

Embedding Infinispan 13.0

Table of Contents

1. Configuring the Infinispan Maven Repository	1
1.1. Configuring Your Infinispan POM	1
2. Installing Infinispan in Library Mode	2
3. Running Infinispan as an Embedded Library	3
4. Setting Up Infinispan Clusters	4
4.1. Default JGroups Stacks	4
4.2. Cluster Discovery Protocols	5
4.2.1. PING	5
4.2.2. TCPPING	5
4.2.3. MPING	6
4.2.4. TCPGOSSIP	6
4.2.5. JDBC_PING	7
4.2.6. DNS_PING	7
4.2.7. Cloud Discovery Protocols	8
4.3. Using the Default JGroups Stacks	8
4.4. Customizing JGroups Stacks	9
4.4.1. Inheritance Attributes	11
4.5. Using JGroups System Properties	11
4.5.1. Cluster Transport Properties	12
4.5.2. System Properties for Cloud Discovery Protocols	12
4.6. Using Inline JGroups Stacks	13
4.7. Using External JGroups Stacks	14
4.8. Using Custom JChannels	15
4.9. Encrypting Cluster Transport	15
4.9.1. Infinispan Cluster Security	15
4.9.2. Configuring Cluster Transport with Asymmetric Encryption	17
4.9.3. Configuring Cluster Transport with Symmetric Encryption	18
4.10. TCP and UDP Ports for Cluster Traffic	20

Chapter 1. Configuring the Infinispan Maven Repository

Infinispan Java distributions are available from Maven.

Infinispan artifacts are available from Maven central. See the [org.infinispan](#) group for available Infinispan artifacts.

1.1. Configuring Your Infinispan POM

Maven uses configuration files called Project Object Model (POM) files to define projects and manage builds. POM files are in XML format and describe the module and component dependencies, build order, and targets for the resulting project packaging and output.

Procedure

1. Open your project `pom.xml` for editing.
2. Define the `version.infinispan` property with the correct Infinispan version.
3. Include the `infinispan-bom` in a `dependencyManagement` section.

The Bill Of Materials (BOM) controls dependency versions, which avoids version conflicts and means you do not need to set the version for each Infinispan artifact you add as a dependency to your project.

4. Save and close `pom.xml`.

The following example shows the Infinispan version and BOM:

```
<properties>
  <version.infinispan>13.0.0.Dev02</version.infinispan>
</properties>

<dependencyManagement>
  <dependencies>
    <dependency>
      <groupId>org.infinispan</groupId>
      <artifactId>infinispan-bom</artifactId>
      <version>${version.infinispan}</version>
      <type>pom</type>
      <scope>import</scope>
    </dependency>
  </dependencies>
</dependencyManagement>
```

Next Steps

Add Infinispan artifacts as dependencies to your `pom.xml` as required.

Chapter 2. Installing Infinispan in Library Mode

Add Infinispan as an embedded library in your project.

Procedure

- Add the `infinispan-core` artifact as a dependency in your `pom.xml` as follows:

```
<dependencies>
  <dependency>
    <groupId>org.infinispan</groupId>
    <artifactId>infinispan-core</artifactId>
  </dependency>
</dependencies>
```

Chapter 3. Running Infinispan as an Embedded Library

Learn how to run Infinispan as an embedded data store in your project.

Procedure

- Initialize the default Cache Manager and add a cache definition as follows:

```
GlobalConfigurationBuilder global = GlobalConfigurationBuilder.  
defaultClusteredBuilder();  
DefaultCacheManager cacheManager = new DefaultCacheManager(global.build());  
ConfigurationBuilder builder = new ConfigurationBuilder();  
builder.clustering().cacheMode(CacheMode.DIST_SYNC);  
cacheManager.administration().withFlags(CacheContainerAdmin.AdminFlag.VOLATILE).getOrCreateCache("myCache", builder.build());
```

The preceding code initializes a default, clustered Cache Manager. Cache Managers contain your cache definitions and control cache lifecycles.

