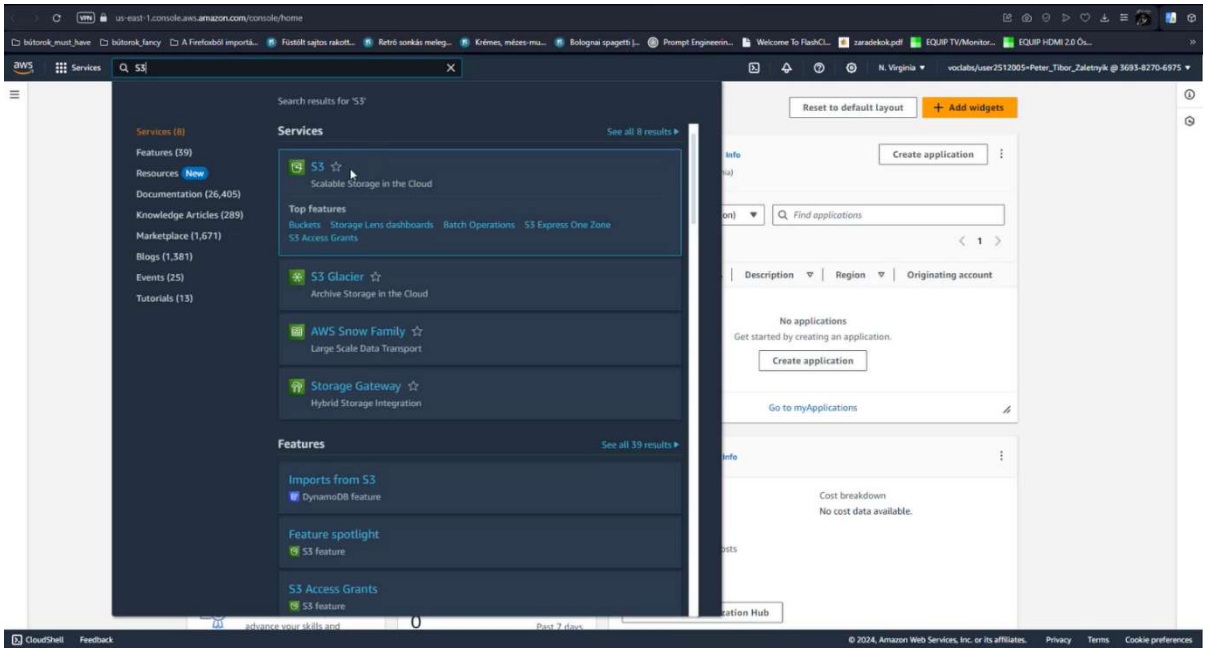
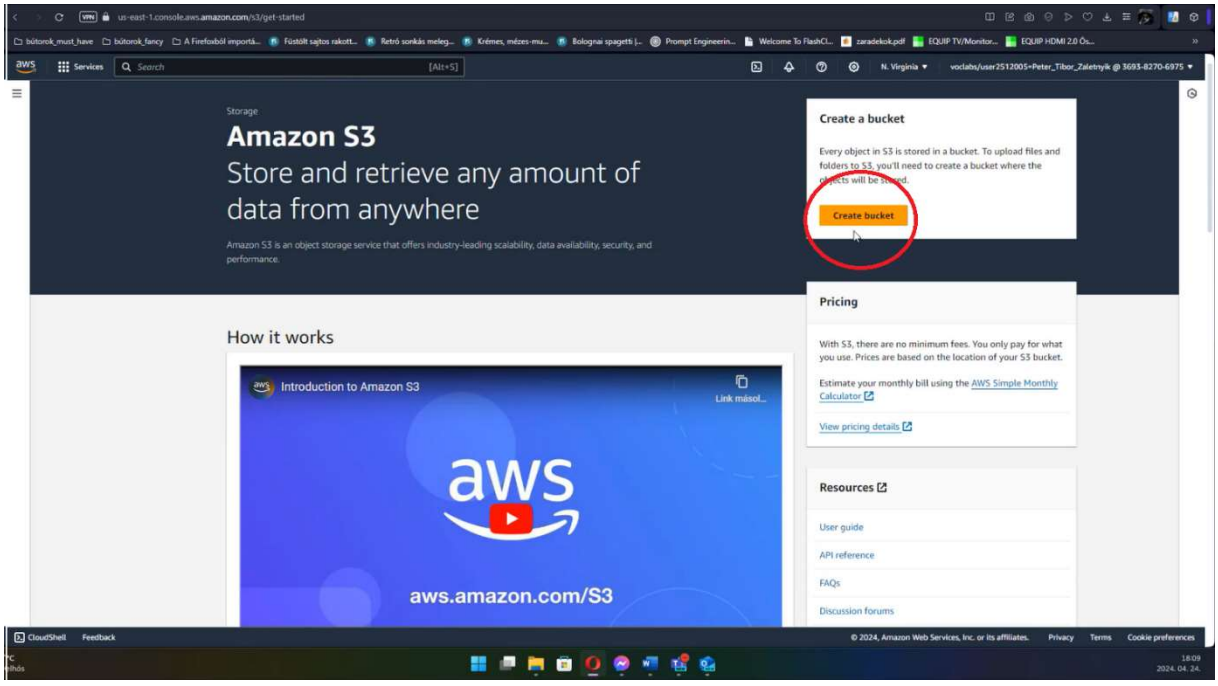
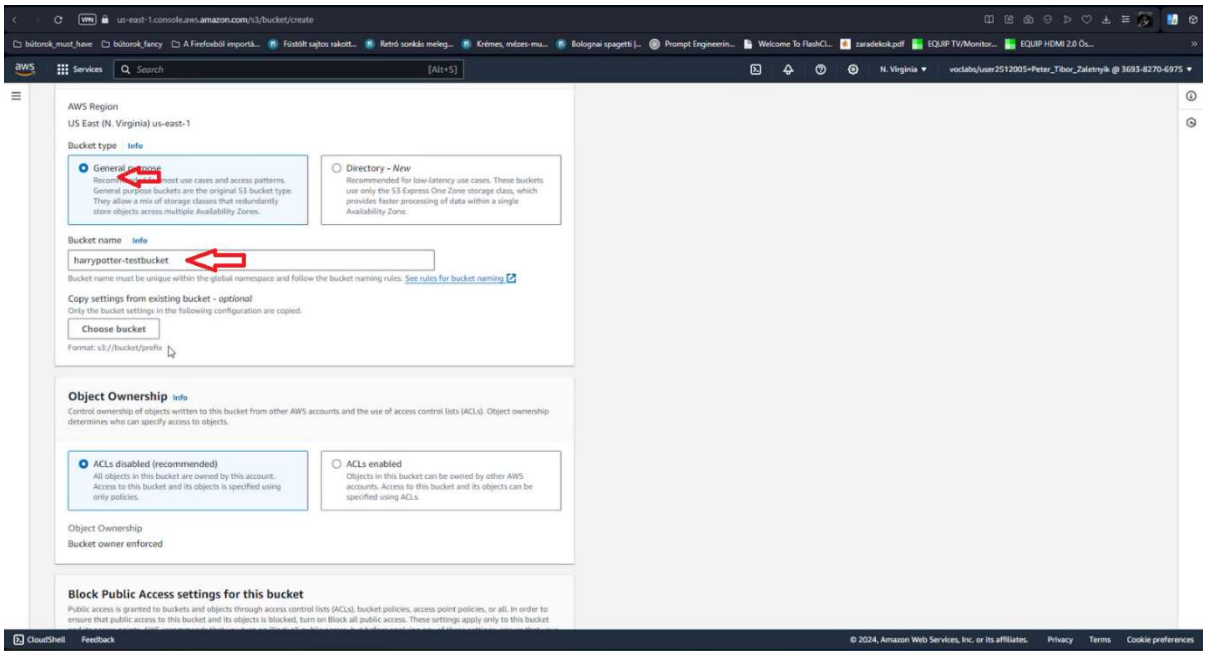
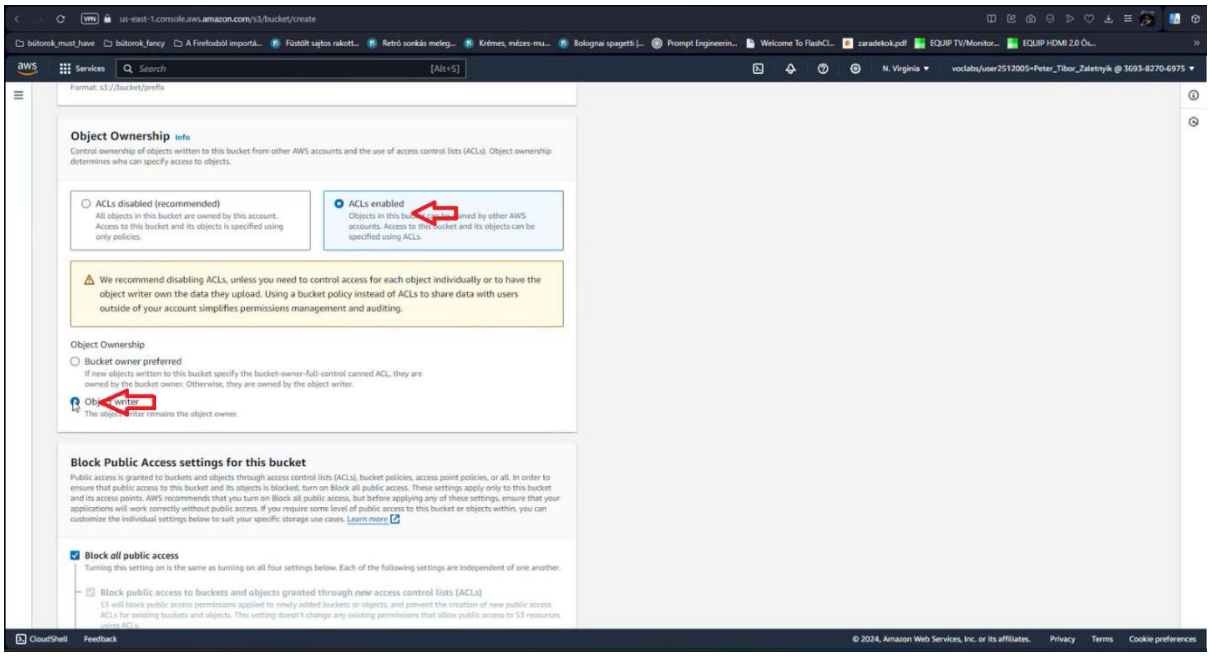
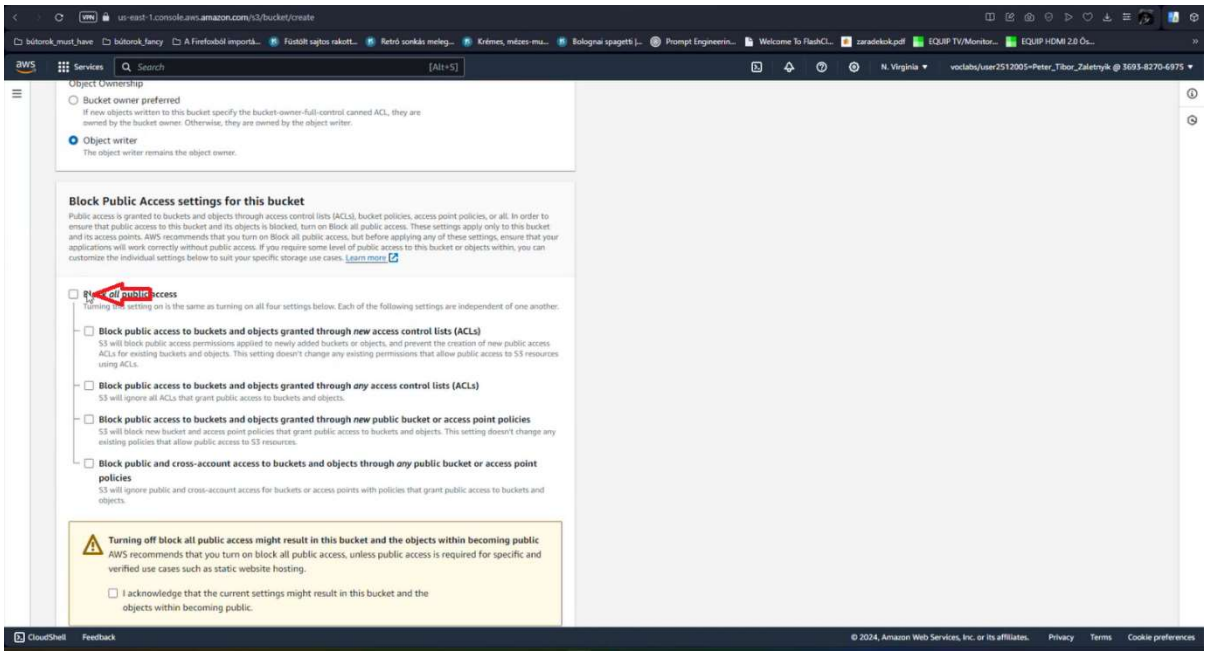
I. lépés S3 bucket configurálás:

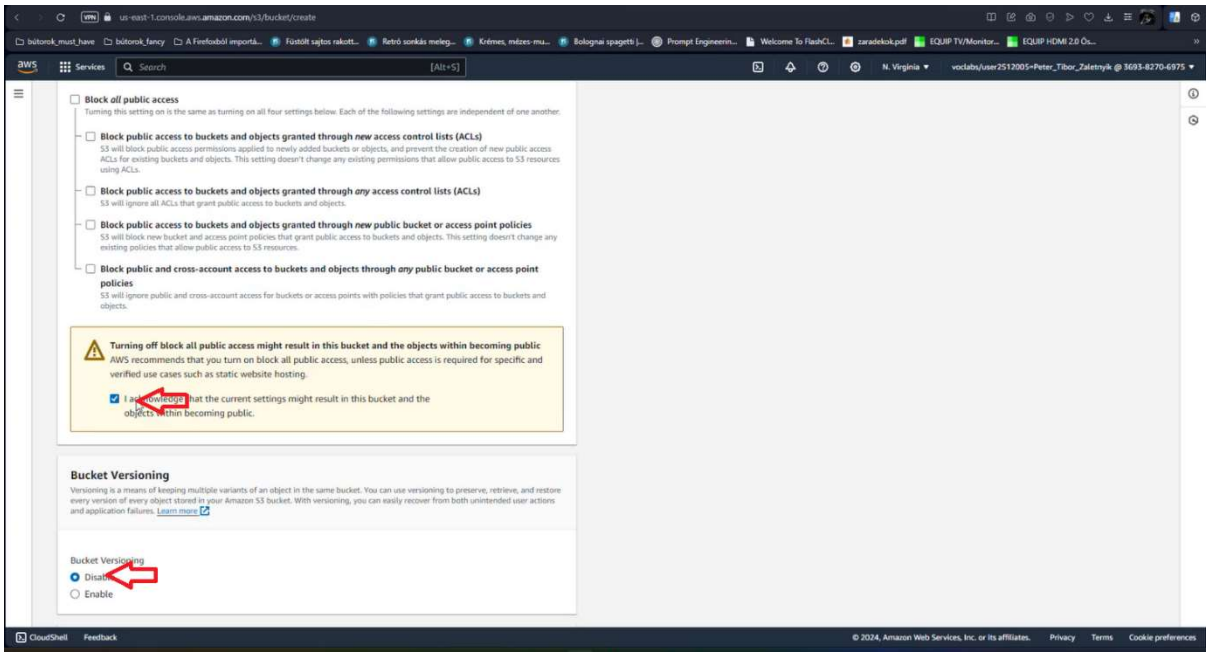


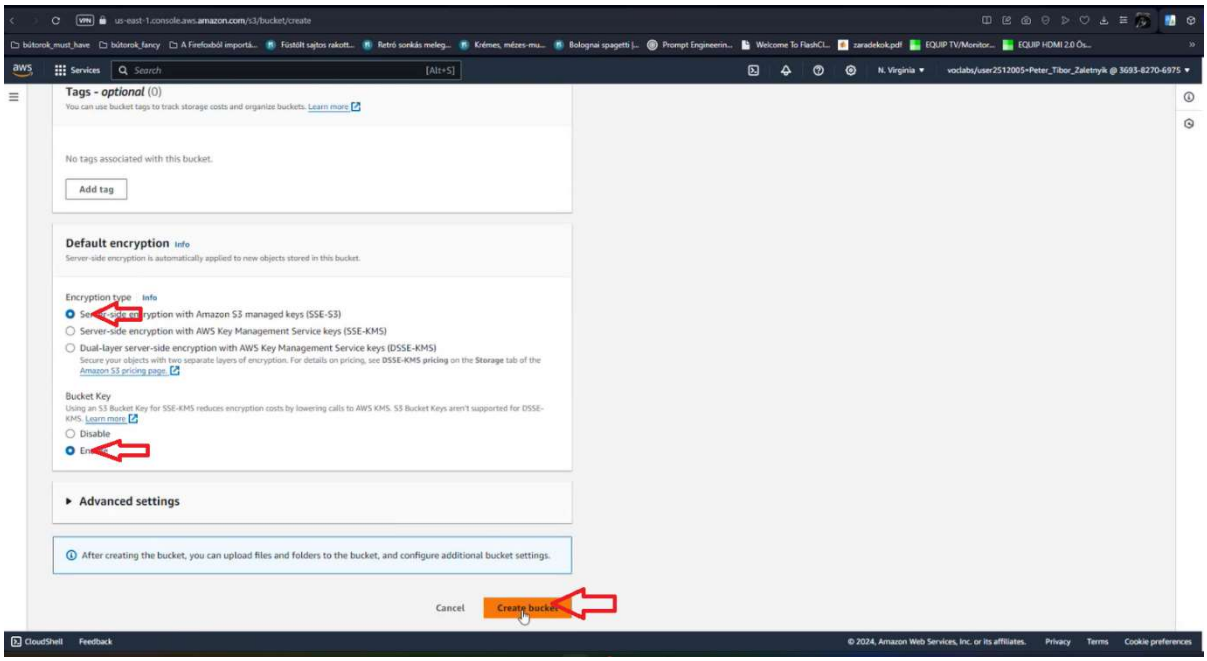



us-east-1.console.aws.amazon.com/s3/bucket/create
Services
Search
[Alt+S]
N. Virginia
AWS Region
US East (N. Virginia) us-east-1
Bucket type Info
General purpose
Directory - New
Bucket name Info
harrypotter-testbucket
Bucket name must be unique within the global namespace and follow the bucket naming rules. See rules for bucket naming
Copy settings from existing bucket - optional
Only the bucket settings in the following configuration are copied.
Choose bucket
Format: s3://bucket/prefix
Object Ownership Info
Control ownership of objects written to this bucket from other AWS accounts and the use of access control lists (ACLs). Object ownership determines who can specify access to objects.
ACLs disabled (recommended)
All objects in this bucket are owned by this account. Access to this bucket and its objects is specified using only policies.
ACLs enabled
Objects in this bucket can be owned by other AWS accounts. Access to this bucket and its objects can be specified using ACLs.
Object Ownership
Bucket owner enforced
Block Public Access settings for this bucket
Public access is granted to buckets and objects through access control lists (ACLs), bucket policies, access point policies, or all. In order to ensure that public access to this bucket and its objects is blocked, turn on Block all public access. These settings apply only to this bucket
CloudShell
Feedback
© 2024, Amazon Web Services, Inc. or its affiliates.
Privacy
Terms
Cookie preferences

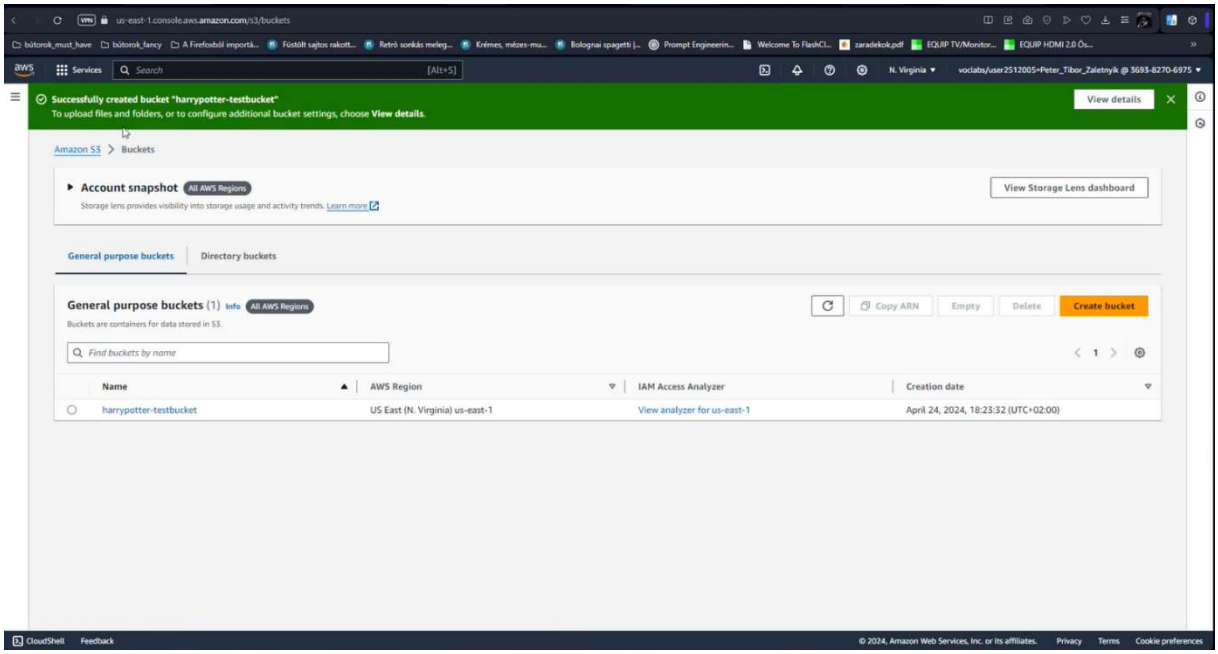

us-east-1.console.aws.amazon.com/s3/bucket/create
Services
Search
[Alt+S]
N. Virginia
Format: s3://bucket/prefix
Object Ownership Info
Control ownership of objects written to this bucket from other AWS accounts and the use of access control lists (ACLs). Object ownership determines who can specify access to objects.
ACLs disabled (recommended)
All objects in this bucket are owned by this account. Access to this bucket and its objects is specified using only policies.
ACLs enabled
Objects in this bucket can be owned by other AWS accounts. Access to this bucket and its objects can be specified using ACLs.
We recommend disabling ACLs, unless you need to control access for each object individually or to have the object writer own the data they upload. Using a bucket policy instead of ACLs to share data with users outside of your account simplifies permissions management and auditing.
Object Ownership
Bucket owner preferred
If new objects written to this bucket specify the bucket-owner-full-control canned ACL, they are owned by the bucket owner. Otherwise, they are owned by the object writer.
Object writer
The objects writer remains the object owner.
Block Public Access settings for this bucket
Public access is granted to buckets and objects through access control lists (ACLs), bucket policies, access point policies, or all. In order to ensure that public access to this bucket and its objects is blocked, turn on Block all public access. These settings apply only to this bucket and its access points. AWS recommends that you turn on Block all public access, but before applying any of these settings, ensure that your applications will work correctly without public access. If you require some level of public access to this bucket or objects within, you can customize the individual settings below to suit your specific storage use cases. Learn more
Block all public access
Turning this setting on is the same as turning on all four settings below. Each of the following settings are independent of one another.
Block public access to buckets and objects granted through new access control lists (ACLs)
S3 will block public access permissions applied to newly added buckets or objects, and prevent the creation of new public access ACLs for existing buckets and objects. This setting doesn't change any existing permissions that allow public access to S3 resources
CloudShell
Feedback
© 2024, Amazon Web Services, Inc. or its affiliates.
Privacy
Terms
Cookie preferences


us-east-1.console.aws.amazon.com/s3/bucket/create
Services
Search
[Alt+S]
N. Virginia
Object Ownership
Bucket owner preferred
If new objects written to this bucket specify the bucket-owner-full-control canned ACL, they are owned by the bucket owner. Otherwise, they are owned by the object writer.
Object writer
The object writer remains the object owner.
Block Public Access settings for this bucket
Public access is granted to buckets and objects through access control lists (ACLs), bucket policies, access point policies, or all. In order to ensure that public access to this bucket and its objects is blocked, turn on Block all public access. These settings apply only to this bucket and its access points. AWS recommends that you turn on Block all public access, but before applying any of these settings, ensure that your applications will work correctly without public access. If you require some level of public access to this bucket or objects within, you can customize the individual settings below to suit your specific storage use cases. Learn more
Block all public access
Turning this setting on is the same as turning on all four settings below. Each of the following settings are independent of one another.
Block public access to buckets and objects granted through new access control lists (ACLs)
S3 will block public access permissions applied to newly added buckets or objects, and prevent the creation of new public access ACLs for existing buckets and objects. This setting doesn't change any existing permissions that allow public access to S3 resources using ACLs.
Block public access to buckets and objects granted through any access control lists (ACLs)
S3 will ignore all ACLs that grant public access to buckets and objects.
Block public access to buckets and objects granted through new public bucket or access point policies
S3 will block new bucket and access point policies that grant public access to buckets and objects. This setting doesn't change any existing policies that allow public access to S3 resources.
Block public and cross-account access to buckets and objects through any public bucket or access point policies
S3 will ignore public and cross-account access for buckets or access points with policies that grant public access to buckets and objects.
Turning off block all public access might result in this bucket and the objects within becoming public
AWS recommends that you turn on block all public access, unless public access is required for specific and verified use cases such as static website hosting.
I acknowledge that the current settings might result in this bucket and the objects within becoming public.
CloudShell
Feedback
© 2024, Amazon Web Services, Inc. or its affiliates.
Privacy
Terms
Cookie preferences

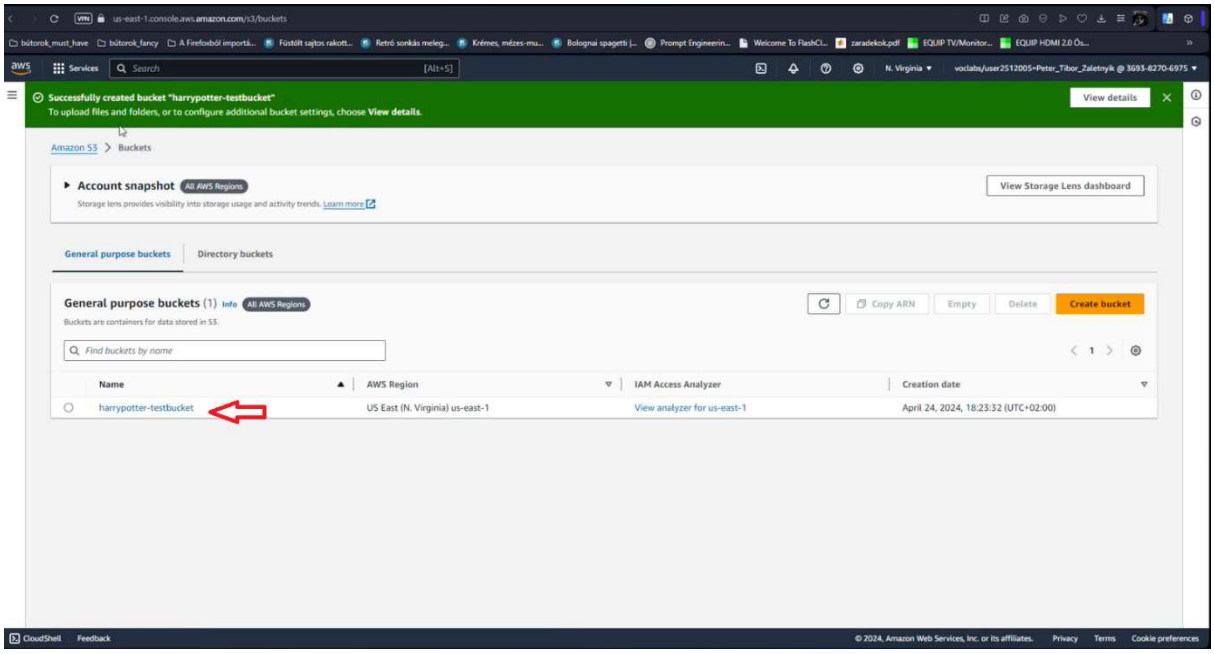

us-east-1.console.aws.amazon.com/s3/bucket/create
Services
Search
[Alt+S]
N. Virginia
Block all public access
Block public access to buckets and objects granted through new access control lists (ACLs)
Block public access to buckets and objects granted through any access control lists (ACLs)
Block public access to buckets and objects granted through new public bucket or access point policies
Block public and cross-account access to buckets and objects through any public bucket or access point policies
Turning off block all public access might result in this bucket and the objects within becoming public
AWS recommends that you turn on block all public access, unless public access is required for specific and verified use cases such as static website hosting.
I acknowledge that the current settings might result in this bucket and the objects within becoming public.
Bucket Versioning
Versioning is a means of keeping multiple variants of an object in the same bucket. You can use versioning to preserve, retrieve, and restore every version of every object stored in your Amazon S3 bucket. With versioning, you can easily recover from both unintended user actions and application failures. Learn more
Bucket Versioning
Disable
Enable
CloudShell
Feedback
© 2024, Amazon Web Services, Inc. or its affiliates.
Privacy
Terms
Cookie preferences



