Leveraging Secure Discovery Server in ROS 2

Speaker:
- Eduardo Ponz Segrelles, Project Manager @ eProsima
  eduardoponz@eprosima.com
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)

Multicast

Node₁  Node₃  Node₂  Node₄

SDP Topic Discovery Phase (EDP)

Topic₁  Topic₂

Node₁  Node₂

Node₃  Node₄
ROS 2 Discovery Server

Out-of-the-box discovery (SDP)

SDP Node Discovery Phase (PDP)

Multicast

Node₁  Node₃  Node₂  Node₄

SDP Topic Discovery Phase (EDP)

Topic₁

Topic₂

Node₁  Node₂

Node₃  Node₄

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)

No configuration
ROS 2 Nodes discover each other automatically

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)

Multicast

Node₁  Node₃  Node₂  Node₄

SDP Topic Discovery Phase (EDP)

Topic₁  Topic₂

Node₁  Node₂

Node₃  Node₄

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

- Client Node\(_1\)
- Client Node\(_2\)
- Client Node\(_3\)
- Client Node\(_4\)

Discovery Server
ROS 2 Discovery Server

Discovery Server mechanism

Client Node_1

Client Node_2

Pub_1

Discovery Server

Client Node_3

Client Node_4
ROS 2 Discovery Server

Discovery Server mechanism

Client Node₁

Topic₁

Pub₁

Sub₁

Discovery Server

Client Node₂

Client Node₃

Client Node₄
ROS 2 Discovery Server

Discovery Server mechanism

Client Node\textsubscript{1} \rightarrow \text{Topic}_1 \rightarrow \text{Client Node}_3

Sub\textsubscript{1} \rightarrow \text{Pub}_1 \rightarrow \text{Pub}_1 \rightarrow \text{Sub}_1

Discovery Server

Client Node\textsubscript{2} \rightarrow \text{Pub}_1

Client Node\textsubscript{4} \rightarrow \text{Sub}_1
ROS 2 Discovery Server

Discovery Server mechanism

Client Node 1

Client Node 3

Discovery Server

Client Node 2

Client Node 4

Sub 1

Pub 1

Sub 1

Pub 1

Sub 2

Pub 2

Topic 1

Topic 2
ROS 2 Discovery Server

Discovery Server mechanism

Client Node \(_1\)

Client Node \(_3\)

Client Node \(_2\)

Client Node \(_4\)

Discovery Server

Topic \(_1\)

Topic \(_2\)

Sub \(_1\)

Pub \(_1\)

Sub \(_1\)

Pub \(_1\)

Sub \(_2\)

Pub \(_2\)

Sub \(_2\)

Pub \(_2\)
ROS 2 Discovery Server

**Discovery Server mechanism**

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

Diagram:
- Client Node_1
- Client Node_2
- Client Node_3
- Client Node_4

- **Topics:**
  - Topic_1
  - Topic_2

- **Subscriptions:**
  - Sub_1
  - Sub_2

- **Publications:**
  - Pub_1
  - Pub_2
ROS 2 Discovery Server

Discovery Server mechanism

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

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 an 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

Client Node → Discovery Server → Client Node

Client Node → Discovery Server → Client Node

Client Node → Discovery Server → Client Node
ROS 2 Discovery Server

Discovery Server deployment and configuration

Server redundancy

Client Node

Client Node

Client Node

Discovery Server

Discovery Server

LAN Segmentation

Client Node

Discovery Server

Client Node

Discovery Server

Client Node
ROS 2 Discovery Server

Discovery Server deployment and configuration

Server redundancy

Client Node

Client Node

Client Node

Discovery Server

Discovery Server

Bridging segments

Client Node

Discovery Server

Client Node

Discovery Server

Client Node

Client Node
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"
Deploy a Discovery Server
Instantiating a Discover Server is as simple as running one CLI command

$ fastdds discovery -i 0

Configure nodes as Clients
Nodes are configured as Clients using an environment variable

$ export ROS_DISCOVERY_SERVER="192.168.1.54"

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
Root CA
- private key
- certificate
DDS Security
Understanding the security infrastructure

- Root CA
  - private key
  - certificate

- Identity CA
  - private key
  - certificate
Root CA
- private key
- certificate

Identity CA
- private key
- certificate

App Identity
- private key
- certificate
DDS Security
Understanding the security infrastructure

Root CA
- private key
- certificate

Identity CA
- private key
- certificate

App Identity
- private key
- certificate

Used by nodes for authentication & encryption/decryption
Root CA
- private key
- certificate

Identity CA
- private key
- certificate

Permissions CA
- private key
- certificate

App Identity
- private key
- certificate

Used by nodes for authentication & encryption/decryption
**DDDS Security**

*Understanding the security infrastructure*

- **Root CA**
  - private key
  - certificate

- **Identity CA**
  - private key
  - certificate

- **Permissions CA**
  - private key
  - certificate

- **App Identity**
  - private key
  - certificate

- **Governance policy**

Used by nodes for authentication & encryption/decryption
DDS Security

Understanding the security infrastructure

Root CA
- private key
- certificate

Identity CA
- private key
- certificate

Permissions CA
- private key
- certificate

App Identity
- private key
- certificate

Governance policy

Used by nodes for authentication & encryption/decryption

Encryption policies & Domain-wide rules
 DDS Security
Understanding the security infrastructure

Root CA
- private key
- certificate

Identity CA
- private key
- certificate

Permissions CA
- private key
- certificate

App Identity
- private key
- certificate

Governance policy

Permissions policy

Encryption policies & Domain-wide rules

Used by nodes for authentication & encryption/decryption
DDS Security
Understanding the security infrastructure

Root CA
- private key
- certificate

Identity CA
- private key
- certificate

Permissions CA
- private key
- certificate

App Identity
- private key
- certificate

Governance policy

Permissions policy

Encryption policies & Domain-wide rules

Node-specific topic access control policies

Used by nodes for authentication & encryption/decryption
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>
## 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)

```bash
$ fastdds discovery -i 0 -x <config_xml>
```
SROS 2 Discovery Server
Demonstration
ROS 2 Record & Replay

Discovery Server

SROS 2