lintas jaringan ke dan dari sumber daya Azure di jaringan virtual Azure. Kelompok keamanan jaringan berisi aturan keamanan yang memungkinkan atau menolak lalu lintas jaringan masuk ke, atau, lalu lintas jaringan keluar dari, beberapa jenis sumber daya Azure. NSG berguna untuk mengontrol arus lalu lintas antara subnet VM atau membatasi komunikasi keluar oleh sumber daya dalam Azure VNet ke internet, yang diaktifkan secara default.

Gambar berikut ini mengilustrasikan skenario yang berbeda tentang bagaimana kelompok keamanan jaringan dapat disebarkan untuk memungkinkan lalu lintas jaringan ke dan dari internet melalui port TCP 80:

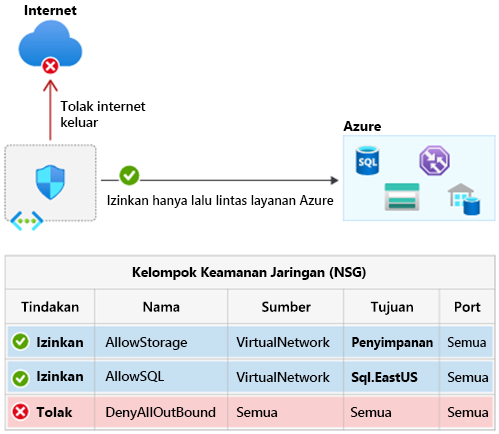


Grup keamanan aplikasi (ASG) juga dapat digunakan untuk mengonfigurasi keamanan jaringan sebagai ekstensi alami dari struktur aplikasi, mengizinkan Anda untuk mengelompokkan komputer virtual dan menentukan kebijakan keamanan jaringan berdasarkan grup tersebut. Anda dapat menggunakan kembali kebijakan keamanan Anda dengan skala tanpa pemeliharaan manual alamat IP eksplisit. Platform menangani kompleksitas alamat IP eksplisit dan beberapa set aturan, sangat menyederhanakan proses definisi aturan NSG.

1. **Tag layanan**

Tag layanan mewakili sekelompok awalan alamat IP dari layanan Azure tertentu. Microsoft mengelola awalan alamat yang di mencakup tag layanan dan secara otomatis memperbarui tag layanan saat alamat berubah, meminimalkan kompleksitas pembaruan yang sering terjadi pada aturan keamanan jaringan.

Anda dapat menggunakan tag layanan sebagai pengganti alamat IP tertentu saat Anda membuat aturan keamanan untuk menentukan kontrol akses jaringan pada grup keamanan jaringan atau Azure Firewall. Dengan menentukan nama tag layanan, misalnya ApiManagement di bidang sumber atau tujuan yang sesuai dari suatu aturan, Anda dapat mengizinkan atau menolak lalu lintas untuk layanan yang sesuai.



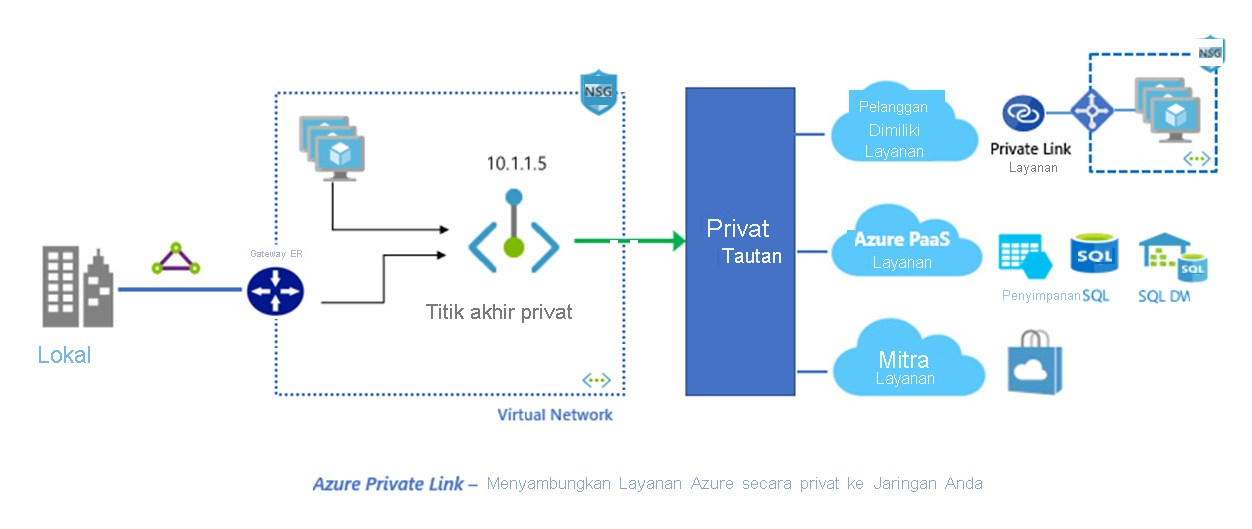
1. **Titik akhir privat & Private Link**

Ruang kerja Azure Machine Learning dapat menggunakan Azure Private Link untuk membuat titik akhir privat di balik VNet. Azure Private Link adalah teknologi yang dirancang untuk menyediakan konektivitas ke layanan PaaS tertentu. Ini menyediakan himpunan alamat IP privat yang dapat digunakan untuk mengakses ruang kerja dari dalam VNet. Beberapa layanan yang diandalkan Azure Machine Learning juga dapat menggunakan Azure Private Link, tetapi beberapa mengandalkan grup keamanan jaringan atau perutean yang ditentukan pengguna.

