

Security



Nuri Halperin

@nurih | www.plusnconsulting.com

Mongo V3

Basic
Authentication

Robust
Authorization

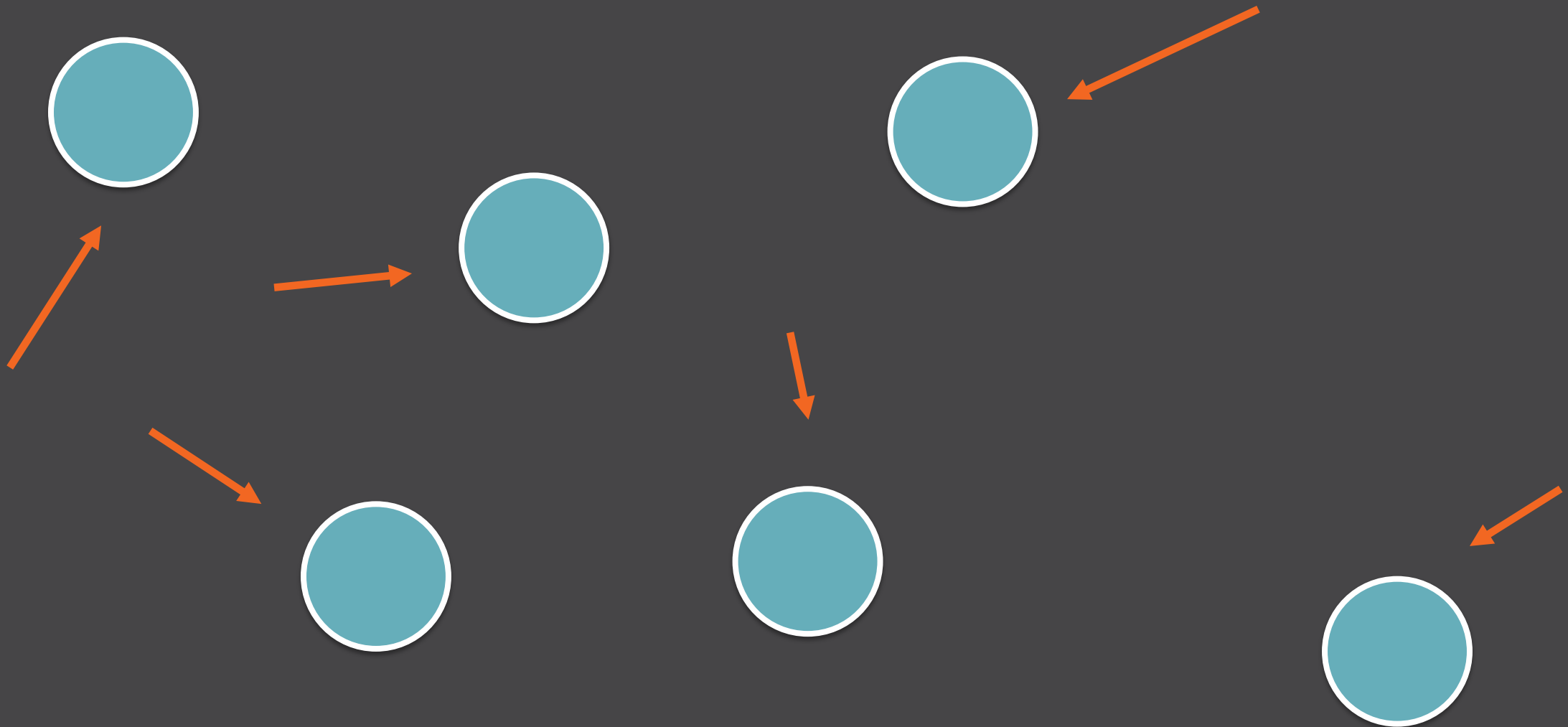
SSL

Server-Server
Authentication

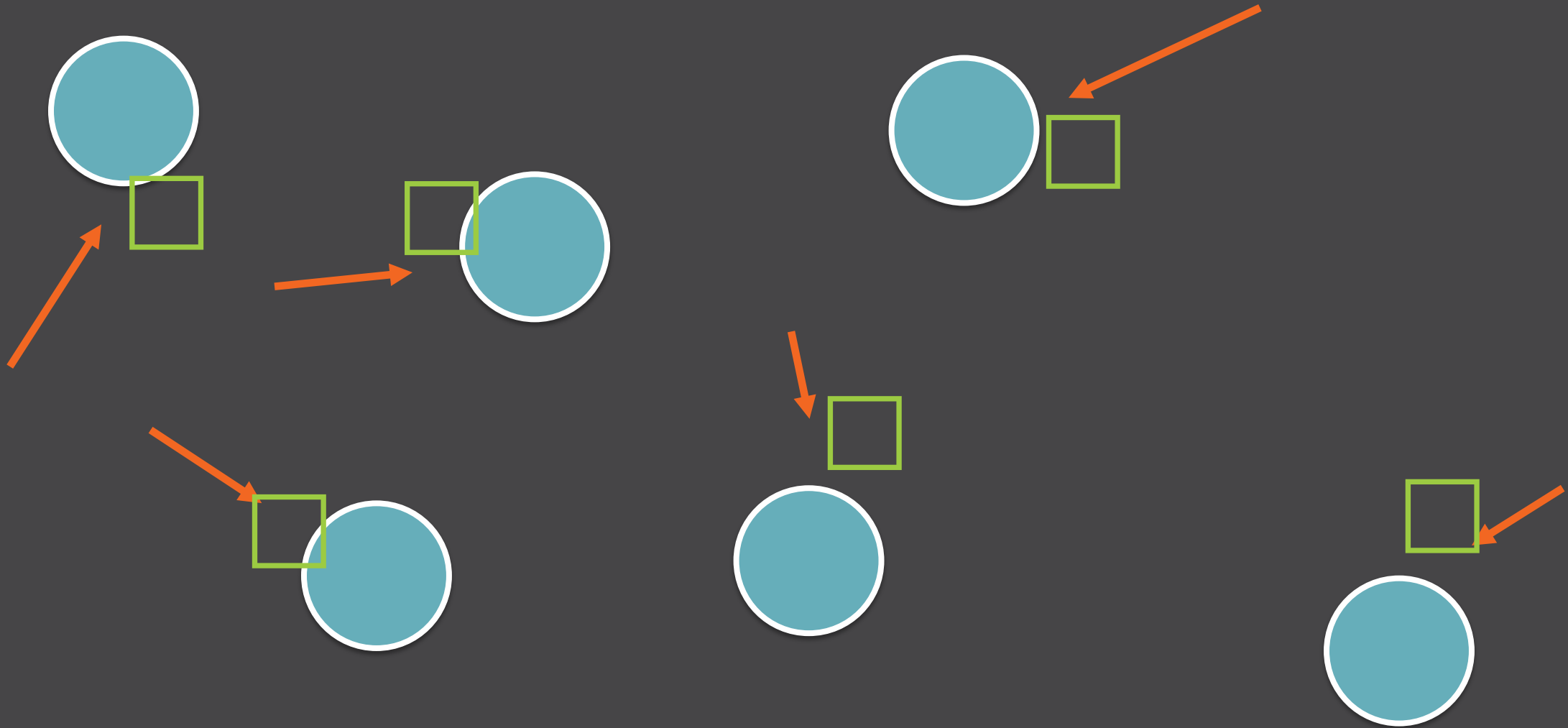
LDAP / Kerberos

Encryption
At Rest

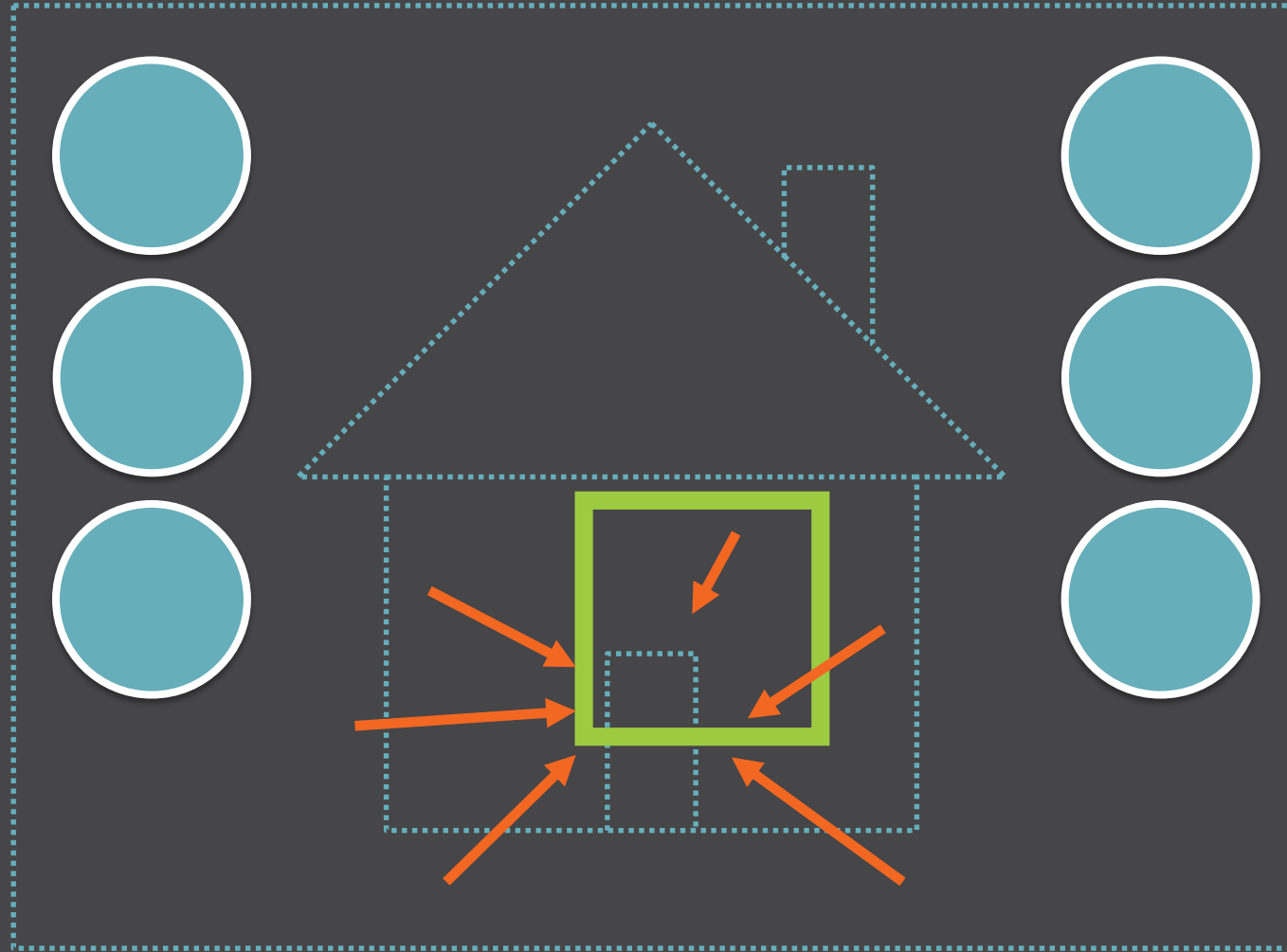
Surface Area



Surface Area



Surface Area



Surface Dimensions

Network

Storage

Access

Network Ports

Process	Role	Default Port
mongod	Stand-alone	27017
	--shardsvr	27018
	--configsvr	27019
mongos	N/A	27017
mongod	Status page (off)	+1000

Network Ports

- ☐ Port Obfuscation
- ☒ Port Restriction (firewall etc.)

Process	Role	Default Port
mongod	Stand-alone	27017
	--shardsvr	27018
	--configsvr	27019
mongos	N/A	27017
mongod	Status page (off)	+1000