Infinispan does not provide default cache definitions so after initializing the default Cache Manager, you need to add at least one cache instance. This example uses the `ConfigurationBuilder` class to create a cache definition that uses the distributed, synchronous cache mode. You then call the `getOrCreateCache()` method that either creates a cache named "myCache" on all nodes in the cluster or returns it if it already exists.

Next steps

Now that you have a running Cache Manager with a cache created, you can add some more cache definitions, put some data into the cache, or configure Infinispan as needed.

Reference

- [Configuring Infinispan Programmatically](#)
- [org.infinispan.configuration.global.GlobalConfigurationBuilder](#)
- [org.infinispan.manager.EmbeddedCacheManager](#)
- [org.infinispan.Cache](#)

Chapter 4. Setting Up Infinispan Clusters

Infinispan requires a transport layer so nodes can automatically join and leave clusters. The transport layer also enables Infinispan nodes to replicate or distribute data across the network and perform operations such as re-balancing and state transfer.

4.1. Default JGroups Stacks

Infinispan provides default JGroups stack files, `default-jgroups-*.xml`, in the `default-configs` directory inside the `infinispan-core-13.0.0.Dev02.jar` file.

File name	Stack name	Description
<code>default-jgroups-udp.xml</code>	<code>udp</code>	Uses UDP for transport and UDP multicast for discovery. Suitable for larger clusters (over 100 nodes) or if you are using replicated caches or invalidation mode. Minimizes the number of open sockets.
<code>default-jgroups-tcp.xml</code>	<code>tcp</code>	Uses TCP for transport and the <code>MPING</code> protocol for discovery, which uses <code>UDP</code> multicast. Suitable for smaller clusters (under 100 nodes) <i>only if</i> you are using distributed caches because TCP is more efficient than UDP as a point-to-point protocol.
<code>default-jgroups-kubernetes.xml</code>	<code>kubernetes</code>	Uses TCP for transport and <code>DNS_PING</code> for discovery. Suitable for Kubernetes and Red Hat OpenShift nodes where UDP multicast is not always available.
<code>default-jgroups-ec2.xml</code>	<code>ec2</code>	Uses TCP for transport and <code>NATIVE_S3_PING</code> for discovery. Suitable for Amazon EC2 nodes where UDP multicast is not available. Requires additional dependencies.
<code>default-jgroups-google.xml</code>	<code>google</code>	Uses TCP for transport and <code>GOOGLE_PING2</code> for discovery. Suitable for Google Cloud Platform nodes where UDP multicast is not available. Requires additional dependencies.
<code>default-jgroups-azure.xml</code>	<code>azure</code>	Uses TCP for transport and <code>AZURE_PING</code> for discovery. Suitable for Microsoft Azure nodes where UDP multicast is not available. Requires additional dependencies.

Additional resources

- [JGroups Protocols](#)

4.2. Cluster Discovery Protocols

Infinispan supports different protocols that allow nodes to automatically find each other on the network and form clusters.

There are two types of discovery mechanisms that Infinispan can use:

- Generic discovery protocols that work on most networks and do not rely on external services.
- Discovery protocols that rely on external services to store and retrieve topology information for Infinispan clusters.

For instance the DNS_PING protocol performs discovery through DNS server records.



Running Infinispan on hosted platforms requires using discovery mechanisms that are adapted to network constraints that individual cloud providers impose.

Reference

- [JGroups Discovery Protocols](#)

4.2.1. PING

PING, or UDPPING is a generic JGroups discovery mechanism that uses dynamic multicasting with the UDP protocol.

When joining, nodes send PING requests to an IP multicast address to discover other nodes already in the Infinispan cluster. Each node responds to the PING request with a packet that contains the address of the coordinator node and its own address. C=coordinator's address and A=own address. If no nodes respond to the PING request, the joining node becomes the coordinator node in a new cluster.

PING configuration example

```
<config>
  <PING num_discovery_runs="3"/>
  <!-- JGroups stack configuration. -->
</config>
```

Additional resources

- [JGroups PING](#)

4.2.2. TCPING

TCPING is a generic JGroups discovery mechanism that uses a list of static addresses for cluster members.