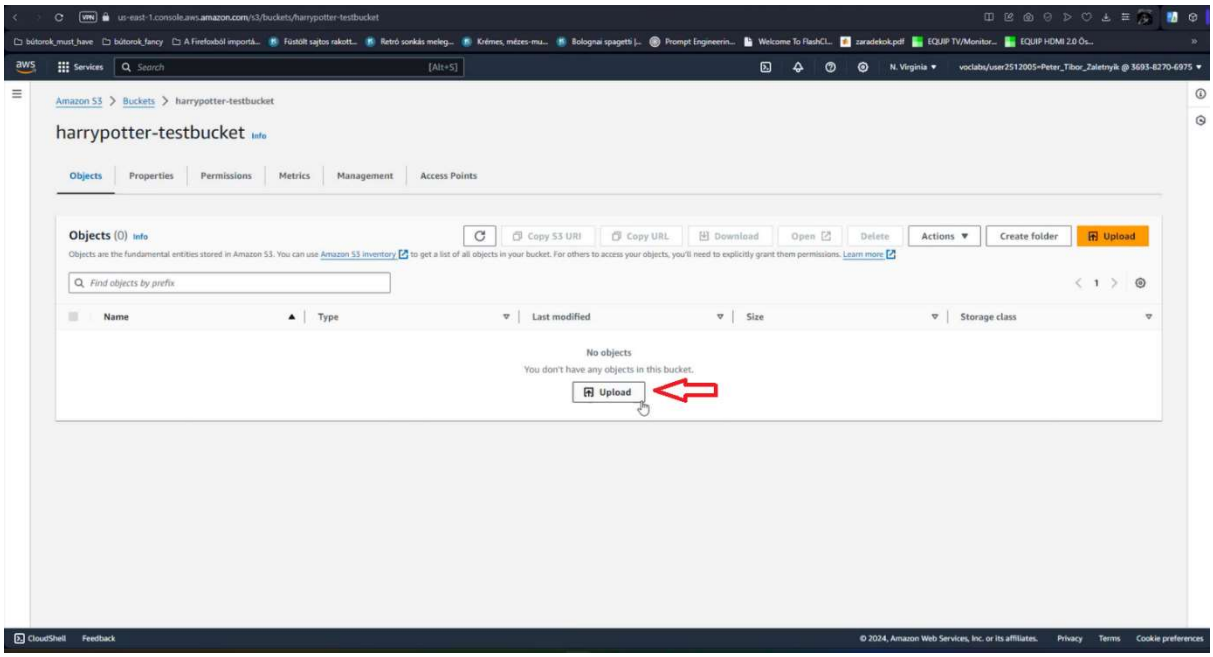
A Bucket létrehozásra került:



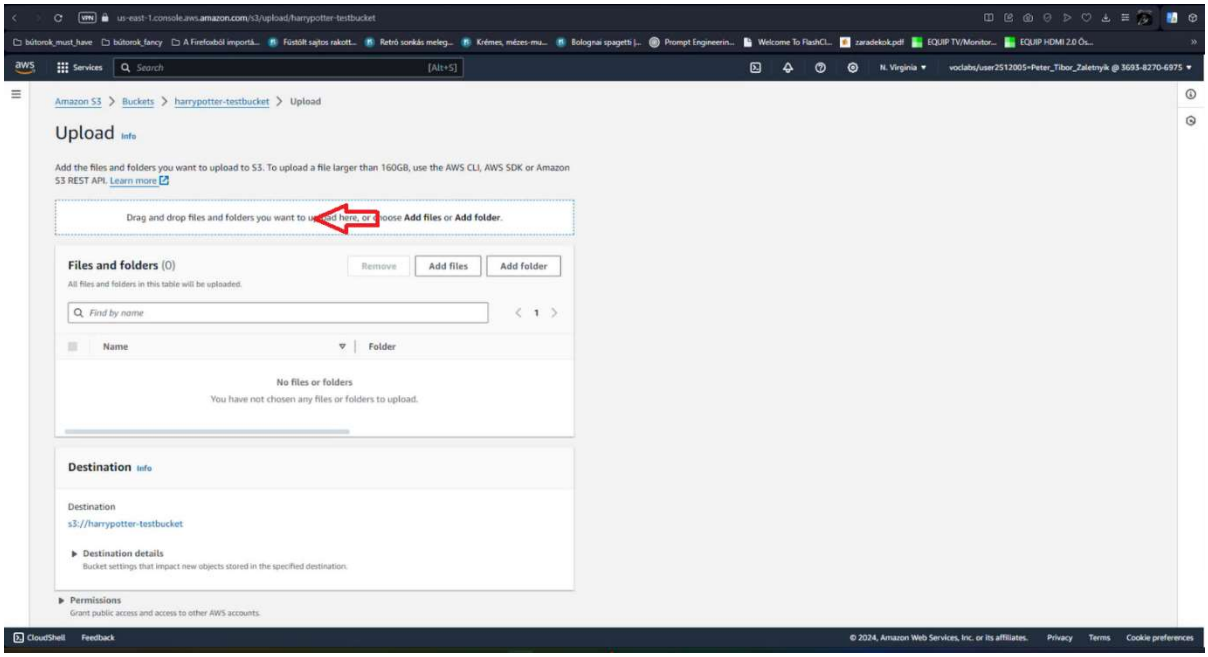
Kiválasztjuk a létrehozott bucket-ot:



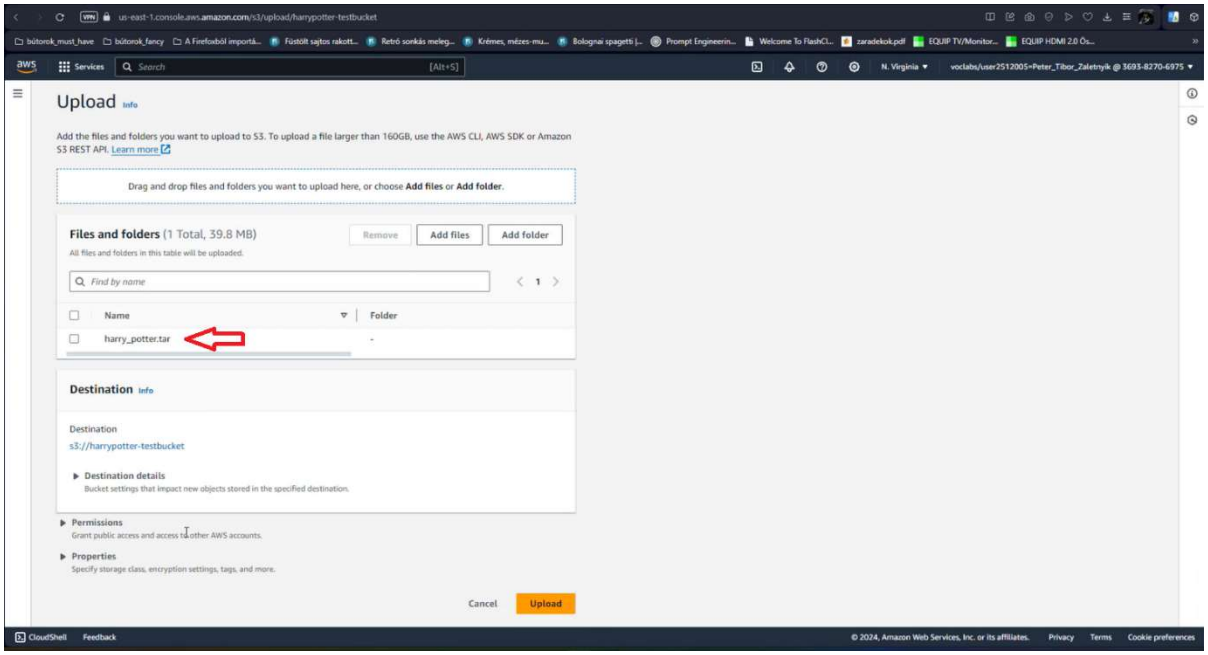
Jelenleg üres fel kell tölteni adattal:

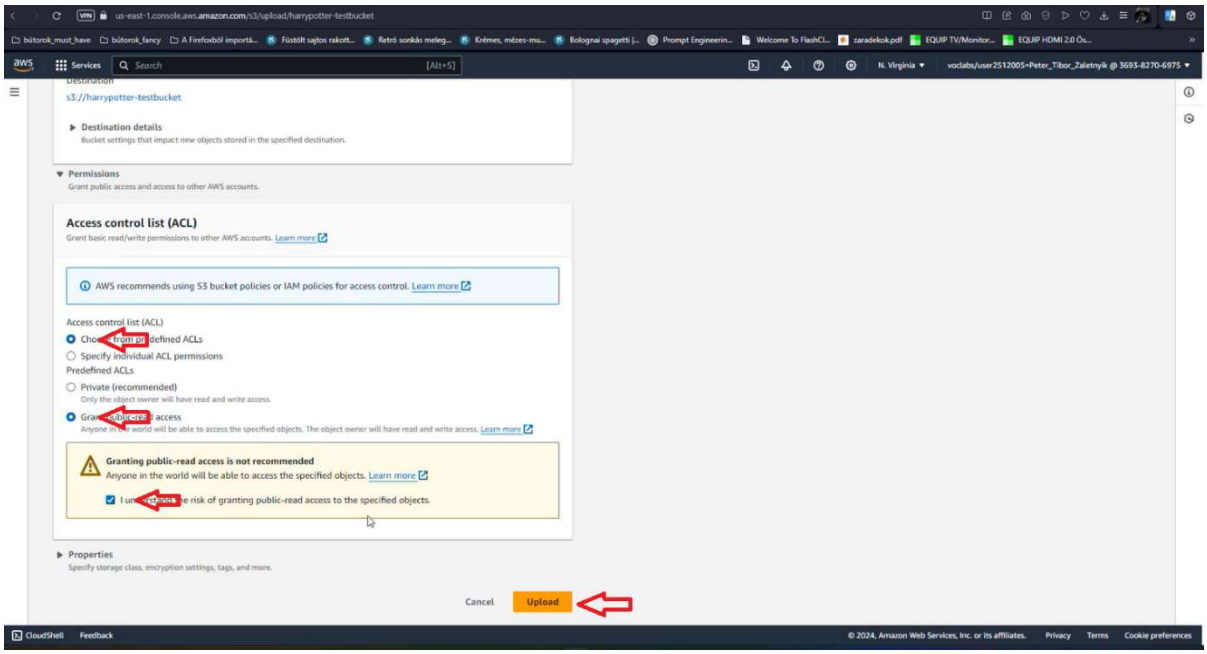


Megfogjuk és a kért ablakba húzzuk (*drag and drop*) a kiválasztott fájlt vagy mappát:

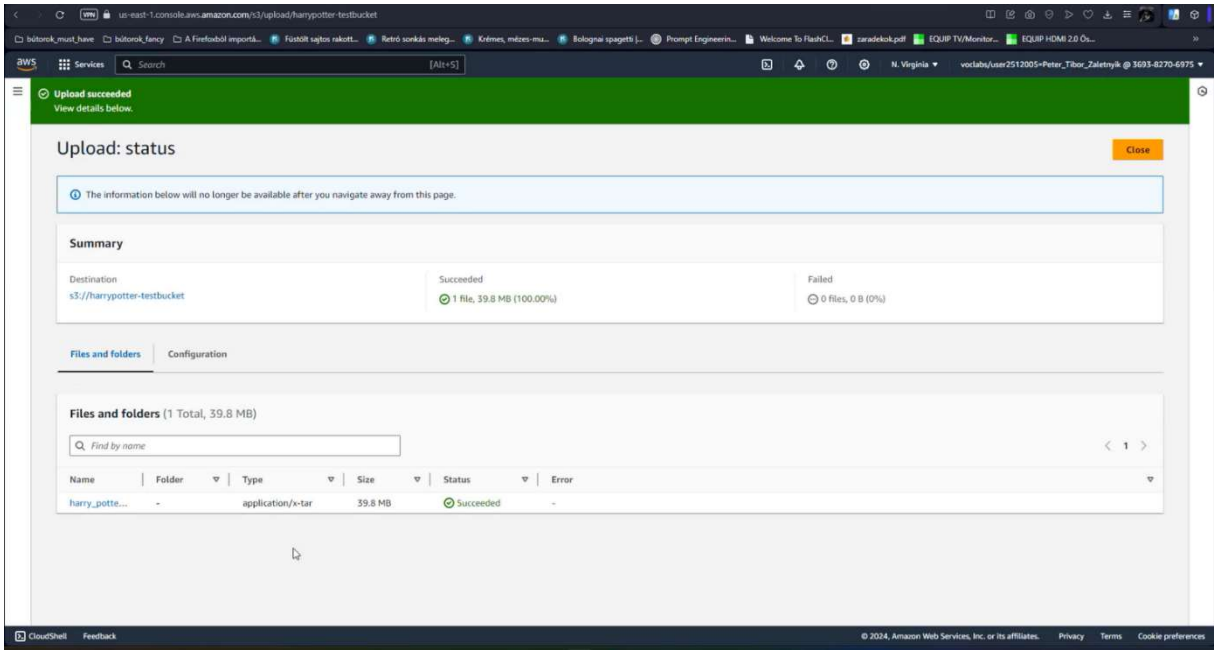


Ezt követően meg is jelenik a felületen:

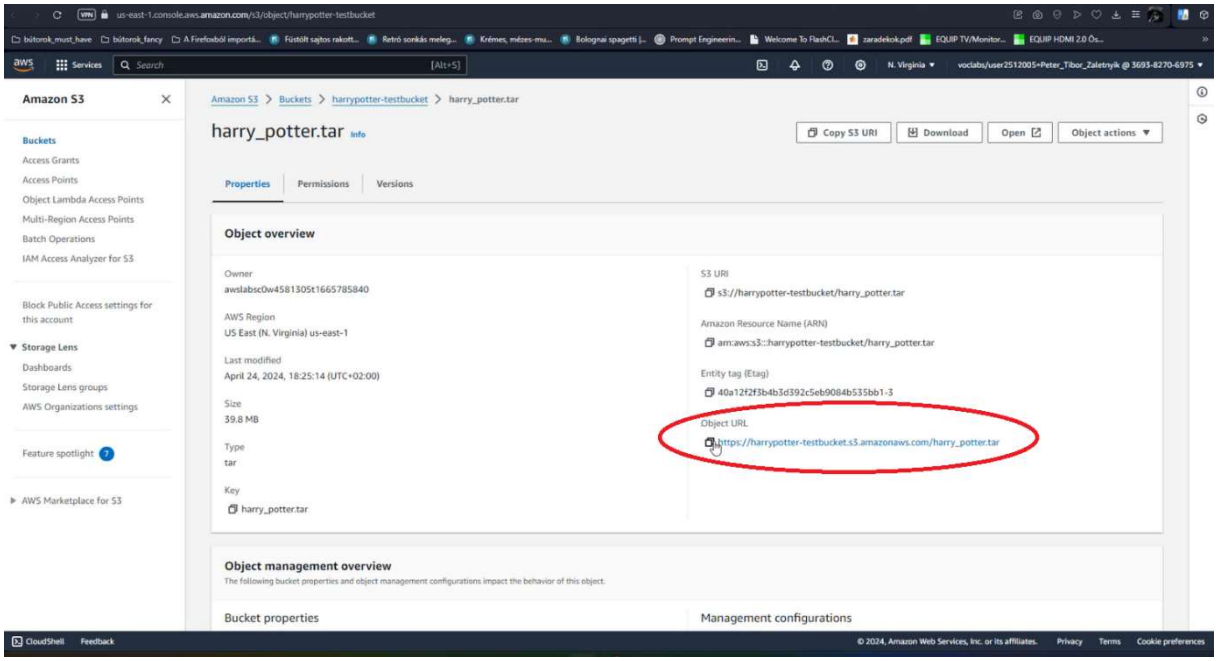




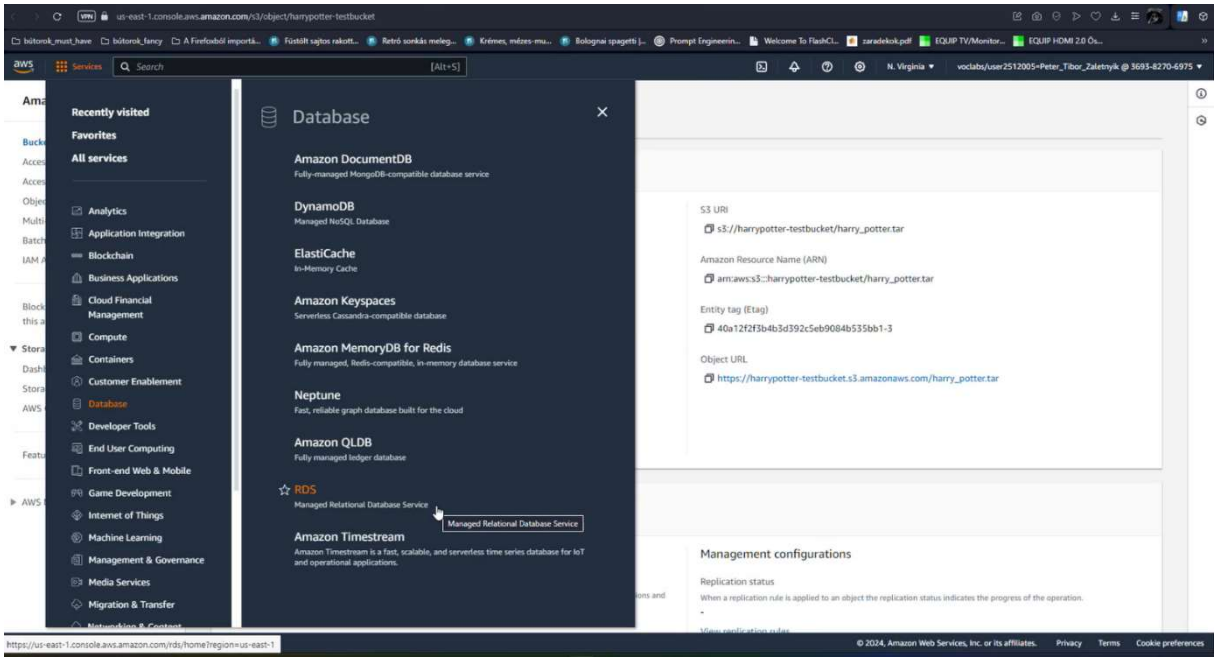
A feltöltés sikerült:

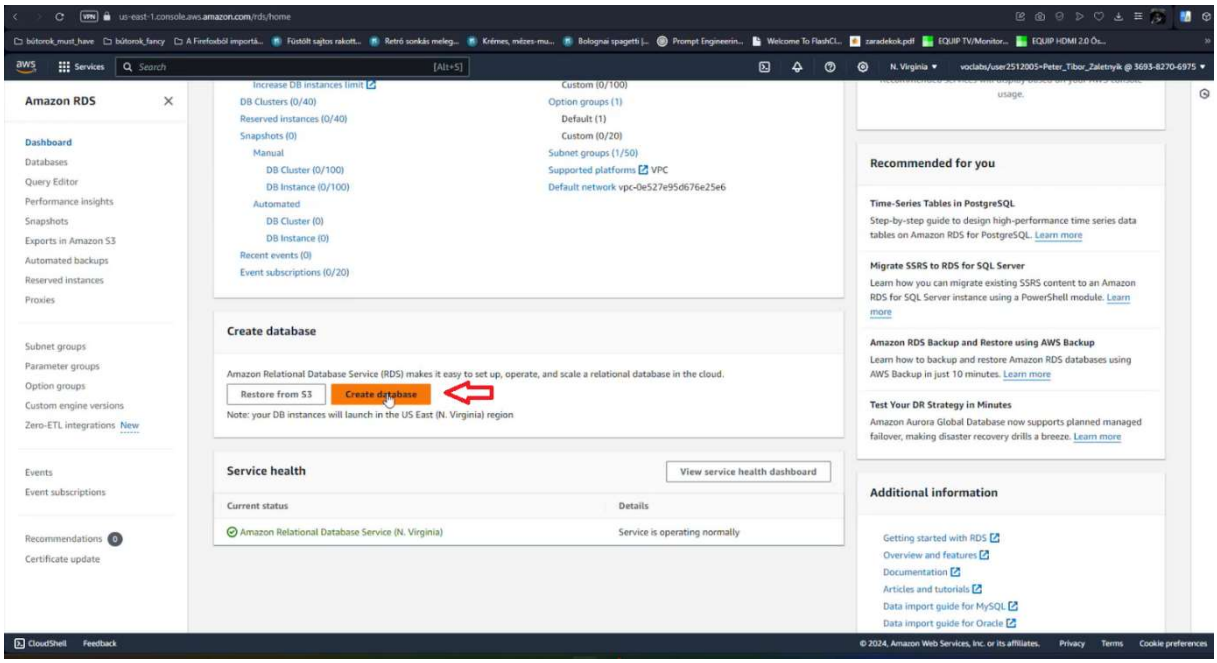


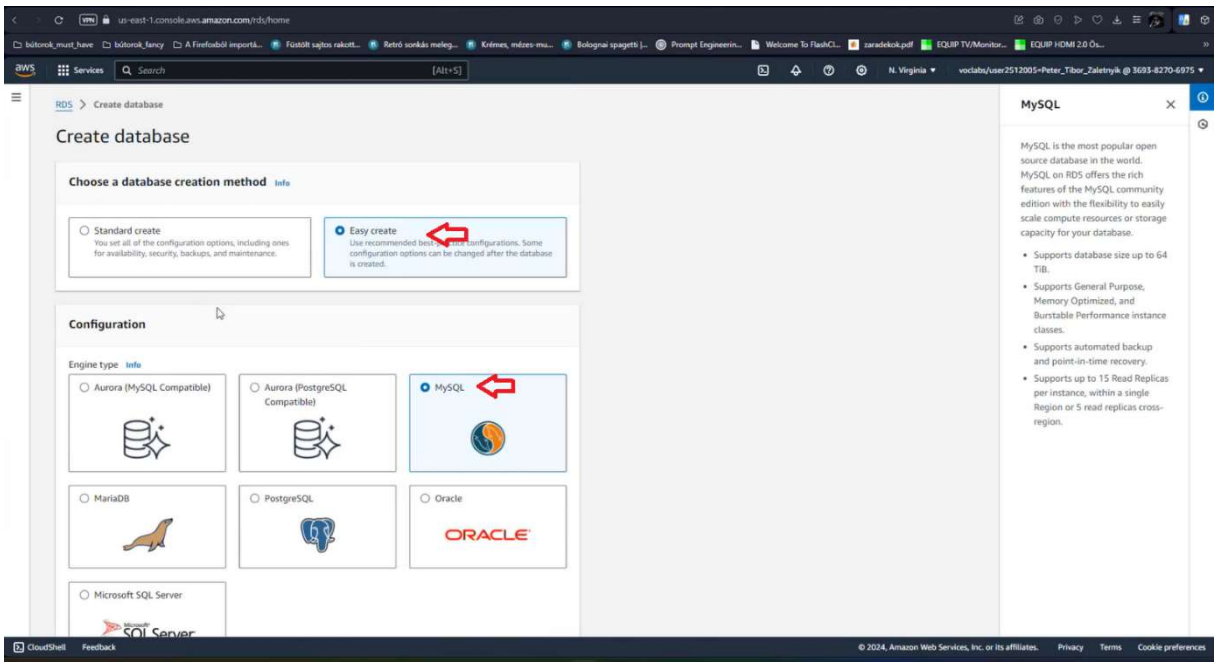
Ha kiválasztjuk a .tar fájlt, meg tudjuk nézni az URL-jét ami majd a későbbiekben szükséges lesz a webszerverre való feltöltéshez:

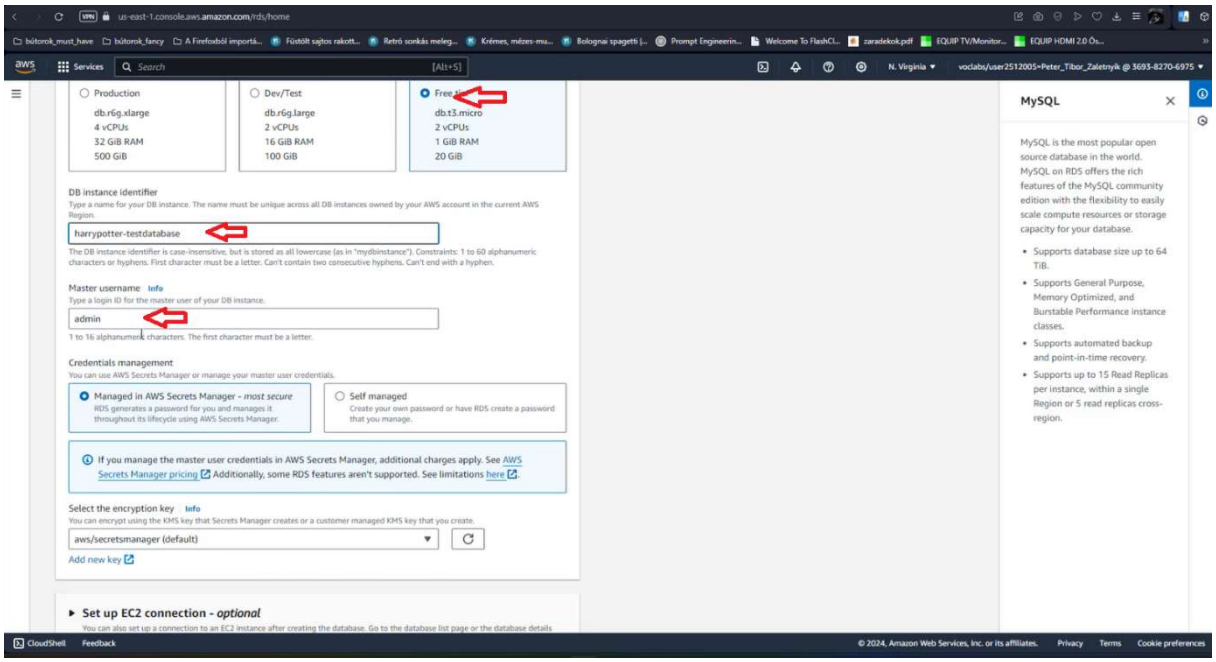


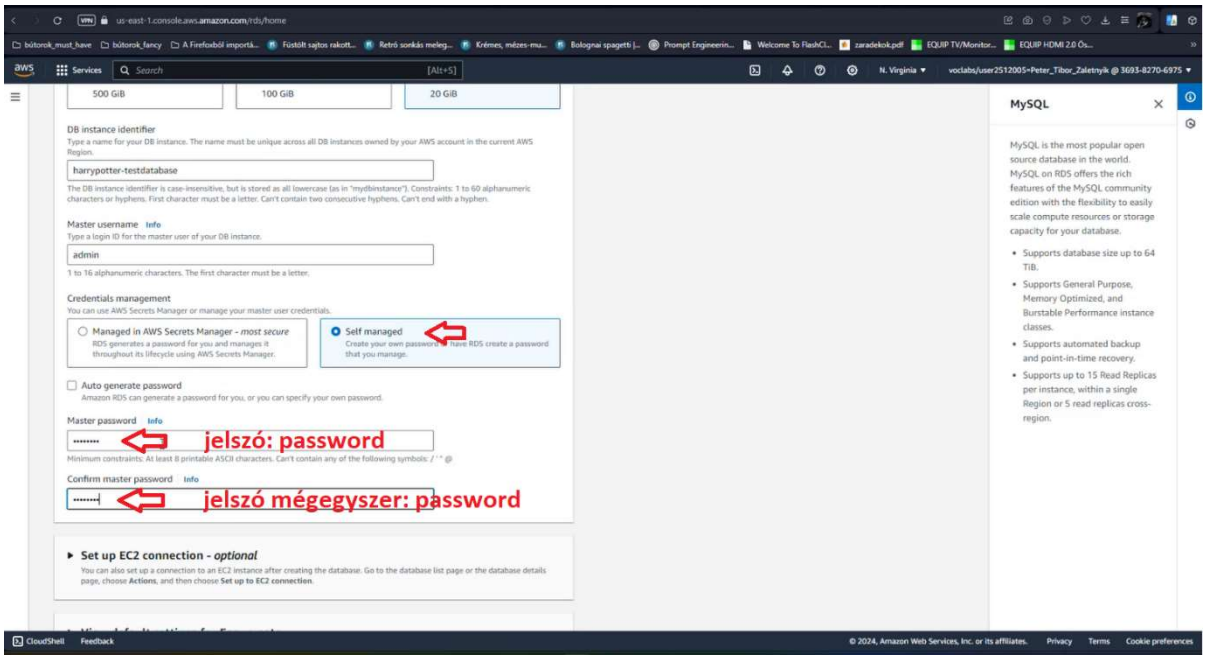
II. ***<u>RDS létrehozása:</u>***

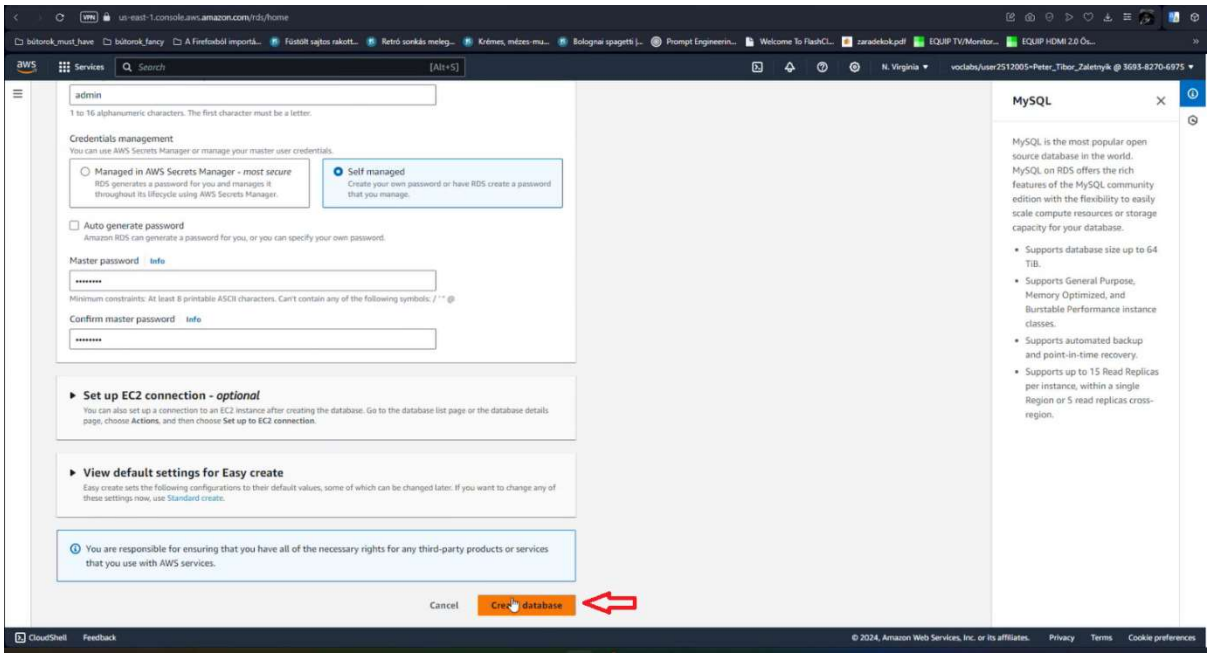



Amazon RDS
Dashboard
Databases
Query Editor
Performance insights
Snapshots
Exports in Amazon S3
Automated backups
Reserved instances
Proxies
Subnet groups
Parameter groups
Option groups
Custom engine versions
Zero-ETL integrations New
Events
Event subscriptions
Recommendations 0
Certificate update
Increase DB instances limit
DB Clusters (0/40)
Reserved instances (0/40)
Snapshots (0)
Manual
DB Cluster (0/100)
DB Instance (0/100)
Automated
DB Cluster (0)
DB Instance (0)
Recent events (0)
Event subscriptions (0/20)
Custom (0/100)
Option groups (1)
Default (1)
Custom (0/20)
Subnet groups (1/50)
Supported platforms VPC
Default network vpc-0e527e95d676e25e6
Create database
Amazon Relational Database Service (RDS) makes it easy to set up, operate, and scale a relational database in the cloud.
Restore from S3
Create database
Note: your DB instances will launch in the US East (N. Virginia) region
Service health
View service health dashboard
Current status
Details
Amazon Relational Database Service (N. Virginia)
Service is operating normally
Recommended for you
Time-Series Tables in PostgreSQL
Step-by-step guide to design high-performance time series data tables on Amazon RDS for PostgreSQL. Learn more
Migrate SSRS to RDS for SQL Server
Learn how you can migrate existing SSRS content to an Amazon RDS for SQL Server instance using a PowerShell module. Learn more
Amazon RDS Backup and Restore using AWS Backup
Learn how to backup and restore Amazon RDS databases using AWS Backup in just 10 minutes. Learn more
Test Your DR Strategy in Minutes
Amazon Aurora Global Database now supports planned managed failover, making disaster recovery drills a breeze. Learn more
Additional information
Getting started with RDS
Overview and features
Documentation
Articles and tutorials
Data import guide for MySQL
Data import guide for Oracle
CloudShell
Feedback
© 2024, Amazon Web Services, Inc. or its affiliates.
Privacy
Terms
Cookie preferences

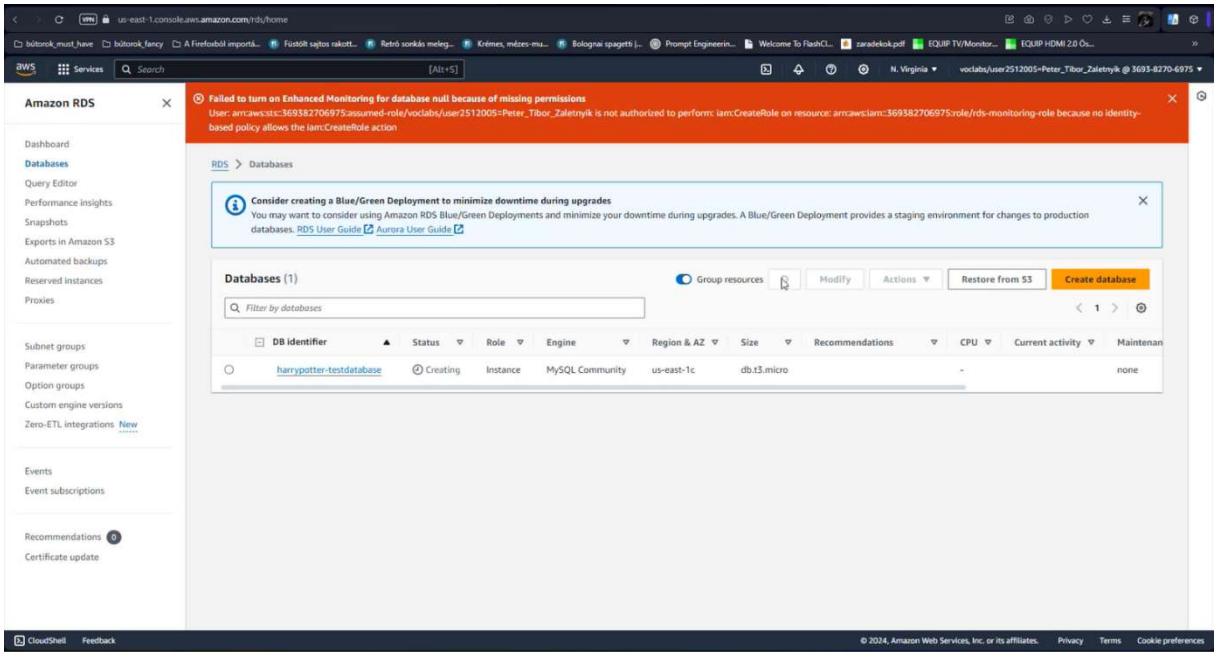

RDS > Create database
Create database
Choose a database creation method Info
Standard create
You set all of the configuration options, including ones for availability, security, backups, and maintenance.
Easy create
Use recommended best-practice configurations. Some configuration options can be changed after the database is created.
Configuration
Engine type Info
Aurora (MySQL Compatible)
Aurora (PostgreSQL Compatible)
MySQL
MariaDB
PostgreSQL
Oracle
Microsoft SQL Server
MySQL
MySQL is the most popular open source database in the world. MySQL on RDS offers the rich features of the MySQL community edition with the flexibility to easily scale compute resources or storage capacity for your database.
Supports database size up to 64 TiB.
Supports General Purpose, Memory Optimized, and Burstable Performance instance classes.
Supports automated backup and point-in-time recovery.
Supports up to 15 Read Replicas per instance, within a single Region or 5 read replicas cross-region.
CloudShell
Feedback
© 2024, Amazon Web Services, Inc. or its affiliates.
Privacy
Terms
Cookie preferences


Production
db.r6g.xlarge
4 vCPUs
32 GiB RAM
500 GiB
Dev/Test
db.r6g.large
2 vCPUs
16 GiB RAM
100 GiB
db.t3.micro
2 vCPUs
1 GiB RAM
20 GiB
DB instance identifier
harrypotter-testdatabase
Master username
admin
Credentials management
Managed in AWS Secrets Manager - most secure
Self managed
Select the encryption key
aws/secretsmanager (default)
Add new key
Set up EC2 connection - optional
MySQL
MySQL is the most popular open source database in the world. MySQL on RDS offers the rich features of the MySQL community edition with the flexibility to easily scale compute resources or storage capacity for your database.
Supports database size up to 64 TiB.
Supports General Purpose, Memory Optimized, and Burstable Performance instance classes.
Supports automated backup and point-in-time recovery.
Supports up to 15 Read Replicas per instance, within a single Region or 5 read replicas cross-region.

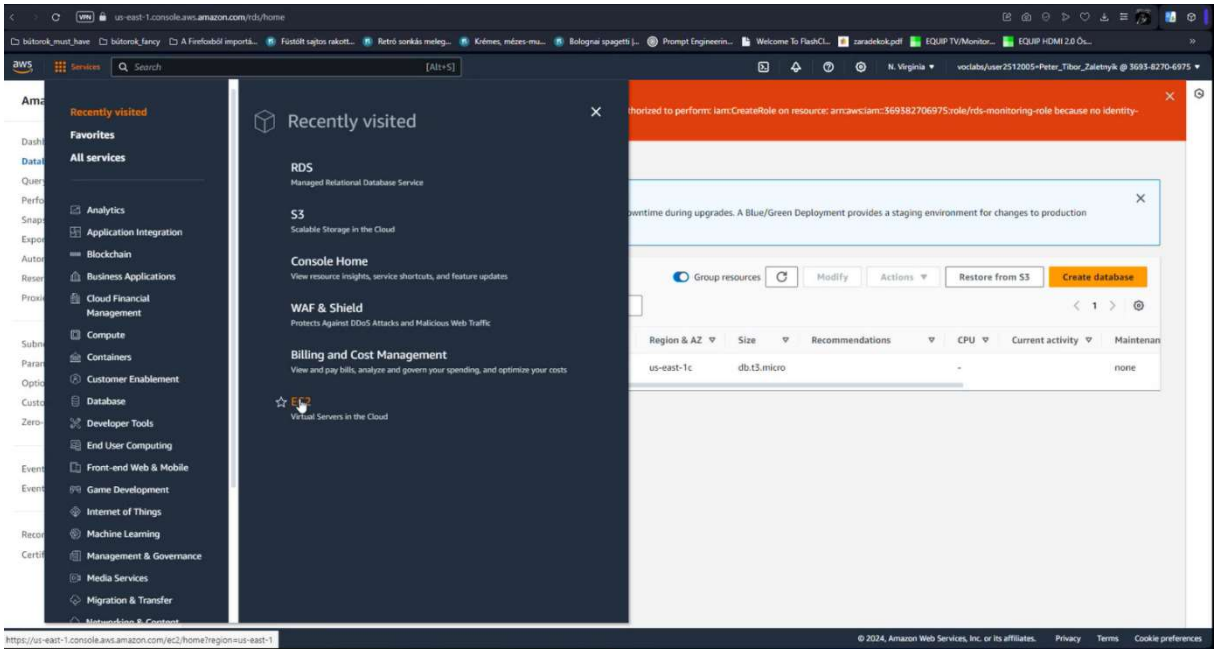

500 GiB
100 GiB
20 GiB
DB instance identifier
harrypotter-testdatabase
Master username
admin
Credentials management
Managed in AWS Secrets Manager - most secure
Self managed
Auto generate password
Master password
jelszó: password
Confirm master password
jelszó mégegyszer: password
Set up EC2 connection - optional
MySQL
MySQL is the most popular open source database in the world. MySQL on RDS offers the rich features of the MySQL community edition with the flexibility to easily scale compute resources or storage capacity for your database.
Supports database size up to 64 TiB.
Supports General Purpose, Memory Optimized, and Burstable Performance instance classes.
Supports automated backup and point-in-time recovery.
Supports up to 15 Read Replicas per instance, within a single Region or 5 read replicas cross-region.