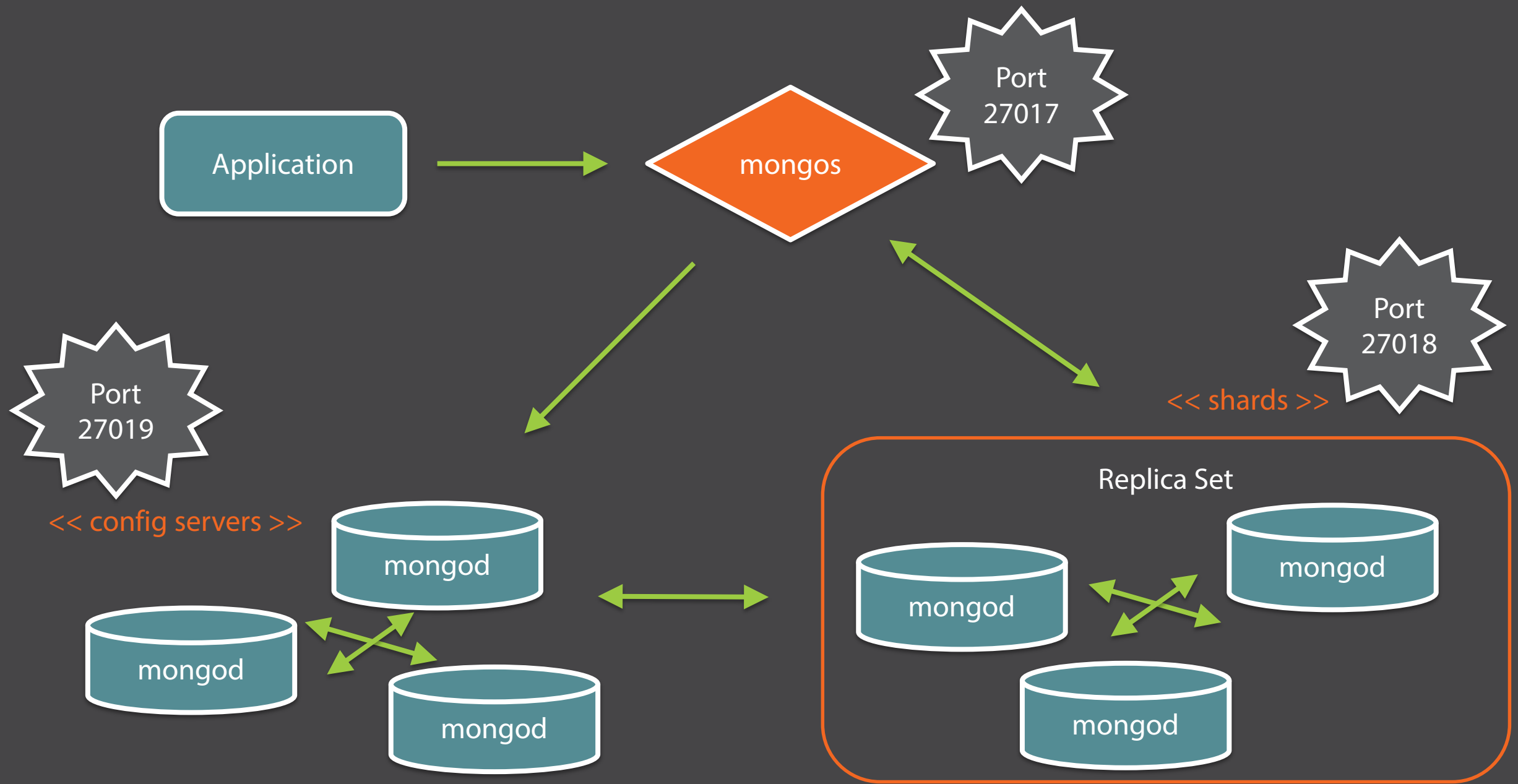
Firewall Rules

- Source Address (Client application)
- Destination Address (Mongo)
- Destination Port

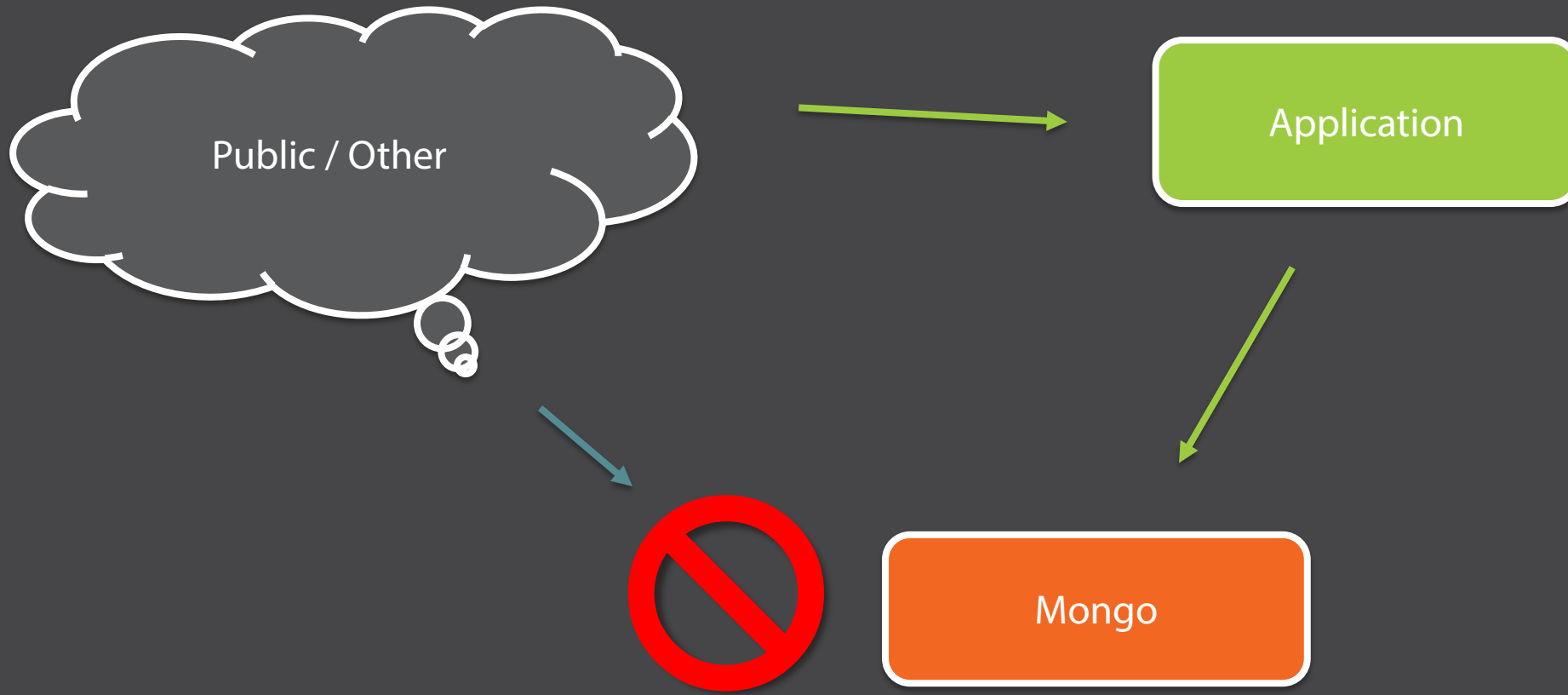


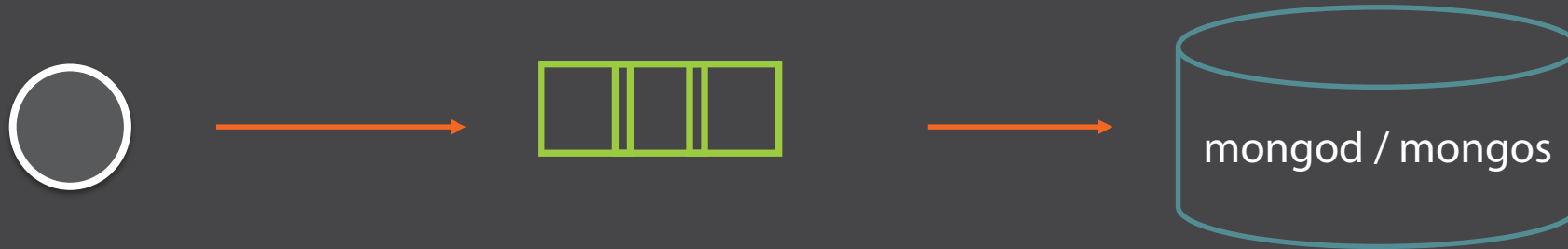
Mongo Server IP Address

- Use ***bindIp*** configuration option
- Bind to minimum necessary on multi-IP server



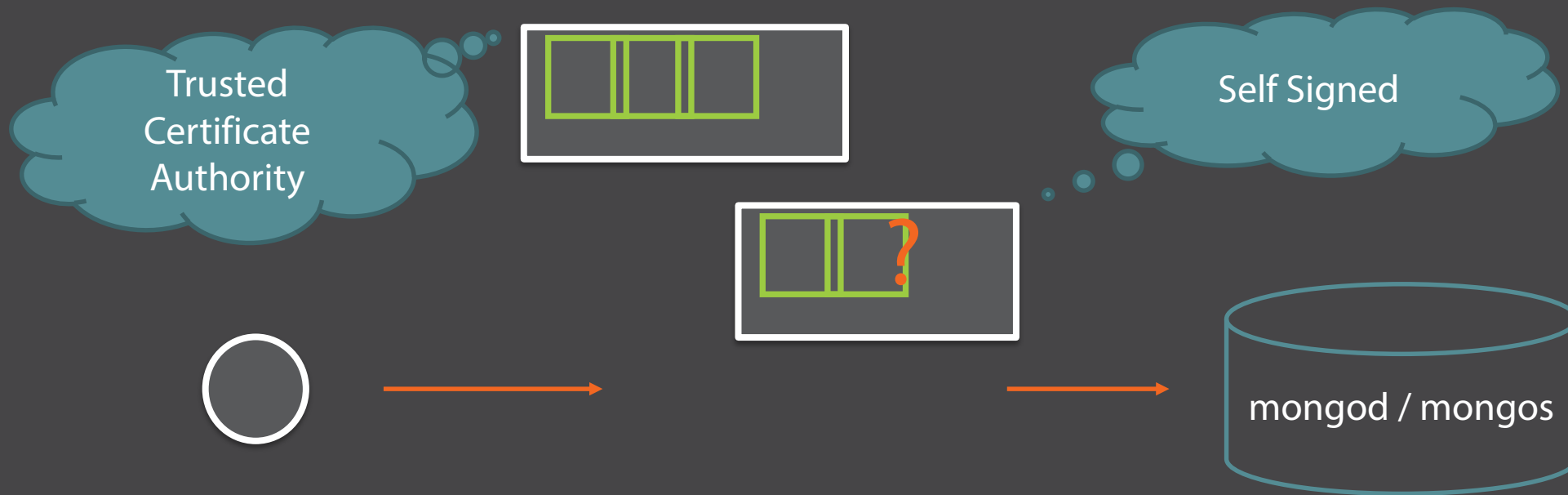
No Public Direct Access!





SSL Support

- Tamper Evident
- Encryption
- Connected Party Validation



SSL Support

- Tamper Evident
- Encryption
- Connected Party Validation

```
mode: [ requireSSL | allowSSL | preferSSL | disabled ]
```

SSL Mode

- Disabled by default

Data File Protection



Actual Files

File Content

Data File Protection

Actual Files

- Set Permissions

File Content

Data File Protection

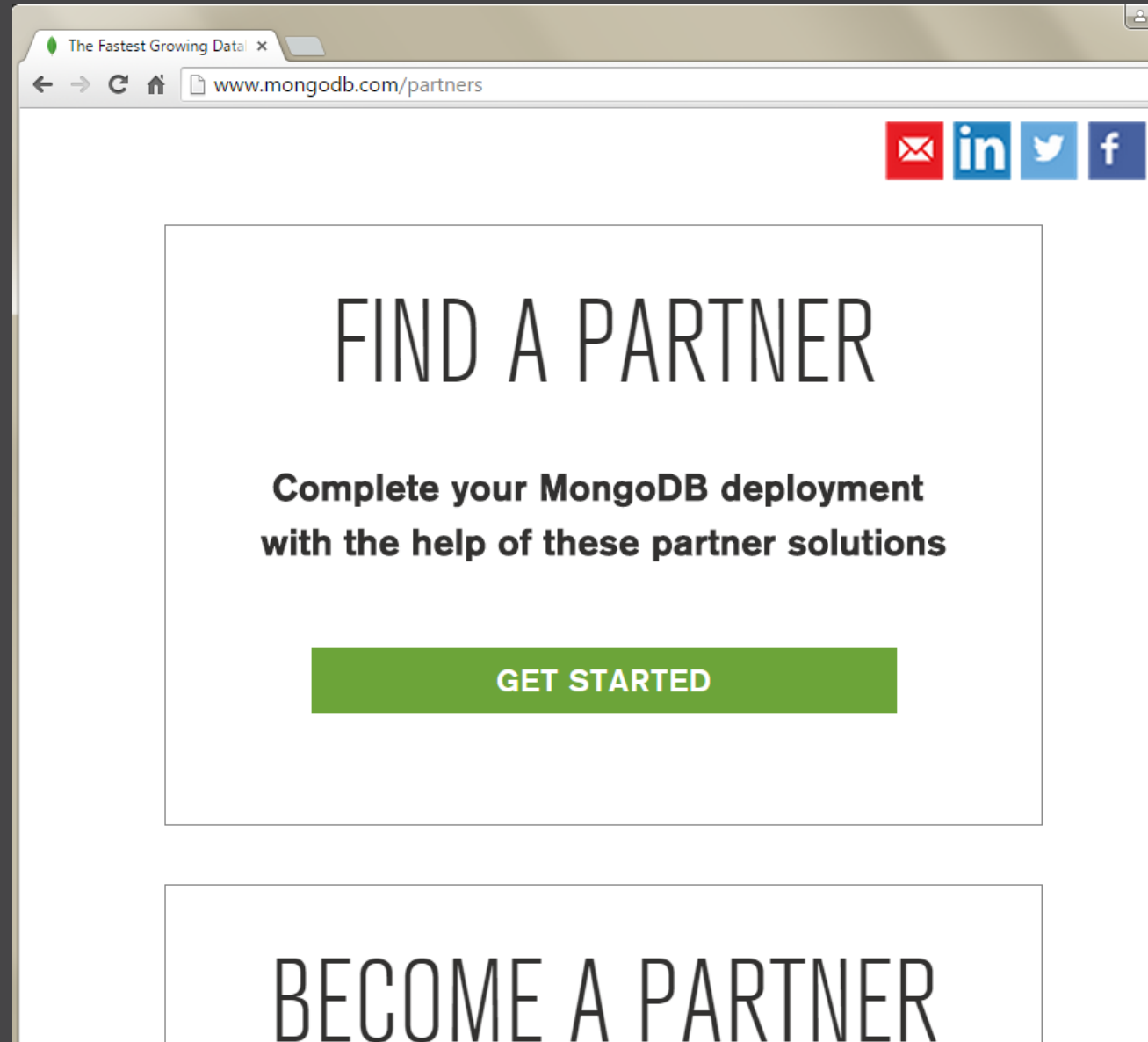
Actual Files

- Set Permissions

File Content

- Encryption at rest
- Field data encryption

mongodb.com/partners



Who's There?



Authentication & Authorization

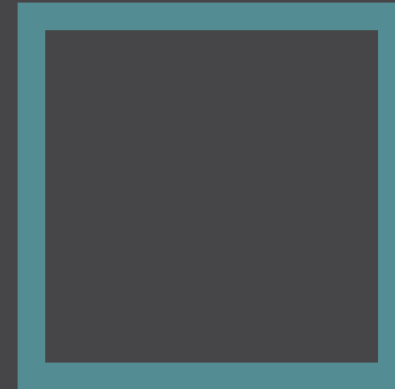
"Who Are You?"

"Bob"

"What do you want?"

"Read Collection"

"OK"

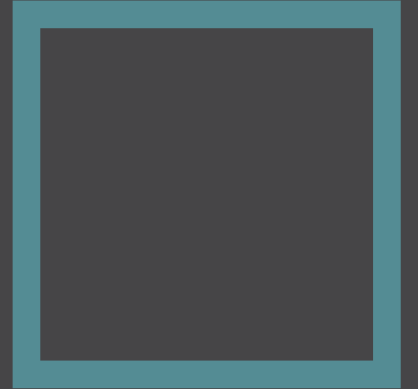


Authorization

Read Collection	Write Document
List Collections	Create User
Create Database	Backup
Restore	Administer Shards
Kill Cursor	...

"What do you want?"

"Read Collection"



Roles

readWrite

- Read Collection
- Write Document
- List Collections
- ...

userAdmin

- Create User
- Grant User Permissions
- Create Role
- ...

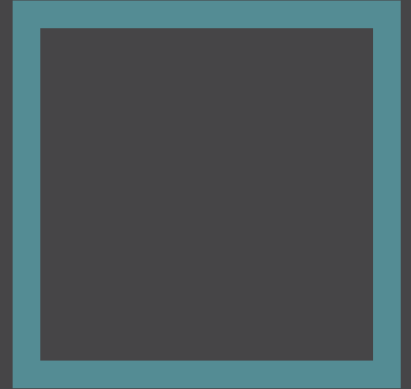
dbAdmin

- dbStats
- repairDatabase
- ...

...

"What do you want?"

"Read Collection"



Root

Very powerful!

Use with caution!

Give (almost) nobody!

userAdminAnyDatabase

Very powerful!

Use with caution!

Create users

Grants permissions

Can "upgrade" self

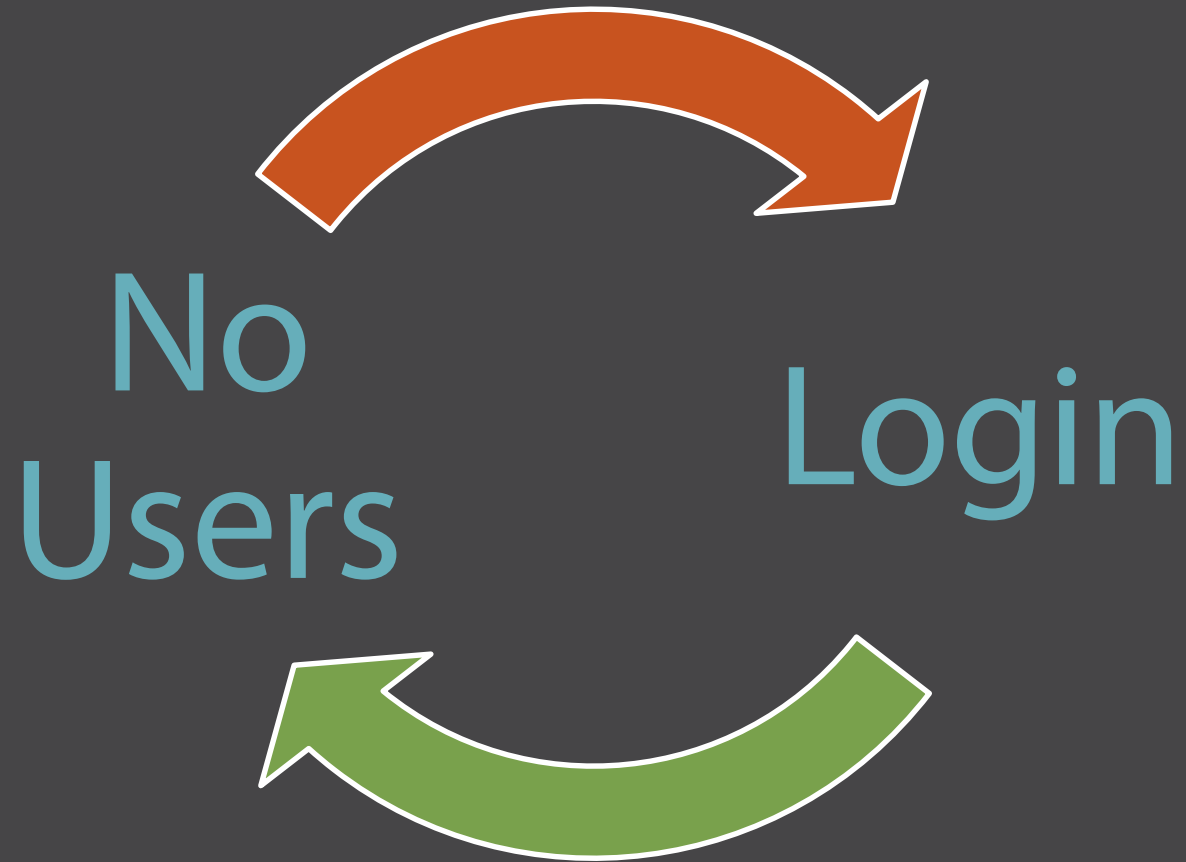
read

Read collections
Database specific

readWrite

Anything "read" can do
+ Write non-system collections
Database specific

Circular Dependency?



```
db.createUser( {...})
```

```
db.dropUser("bob")
```

Role expressed as object:
Applies to 'myDB'

```
db.grantRolesToUser("bob", [{db: "myDB", role: "read"}])
```

```
db.revokeRolesFromUser("bob", ["read"])
```

Role expressed as string:
Applies current db

User Management Functions

Run as userAdmin or as userAdminAnyDatabase

Role can be specified as bare string or object

```
> db.createUser( {...})  
> db.grantRolesToUser("bob", [{db: "myDB", role:"read"}])  
> db.logout("bob")  
> db.auth("bob", "1234")
```

```
// cmd line
```

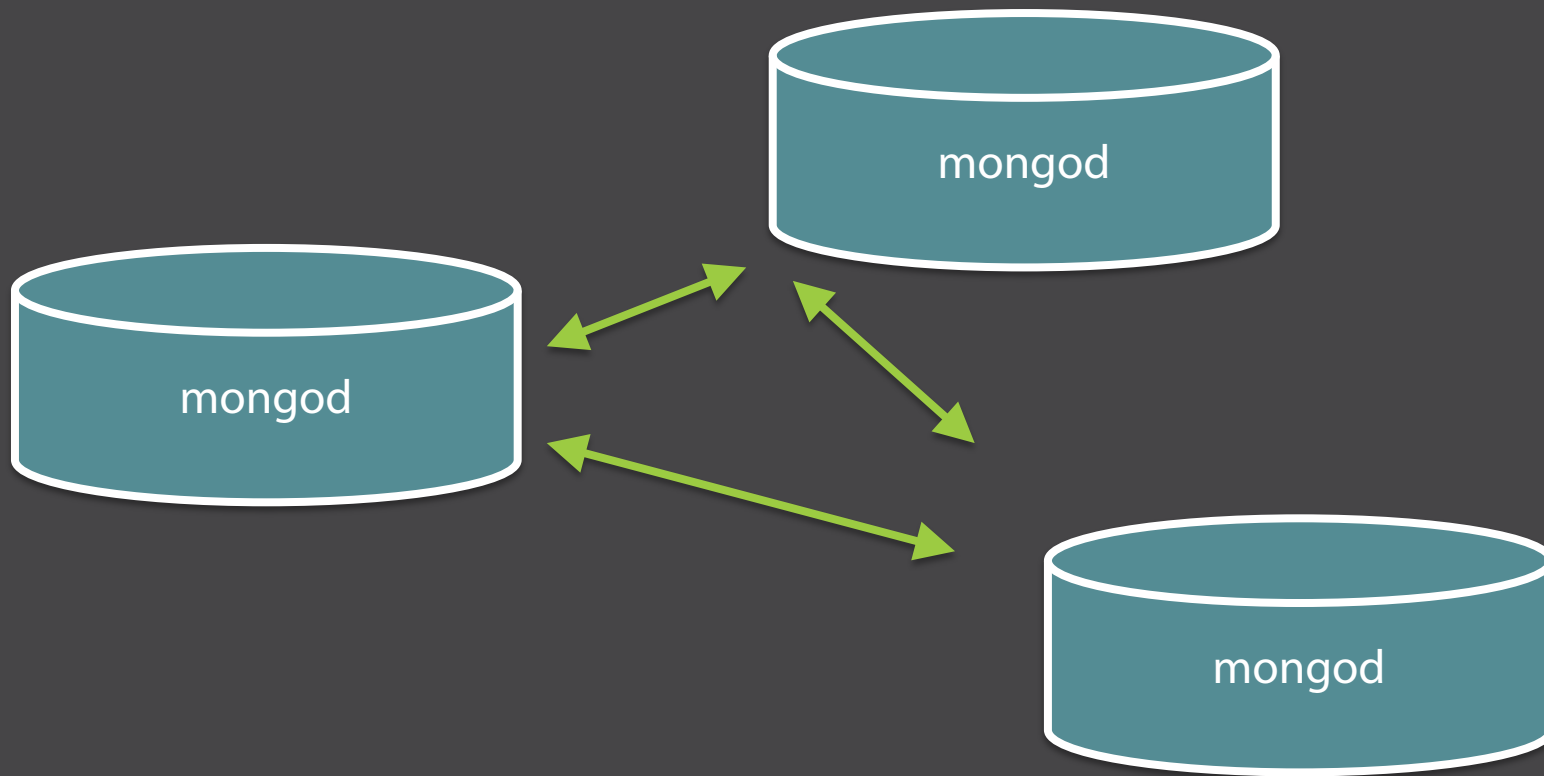
```
mongo --username bob --password 1234 --authenticationDatabase myDB
```

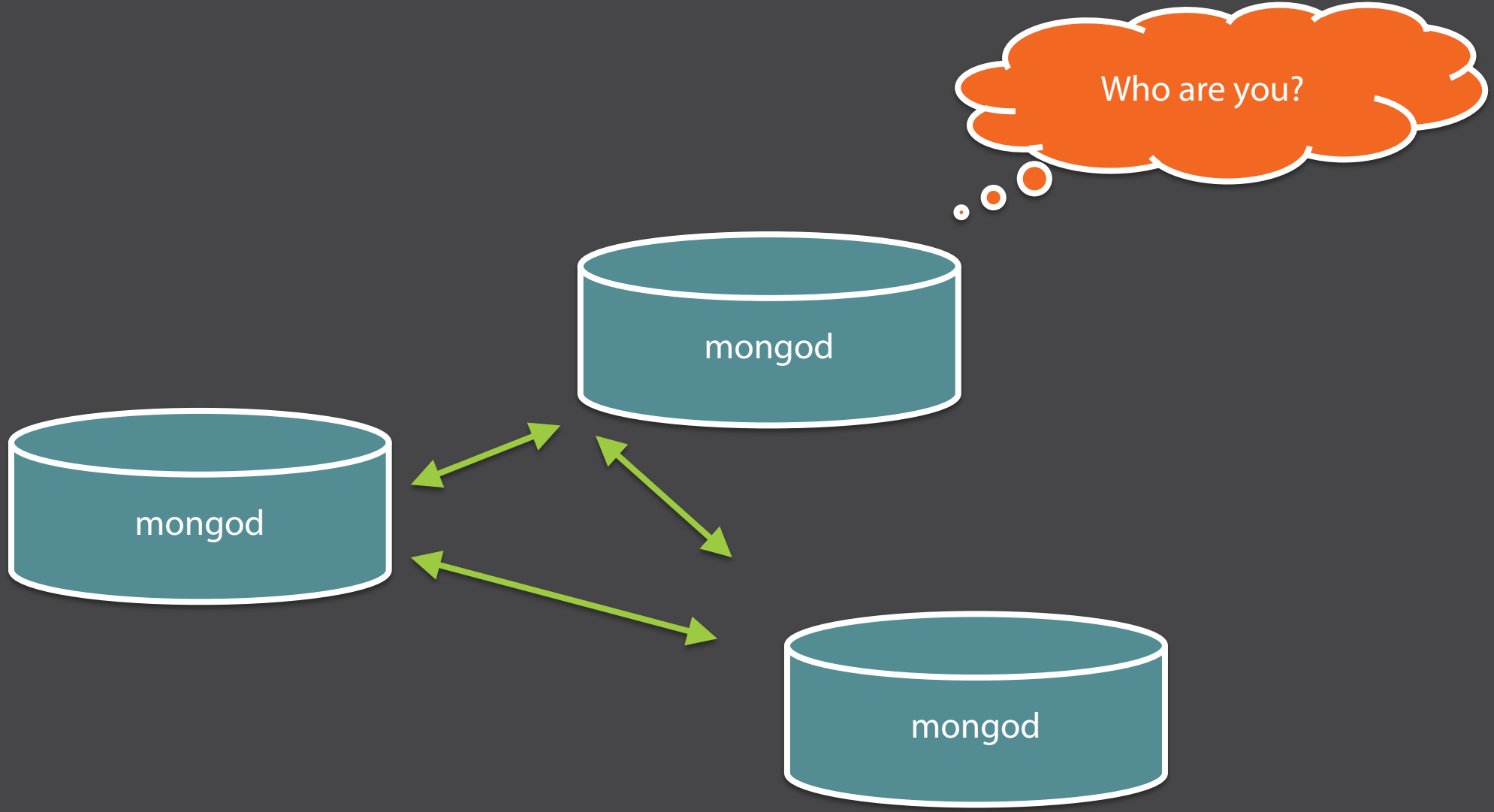
Authentication & Authorization

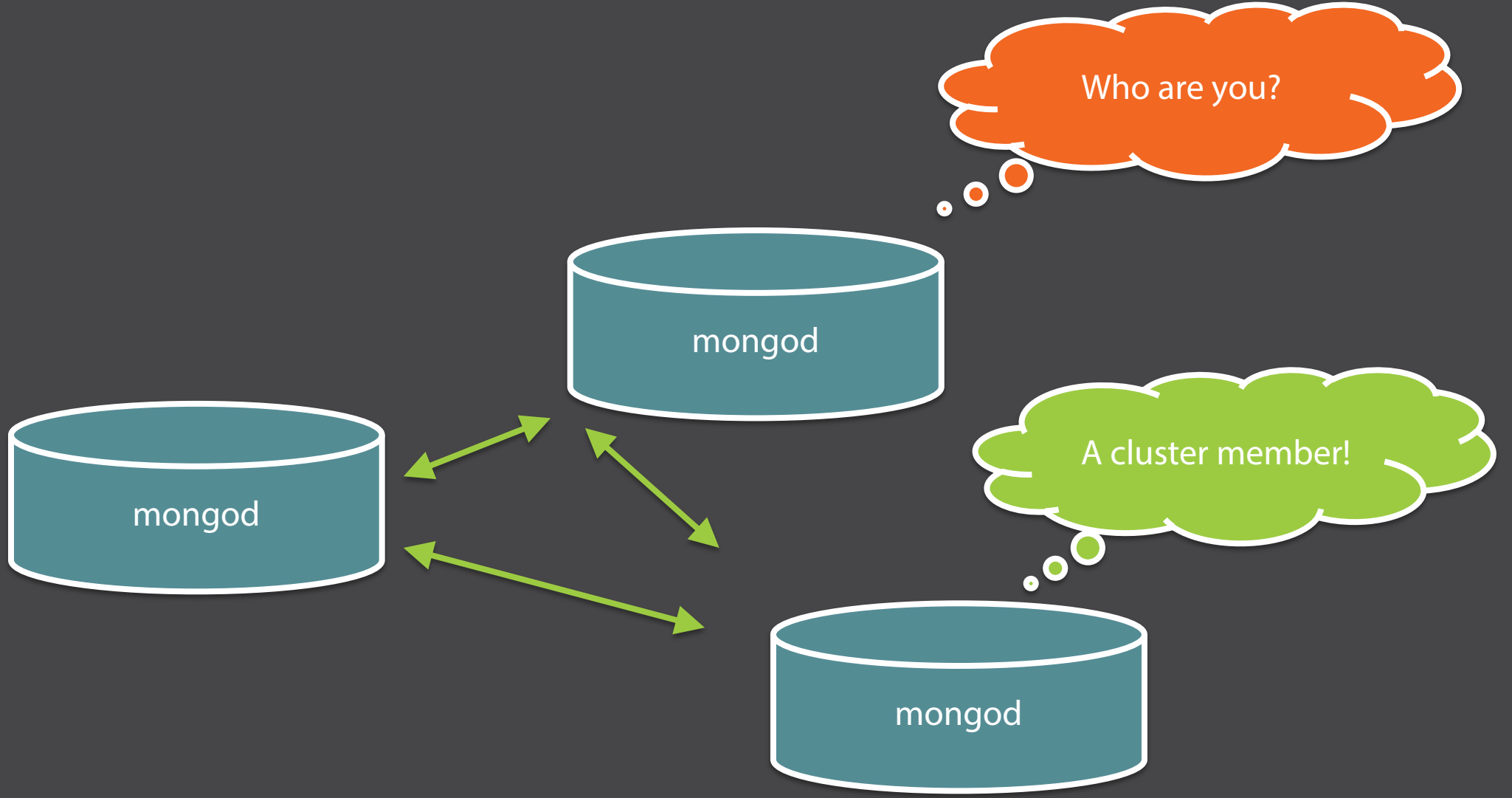
Run as userAdmin or as userAdminAnyDatabase