With TCPING, you manually specify the IP address or hostname of each node in the Infinispan cluster as part of the JGroups stack, rather than letting nodes discover each other dynamically.

TCPPING configuration example

```
<config>
  <TCP bind_port="7800" />
  <TCPPING timeout="3000"
    initial_hosts=
      "${jgroups.tcpping.initial_hosts:hostname1[port1],hostname2[port2]}"
    port_range="0"
    num_initial_members="3"/>
  <!-- JGroups stack configuration. -->
</config>
```

Additional resources

- [JGroups TCPPING](#)

4.2.3. MPING

MPING uses IP multicast to discover the initial membership of Infinispan clusters.

You can use MPING to replace TCPPING discovery with TCP stacks and use multicasting for discovery instead of static lists of initial hosts. However, you can also use MPING with UDP stacks.

MPING configuration example

```
<config>
  <MPING mcast_addr="${jgroups.mcast_addr:228.6.7.8}"
    mcast_port="${jgroups.mcast_port:46655}"
    num_discovery_runs="3"
    ip_ttl="${jgroups.udp.ip_ttl:2}"/>
  <!-- JGroups stack configuration. -->
</config>
```

Additional resources

- [JGroups MPING](#)

4.2.4. TCPGOSSIP

Gossip routers provide a centralized location on the network from which your Infinispan cluster can retrieve addresses of other nodes.

You inject the address (**IP:PORT**) of the Gossip router into Infinispan nodes as follows:

1. Pass the address as a system property to the JVM; for example, `-DGossipRouterAddress="10.10.2.4[12001]"`.
2. Reference that system property in the JGroups configuration file.

Gossip router configuration example

```
<config>
  <TCP bind_port="7800" />
  <TCPOSSIP timeout="3000"
    initial_hosts="${GossipRouterAddress}"
    num_initial_members="3" />
  <!-- JGroups stack configuration. -->
</config>
```

Additional resources

- [JGroups Gossip Router](#)

4.2.5. JDBC_PING

JDBC_PING uses shared databases to store information about Infinispan clusters. This protocol supports any database that can use a JDBC connection.

Nodes write their IP addresses to the shared database so joining nodes can find the Infinispan cluster on the network. When nodes leave Infinispan clusters, they delete their IP addresses from the shared database.

JDBC_PING configuration example

```
<config>
  <JDBC_PING connection_url="jdbc:mysql://localhost:3306/database_name"
    connection_username="user"
    connection_password="password"
    connection_driver="com.mysql.jdbc.Driver"/>
  <!-- JGroups stack configuration. -->
</config>
```



Add the appropriate JDBC driver to the classpath so Infinispan can use JDBC_PING.

Additional resources

- [JDBC_PING](#)
- [JDBC_PING Wiki](#)

4.2.6. DNS_PING

JGroups DNS_PING queries DNS servers to discover Infinispan cluster members in Kubernetes environments such as OKD and Red Hat OpenShift.

DNS_PING configuration example

```
<config>
  <dns.DNS_PING dns_query="myservice.myproject.svc.cluster.local" />
  <!-- JGroups stack configuration. -->
</config>
```

Additional resources

- [JGroups DNS_PING](#)
- [DNS for Services and Pods](#) (Kubernetes documentation for adding DNS entries)

4.2.7. Cloud Discovery Protocols

Infinispan includes default JGroups stacks that use discovery protocol implementations that are specific to cloud providers.

Discovery protocol	Default stack file	Artifact	Version
NATIVE_S3_PING	default-jgroups-ec2.xml	org.jgroups.aws:s3:native-s3-ping	1.0.0.Final
GOOGLE_PING2	default-jgroups-google.xml	org.jgroups.google:jgroups-google	1.0.0.Final
AZURE_PING	default-jgroups-azure.xml	org.jgroups.azure:jgroups-azure	1.3.0.Final

Providing Dependencies for Cloud Discovery Protocols

To use `NATIVE_S3_PING`, `GOOGLE_PING2`, or `AZURE_PING` cloud discovery protocols, you need to provide dependent libraries to Infinispan.

Procedure

- Add the artifact dependencies to your project `pom.xml`.

You can then configure the cloud discovery protocol as part of a JGroups stack file or with system properties.

Additional resources

- [JGroups NATIVE_S3_PING](#)
- [JGroups GOOGLE_PING2](#)
- [JGroups AZURE_PING](#)

4.3. Using the Default JGroups Stacks

Infinispan uses JGroups protocol stacks so nodes can send each other messages on dedicated cluster channels.

Infinispan provides preconfigured JGroups stacks for `UDP` and `TCP` protocols. You can use these

default stacks as a starting point for building custom cluster transport configuration that is optimized for your network requirements.

Procedure

Do one of the following to use one of the default JGroups stacks:

- Use the `stack` attribute in your `infinispan.xml` file.

```
<infinispan>
  <cache-container default-cache="replicatedCache">
    <!-- Use the default UDP stack for cluster transport. -->
    <transport cluster="${infinispan.cluster.name}"
              stack="udp"
              node-name="${infinispan.node.name:}"/>
  </cache-container>
</infinispan>
```

- Use the `addProperty()` method to set the JGroups stack file:

```
GlobalConfiguration globalConfig = new GlobalConfigurationBuilder().transport()
    .defaultTransport()
    .clusterName("qa-cluster")
    .addProperty("configurationFile", "default-jgroups-udp.xml") ①
    .build();
```

① Uses the `default-jgroups-udp.xml` stack for cluster transport.

Verification

Infinispan logs the following message to indicate which stack it uses:

```
[org.infinispan.CLUSTER] ISPN000078: Starting JGroups channel cluster with stack udp
```

4.4. Customizing JGroups Stacks

Adjust and tune properties to create a cluster transport configuration that works for your network requirements.

Infinispan provides attributes that let you extend the default JGroups stacks for easier configuration. You can inherit properties from the default stacks while combining, removing, and replacing other properties.

Procedure

1. Create a new JGroups stack declaration in your `infinispan.xml` file.
2. Add the `extends` attribute and specify a JGroups stack to inherit properties from.
3. Use the `stack.combine` attribute to modify properties for protocols configured in the inherited

stack.

4. Use the `stack.position` attribute to define the location for your custom stack.
5. Specify the stack name as the value for the `stack` attribute in the `transport` configuration.

For example, you might evaluate using a Gossip router and symmetric encryption with the default TCP stack as follows:

```
<infinispan>
  <jgroups>
    <!-- Creates a custom JGroups stack named "my-stack". -->
    <!-- Inherits properties from the default TCP stack. -->
    <stack name="my-stack" extends="tcp">
      <!-- Uses TCPGOSSIP as the discovery mechanism instead of MPING -->
      <TCPGOSSIP initial_hosts=
        "${jgroups.tunnel.gossip_router_hosts:localhost[12001]}"
        stack.combine="REPLACE"
        stack.position="MPING" />
      <!-- Removes the FD_SOCK protocol from the stack. -->
      <FD_SOCK stack.combine="REMOVE"/>
      <!-- Modifies the timeout value for the VERIFY_SUSPECT protocol. -->
      <VERIFY_SUSPECT timeout="2000"/>
      <!-- Adds SYM_ENCRYPT to the stack after VERIFY_SUSPECT. -->
      <SYM_ENCRYPT sym_algorithm="AES"
        keystore_name="mykeystore.p12"
        keystore_type="PKCS12"
        store_password="changeit"
        key_password="changeit"
        alias="myKey"
        stack.combine="INSERT_AFTER"
        stack.position="VERIFY_SUSPECT" />
    </stack>
    <cache-container name="default" statistics="true">
      <!-- Uses "my-stack" for cluster transport. -->
      <transport cluster="${infinispan.cluster.name}"
        stack="my-stack"
        node-name="${infinispan.node.name:}"/>
    </cache-container>
  </jgroups>
</infinispan>
```

6. Check Infinispan logs to ensure it uses the stack.

```
[org.infinispan.CLUSTER] ISPN000078: Starting JGroups channel cluster with stack
my-stack
```

4.4.1. Inheritance Attributes

When you extend a JGroups stack, inheritance attributes let you adjust protocols and properties in the stack you are extending.

- `stack.position` specifies protocols to modify.
- `stack.combine` uses the following values to extend JGroups stacks:

Value	Description
COMBINE	Overrides protocol properties.
REPLACE	Replaces protocols.
INSERT_AFTER	<p>Adds a protocol into the stack after another protocol. Does not affect the protocol that you specify as the insertion point.</p> <p>Protocols in JGroups stacks affect each other based on their location in the stack. For example, you should put a protocol such as <code>NAKACK2</code> after the <code>SYM_ENCRYPT</code> or <code>ASYM_ENCRYPT</code> protocol so that <code>NAKACK2</code> is secured.</p>
INSERT_BEFORE	<p>Inserts a protocols into the stack before another protocol. Affects the protocol that you specify as the insertion point.</p>
REMOVE	Removes protocols from the stack.

4.5. Using JGroups System Properties

Pass system properties to Infinispan at startup to tune cluster transport.

Procedure

- Use `-D<property-name>=<property-value>` arguments to set JGroups system properties as required.

For example, set a custom bind port and IP address as follows:

```
$ java -cp ... -Djgroups.bind.port=1234 -Djgroups.bind.address=192.0.2.0
```



When you embed Infinispan clusters in clustered WildFly applications, JGroups system properties can clash or override each other.

For example, you do not set a unique bind address for either your Infinispan cluster or your WildFly application. In this case both Infinispan and your WildFly application use the JGroups default property and attempt to form clusters using the same bind address.

4.5.1. Cluster Transport Properties

Use the following properties to customize JGroups cluster transport.

System Property	Description	Default Value	Required/Optional
<code>jgroups.bind.address</code>	Bind address for cluster transport.	<code>SITE_LOCAL</code>	Optional
<code>jgroups.bind.port</code>	Bind port for the socket.	<code>7800</code>	Optional
<code>jgroups.mcast_addr</code>	IP address for multicast, both discovery and inter-cluster communication. The IP address must be a valid "class D" address that is suitable for IP multicast.	<code>228.6.7.8</code>	Optional
<code>jgroups.mcast_port</code>	Port for the multicast socket.	<code>46655</code>	Optional
<code>jgroups.ip_ttl</code>	Time-to-live (TTL) for IP multicast packets. The value defines the number of network hops a packet can make before it is dropped.	<code>2</code>	Optional
<code>jgroups.thread_pool.min_threads</code>	Minimum number of threads for the thread pool.	<code>0</code>	Optional
<code>jgroups.thread_pool.max_threads</code>	Maximum number of threads for the thread pool.	<code>200</code>	Optional
<code>jgroups.join_timeout</code>	Maximum number of milliseconds to wait for join requests to succeed.	<code>2000</code>	Optional
<code>jgroups.thread_dump_threshold</code>	Number of times a thread pool needs to be full before a thread dump is logged.	<code>10000</code>	Optional

Reference

- [JGroups System Properties](#)
- [JGroups Protocol List](#)

4.5.2. System Properties for Cloud Discovery Protocols

Use the following properties to configure JGroups discovery protocols for hosted platforms.

Amazon EC2

System properties for configuring `NATIVE_S3_PING`.

System Property	Description	Default Value	Required/Optional
<code>jgroups.s3.region_name</code>	Name of the Amazon S3 region.	No default value.	Optional
<code>jgroups.s3.bucket_name</code>	Name of the Amazon S3 bucket. The name must exist and be unique.	No default value.	Optional

Google Cloud Platform

System properties for configuring `GOOGLE_PING2`.

System Property	Description	Default Value	Required/Optional
<code>jgroups.google.bucket_name</code>	Name of the Google Compute Engine bucket. The name must exist and be unique.	No default value.	Required

Azure

System properties for `AZURE_PING`.

System Property	Description	Default Value	Required/Optional
<code>jboss.jgroups.azure_ping.storage_account_name</code>	Name of the Azure storage account. The name must exist and be unique.	No default value.	Required
<code>jboss.jgroups.azure_ping.storage_access_key</code>	Name of the Azure storage access key.	No default value.	Required
<code>jboss.jgroups.azure_ping.container</code>	Valid DNS name of the container that stores ping information.	No default value.	Required

Kubernetes

System properties for `DNS_PING`.

System Property	Description	Default Value	Required/Optional
<code>jgroups.dns.query</code>	Sets the DNS record that returns cluster members.	No default value.	Required

4.6. Using Inline JGroups Stacks

You can insert complete JGroups stack definitions into `infinispan.xml` files.

Procedure

- Embed a custom JGroups stack declaration in your `infinispan.xml` file.

```
<infinispan>
  <!-- Contains one or more JGroups stack definitions. -->
  <jgroups>
    <!-- Defines a custom JGroups stack named "prod". -->
    <stack name="prod">
      <TCP bind_port="7800" port_range="30" recv_buf_size="20000000" send_buf_size
="640000"/>
      <MPING break_on_coord_rsp="true"
mcast_addr="${jgroups.mping.mcast_addr:228.2.4.6}"
mcast_port="${jgroups.mping.mcast_port:43366}"
num_discovery_runs="3"
ip_ttl="${jgroups.udp.ip_ttl:2}"/>
      <MERGE3 />
      <FD_SOCK />
      <FD_ALL timeout="3000" interval="1000" timeout_check_interval="1000" />
      <VERIFY_SUSPECT timeout="1000" />
      <pbcast.NAKACK2 use_mcast_xmit="false" xmit_interval="100"
xmit_table_num_rows="50"
xmit_table_msgs_per_row="1024"
xmit_table_max_compaction_time="30000" />
      <UNICAST3 xmit_interval="100" xmit_table_num_rows="50"
xmit_table_msgs_per_row="1024"
xmit_table_max_compaction_time="30000" />
      <pbcast.STABLE stability_delay="200" desired_avg_gossip="2000" max_bytes="1M"
/>
      <pbcast.GMS print_local_addr="false" join_timeout=
"${jgroups.join_timeout:2000}" />
      <UFC max_credits="4m" min_threshold="0.40" />
      <MFC max_credits="4m" min_threshold="0.40" />
      <FRAG3 />
    </stack>
  </jgroups>
  <cache-container default-cache="replicatedCache">
    <!-- Uses "prod" for cluster transport. -->
    <transport cluster="${infinispan.cluster.name}"
stack="prod"
node-name="${infinispan.node.name:}"/>
  </cache-container>
</infinispan>
```

4.7. Using External JGroups Stacks

Reference external files that define custom JGroups stacks in `infinispan.xml` files.

Procedure

1. Put custom JGroups stack files on the application classpath.

Alternatively you can specify an absolute path when you declare the external stack file.

2. Reference the external stack file with the `stack-file` element.

```
<infinispan>
  <jgroups>
    <!-- Creates a "prod-tcp" stack that references an external file. -->
    <stack-file name="prod-tcp" path="prod-jgroups-tcp.xml"/>
  </jgroups>
  <cache-container default-cache="replicatedCache">
    <!-- Use the "prod-tcp" stack for cluster transport. -->
    <transport stack="prod-tcp" />
    <replicated-cache name="replicatedCache"/>
  </cache-container>
  <!-- Cache configuration goes here. -->
</infinispan>
```

4.8. Using Custom JChannels

Construct custom JGroups JChannels as in the following example:

```
GlobalConfigurationBuilder global = new GlobalConfigurationBuilder();
JChannel jchannel = new JChannel();
// Configure the jchannel as needed.
JGroupsTransport transport = new JGroupsTransport(jchannel);
global.transport().transport(transport);
new DefaultCacheManager(global.build());
```



Infinispan cannot use custom JChannels that are already connected.

Reference

[JGroups JChannel](#)

4.9. Encrypting Cluster Transport

Secure cluster transport so that nodes communicate with encrypted messages. You can also configure Infinispan clusters to perform certificate authentication so that only nodes with valid identities can join.

4.9.1. Infinispan Cluster Security

To secure cluster traffic, you configure Infinispan nodes to encrypt JGroups message payloads with secret keys.

Infinispan nodes can obtain secret keys from either:

- The coordinator node (asymmetric encryption).
- A shared keystore (symmetric encryption).

Retrieving secret keys from coordinator nodes

You configure asymmetric encryption by adding the `ASYM_ENCRYPT` protocol to a JGroups stack in your Infinispan configuration. This allows Infinispan clusters to generate and distribute secret keys.



When using asymmetric encryption, you should also provide keystores so that nodes can perform certificate authentication and securely exchange secret keys. This protects your cluster from man-in-the-middle (MitM) attacks.

Asymmetric encryption secures cluster traffic as follows:

1. The first node in the Infinispan cluster, the coordinator node, generates a secret key.
2. A joining node performs certificate authentication with the coordinator to mutually verify identity.
3. The joining node requests the secret key from the coordinator node. That request includes the public key for the joining node.
4. The coordinator node encrypts the secret key with the public key and returns it to the joining node.
5. The joining node decrypts and installs the secret key.
6. The node joins the cluster, encrypting and decrypting messages with the secret key.

Retrieving secret keys from shared keystores

You configure symmetric encryption by adding the `SYM_ENCRYPT` protocol to a JGroups stack in your Infinispan configuration. This allows Infinispan clusters to obtain secret keys from keystores that you provide.

1. Nodes install the secret key from a keystore on the Infinispan classpath at startup.
2. Node join clusters, encrypting and decrypting messages with the secret key.

Comparison of asymmetric and symmetric encryption

`ASYM_ENCRYPT` with certificate authentication provides an additional layer of encryption in comparison with `SYM_ENCRYPT`. You provide keystores that encrypt the requests to coordinator nodes for the secret key. Infinispan automatically generates that secret key and handles cluster traffic, while letting you specify when to generate secret keys. For example, you can configure clusters to generate new secret keys when nodes leave. This ensures that nodes cannot bypass certificate authentication and join with old keys.

`SYM_ENCRYPT`, on the other hand, is faster than `ASYM_ENCRYPT` because nodes do not need to exchange keys with the cluster coordinator. A potential drawback to `SYM_ENCRYPT` is that there is no configuration to automatically generate new secret keys when cluster membership changes. Users are responsible for generating and distributing the secret keys that nodes use to encrypt cluster traffic.

4.9.2. Configuring Cluster Transport with Asymmetric Encryption

Configure Infinispan clusters to generate and distribute secret keys that encrypt JGroups messages.

Procedure

1. Create a keystore with certificate chains that enables Infinispan to verify node identity.
2. Place the keystore on the classpath for each node in the cluster.

For Infinispan Server, you put the keystore in the \$ISPN_HOME directory.

3. Add the `SSL_KEY_EXCHANGE` and `ASYM_ENCRYPT` protocols to a JGroups stack in your Infinispan configuration, as in the following example:

```
<infinispan>
  <jgroups>
    <!-- Creates a secure JGroups stack named "encrypt-tcp" that extends the
    default TCP stack. -->
    <stack name="encrypt-tcp" extends="tcp">
      <!-- Adds a keystore that nodes use to perform certificate authentication.
      -->
      <!-- Uses the stack.combine and stack.position attributes to insert
      SSL_KEY_EXCHANGE into the default TCP stack after VERIFY_SUSPECT. -->
      <SSL_KEY_EXCHANGE keystore_name="mykeystore.jks"
        keystore_password="changeit"
        stack.combine="INSERT_AFTER"
        stack.position="VERIFY_SUSPECT"/>
      <!-- Configures ASYM_ENCRYPT -->
      <!-- Uses the stack.combine and stack.position attributes to insert
      ASYM_ENCRYPT into the default TCP stack before pbcst.NAKACK2. -->
      <!-- The use_external_key_exchange = "true" attribute configures nodes to use
      the 'SSL_KEY_EXCHANGE' protocol for certificate authentication. -->
      <ASYM_ENCRYPT asym_keylength="2048"
        asym_algorithm="RSA"
        change_key_on_coord_leave = "false"
        change_key_on_leave = "false"
        use_external_key_exchange = "true"
        stack.combine="INSERT_BEFORE"
        stack.position="pbcst.NAKACK2"/>
    </stack>
  </jgroups>
  <cache-container name="default" statistics="true">
    <!-- Configures the cluster to use the JGroups stack. -->
    <transport cluster="${infinispan.cluster.name}"
      stack="encrypt-tcp"
      node-name="${infinispan.node.name:}"/>
  </cache-container>
</infinispan>
```