Ada dua komponen utama Azure Private Link:

* **Titik akhir privat** – antarmuka jaringan yang tersambung ke jaringan virtual Anda, yang ditetapkan dengan alamat IP privat. Ini digunakan untuk tersambung secara privat dan aman ke layanan yang didukung oleh Azure Private Link atau Layanan Tautan Privat yang mungkin Anda atau mitra miliki.
* **Layanan Private Link** – layanan Anda sendiri, didukung oleh Azure Private Link yang berjalan di belakang Penyeimbang Beban Standar Azure, diaktifkan untuk akses Private Link. Layanan ini dapat disambungkan secara privat dan digunakan menggunakan Titik Akhir Privat yang disebarkan di jaringan virtual pengguna.

Saat Anda membuat titik akhir privat untuk sumber daya Azure, konektivitas yang aman antara klien di jaringan virtual dan sumber daya Azure Anda akan dibuat. Anda dapat menggunakan titik akhir privat untuk berkomunikasi dan memasukkan peristiwa langsung dari jaringan virtual ke sumber daya Azure dengan aman melalui tautan privat tanpa melalui internet publik, sehingga meningkatkan keamanan. Titik akhir privat diberi alamat IP dari rentang alamat IP jaringan virtual Anda. Layanan ini fleksibel, memungkinkan koneksi antara VNet dengan ruang alamat yang tumpang tindih dan menyambungkan sumber daya yang berjalan di wilayah lain, menawarkan jangkauan global.



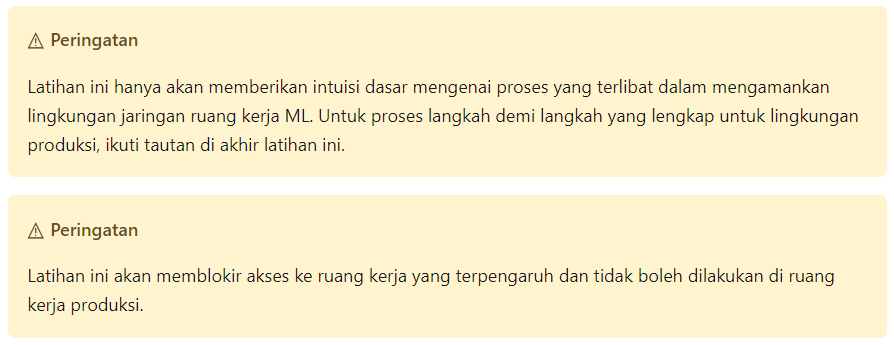
1. **Latihan - Menyiapkan Azure Virtual Network yang aman**

Azure Virtual Network (VNet) : ( <https://learn.microsoft.com/id-id/azure/virtual-network/virtual-networks-overview> ) mirip dengan jaringan tradisional tetapi dengan manfaat tambahan yang disediakan oleh infrastruktur Azure.

VNet memungkinkan sumber daya, seperti komputer virtual (VM) dan ruang kerja ML, untuk berkomunikasi dengan aman satu sama lain dan jaringan lain atau internet.

Seorang teknisi Machine Learning dapat menggunakannya dalam berbagai skenario, seperti menautkan VM ke data yang disimpan secara lokal, membatasi akses ke API pelatihan sehingga hanya personel dari lab mereka yang dapat melihatnya, atau mengekspos titik akhir inferensi ke internet.

Dalam latihan ini, kita akan membuat VNet dan menggunakannya untuk mengamankan akses ke ruang kerja yang kita buat di latihan sebelumnya. Meskipun latihan ini memberikan intuisi tentang mekanisme mengamankan ruang kerja, ini bukanlah solusi yang lengkap. Lihat dokumentasi yang ditautkan di akhir latihan untuk instruksi lengkap.



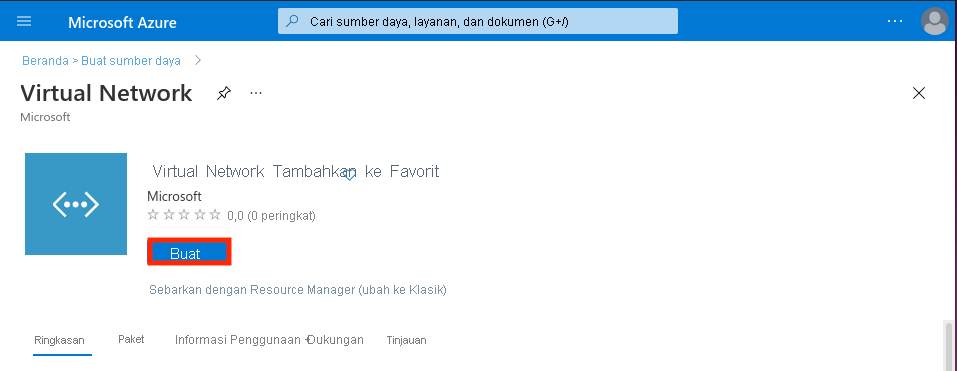
1. **Prasyarat**

* Pengetahuan dasar konsep jaringan.
* Akun dan langganan Azure.
* Grup sumber daya Ruang Kerja Azure Machine Learning seperti yang dibuat dalam latihan sebelumnya.

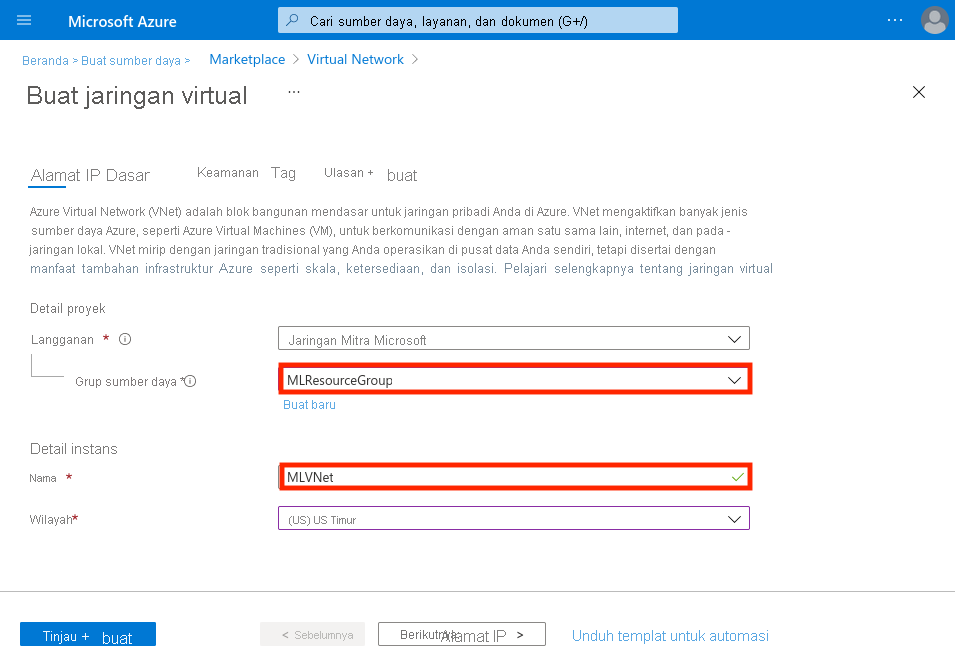
1. **Masuk ke Azure**

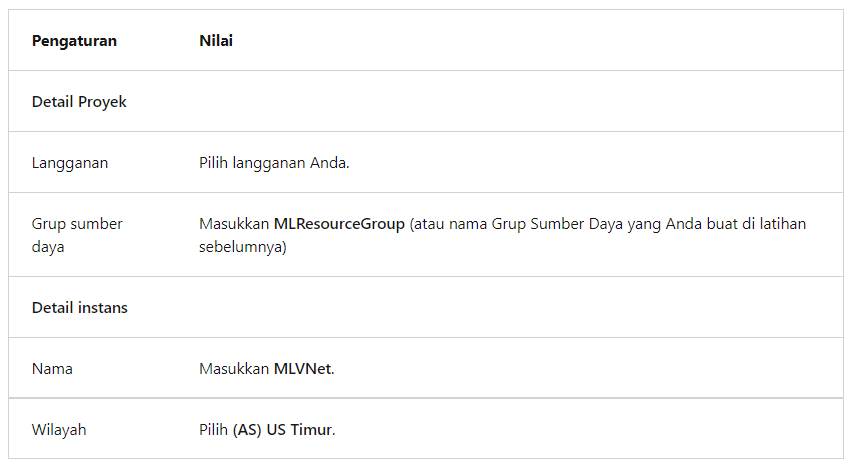
* Masuk ke portal Azure.

1. **Buat VNet**
2. Di portal Azure, Pilih **Buat sumber daya** di sudut kiri atas portal.
3. Pada kotak pencarian, masukkan **Jaringan Virtual.** Pilih **Jaringan Virtual** dalam hasil pencarian.
4. Pada halaman **Jaringan Virtua**l, pilih **Buat**.

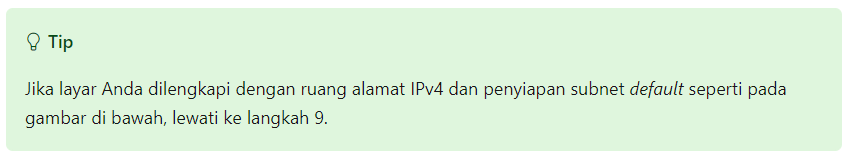


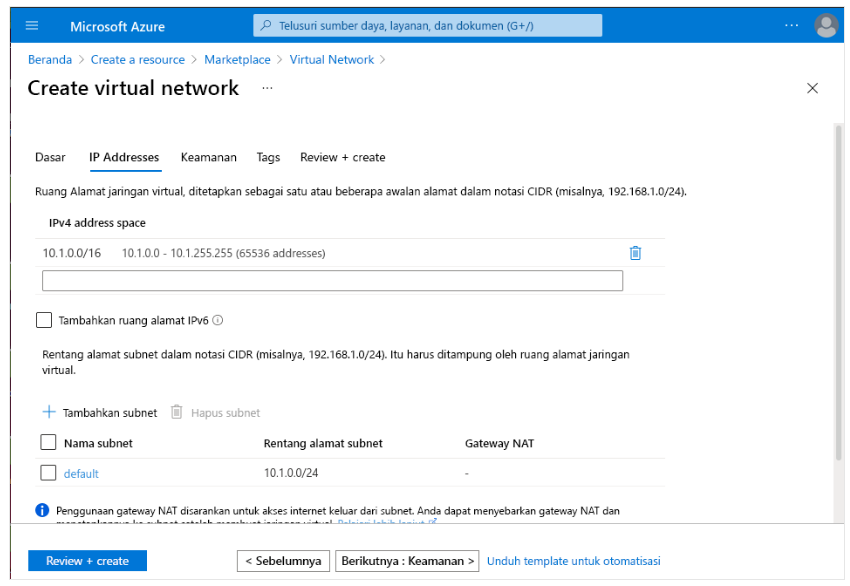
1. Di **Buat jaringan virtual,** masukkan atau pilih informasi ini di tab **Dasar**:



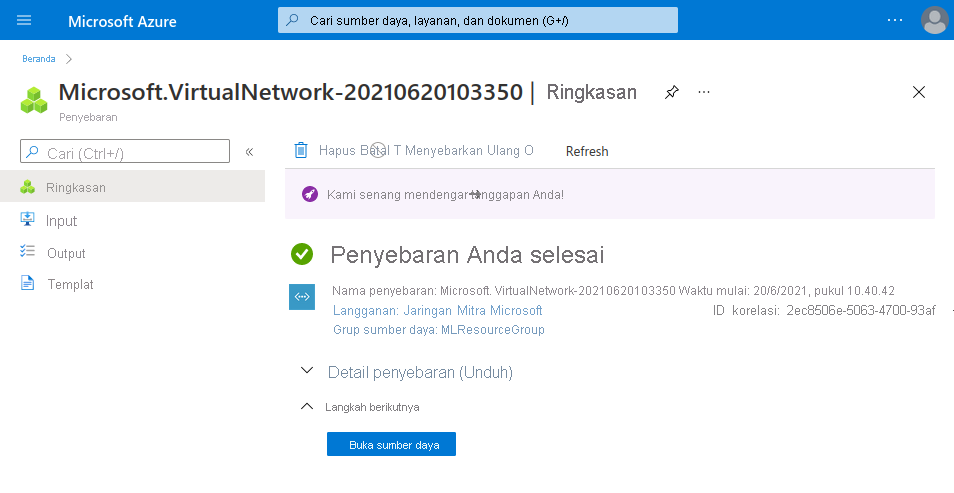


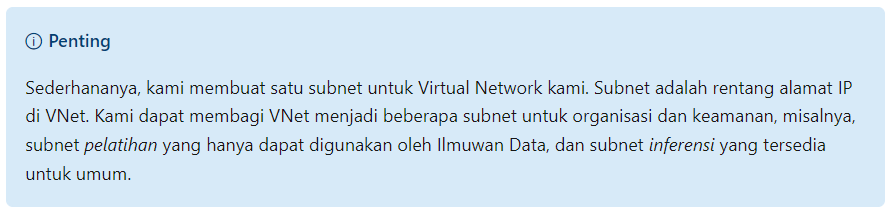
1. Pilih tab **Alamat IP** atau pilih tombol **Berikutnya: Alamat IP** di bagian bawah halaman.





1. Di **ruang alamat IPv4**, pilih ruang alamat yang tersedia dan ubah menjadi **10.1.0.0/16.**
2. Pilih **+ Tambahkan subnet,** lalu masukkan **default** untuk **Nama subnet** dan **10.1.0.0/24** untuk **Rentang alamat subnet.**
3. Pilih **Tambahkan**.
4. Pilih tab **Tinjau + buat** atau pilih tombol **Tinjau + buat.**
5. Pilih **Buat** dan tunggu beberapa saat hingga penerapan selesai:

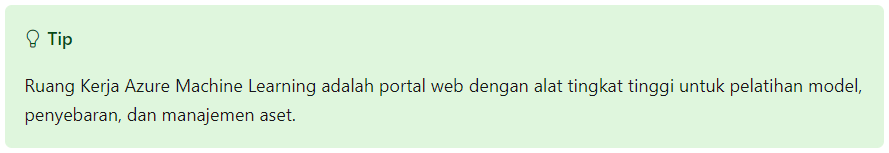




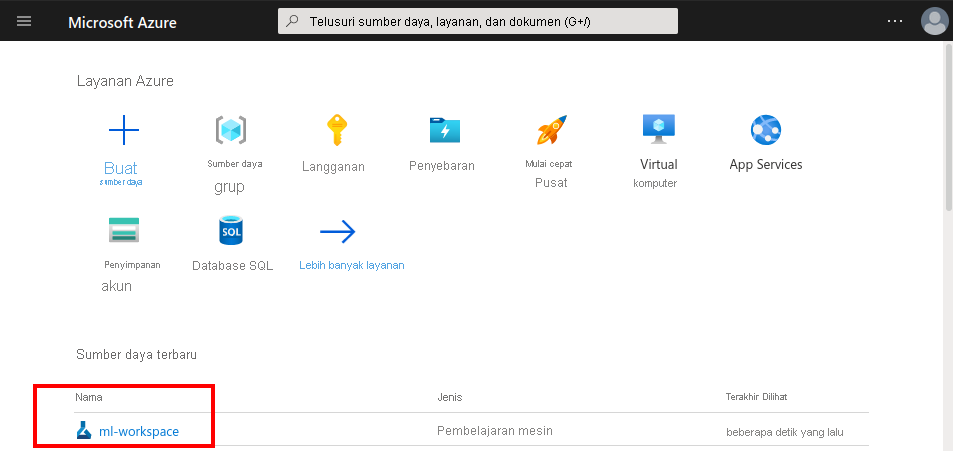
1. **Menguji akses ruang kerja**

Kami baru saja menambahkan VNet ke grup sumber daya kami, tetapi apakah itu membatasi akses ke **ml-workspace** kami?

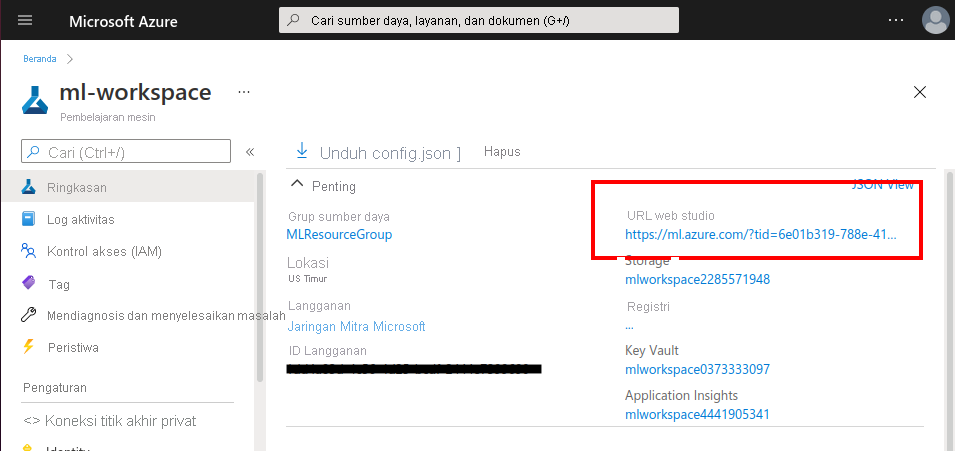
Kami dapat mengujinya menggunakan Azure Machine Learning Studio ( <https://learn.microsoft.com/id-id/azure/machine-learning/overview-what-is-azure-machine-learning#studio> ) untuk mengakses konten ruang kerja.