Use strong passwords

Don't share credentials









What's the secret key?

Here's my secret key.

Let me compare to mine.

Yours matches mine!



Key File

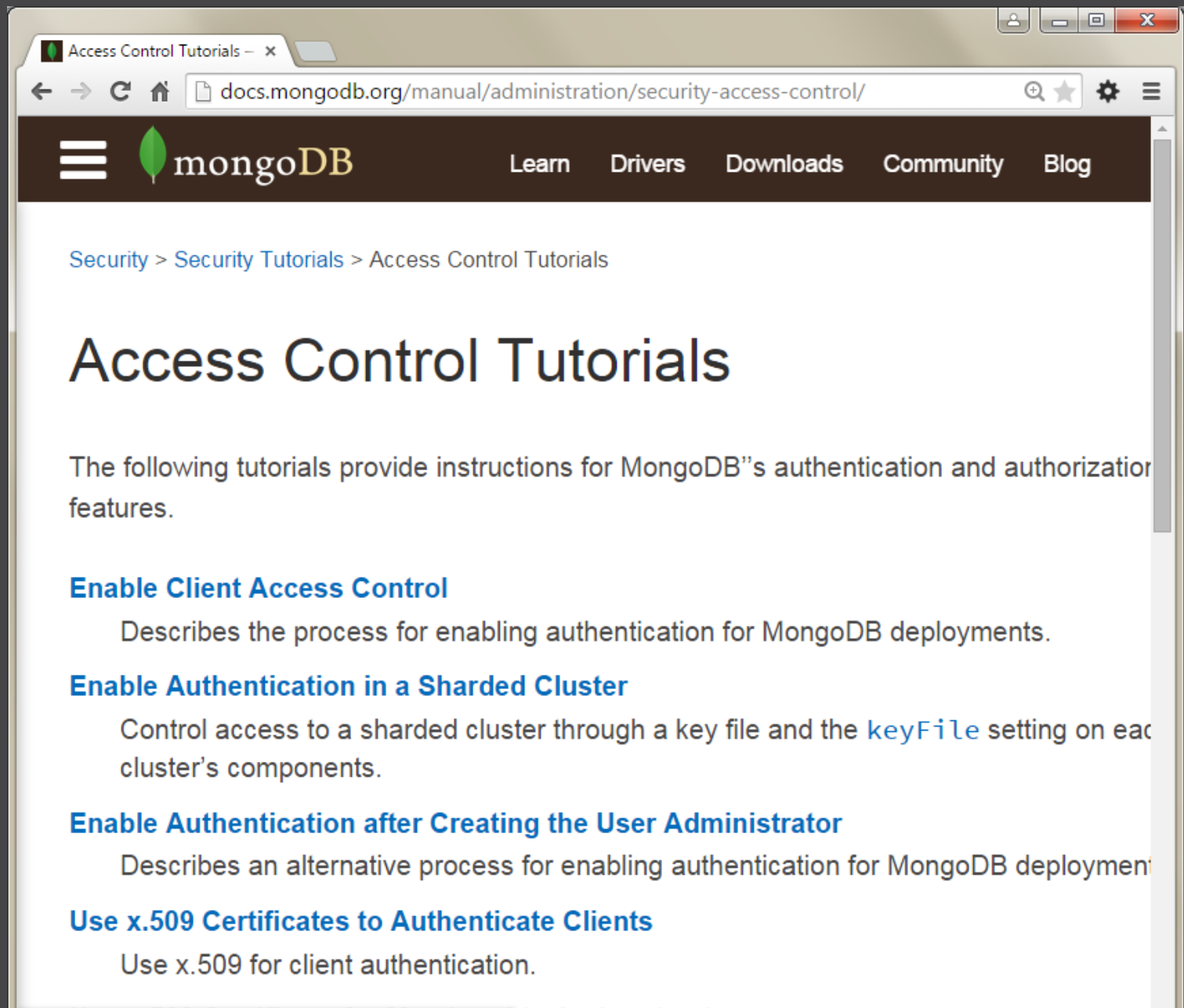


Arbitrary content

6 – 1024 characters

Base64 characters only

User-only file read permissions



The screenshot shows a web browser window with the title 'Access Control Tutorials - x'. The address bar displays the URL 'docs.mongodb.org/manual/administration/security-access-control/'. The browser's navigation bar includes back, forward, and search icons. The MongoDB logo is prominently displayed on the left, with navigation links for 'Learn', 'Drivers', 'Downloads', 'Community', and 'Blog' on the right. The breadcrumb trail reads 'Security > Security Tutorials > Access Control Tutorials'. The main heading is 'Access Control Tutorials'. Below it, a paragraph states: 'The following tutorials provide instructions for MongoDB's authentication and authorization features.' A list of four tutorials follows, each with a blue title and a brief description:

- Enable Client Access Control**
Describes the process for enabling authentication for MongoDB deployments.
- Enable Authentication in a Sharded Cluster**
Control access to a sharded cluster through a key file and the `keyFile` setting on each cluster's components.
- Enable Authentication after Creating the User Administrator**
Describes an alternative process for enabling authentication for MongoDB deployment.
- Use x.509 Certificates to Authenticate Clients**
Use x.509 for client authentication.

Summary