Verification

When you start your Infinispan cluster, the following log message indicates that the cluster is using the secure JGroups stack:

```
[org.infinispan.CLUSTER] ISPN000078: Starting JGroups channel cluster with stack
<encrypted_stack_name>
```

Infinispan nodes can join the cluster only if they use **ASYM_ENCRYPT** and can obtain the secret key from the coordinator node. Otherwise the following message is written to Infinispan logs:

```
[org.jgroups.protocols.ASYM_ENCRYPT] <hostname>: received message without encrypt
header from <hostname>; dropping it
```

Reference

The example **ASYM_ENCRYPT** configuration in this procedure shows commonly used parameters. Refer to JGroups documentation for the full set of available parameters.

- [JGroups 4 Manual](#)
- [JGroups 4.2 Schema](#)

4.9.3. Configuring Cluster Transport with Symmetric Encryption

Configure Infinispan clusters to encrypt JGroups messages with secret keys from keystores that you provide.

Procedure

1. Create a keystore that contains a secret key.
2. Place the keystore on the classpath for each node in the cluster.

For Infinispan Server, you put the keystore in the \$ISPN_HOME directory.

3. Add the **SYM_ENCRYPT** protocol to a JGroups stack in your Infinispan configuration.

```

<infinispan>
  <jgroups>
    <!-- Creates a secure JGroups stack named "encrypt-tcp" that extends the default
    TCP stack. -->
    <stack name="encrypt-tcp" extends="tcp">
      <!-- Adds a keystore from which nodes obtain secret keys. -->
      <!-- Uses the stack.combine and stack.position attributes to insert SYM_ENCRYPT
      into the default TCP stack after VERIFY_SUSPECT. -->
      <SYM_ENCRYPT keystore_name="myKeystore.p12"
        keystore_type="PKCS12"
        store_password="changeit"
        key_password="changeit"
        alias="myKey"
        stack.combine="INSERT_AFTER"
        stack.position="VERIFY_SUSPECT"/>
    </stack>
  </jgroups>
  <cache-container name="default" statistics="true">
    <!-- Configures the cluster to use the JGroups stack. -->
    <transport cluster="${infinispan.cluster.name}"
      stack="encrypt-tcp"
      node-name="${infinispan.node.name:}"/>
  </cache-container>
</infinispan>

```

Verification

When you start your Infinispan cluster, the following log message indicates that the cluster is using the secure JGroups stack:

```
[org.infinispan.CLUSTER] ISPN000078: Starting JGroups channel cluster with stack
<encrypted_stack_name>
```

Infinispan nodes can join the cluster only if they use `SYM_ENCRYPT` and can obtain the secret key from the shared keystore. Otherwise the following message is written to Infinispan logs:

```
[org.jgroups.protocols.SYM_ENCRYPT] <hostname>: received message without encrypt
header from <hostname>; dropping it
```

Reference

The example `SYM_ENCRYPT` configuration in this procedure shows commonly used parameters. Refer to JGroups documentation for the full set of available parameters.

- [JGroups 4 Manual](#)
- [JGroups 4.2 Schema](#)

4.10. TCP and UDP Ports for Cluster Traffic

Infinispan uses the following ports for cluster transport messages:

Default Port	Protocol	Description
7800	TCP/UDP	JGroups cluster bind port
46655	UDP	JGroups multicast

Cross-Site Replication

Infinispan uses the following ports for the JGroups RELAY2 protocol:

7900

For Infinispan clusters running on Kubernetes.

7800

If using UDP for traffic between nodes and TCP for traffic between clusters.

7801

If using TCP for traffic between nodes and TCP for traffic between clusters.