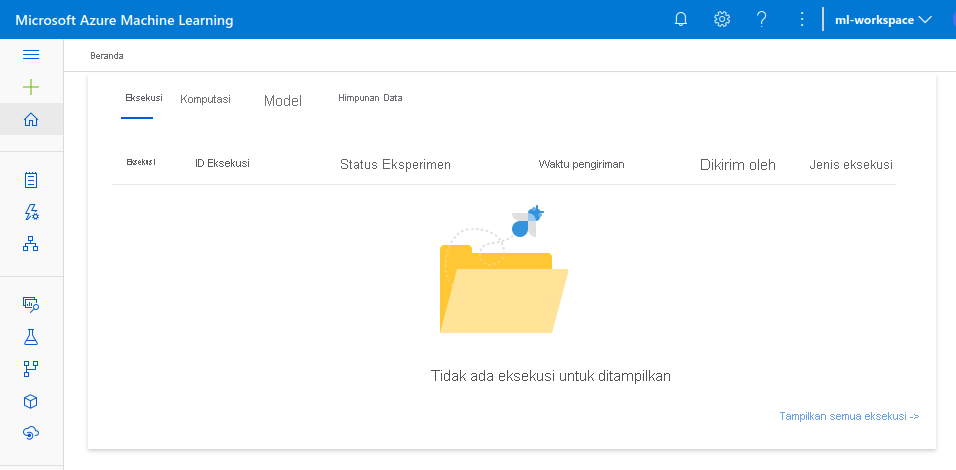
1. Pilih **Beranda** untuk kembali ke beranda
2. Pilih **ml-workspace** pada daftar sumber daya terbaru:



1. Pilih **URL web Studio** untuk ruang kerja Anda:



1. Azure Machine Learning Studio akan terbuka di tab atau jendela baru. Gulir ke bawah hingga Anda dapat melihat tab di bawah (Jalankan, Komputasi, Model, dan Himpunan Data):



Setiap tab di atas mewakili "folder" yang menyimpan sumber daya yang akan Anda dan tim Anda gunakan dalam Machine Learning.

Meskipun Anda mungkin belum memiliki objek apa pun di sana, seperti pada gambar di atas, seharusnya tidak ada peringatan atau pesan kesalahan, artinya belum ada pembatasan akses jaringan pada sumber daya tersebut.

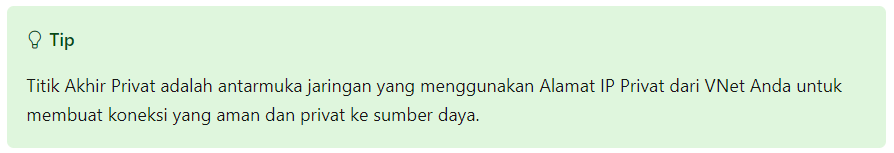
1. **Akses jaringan yang aman ke Ruang Kerja ML**

Sejauh ini kami telah membuat dua sumber daya independen:

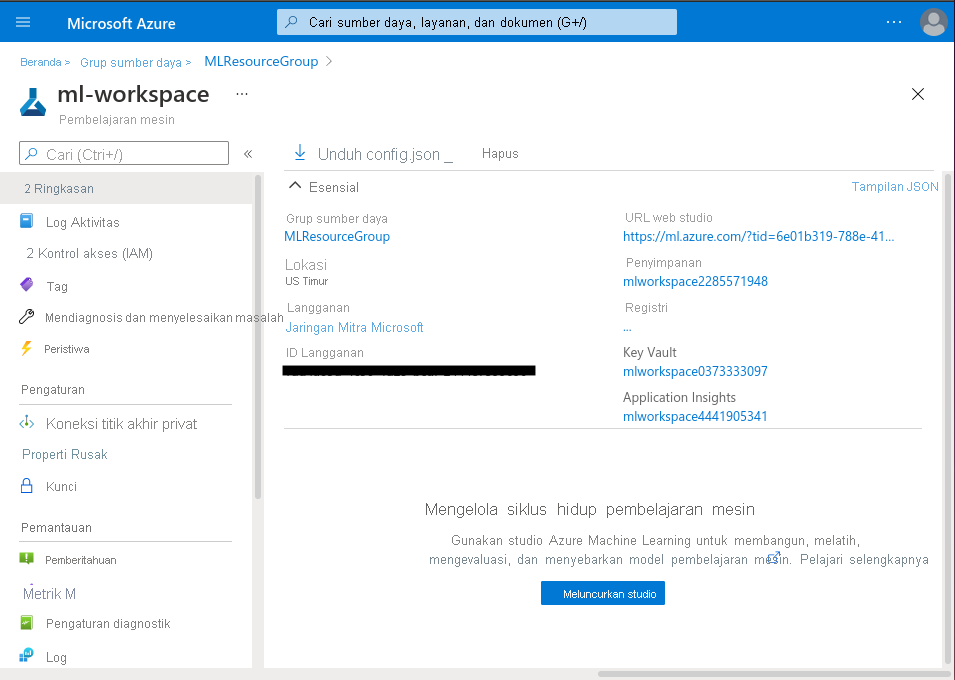
* Ruang kerja ML **(ml-workspace)**
* VNe**t (MLVNet)**

Kami sekarang harus menyambungkan keduanya sehingga lalu lintas jaringan ruang kerja harus melalui VNet kami. Dengan kata lain, kami ingin ruang kerja kami **hanya**tersedia untuk sumber daya yang tersambung ke jaringan virtual **MLVNet**.

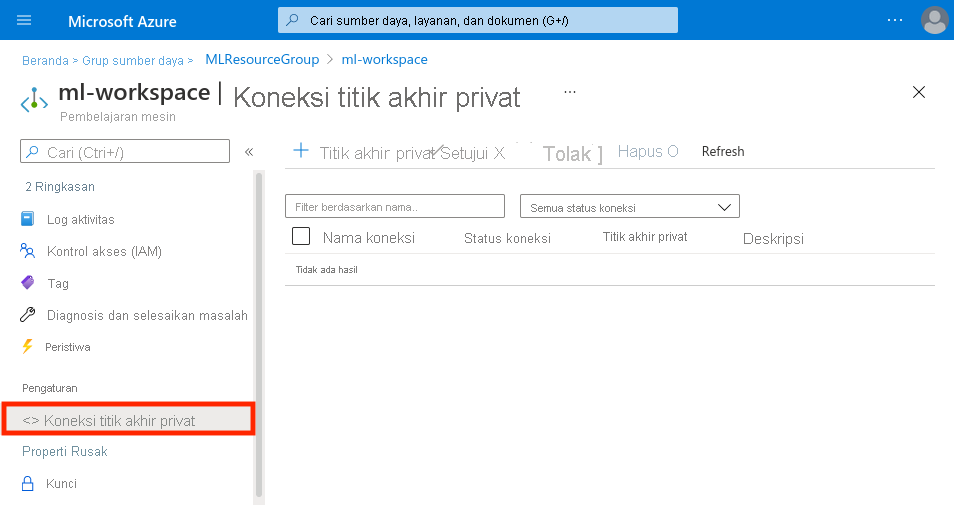
Untuk menyempurnakannya, kita perlu menentukan**[Titik Akhir Privat](https://learn.microsoft.com/id-id/azure/private-link/private-endpoint-overview)**  ( <https://learn.microsoft.com/id-id/azure/private-link/private-endpoint-overview> ) untuk sumber daya ml-workspace.



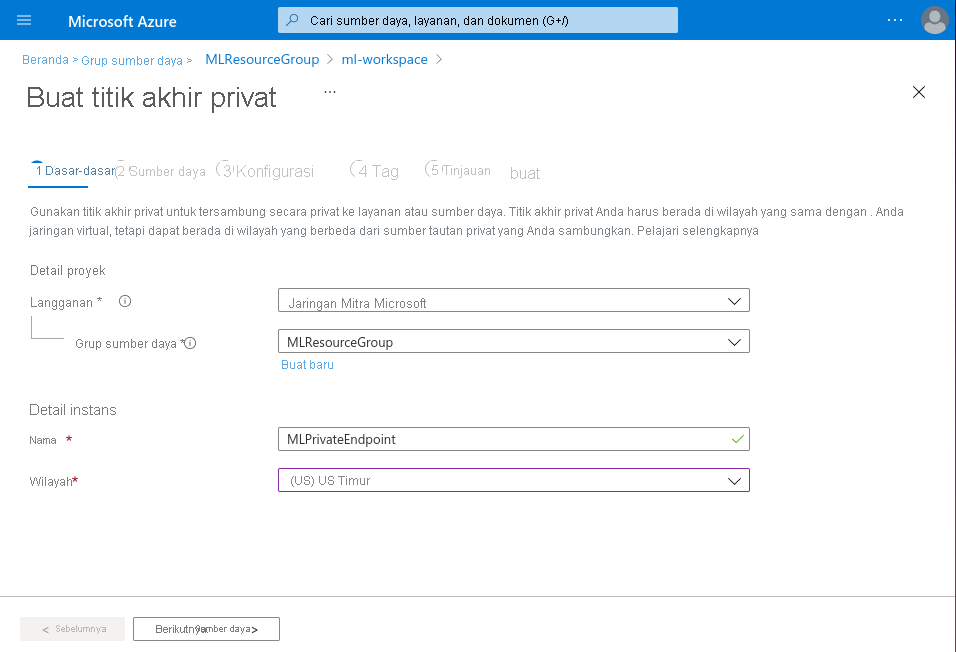
1. **Membuat Titik Akhir Privat**
2. Buka "Beranda", pilih **Grup Sumber Daya**, pilih grup sumber daya **MLResourceGroup**, lalu pilih ruang kerja **ml\_workspace** Anda:



1. Di menu sebelah kiri, pilih **Koneksi titik akhir privat:**

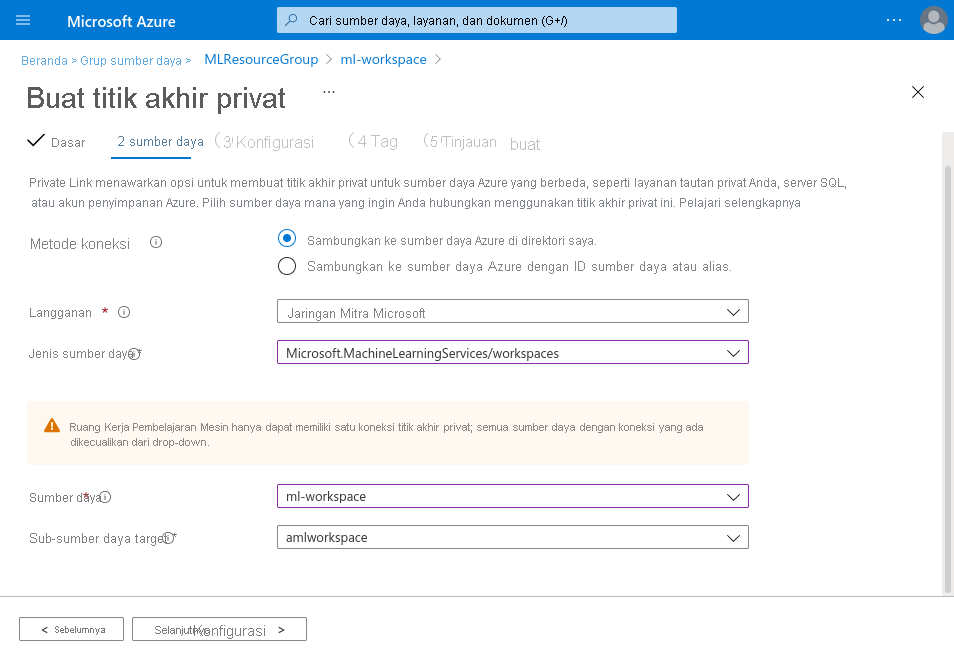


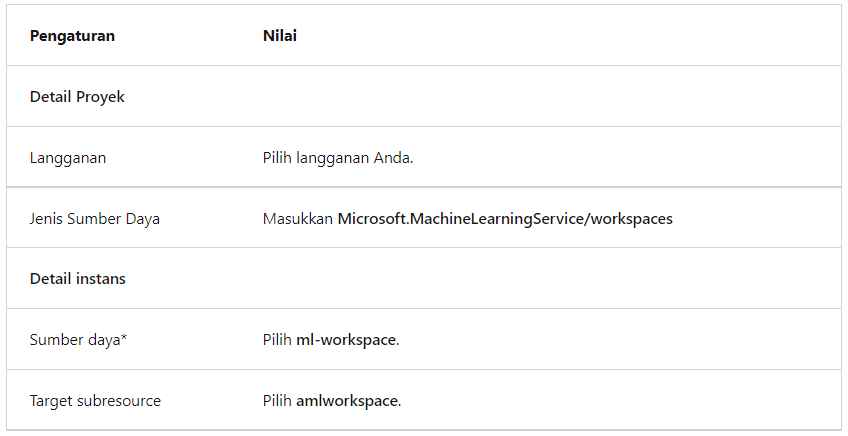
1. Pilih **Titik Akhir Privat** dan isi formulir dengan nilai berikut:





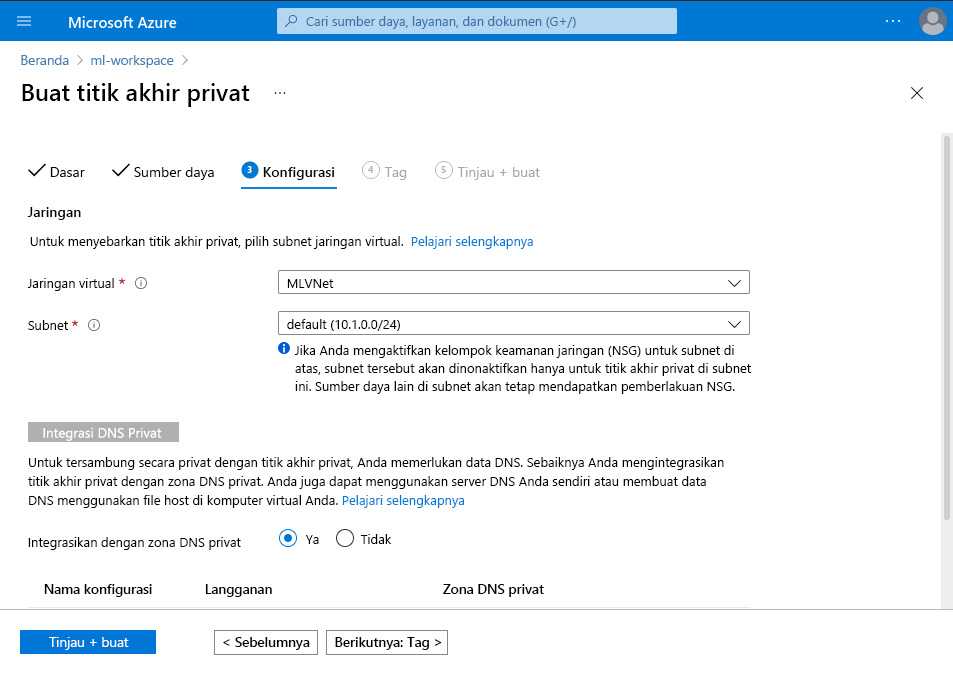
1. Pilih tombol **Berikutnya: Sumber Daya** >.
2. Di tab **Sumber Daya**, gunakan nilai di bawah





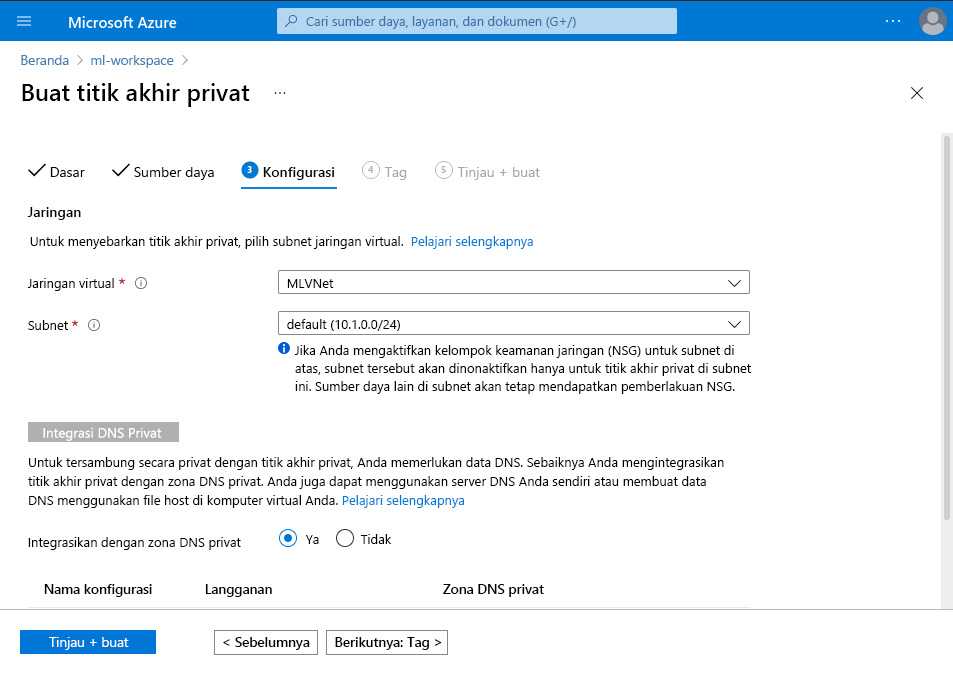
1. Pilih tombol **Berikutnya: Konfigurasi >**.

* Biarkan default yang disarankan:





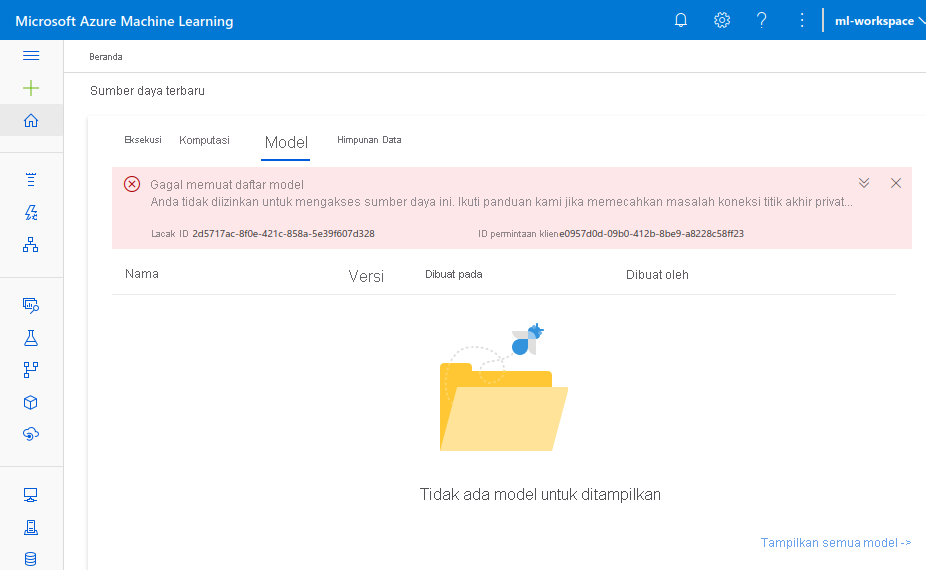
1. Pilih **Tinjau + Buat** untuk memvalidasi penyebaran, lalu pilih **Buat** untuk menyebarkan titik akhir (ini bisa memakan waktu beberapa saat):



1. **Menguji konfigurasi jaringan**

Kami dapat memastikan ruang kerja kami ada di dalam VNet sekarang dengan menguji apakah kami masih memiliki akses ke sumber dayanya:

1. Muat ulang jendela Azure Machine Learning Studio (atau buka Studio kembali):



1. Seperti yang ditunjukkan peringatan, akses ke sumber daya tersebut sedang diblokir. Itu terjadi karena ruang kerja Anda sekarang berada di dalam VNet, dan dikonfigurasi untuk memblokir semua permintaan yang tidak berasal dari dalam subnet default yang kami buat (ingat kami mencoba mengaksesnya dari **luar** perimeter jaringan).
2. **Diamankan tetapi tidak dapat diakses**

Anda baru saja mengamankan akses jaringan ke ruang kerja ML Anda.

Perhatikan bahwa dengan cara yang sama Anda tidak dapat mengaksesnya, begitu juga sumber daya lain di organisasi Anda yang bukan bagian dari subnet.

Membuka segalanya sehingga sumber daya dapat tersambung memerlukan beberapa perencanaan strategis!

Dianjurkan membaca panduan **cara mengamankan ruang kerja menggunakan vnet** ( <https://learn.microsoft.com/id-id/azure/machine-learning/how-to-secure-workspace-vnet?tabs=pe%2Ccli> )kami untuk referensi yang lebih mendalam.

1. **Ringkasan**

Di unit ini Anda telah membahas topik berikut:

* Apa yang dimaksud Virtual Network dan beberapa kegunaannya
* Membuat Azure Virtual Network
* Membuat subnet di Virtual Network
* Cara menggunakan Titik Akhir Privat untuk mengamankan akses jaringan ke ruang kerja Machine Learning Anda
* Mengakses ruang kerja menggunakan Azure Machine Learning Studio dan memeriksa apakah sumber daya diblokir

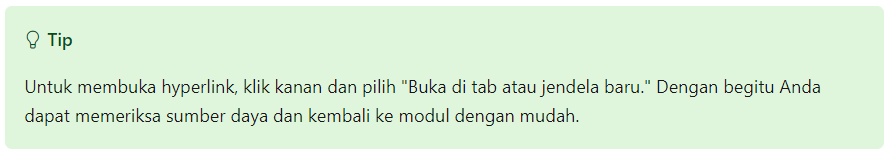
**8. Ringkasan**

Dalam modul ini, Anda mempelajari tentang beberapa alat yang disediakan Azure Machine Learning untuk mengamankan data dan lingkungan pelatihan Anda.

Setelah Anda melihat modul ini, Anda seharusnya dapat:

* Menerapkan dan memahami Kontrol Akses Berbasis Peran dalam Azure Machine Learning
* Menjelaskan bagaimana rahasia dikelola di Azure Machine Learning
* Letakkan ruang kerja Azure Machine Learning di Azure Virtual Network

1. **Menggunakan sumber daya ini untuk menemukan lebih banyak**



* Dokumentasi kontrol akses berbasis peran Azure Machine Learning

**Link** : <https://learn.microsoft.com/id-id/azure/role-based-access-control/>

* Apa itu Azure Virtual Network?

**Link** : <https://learn.microsoft.com/id-id/azure/virtual-network/virtual-networks-overview>

* Konsep dan praktik terbaik Azure Virtual Network

**Link** : <https://learn.microsoft.com/id-id/azure/virtual-network/concepts-and-best-practices>

* Sumber daya ruang kerja Azure Machine Learning yang aman menggunakan jaringan virtual (VNets)

**Link** : <https://learn.microsoft.com/id-id/azure/machine-learning/how-to-network-security-overview>

* Apakah itu Titik Akhir Privat Azure?

**Link** : <https://learn.microsoft.com/id-id/azure/private-link/private-endpoint-overview>