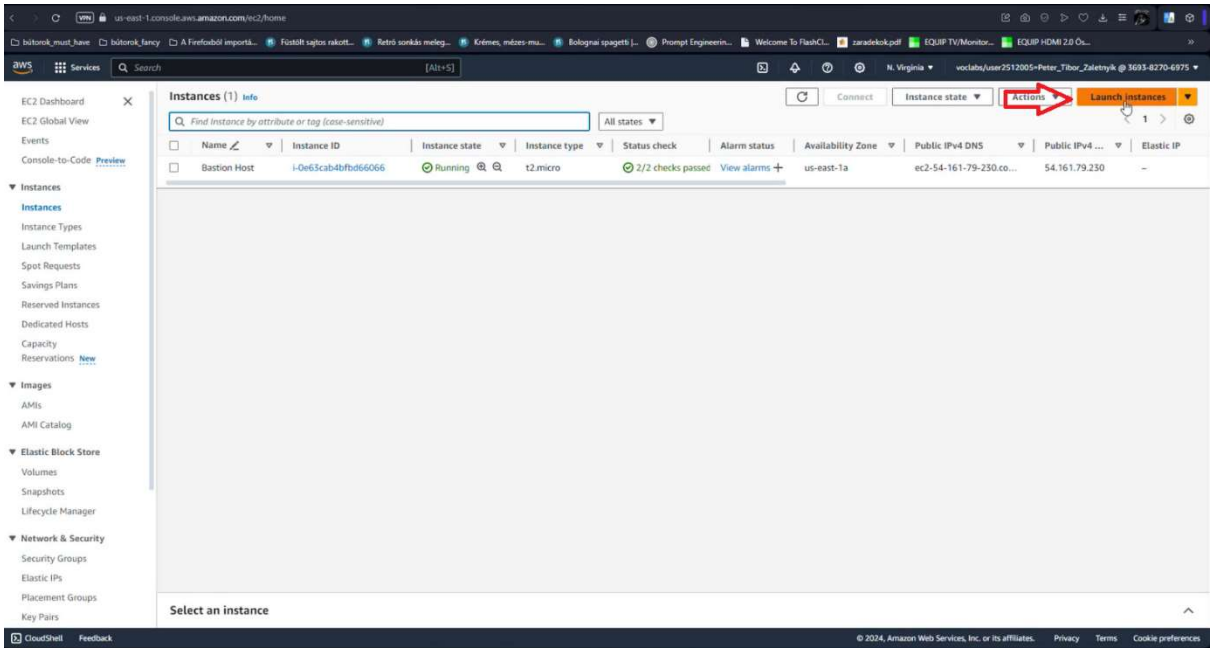


Elkezdődik a létrehozás folyamata, ez egy kis időbe telik addig csinálhatjuk tovább a feladatot:

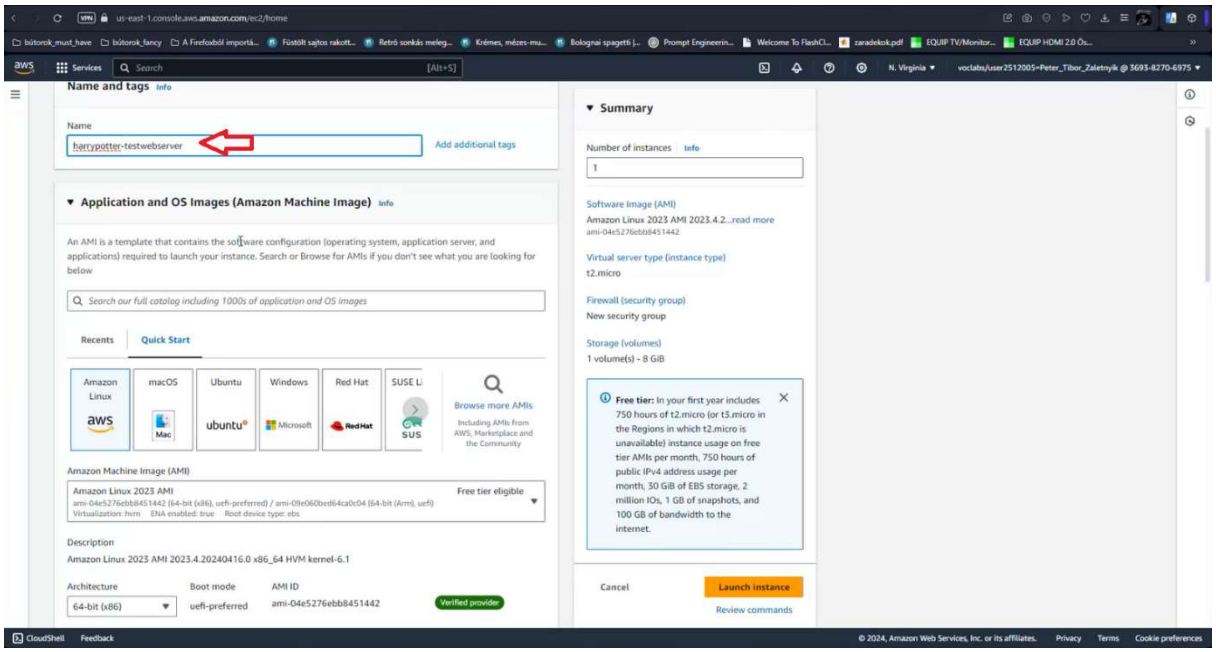


III. Virtuális gép létrehozása:

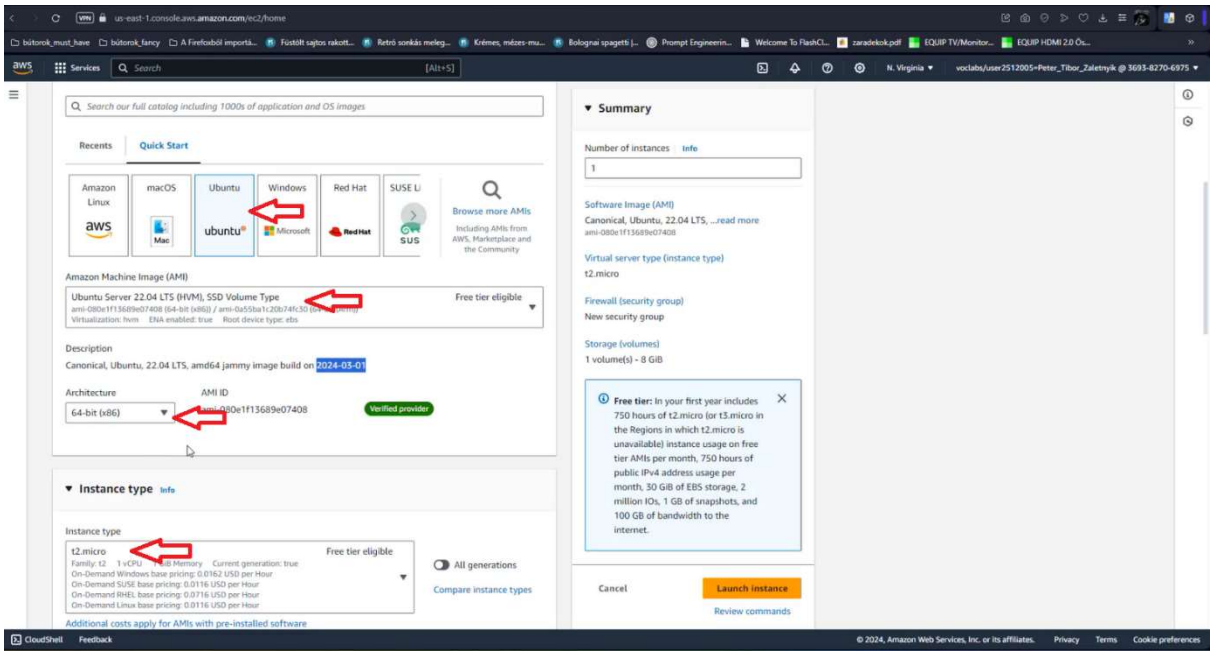




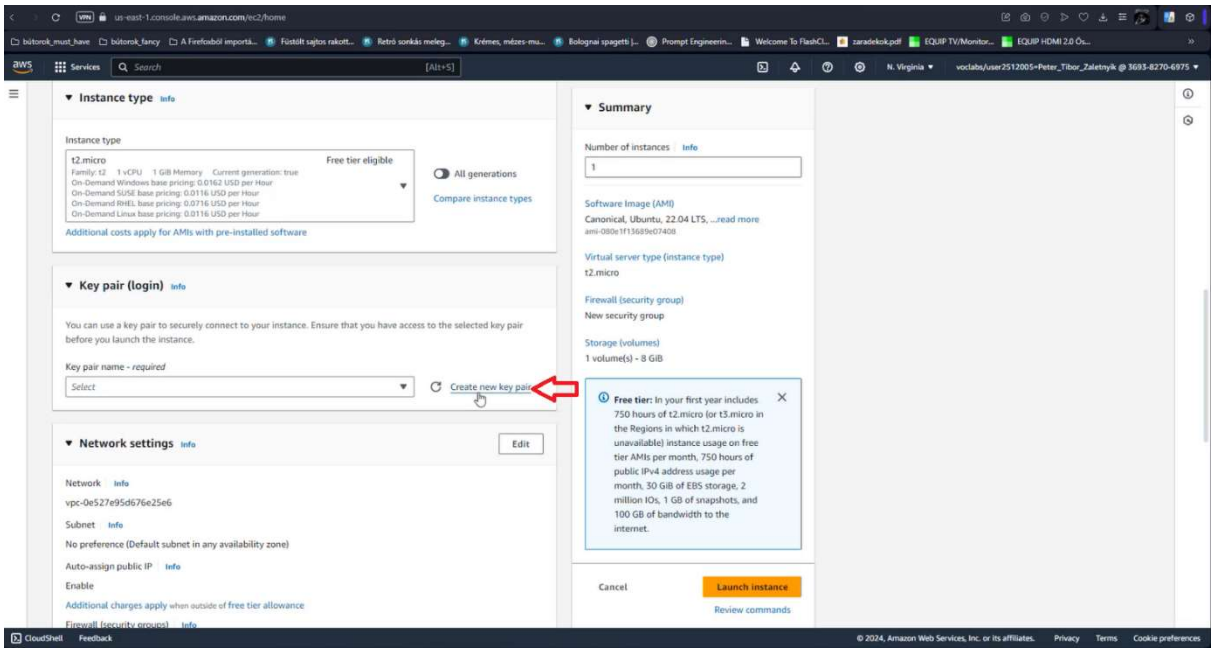
Elnevezzük a szervert:

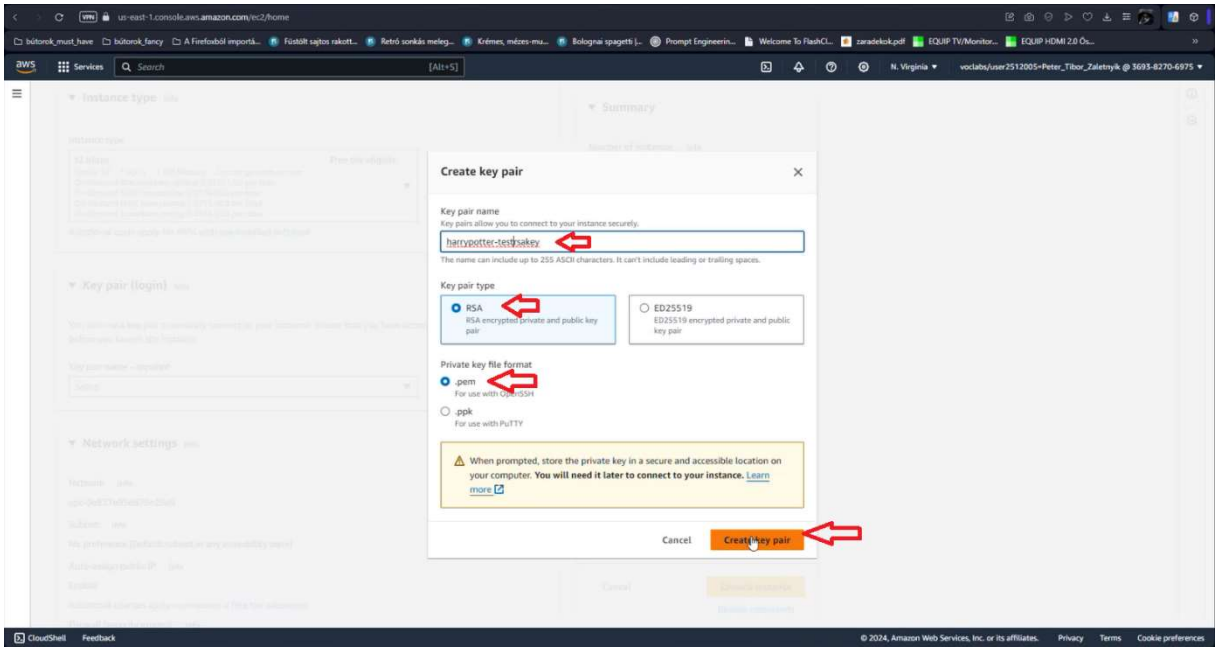


Kiválasztjuk az operációs rendszert és annak komponenseit:

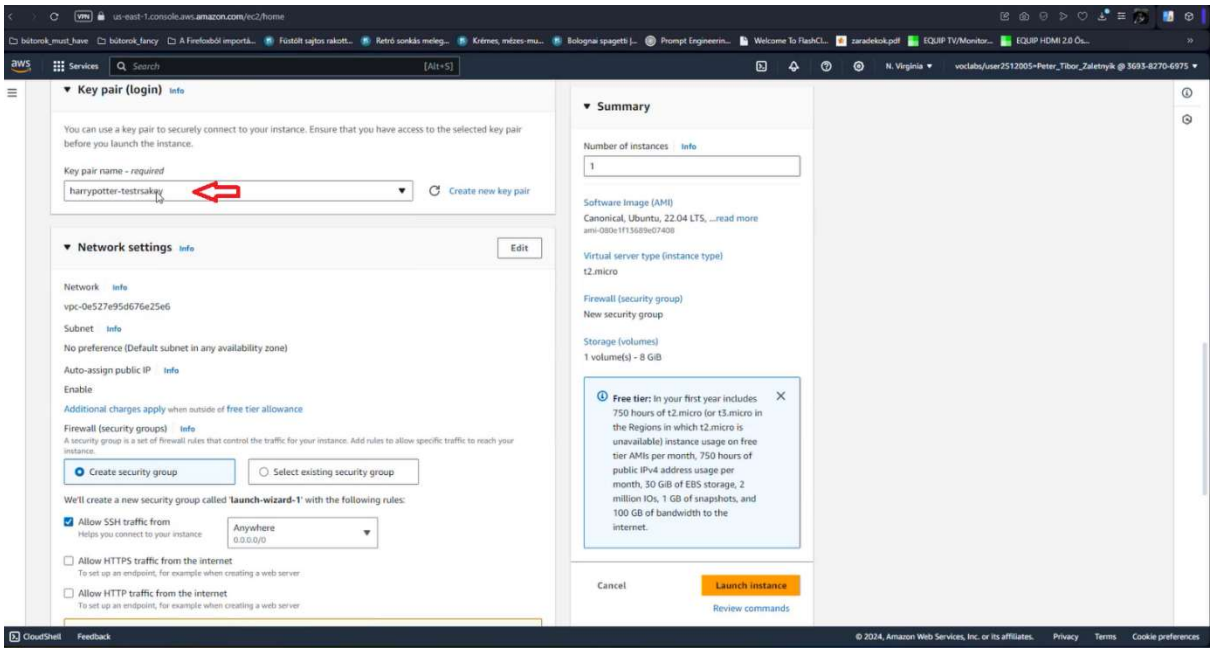


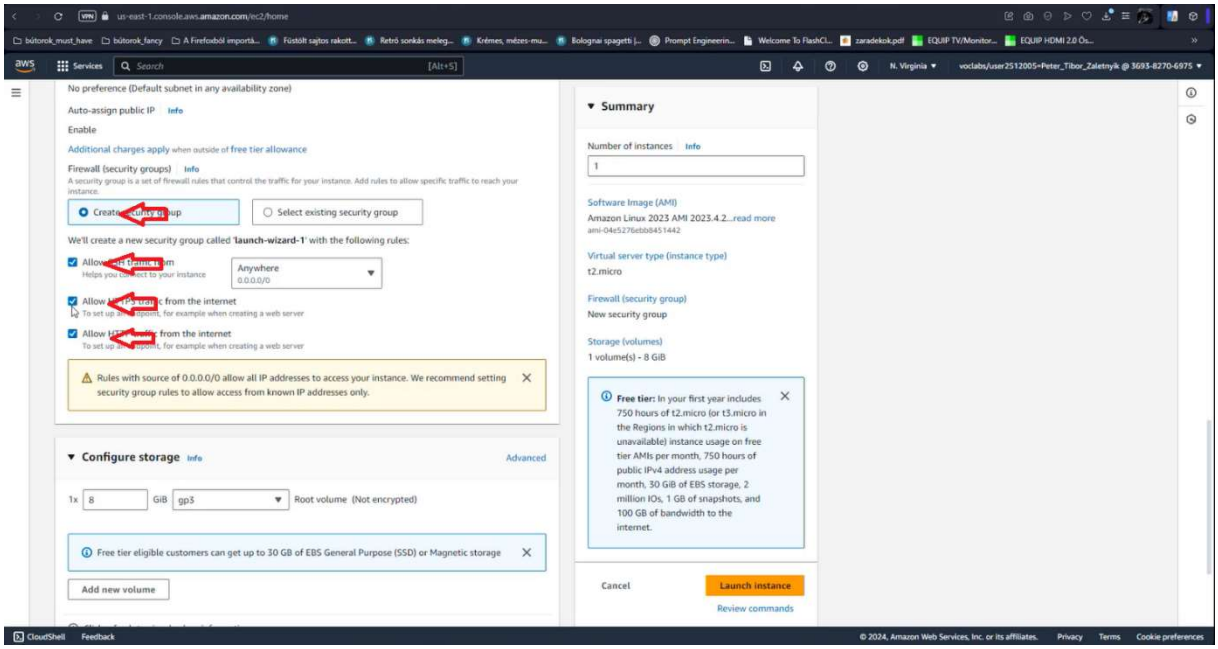
Kulcspár meghatározása:

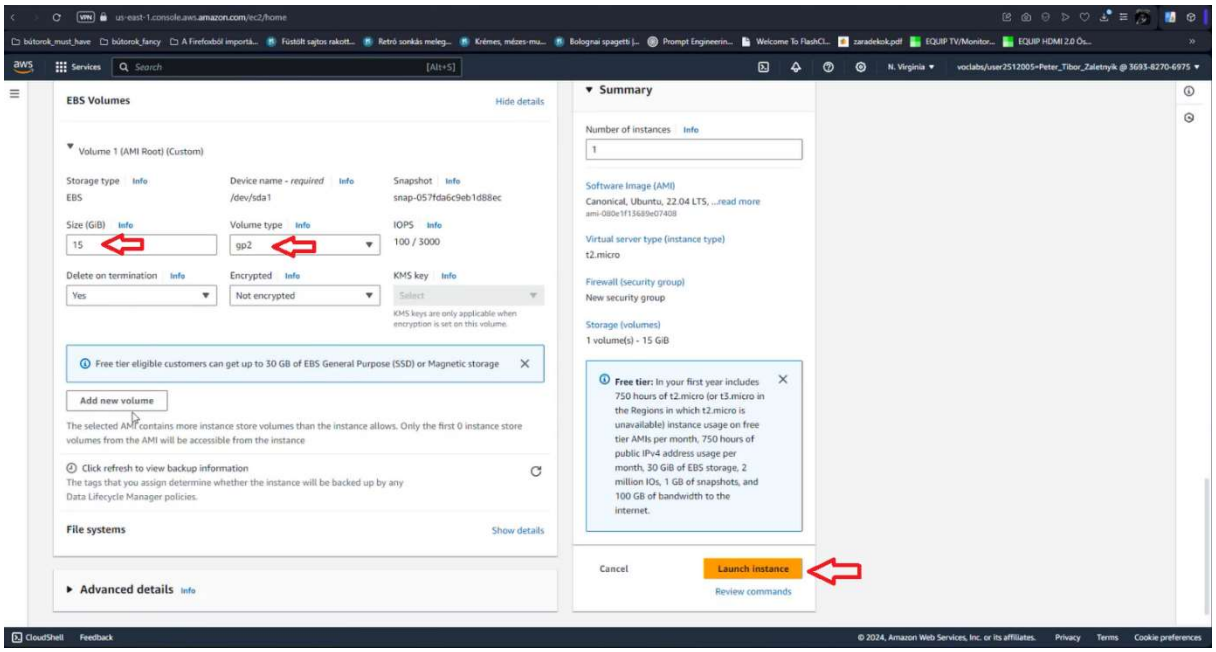




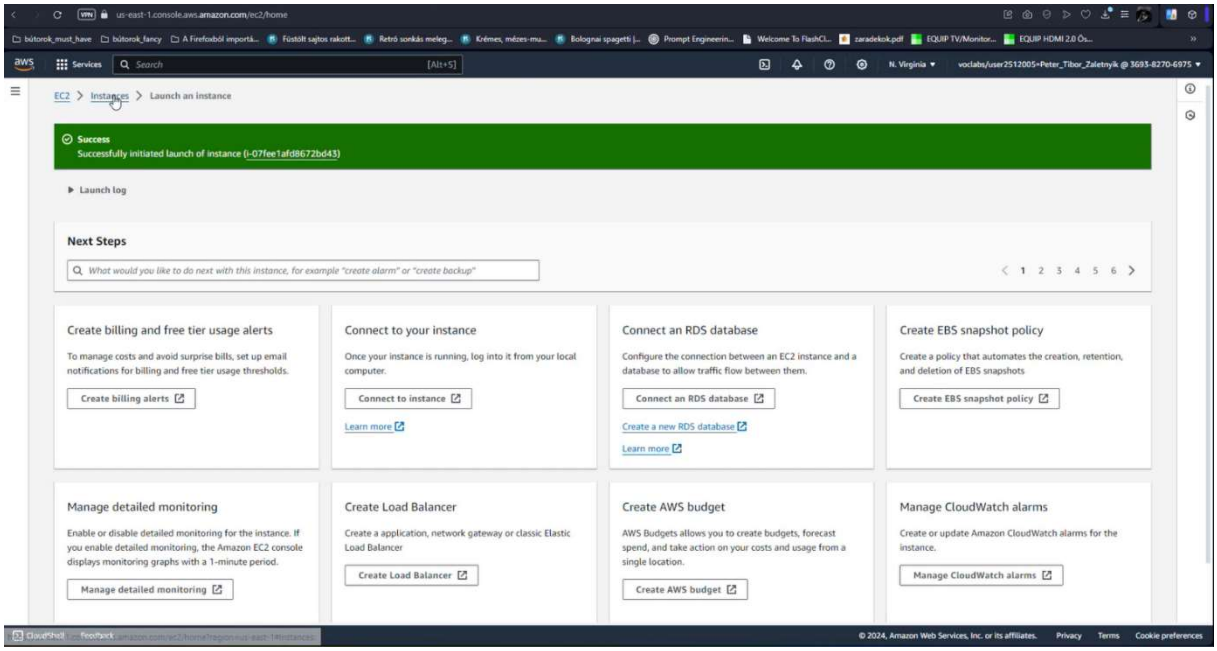
Kiválasztjuk a legördülő menüből a generált kulcsot:





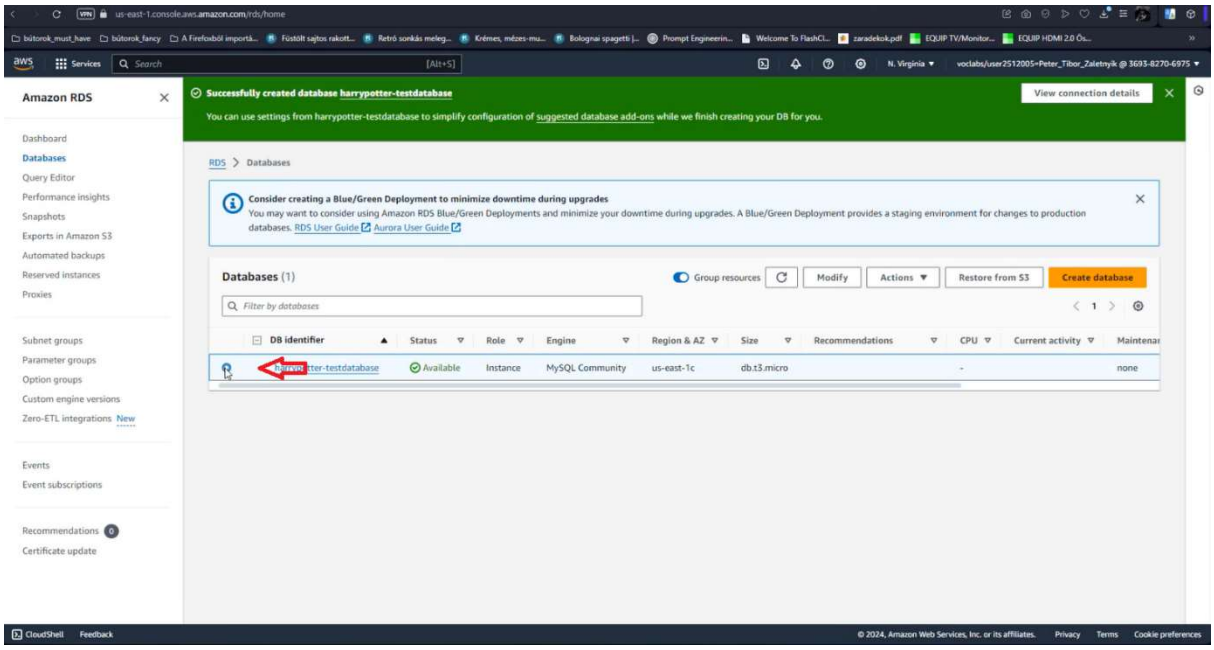


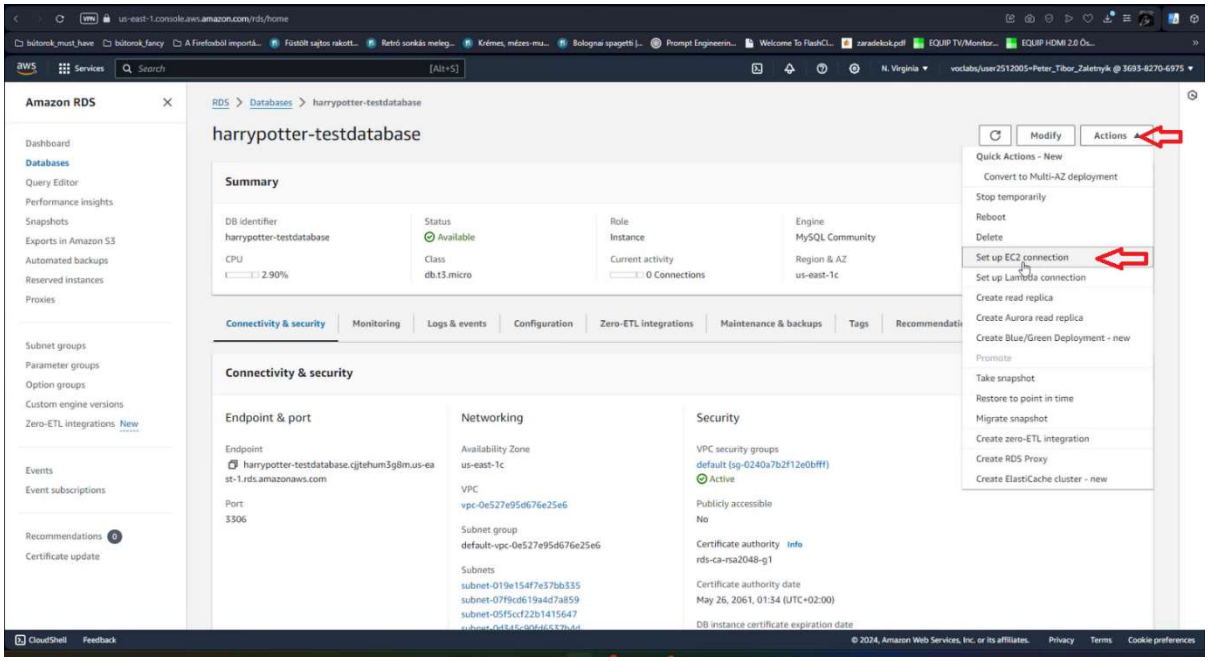
Létrehozta a kért virtuális gépet:

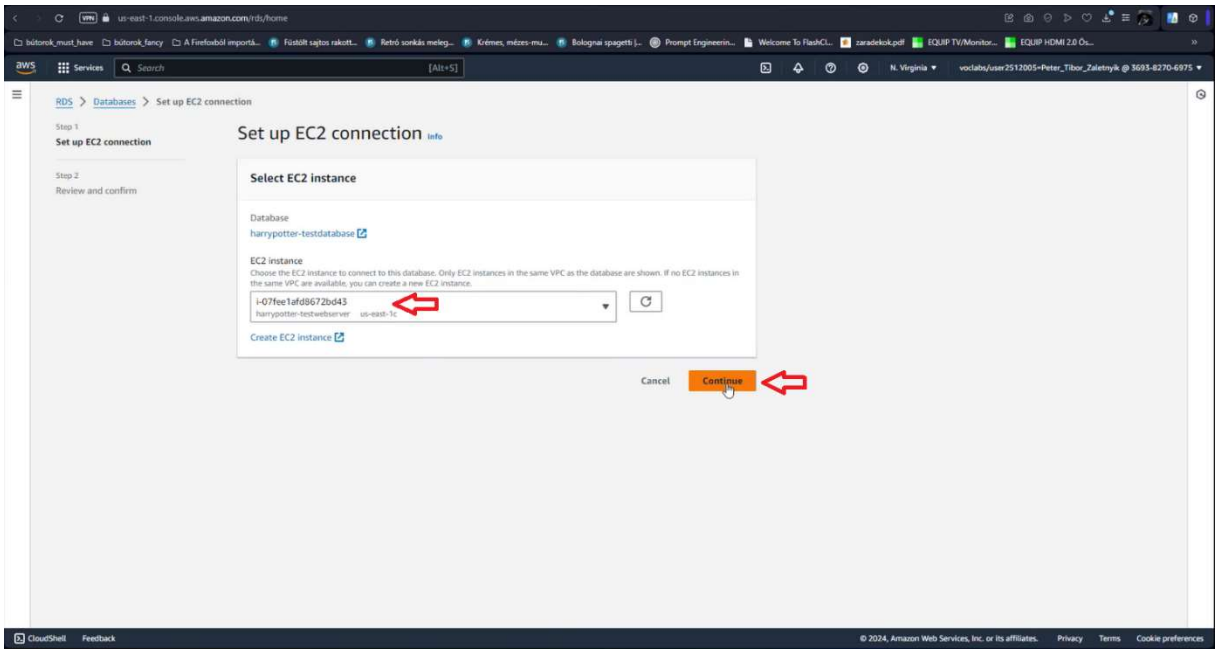


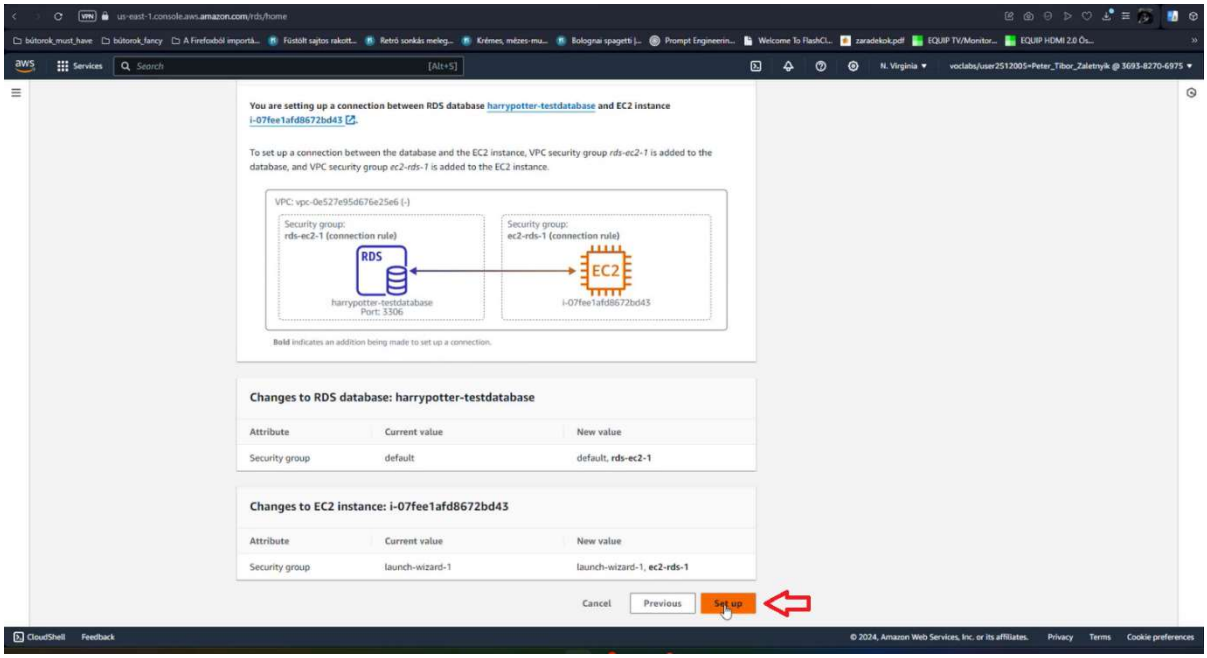
IV. Adatbázis hozzárendelése a létrehozott EC2 virtuális géphez:

Visszalépünk az adatbázis ablakba és kiválasztjuk a létrehozott adatbázist:

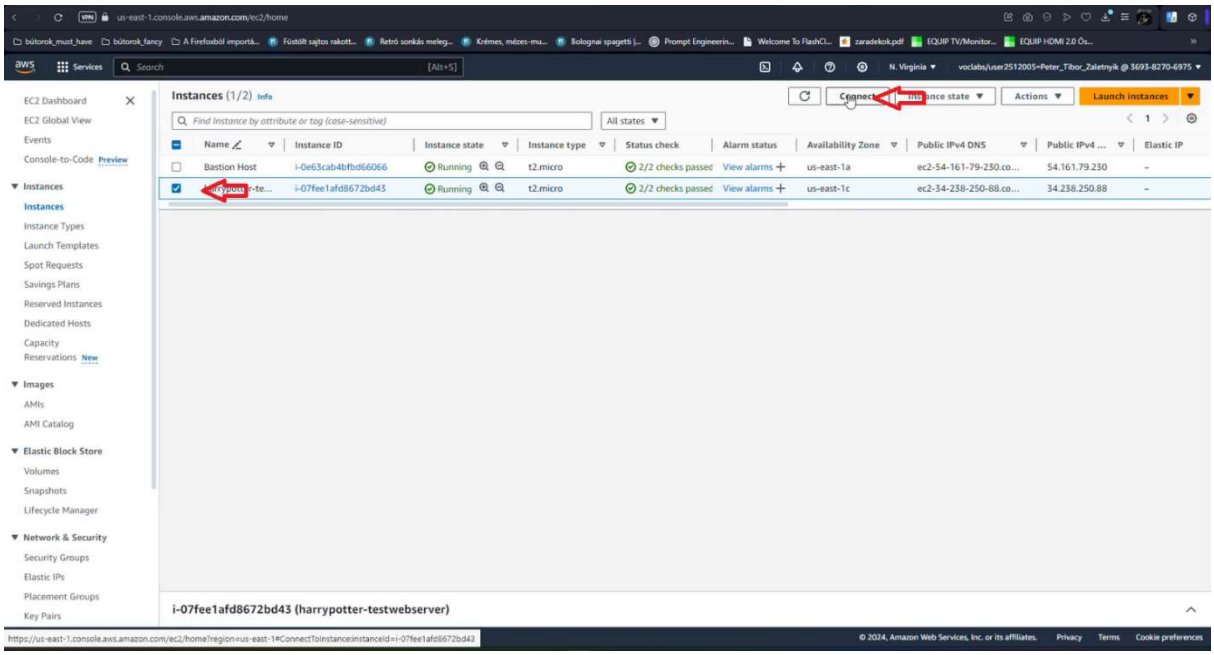


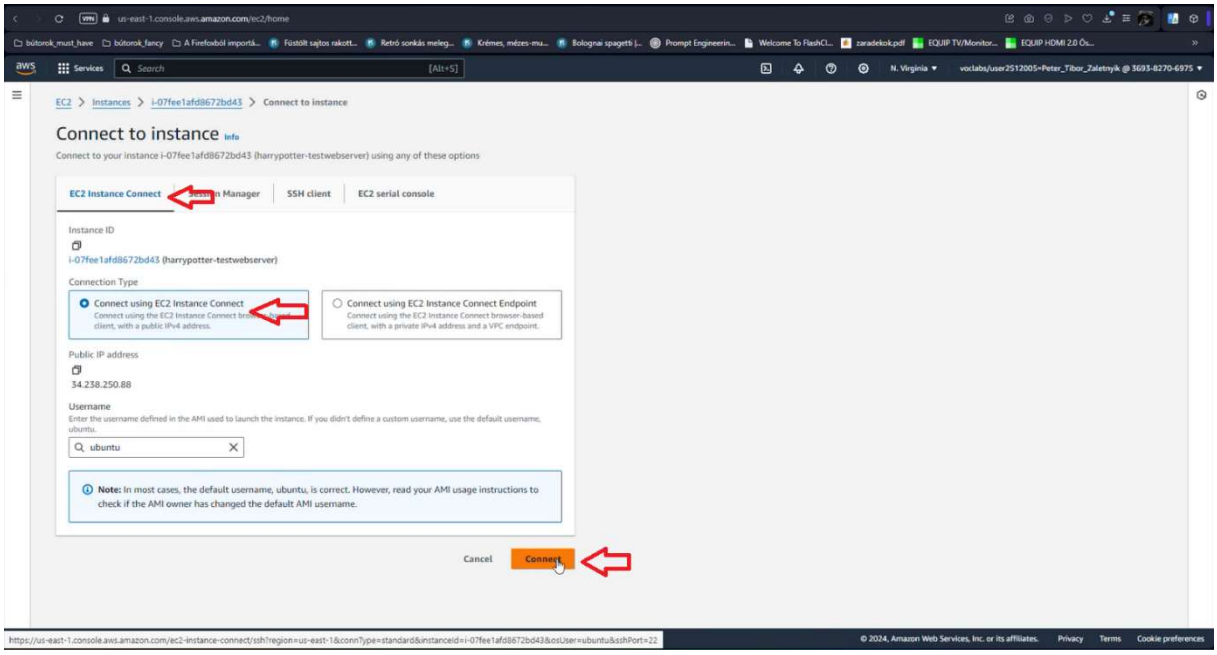



RDS > Databases > Set up EC2 connection
Step 1
Set up EC2 connection
Step 2
Review and confirm
Set up EC2 connection info
Select EC2 instance
Database
harrypotter-testdatabase
EC2 instance
Choose the EC2 instance to connect to this database. Only EC2 instances in the same VPC as the database are shown. If no EC2 instances in the same VPC are available, you can create a new EC2 instance.
i-07fee1afd8672bd43
harrypotter-testwebserver us-east-1c
Create EC2 instance
Cancel
Continue


You are setting up a connection between RDS database harrypotter-testdatabase and EC2 instance i-07fee1afd8672bd43.
To set up a connection between the database and the EC2 instance, VPC security group rds-ec2-1 is added to the database, and VPC security group ec2-rds-1 is added to the EC2 instance.
VPC: vpc-0e527e95d676e25e6 (-)
Security group: rds-ec2-1 (connection rule)
Security group: ec2-rds-1 (connection rule)
RDS
EC2
harrypotter-testdatabase
Port: 3306
i-07fee1afd8672bd43
Bold indicates an addition being made to set up a connection.
Changes to RDS database: harrypotter-testdatabase
Attribute
Current value
New value
Security group
default
default, rds-ec2-1
Changes to EC2 instance: i-07fee1afd8672bd43
Attribute
Current value
New value
Security group
launch-wizard-1
launch-wizard-1, ec2-rds-1
Cancel
Previous
Set up

Amennyiben megjelenik a gép a listában már csatlakozhatunk hozzá:





És be is jelentkeztünk a virtuális gépünkbe: