

17 - Crearea unei politici Azure (10 min)

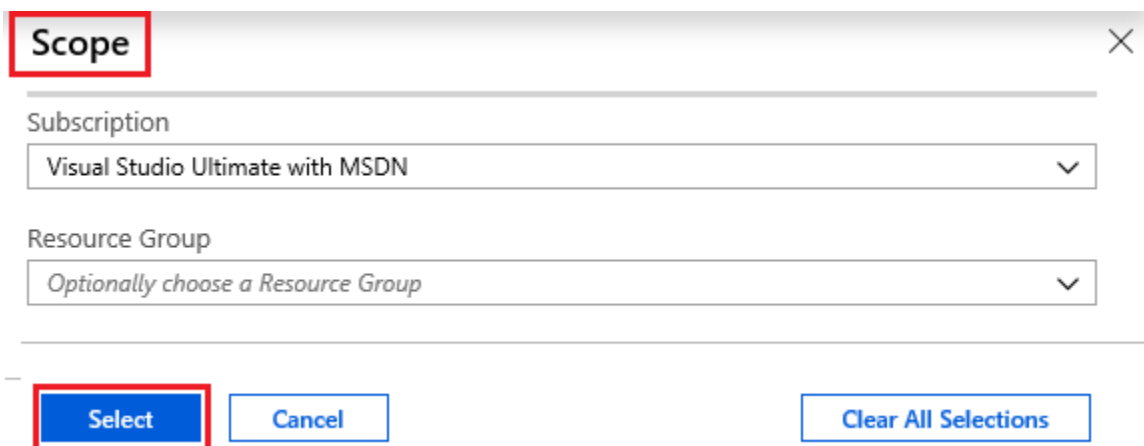
În această demonstrație, vom crea o politică Azure pentru a restricționa implementarea resurselor Azure într-o anumită locație.

Sarcina 1: Creați o atribuire de politică

În această sarcină, vom configura politica de locație permisă și o vom atribui abonamentului nostru.

1. Conectați-vă la [portalul Azure](#) .
2. Din lama **Toate serviciile** , căutați și selectați **Politică** , apoi, în secțiunea **Creare** , faceți clic pe **Definiții** . Acordați-vă un moment pentru a examina lista de definiții de politici încorporate. De exemplu, în meniul derulant **Categorie** , **selectați doar Calcul** . Observați că definiția **SKU-uri pentru dimensiunile permise ale mașinilor virtuale** vă permite să specificați un set de SKU-uri pentru mașini virtuale pe care organizația dvs. le poate implementa.
3. Reveniți la pagina **Politică** , în secțiunea **Creare** , **faceți clic pe Atribuiți** . O atribuire este o politică care a fost atribuită să aibă loc într-un anumit domeniu de aplicare. De exemplu, o definiție ar putea fi atribuită domeniului de aplicare al abonamentului.
4. Faceți clic **pe Atribuire politică** în partea de sus a paginii **Politică - Atribuiți** .
5. Pe pagina **Atribuire politică** , păstrați Domeniul de aplicare implicit.

Setare	Valoare
Domeniu de aplicare	Folosește selecția implicită
Definiția politicii	Faceți clic pe punctele de suspensie, apoi căutați Locații permise , apoi Selectați
Numele sarcinii	Locații permise



Scope [X]

Subscription
Visual Studio Ultimate with MSDN [v]

Resource Group
Optionally choose a Resource Group [v]

Select Cancel Clear All Selections

6.

7. În fila **Parametri** , selectați **Japan West** . Faceți clic pe **Revizuire + creare** , apoi pe **Creare** .

Notă : Un domeniu de aplicare determină resursele sau grupările de resurse cărora li se aplică politica atribuită. În cazul nostru, am putea atribui această politică unui anumit grup de resurse, însă am ales să atribuim politica la nivel de abonament. Rețineți că resursele pot fi excluse pe baza configurației domeniului de aplicare. Excluderile sunt opționale.

Notă : Această definiție a politicii **Locații permise** va specifica o locație în care trebuie implementate toate resursele. Dacă se alege o altă locație, implementarea nu va fi permisă. Pentru mai multe informații, consultați pagina [Exemple de politici Azure](#) .

Available Definitions



Type

All types

Search

location

Policy Definitions (3)

Audit resource location matches resource group location

Built-in

Audit that the resource location matches its resource group location

Allowed locations

Built-in

This policy enables you to restrict the locations your organization can specify when deploying resources. Use to enforce your geo-compliance requirements. Excludes resource groups, Microsoft.AzureActiveDirectory/b2cDirectories, and resources that use the 'global' region.

Allowed locations for resource groups

Built-in

This policy enables you to restrict the locations your organization can create resource groups in. Use to enforce your geo-compliance requirements.

Select

Cancel

8. Atribuirea politicii **Locații permise** este acum listată în panoul **Politică - Atribuirii** și este acum implementată, aplicând politica la nivelul de domeniu specificat (nivel de abonament).

Sarcina 2: Testarea politicii privind locațiile permise

În această sarcină, vom testa politica privind locațiile permise.

1. În Azure Portal, din lama **Toate serviciile**, căutați și selectați **Conturi de stocare**, apoi faceți clic pe **+ Creare**.
2. Configurați contul de stocare (înlocuiți **xxxx** în numele contului de stocare cu litere și cifre astfel încât numele să fie unic la nivel global). Păstrați valorile implicite pentru orice altceva.

Setare	Valoare
Abonament	Folosește valoarea implicită furnizată

Setare	Valoare
Grup de resurse	myRGPolicy (creează nou)
Numele contului de stocare	cont de stocarexxxx
Locație	(SUA) Estul SUA

3. Faceți clic pe **Revizuire + creare** , apoi pe **Creare** .
4. Veți primi eroarea **de implementare eşuată** care indică faptul că resursa a fost interzisă de politică, inclusiv numele politicii **Locații permise** .

Sarcina 3: Ștergerea atribuirii politicii

În această sarcină, vom elimina atribuirea politicii de locație permisă și vom testa.

Vom șterge atribuirea politicii pentru a ne asigura că nu vom fi blocați în nicio activitate viitoare pe care dorim să o desfășurăm.

1. Din lama **Toate serviciile** , căutați și selectați **Politică** , apoi faceți clic pe politica **Locații permise** .


Notă : În panoul **Politică** , puteți vizualiza starea de conformitate a diferitelor politici pe care le-ați atribuit.


Notă : Politica privind locațiile permise poate afișa resurse neconforme. Dacă da, acestea sunt resurse create înainte de atribuirea politicii.


2. Faceți clic pe **Locații permise**. Se va deschide o fereastră de conformitate cu politica privind locațiile permise.
3. Faceți clic **pe Ștergeți atribuirea** în meniul superior. Confirmați că doriți să ștergeți atribuirea politicii făcând clic pe **Da**.

Allowed locations

Policy compliance

 View definition

 Edit assignment

 Delete assignment

 Create Remediation Task

Compliance state ⓘ



Non-compliant

Overall resource compliance ⓘ

0%

0 out of 26

Non-compliant resources ⓘ

26

out of 26

 srv-jump	resourcegroups/myrgfw	 Non-compliant
 srv-work	resourcegroups/myrgfw	 Non-compliant
 mypsvm	resourcegroups/mypsvm	 Non-compliant
 akvtest113	resourcegroups/myrgkv	 Non-compliant
 test-fw-vn	resourcegroups/myrgfw	 Non-compliant
 cs4aa509d922cc7x4eb9x9ae	resourcegroups/cloud-shell-storage-westus	 Non-compliant

- Încercați să creați un alt cont de stocare pentru a vă asigura că politica nu mai este în vigoare.

Notă : Printre scenariile comune în care politica **Locații permise** poate fi utilă se numără:

- *Urmărirea costurilor :* Este posibil să aveți abonamente diferite pentru locații regionale diferite. Politica va asigura că toate resursele sunt implementate în regiunea dorită pentru a facilita urmărirea costurilor.
- *Rezidența datelor și conformitatea cu securitatea :* De asemenea, puteți avea cerințe de rezidență a datelor și puteți crea abonamente per client sau sarcini de lucru specifice și puteți defini faptul că toate resursele trebuie implementate într-un anumit centru de date pentru a asigura cerințele de conformitate cu datele și securitatea.

Felicitări! Ați creat o politică Azure pentru a restricționa implementarea resurselor Azure la un anumit centru de date.

Notă : Pentru a evita costuri suplimentare, puteți elimina opțional acest grup de resurse. Căutați grupuri de resurse, faceți clic pe grupul dvs. de resurse, apoi faceți clic pe **Ștergeți grupul de resurse** . Verificați numele grupului de resurse, apoi faceți clic pe **Ștergeți** . Monitorizați **notificările** pentru a vedea cum se desfășoară ștergerea.