

# EPROSIMA

The  
Middleware  
Experts



## Leveraging Secure Discovery Server in ROS 2

Speaker:

- Eduardo Ponz Segrelles, Project Manager @ eProsimia  
[eduardoponz@eprosima.com](mailto:eduardoponz@eprosima.com)

October 20th, 2023



01

## Motivation

- Out-of-the-box discovery caveats
- Secure deployments



02

## ROS 2 Discovery Server

- Overview
- Configuration options
- Network bandwidth performance



03

## SROS 2 Security capabilities

- Security plugins
- Configuration options
- SROS 2 tooling



04

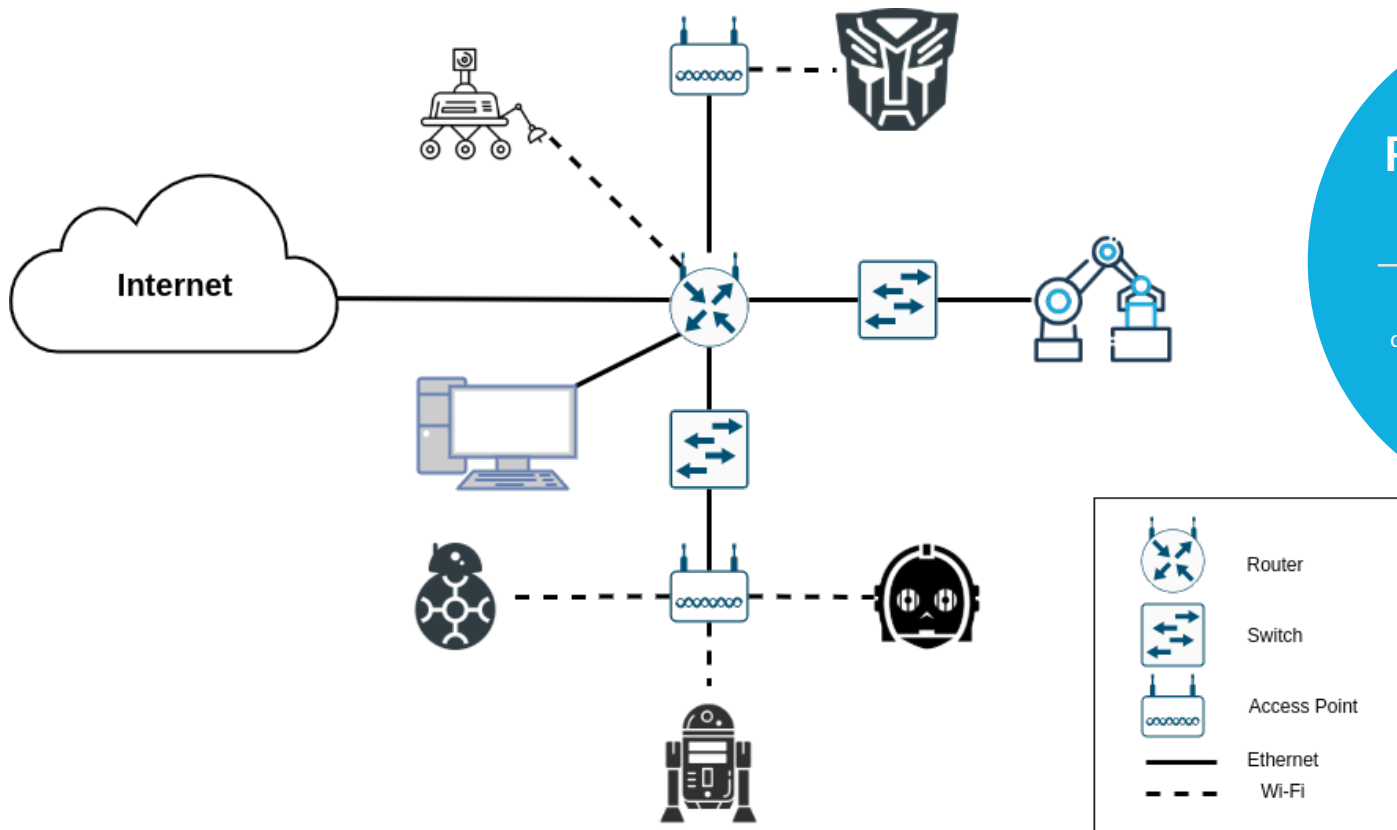
## Deployment example

- Introduction
- Demo



# Motivation

Why using ROS 2 Discovery Server & SROS 2

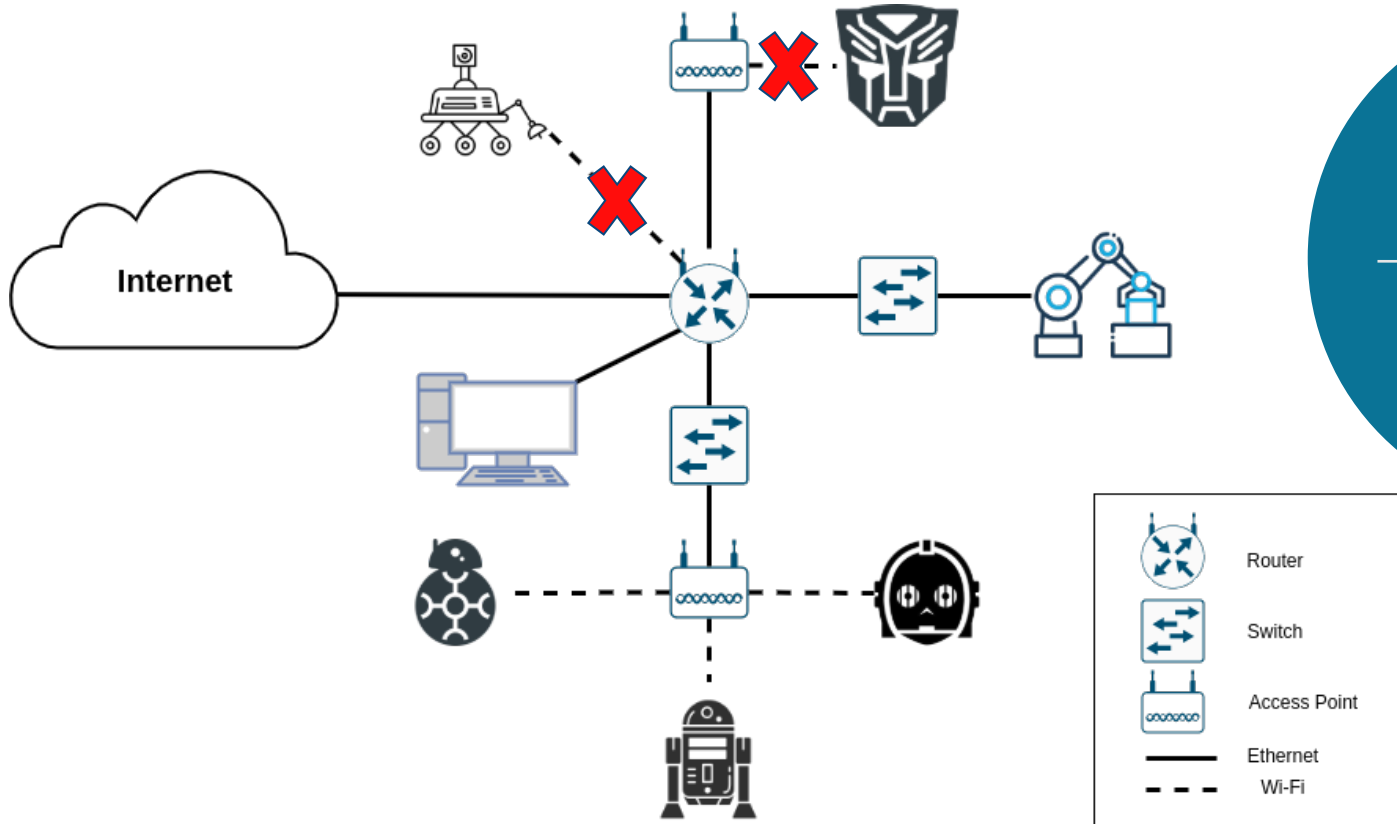


## ROS 2 discovery scalability

Avoid using multicast based discovery and drastically reduce the discovery related traffic by leveraging Discovery Server

# Motivation

Why using ROS 2 Discovery Server & SROS 2



**Secure production deployments**

Properly isolated robots and prevent ill-intentioned external actions on ROS 2 distributed applications



# ROS 2 Discovery Server

---

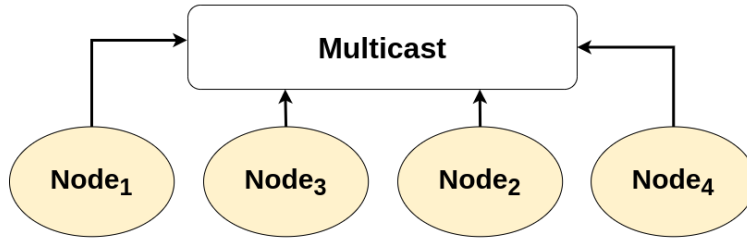
A Fast DDS powered unicast based & centralized discovery mechanism for ROS 2

# ROS 2 Discovery Server

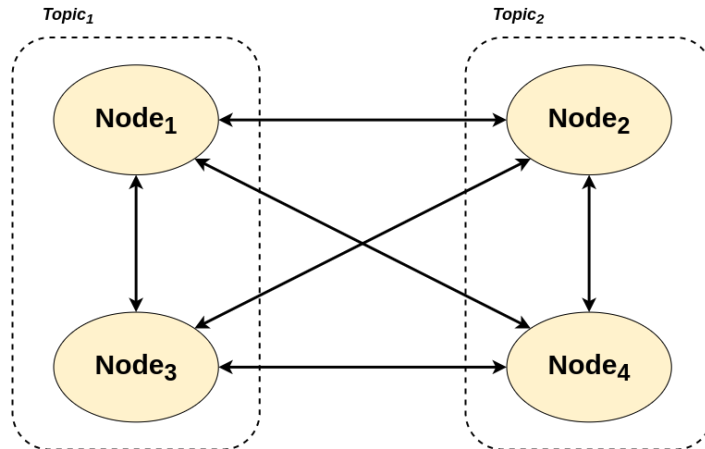
Out-of-the-box discovery (SDP)



## SDP Node Discovery Phase (PDP)



## SDP Topic Discovery Phase (EDP)



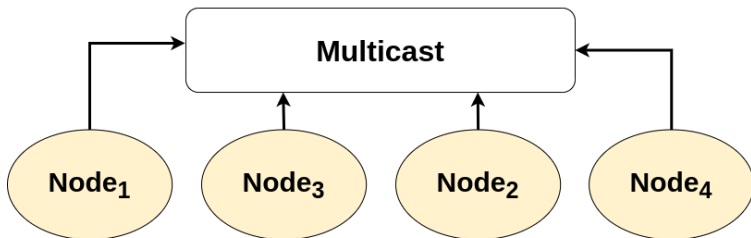


# ROS 2 Discovery Server

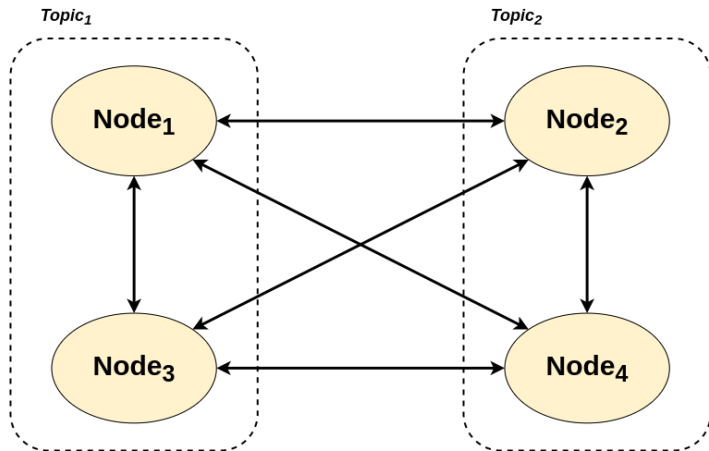
Out-of-the-box discovery (SDP)



## SDP Node Discovery Phase (PDP)



## SDP Topic Discovery Phase (EDP)



1

**No configuration**

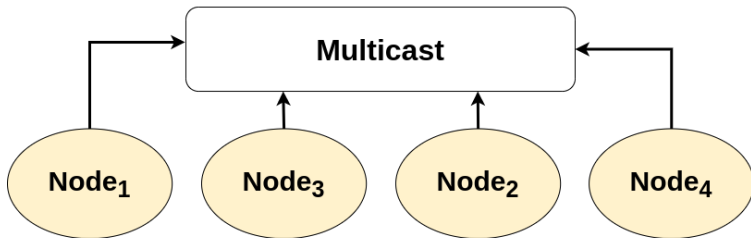
ROS 2 Nodes discover each other automatically

# ROS 2 Discovery Server

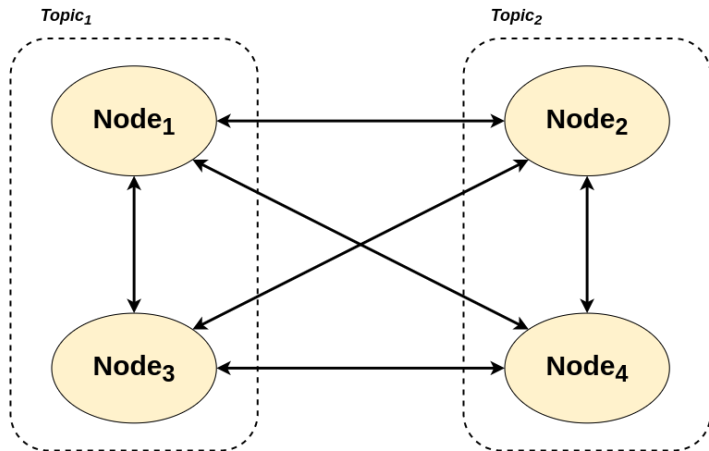
Out-of-the-box discovery (SDP)



## SDP Node Discovery Phase (PDP)



## SDP Topic Discovery Phase (EDP)



1

### No configuration

ROS 2 Nodes discover each other automatically

2

### Traffic heavy

Number of packets increases exponentially with number of ROS 2 contexts

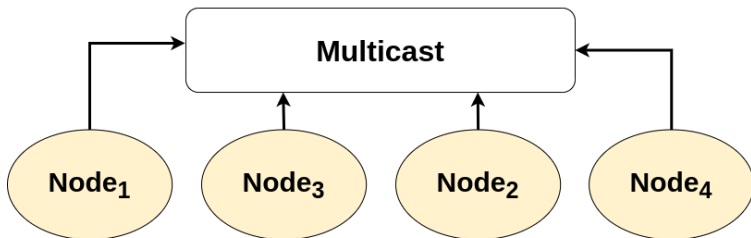


# ROS 2 Discovery Server

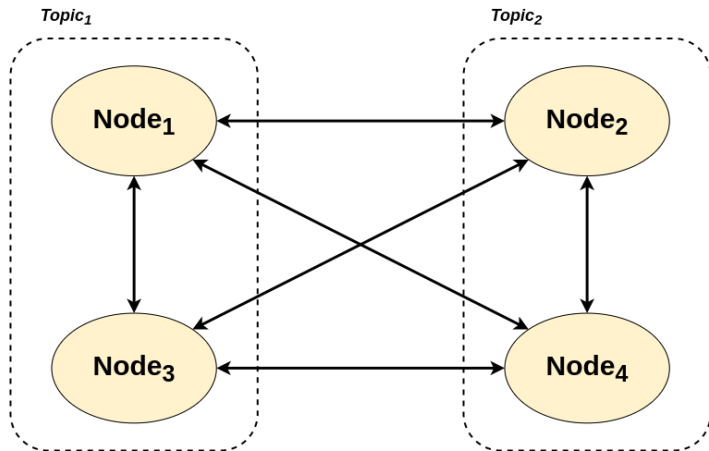
Out-of-the-box discovery (SDP)



## SDP Node Discovery Phase (PDP)



## SDP Topic Discovery Phase (EDP)



1

### No configuration

ROS 2 Nodes discover each other automatically

2

### Traffic heavy

Number of packets increases exponentially with number of ROS 2 contexts

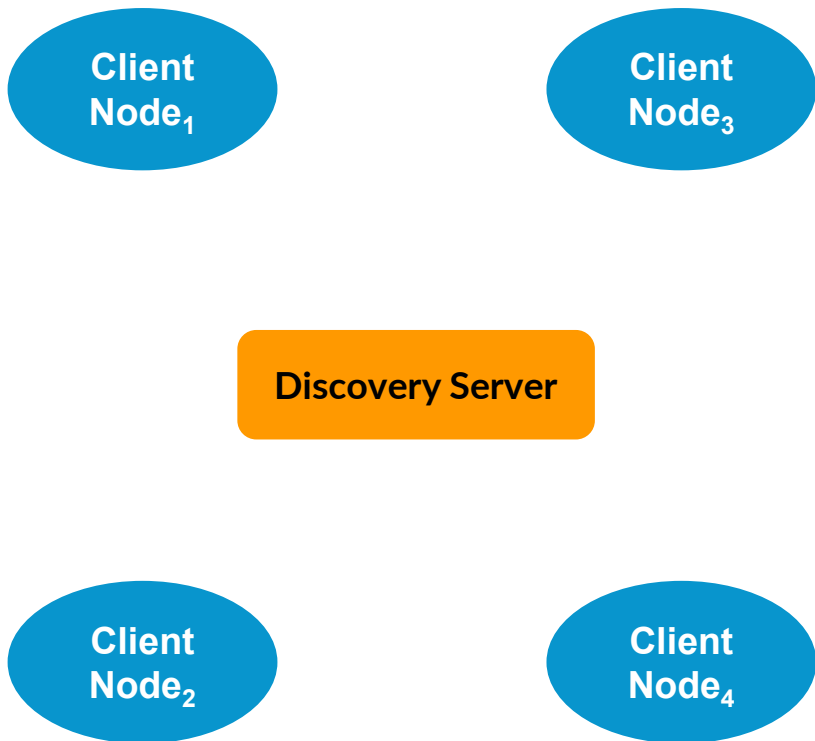
3

### Multicast based

PDP is based on multicast, which may bring problems on WiFi or managed networks

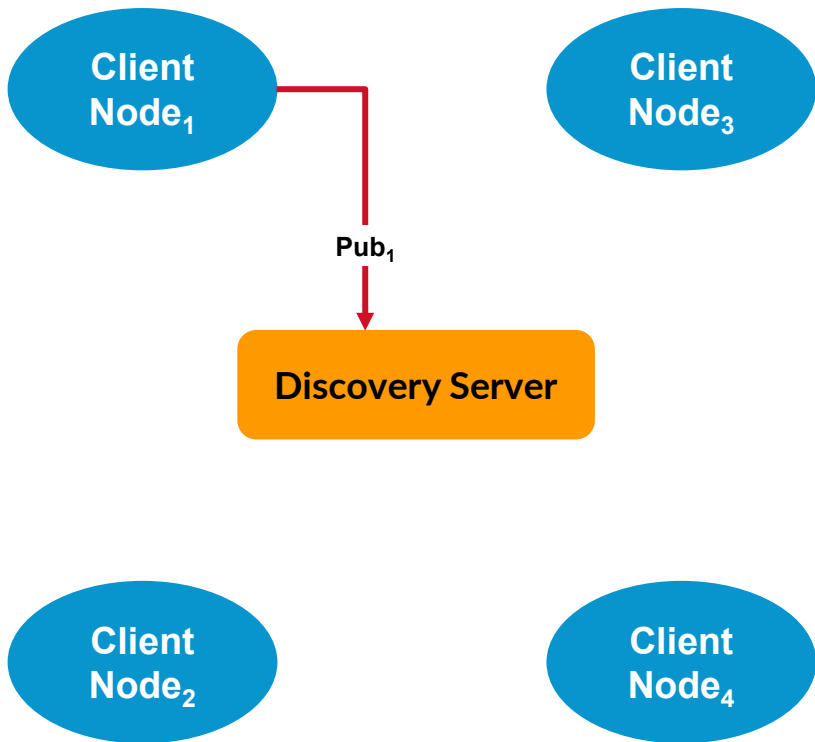
# ROS 2 Discovery Server

*Discovery Server mechanism*



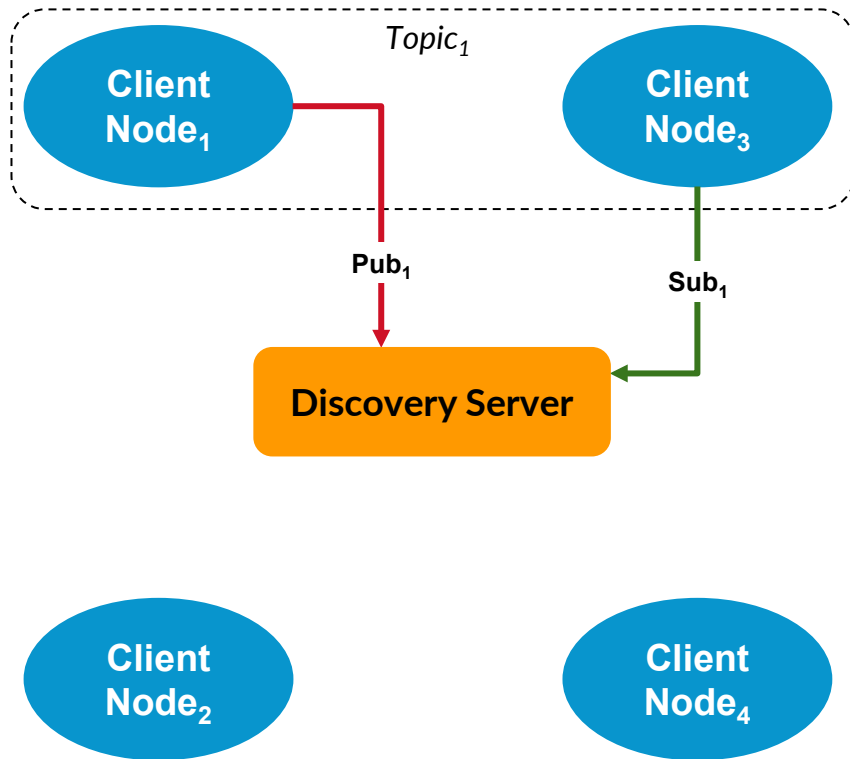
# ROS 2 Discovery Server

Discovery Server mechanism



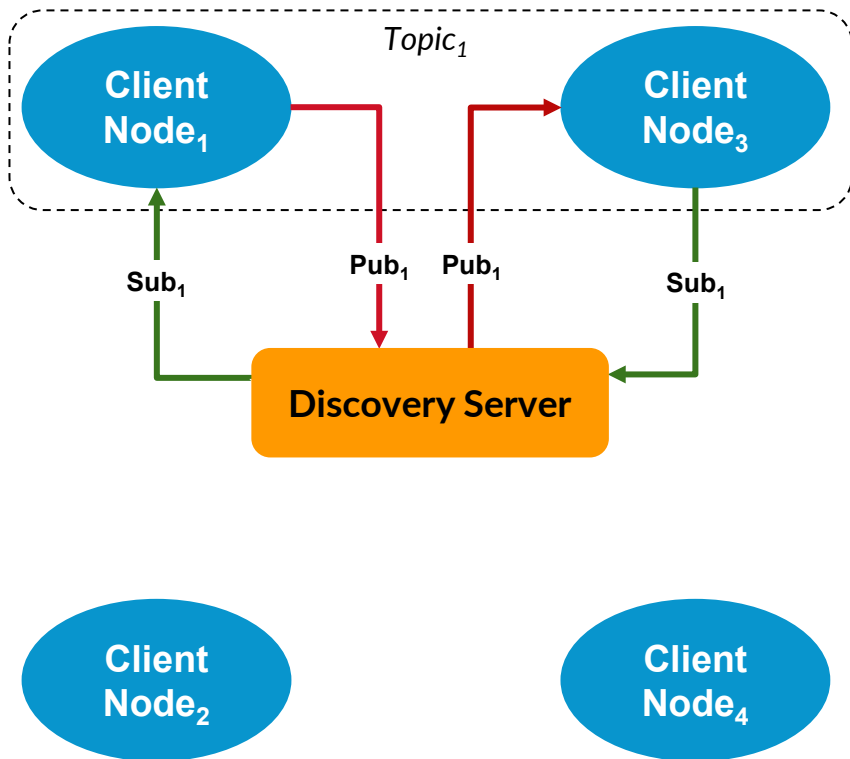
# ROS 2 Discovery Server

Discovery Server mechanism



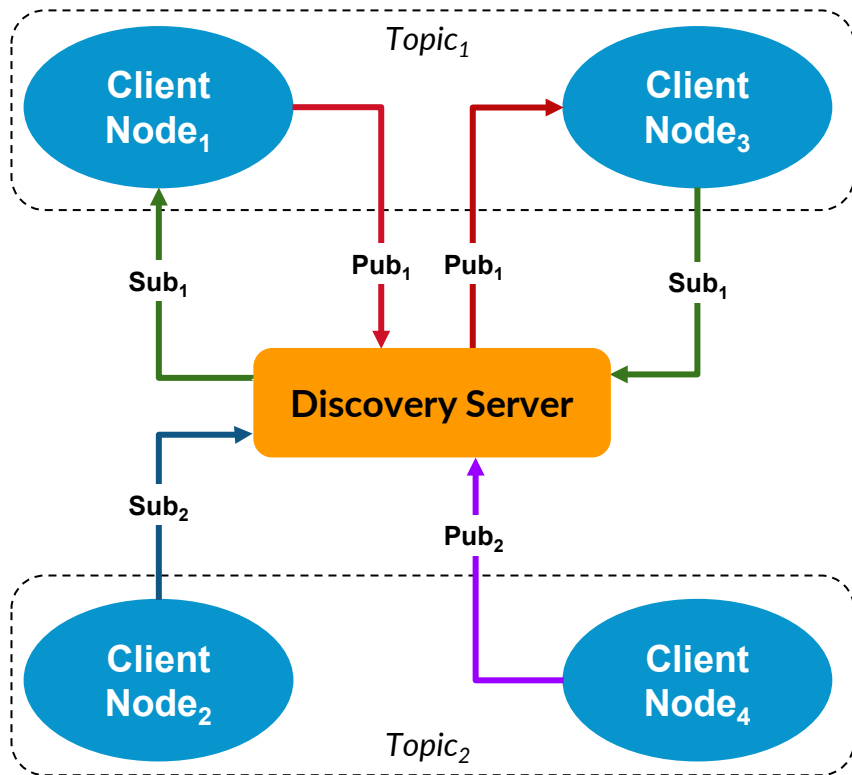
# ROS 2 Discovery Server

Discovery Server mechanism



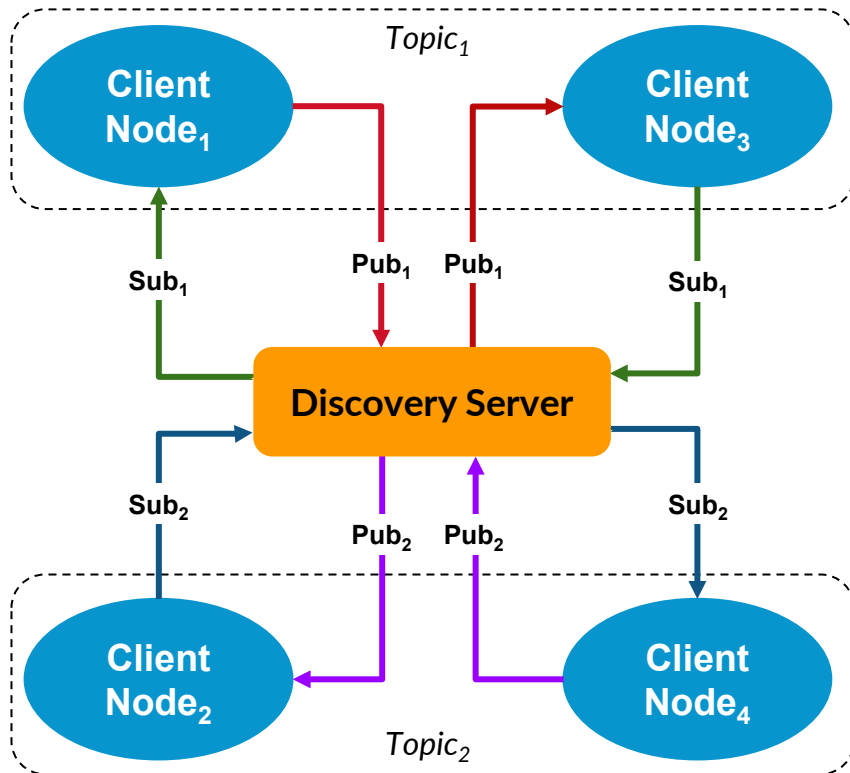
# ROS 2 Discovery Server

Discovery Server mechanism



# ROS 2 Discovery Server

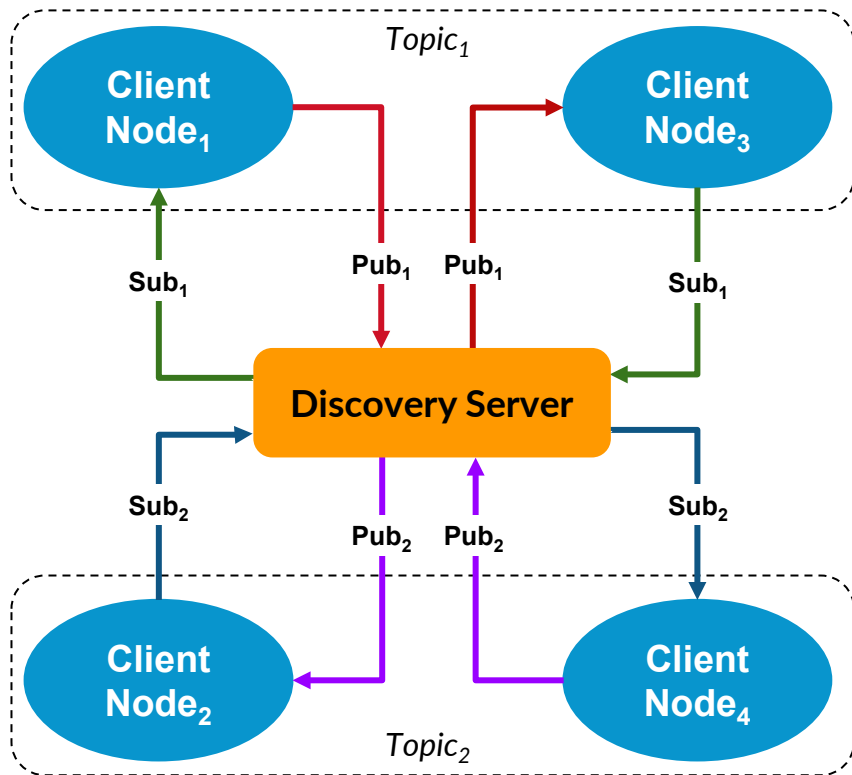
Discovery Server mechanism





# ROS 2 Discovery Server

Discovery Server mechanism



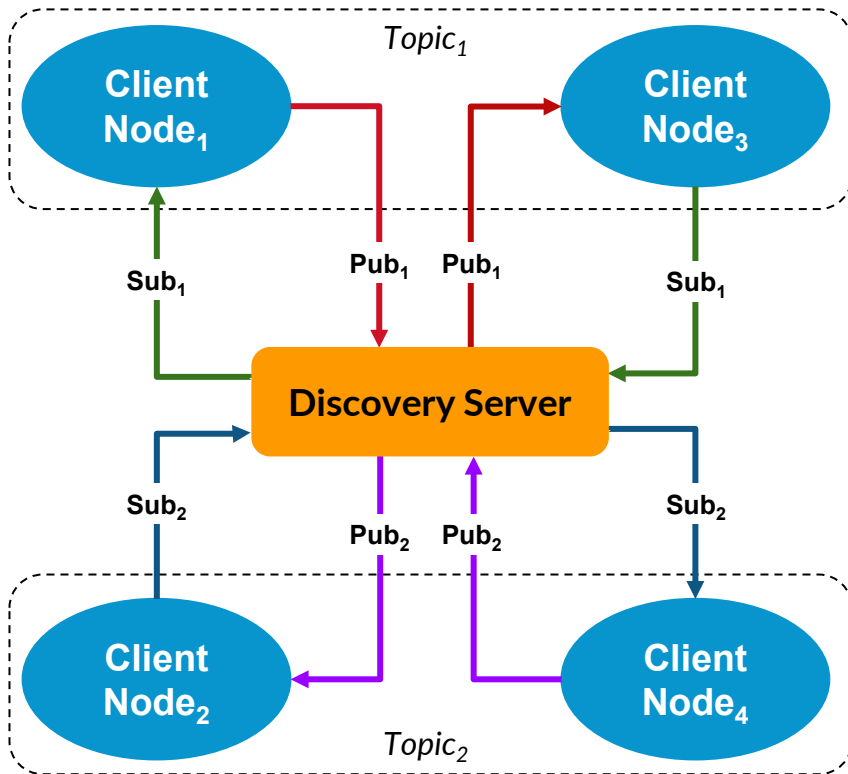
1

## Minimal configuration

Clients only need to know where the Discovery Server is located.

# ROS 2 Discovery Server

Discovery Server mechanism



1

## Minimal configuration

Clients only need to know where the Discovery Server is located.

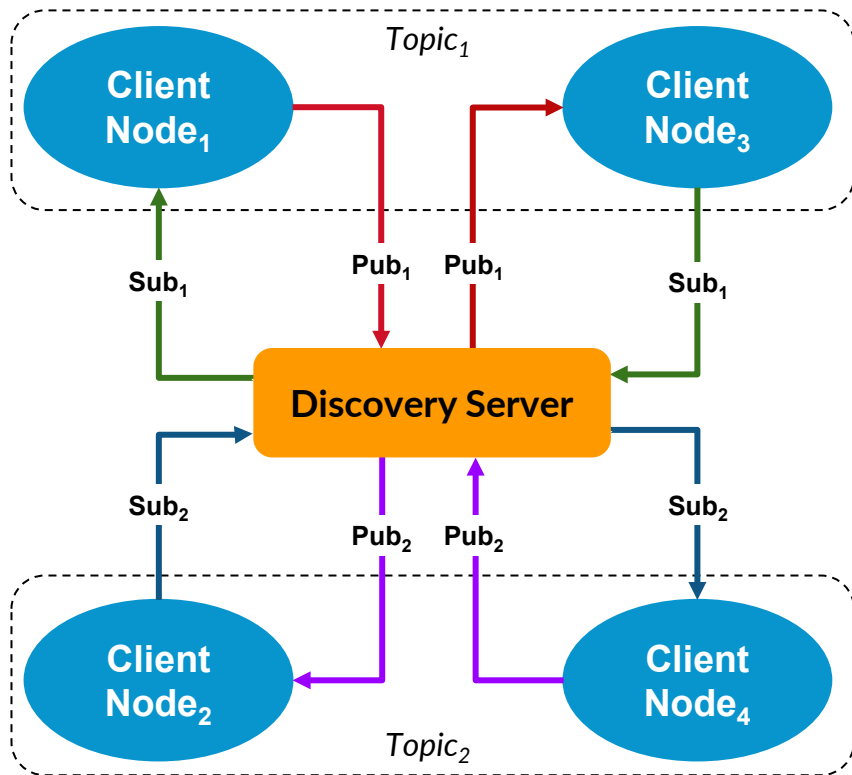
2

## Traffic reduction

Benchmarks show up to a 85% traffic reduction when compared to SDP

# ROS 2 Discovery Server

Discovery Server mechanism



1

## Minimal configuration

Clients only need to know where the Discovery Server is located.

2

## Traffic reduction

Benchmarks show up to a 85% traffic reduction when compared to SDP

3

## Unicast based

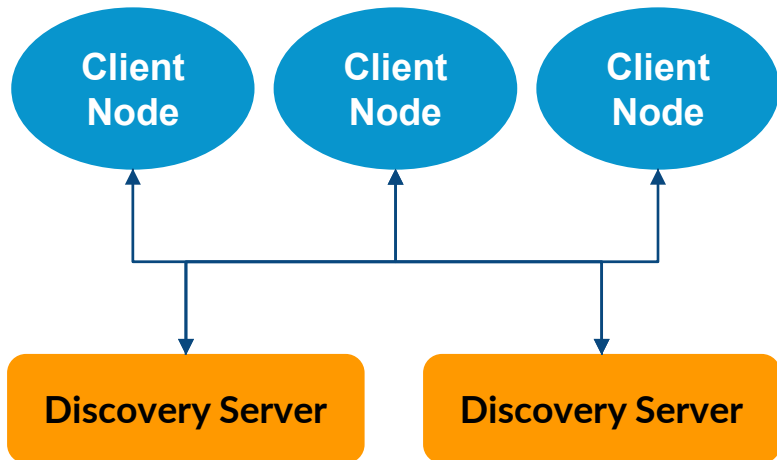
Works out-of-the-box in WiFi and managed networks as it does not require multicast

# ROS 2 Discovery Server

*Discovery Server deployment and configuration*



## Server redundancy

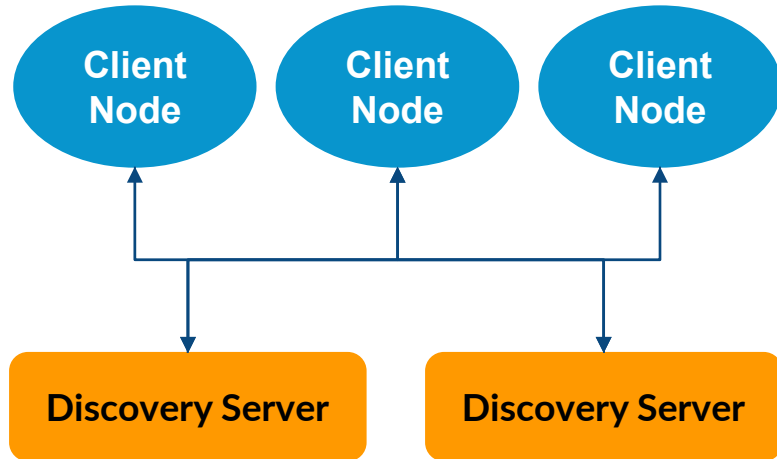


# ROS 2 Discovery Server

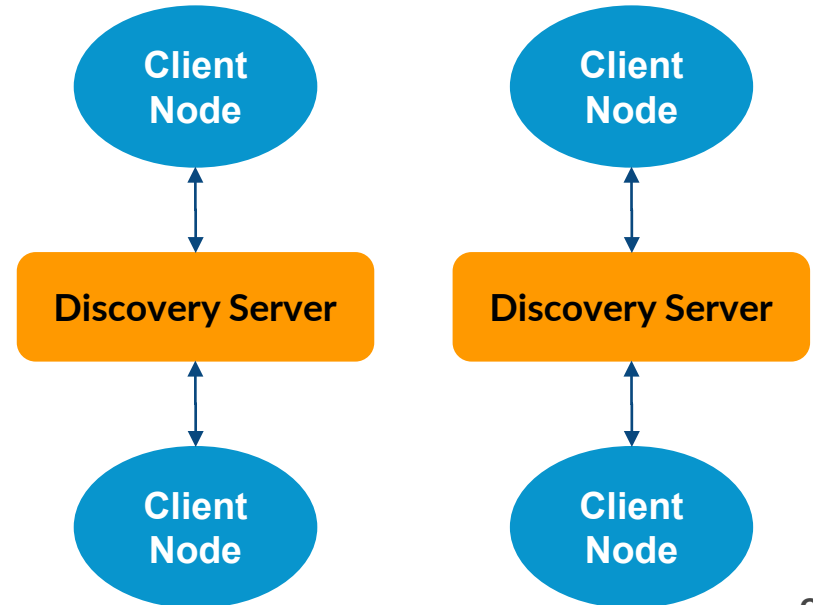
Discovery Server deployment and configuration



## Server redundancy



## LAN Segmentation

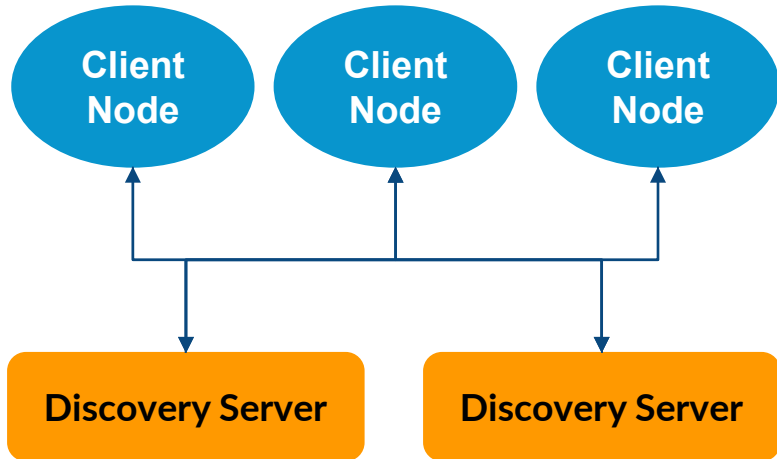


# ROS 2 Discovery Server

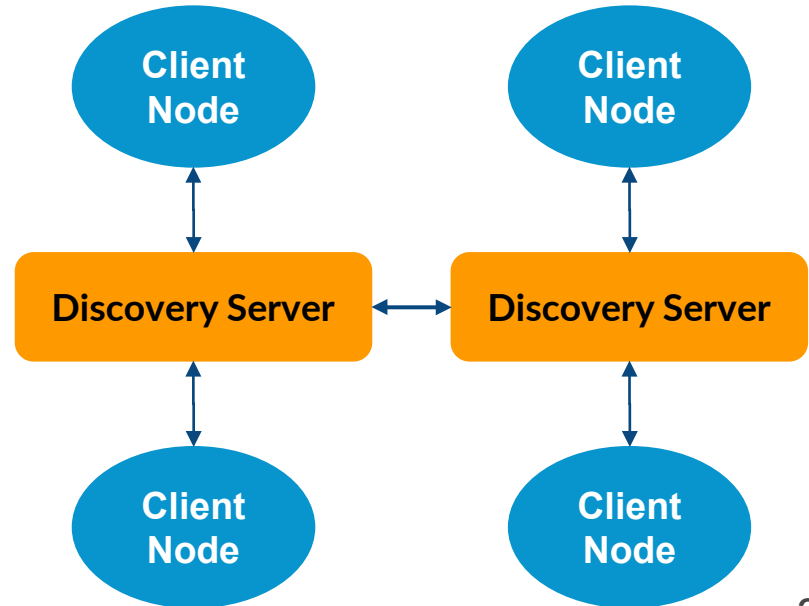
Discovery Server deployment and configuration



## Server redundancy



## Bridging segments



# ROS 2 Discovery Server

*Discovery Server deployment and configuration*



1

## Deploy a Discovery Server

Instantiating a Discover Server is as simple as running one CLI command

```
$ fastdds discovery -i 0
```



# ROS 2 Discovery Server

*Discovery Server deployment and configuration*



1

## Deploy a Discovery Server

Instantiating a Discover Server is as simple as running one CLI command

```
$ fastdds discovery -i 0
```

2

## Configure nodes as Clients

Nodes are configured as Clients using an environment variable

```
$ export ROS_DISCOVERY_SERVER="192.168.1.54"
```

# ROS 2 Discovery Server

*Discovery Server deployment and configuration*



1

## Deploy a Discovery Server

Instantiating a Discover Server is as simple as running one CLI command

```
$ fastdds discovery -i 0
```

2

## Configure nodes as Clients

Nodes are configured as Clients using an environment variable

```
$ export ROS_DISCOVERY_SERVER="192.168.1.54"
```

3

## Advanced configurations

Update list of Server in run-time, Super Client, etc.



## SROS 2

ROS 2 infrastructure to leverage DDS Security capabilities and protect your ROS 2 applications



# DDS Security

*Several levels of protection*



## **Authentication** (DDS:Auth:PKI-DH)

Authenticate a new Participant  
when joining the network

# DDS Security

Several levels of protection



## Authentication (DDS:Auth:PKI-DH)

Authenticate a new Participant  
when joining the network



## Access Control (DDS:Access:Permissions)

Limit the access and  
permissions for the  
Participants in the network

# DDS Security

Several levels of protection



## Authentication (DDS:Auth:PKI-DH)

Authenticate a new Participant  
when joining the network



## Access Control (DDS:Access:Permissions)

Limit the access and  
permissions for the  
Participants in the network



## Encryption (DDS:Crypto:AES-GCM-GMAC)

Encrypt the messages between  
Endpoints

# DDS Security

*Understanding the security infrastructure*



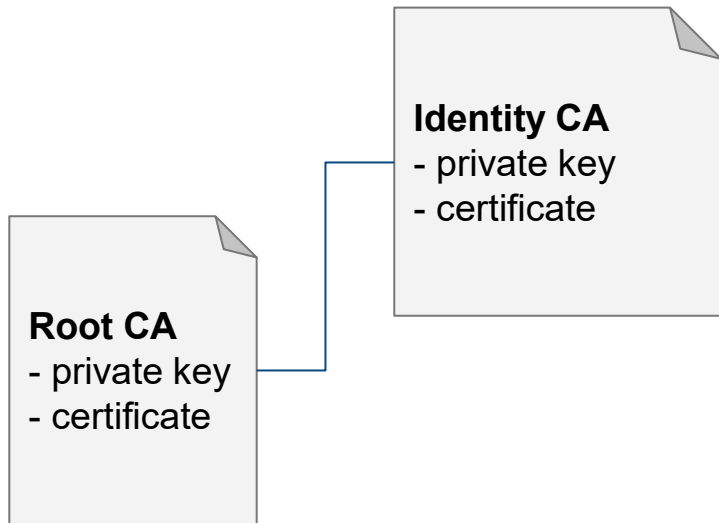
## **Root CA**

- private key
- certificate



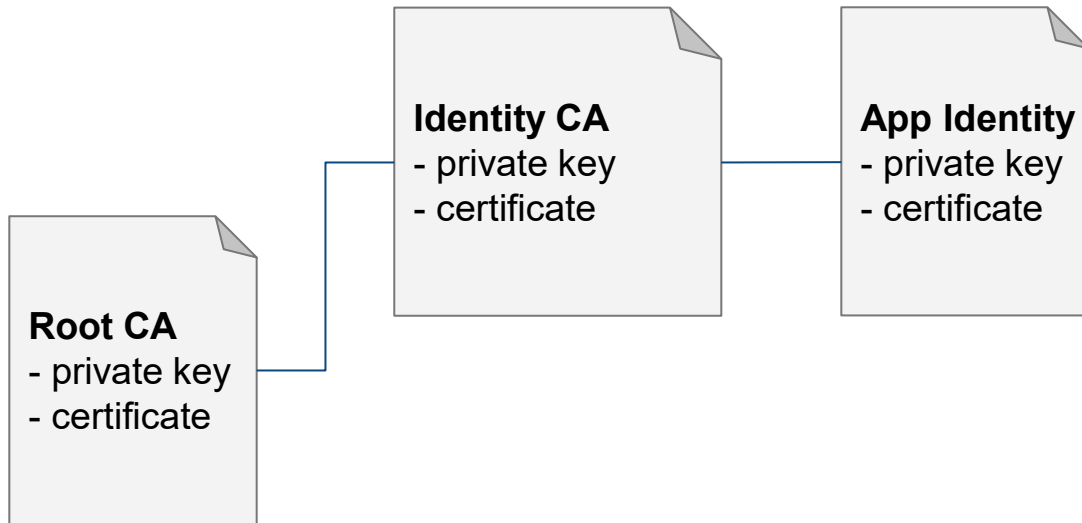
# DDS Security

*Understanding the security infrastructure*



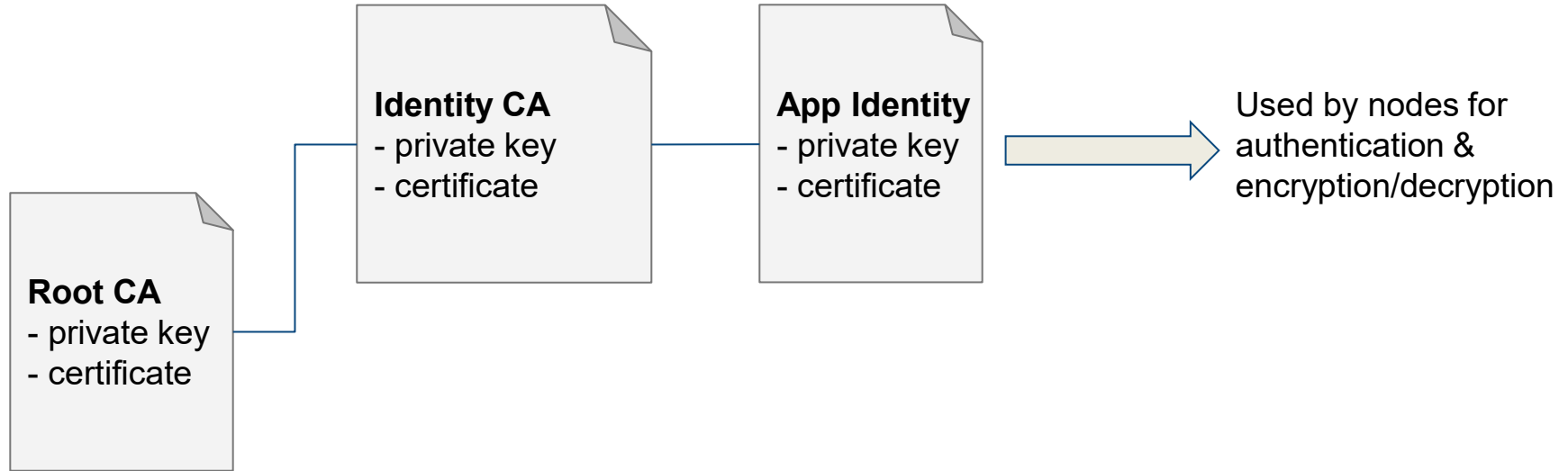
# DDS Security

*Understanding the security infrastructure*



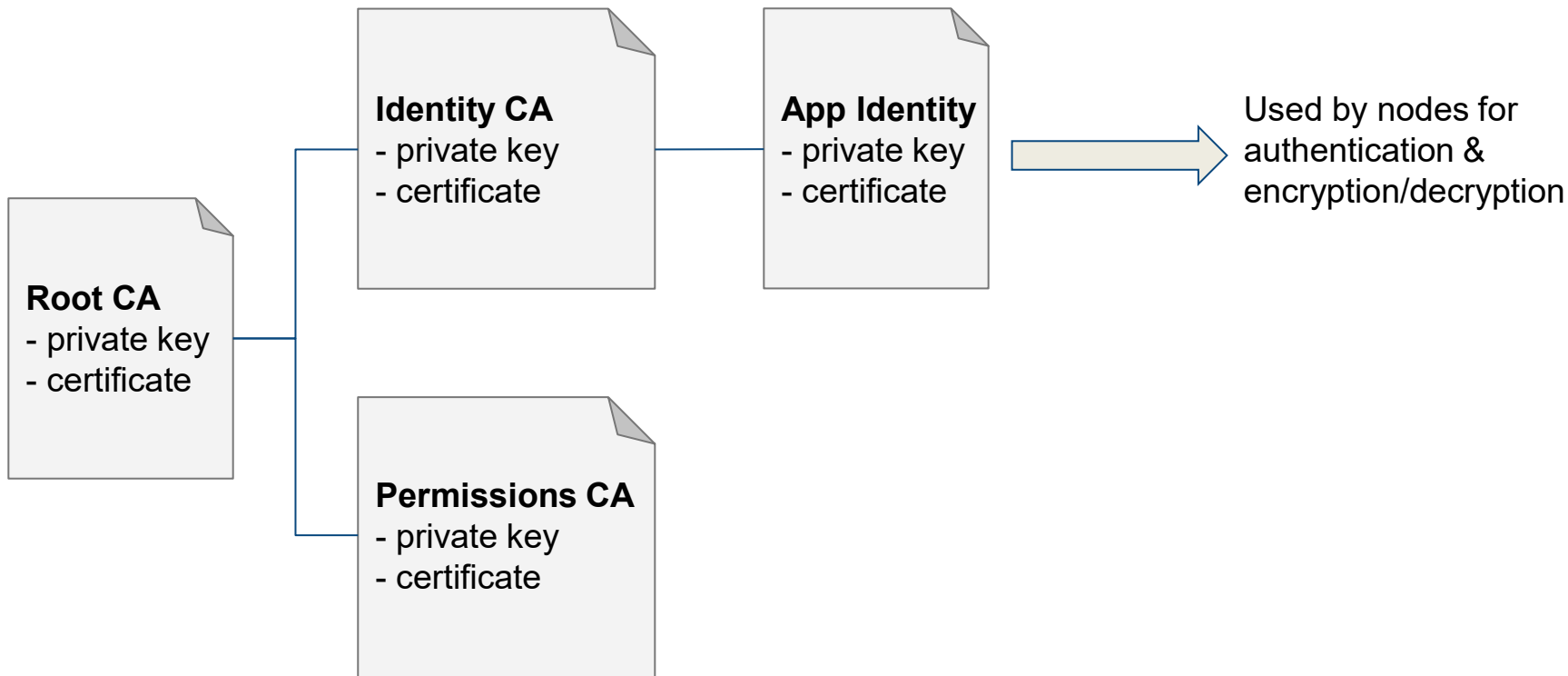
# DDS Security

Understanding the security infrastructure



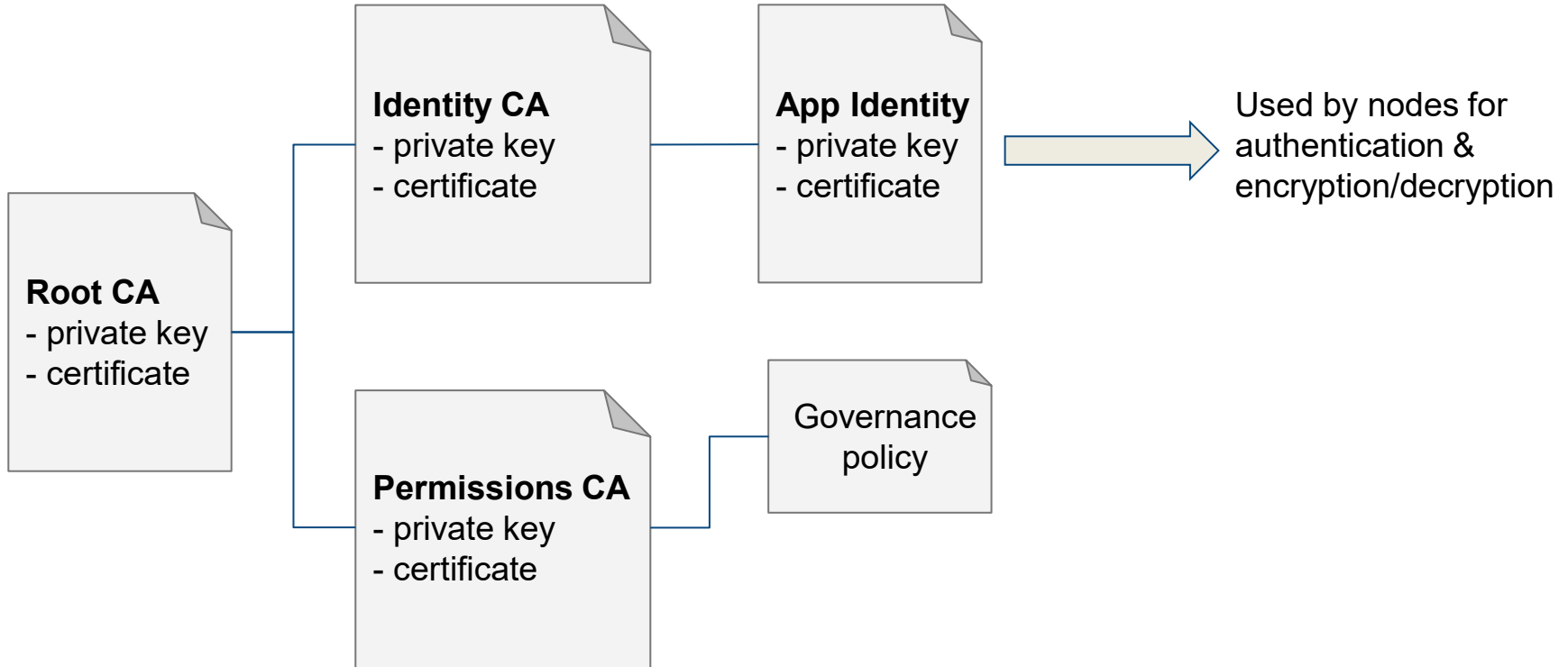
# DDS Security

Understanding the security infrastructure



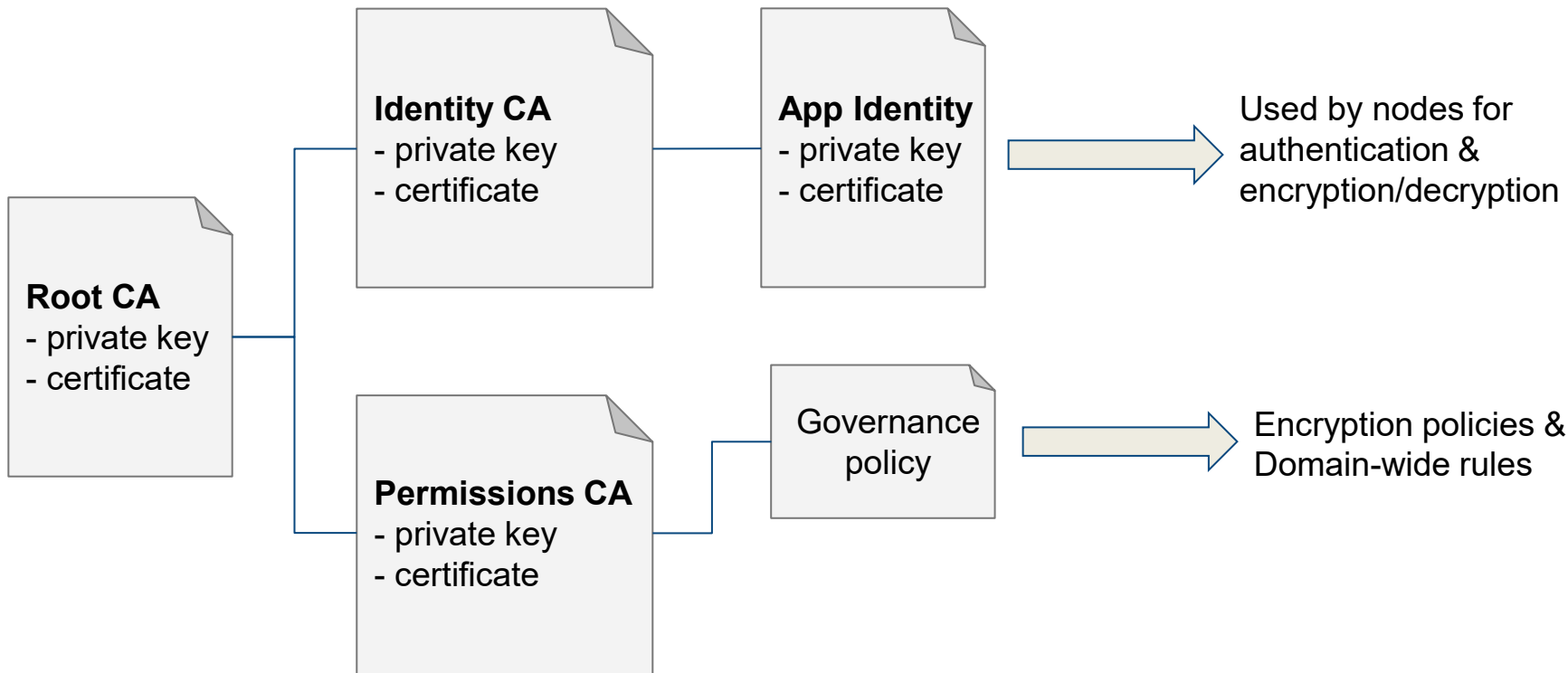
# DDS Security

Understanding the security infrastructure



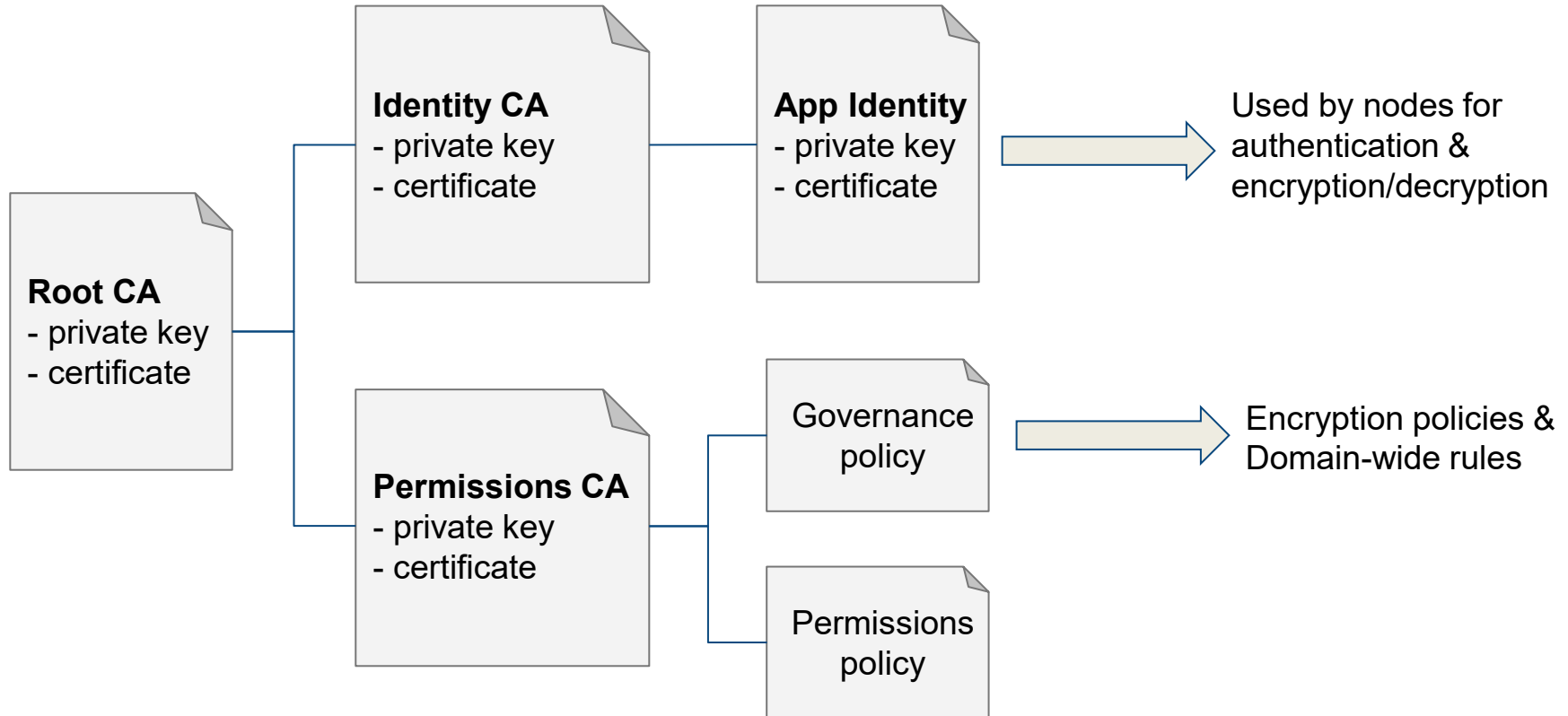
# DDS Security

Understanding the security infrastructure



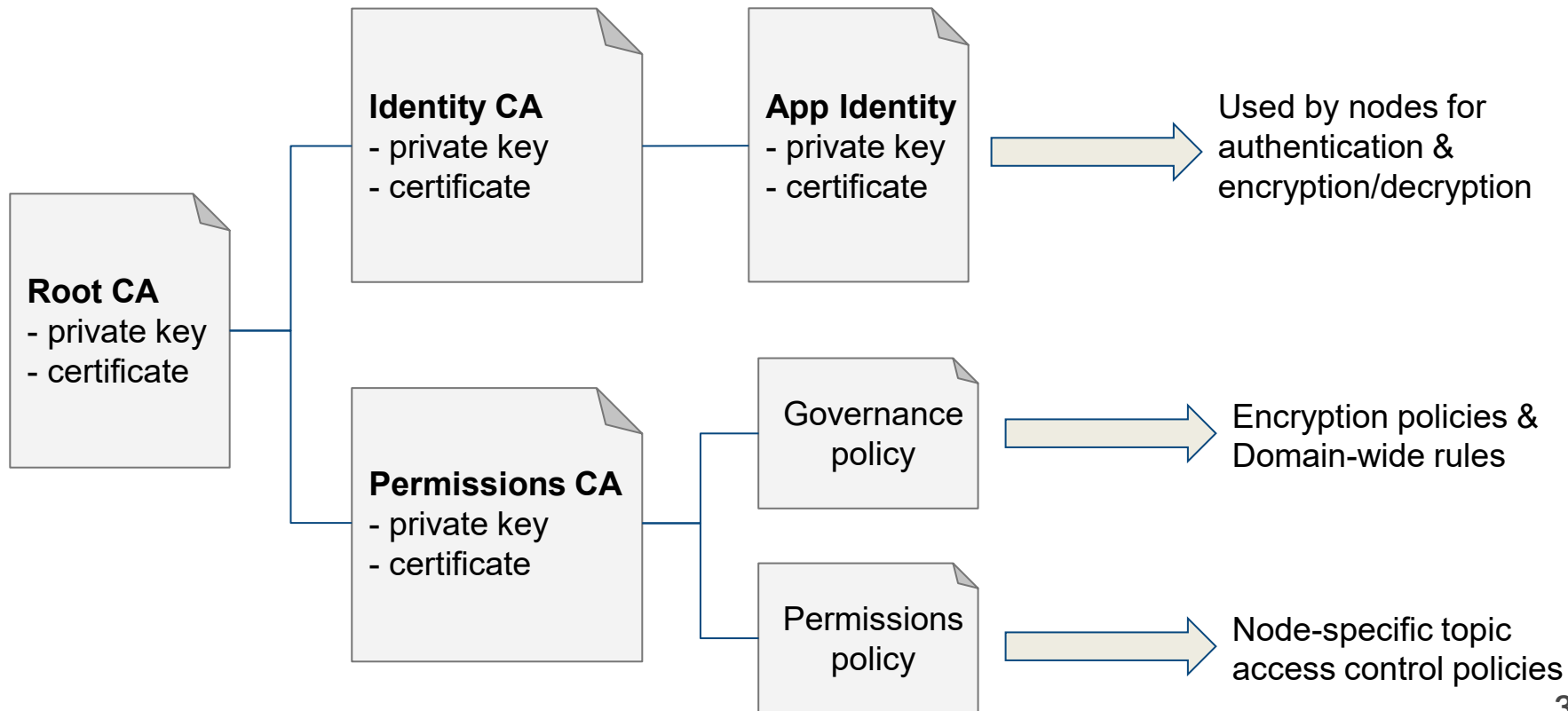
# DDS Security

Understanding the security infrastructure



# DDS Security

Understanding the security infrastructure





# SROS 2 tooling

*SROS 2 CLI for easily enable security in ROS 2*



1

## Create a keystore

Contains public and private certificates and keys, as well as enclaves

```
$ ros2 security create_keystore <store>
```

# SROS 2 tooling

SROS 2 CLI for easily enable security in ROS 2



1

## Create a keystore

Contains public and private certificates and keys, as well as enclaves

```
$ ros2 security create_keystore <store>
```

2

## Create enclaves

Enclave specific certificates and keys, and CA's public certificates

```
$ ros2 security create_enclave <store> <enclave>
```

# SROS 2 tooling

SROS 2 CLI for easily enable security in ROS 2



1

## Create a keystore

Contains public and private certificates and keys, as well as enclaves

```
$ ros2 security create_keystore <store>
```

2

## Create enclaves

Enclave specific certificates and keys, and CA's public certificates

```
$ ros2 security create_enclave <store> <enclave>
```

3

## Configure nodes for SROS 2

Command ROS 2 nodes to use specific enclaves for authentication, access control, and encryption

```
$ export ROS_SECURITY_KEYSTORE=<store>
$ export ROS_SECURITY_ENABLE=true
$ export ROS_SECURITY_STRATEGY=Enforce
$ ros2 run <pkg> <node> --ros-args --enclave <enclave>
```



# SROS 2 & Discovery Server

---

Secure Discovery Server  
configuration & demonstration



# SROS 2 Discovery Server

Secure Discovery Server deployment and configuration



```
# secure_discovery_server.xml
```

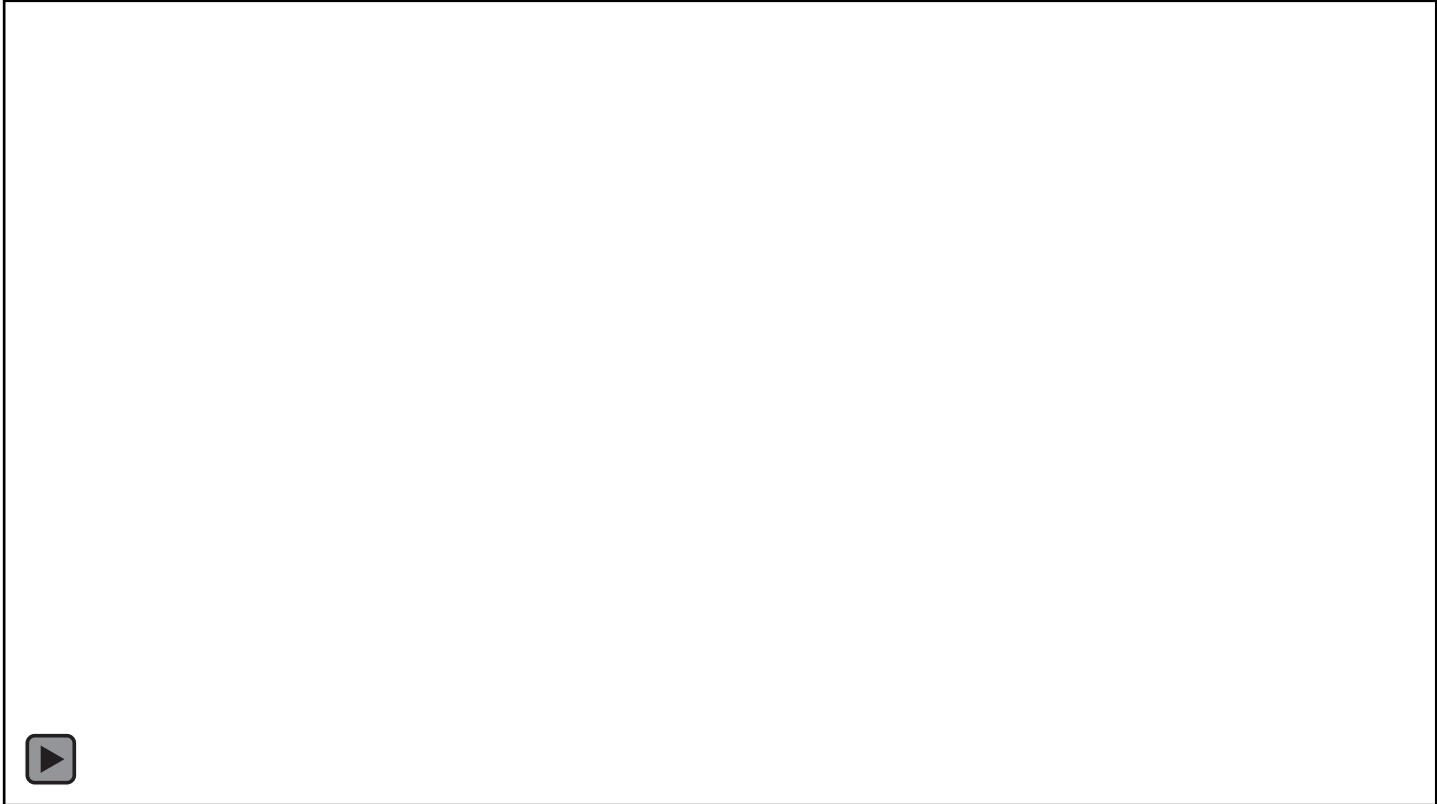
- Discovery Server IP address and port (i.e.: 0.0.0.0:11811)
- Identity CA certificate
- Identity certificate
- Identity private key
- Permissions certificate
- Governance file (signed)
- Permission file (signed)



```
$ fastdds discovery -i 0 -x <config_xml>
```

# SROS 2 Discovery Server

*Demonstration*



# ROS 2 Record & Replay

*ROS 2 Record & Replay documentation and GitHub repository*



Discovery Server



SROS 2





# **EPROSIMA**

The Middleware Experts

[www.eProsima.com](http://www.eProsima.com)



[Linkedin.com/company/eProsima](https://www.linkedin.com/company/eProsima)



[Twitter.com/EProsima](https://twitter.com/EProsima)