Article <u>Pete Greskoff</u> · Jan 10, 2017 9m read

## Creating SSL-Enabled Mirror Using Public Key Infrastructure (PKI)

NB. Please be advised that PKI is not intended to produce certificates for secure production systems. You should make alternate arrangements to create certificates for your productions. NB. PKI is deprecated as of IRIS 2024.1: <u>documentation</u> and <u>announcement</u>.

In this post, I am going to detail how to set up a mirror using SSL, including generating the certificates and keys via the <u>Public Key Infrastructure</u> built in to Caché. The goal of this is to take you from new installations to a working mirror with SSL, including a primary, backup, and DR async member, along with a mirrored database. I will not go into security recommendations or restricting access to the files. This is meant to just simply get a mirror up and running. Example screenshots are taken on a 2016.1 version of Caché, so yours may look slightly different.

Step 1: Configure Certificate Authority (CA) Server

On one of your instances (in my case the one that will be the first mirror member configured), go to the System Management Portal and go to the [System Administration -> Security -> Public Key Infrastructure] page. Here you will ' Configure local Certificate Authority server '.

<b>A</b>	Configuration »	Users
Home	Security »	Roles
	Licensing »	Resources
C DeenSee	Encryption »	Services
		Security Domains
•		Applications »
Ensemble		SSL/TLS Configurations
<b>~</b>		X.509 Credentials
		OAuth 2.0 »
System Operation		System Security »
		Auditing »
		Security Advisor
System Explorer		Mobile Phone
~		Public Key Infrastructure
System Administration		

You can choose whatever File name root (this is the file name only, no path or extension) and Directory you want to have these files in. I ' II use ' CAServer' as the File name root, and the directory will be my <installdir>/mgr/CAServer/. This will avoid future confusion when the client keys and certificates are put into the <installdir>/mgr/ folder, as I ' II be using my first mirror member as the CA Server. Go to the next page. You will then need to enter a password, and I ' II use ' serverpassword ' in my example. You can then assign attribute values for your Distinguished Name. I ' II set Country to ' US ' and Common Name to ' CASrv '. You can accept defaults for validity periods, leave the email section blank, and save.

Attribute Type		Attribute	/alue
Country	US	(Enter the two characte	er country code only)
State or Province			
ocality			
Organization			
Organizational Unit			
Common Name	CASrv		
Common Name * Please enter at lea lidity period for Ce	CASrv ast one / rtificate	Attribute Value Authority's Certificate	(days) 3650
Common Name * Please enter at lea lidity period for Ce lidity period for Ce onfigure email	CASrv ast one / rtificate rtificate	Attribute Value Authority's Certificate s issued by Certificate	(days) 3650 Authority (days) 365
Common Name * Please enter at lea lidity period for Cer lidity period for Cer onfigure email MTP server	CASrv ast one / rtificate rtificate	Attribute Value Authority's Certificate s issued by Certificate SMTP username	(days) 3650 Authority (days) 365
Common Name * Please enter at lea lidity period for Cel lidity period for Cel onfigure email MTP server MTP password	CASrv ast one a rtificate rtificate	Attribute Value Authority's Certificate s issued by Certificate SMTP username Confirm password	(days) 3650 Authority (days) 365
Common Name * Please enter at lea lidity period for Cel lidity period for Cel onfigure email MTP server MTP password Certificate Authority s	CASrv ast one / rtificate rtificate	Attribute Value Authority's Certificate s issued by Certificate SMTP username Confirm password dministrator's email addr	(days) 3650 Authority (days) 365

You should see a message about files getting generated (.cer, .key, and .srl) in the directory you configured.

Step 2: Generate Key/Certificate For First Mirror Member

At this point, you need to generate the certificate and keys for the instance that will become your first mirror member. This time, go to the System Management Portal where you will set up the first mirror member, and go to the [System Administration -> Security -> Public Key Infrastructure] page again (see screenshot above). You need to 'Configure local Certificate Authority client'. For the 'Certificate Authority server hostname', you need to put either the machine name or IP address of the instance you used for step 1, and for the 'Certificate Authority WebServer port number' use that instance's web server port (you can get this from the URL in that instance's Management portal):

# () localhost 57772, csp/sys/sec/%25CSP.UI.Portal.PKI.zen

Make sure you are using the port number for the instance you configured as the CA Server, not the one you are setting up as the client (though they may be the same). You can put your own name as the technical contact (the phone number and email are optional) and save.

Now you should go to 'Submit Certificate Signing Request to Certificate Authority server'. You 'Il need a file name (I'm using 'MachineAclient') and password ('MachineApassword') as well as again setting values for a Distinguished Name (Country='US' and Common Name='MachineA'). Note that for each certificate you make, at least one of these values must be different than what was entered for the CA certificate. Otherwise, you may run into failures at a later step.

## Submit Certificate Signing Request to Certificate Authority server

equired. Valid char	acters: alp	phanumeric, hyphen or underscore.	
assword for Privat	te Key file		
Confirm F	assword	1 1	
ubject Distinguishe	ed Name:	· · · · · · · · · · · · · · · · · · ·	
Attribute Type		Attribute Value	
Country	US	(Enter the two character country code	only)
State or Province			
Locality			
Locality Organization			
Locality Organization Organizational Uni	t		
Locality Organization Organizational Uni Common Name	t Machine	eA	

Certificate Signing Request MachineA\_client successfully submitted to the Certificate Authority at instance PRIM on node WN7-64-BAS-001.ISCINTERNAL.COM. SHA-1 Fingerprint: BC:F6:23:6B:01:11:64:EB:6D:C7:F1:90:08:67:76:26:42:6B:BE:D0

At this point, you ' II need to go to the machine you configured to be your CA Server. From the same page, you need to ' Process pending Certificate Signing Requests'. You should see one like this:

### **Process pending Certificate Signing Requests**

Hostname	Instance	Filename
WIN7-64-BAS-001.ISCINTERNAL.COM	PRIM	MachineA_client Process Delete

You should process this request, leaving default values, and 'Issue Certificate'. You'll need to enter your CA Server password from step 1 ('serverpassword' for me).

Finally, you need to get the certificate. Back on the first mirror member machine, from the same page, go to 'Get Certificate(s) from Certificate Authority server', and click 'Get' like here:

### Get Certificate(s) from Certificate Authority server

Get Certifica	te Authority Certificate	how cortifi	icates for this inst	2000
		now centin	cates for this mist	ance
Issued Cert	tificates			
Serial Number	Hostname	Instance	Filename	•
2	WIN7-64-BAS-001.ISCINTERNAL.CO	M PRIM	MachineA_client	Get

You should then see a message indicating that the certificate was saved in the <install>/mgr/ directory of your instance.

Step 3: Configure The Mirror On First Mirror Member

First, start the ISCAgent per this documentation (and set it to start automatically on system startup if you don 't want to have to do this every time your machine reboots).

Then, in the System Management Portal, go to the [System Administration -> Configuration -> Mirror Settings -> Enable Mirror Service] page to enable the service (if it isn ' t already enabled). Next, go to the ' Create a Mirror ' page in the same menu.

		Configuration »	System Configuration »	Enable Mirror Service
	Home	Security »	Connectivity »	Create a Mirror
		Licensing »	Mirror Settings »	Edit Mirror
	DeepSee	Encryption »	Database Backup »	Edit Async
			CSP Gateway	Join as Failover
-				Join as Async
	Ensemble		SQL and Object Settings »	_
000			Device Settings »	
	Quarteria Que constituen		National Language Settings »	
	System Operation		Zen Reports »	
			Additional Settings »	
	System Explorer			
-	System Administration			

You will need to enter a mirror name ( ' PKIMIRROR ' in my case). You should click ' Set up SSL/TLS ', and then enter the information there. If this is not the same machine where you configured the CA Server, you ' II need to get a copy of the CA Server certificate ( ' CAServer.cer ') on this machine. You can do this in the ' Get Certificate(s) from Certificate Authority server ' page:

#### Certificate Authority Client

- Submit Certificate Signing Request to Certificate Authority server
- Get Certificate(s) from Certificate Authority server
- Configure local Certificate Authority client

#### Certificate Authority Server

- Process pending Certificate Signing Requests
- Configure local Certificate Authority server

Get Certifica	te Authority Certificate	Server			
		show cert	ificates f	or this ins	tance
Issued Cer	tificates				
Serial Number	Hostname		Instance	Filename	
2	PGRESKOFF6440.ISCINTE	RNAL.COM	20161	primcli	Get

Cartificate/a) from Cartificate Authority conver

Back in the 'Set up SSL/TLS' page, the first line is asking for that CA server certificate. You should leave the 'Certificate Revocation list' blank. If you want to use this, please contact the WRC. For 'This server's credentials', you'II need to enter the certificate and key that we generated in step 2. They will be in the <install>/mgr/directory. You'II also need to enter your password here (click the 'Enter new password' button as shown). This password is the one you chose in step 2 ('MachineApassword' for me). In my example, I am only allowing TLS v1.2 protocol as shown below.

#### Creating SSL-Enabled Mirror Using Public Key Infrastructure (PKI) Published on InterSystems Developer Community (https://community.intersystems.com)

Edit SSL/TLS Configurations for Mirror		×
Edit SSL/TLS Configurations for Mirror		User: UnknownUse Namespace: %SY
Use the form below to edit SSL/TLS configurations for Mirror. A	All changes made below will be saved to both %MirrorClient and %MirrorS	erver:
File containing trusted Certificate Authority X.509 certificate	C:\InterSystems\PRIM\mgr\CAServer\CA_Server.cer	Browse
File containing Certificate Revocation List		Browse
This server's credentials	File containing this configuration's ¥ 509 certificate	
	C:\InterSystems\PRIM\mgr\MachineA_client.cer	Browse
	File containing associated private key	
	C:\InterSystems\PRIM\mgr\MachineA_client.key	Browse
	Private key type   RSA DSA	
	Private key nassword	5
	Private key password (confirm)	
Cryptographic settings	Protocols SSLv2 SSLv3 TLSv1.0 TLSv1.1 TLSv	v1.2
	Enabled ciphersuites ALL:IaNULL:IeNULL:IEXP:ISSLv2	
		Cancel Save

For this example, I won't use an arbiter or a Virtual IP, so you can un-check those boxes in the 'Create Mirror' page. We'll accept the defaults for 'Compression', 'Mirror Member Name', and 'Mirror Agent Port' (since I didn't configure the ISCAgent to be on a different port), but I'm going to change the 'Superserver Address' to use an IP instead of a host name (personal preference). Just make sure that the other future mirror members are able to reach this machine at the address you choose. Once you save this, take a look at the mirror monitor [System Operation -> Mirror Monitor]. It should look something like this:

This system is a failover member in mirror PKIMIRROR

or Failover Member Information			er connectio									
Mirror Member Name	This Failover Member WIN7-64-BAS-001/PRIM		Other Failover Member In/a n/a		A	rbiter Addre Failover Mo	ess / ode /	Arbiter no Agent Co	ot configu Introlled	red		
Mirror Private Address	192.168.2.100		n/a		Con	nection Sta	tus	This men	nber is n	ot connect	ted to the a	rbite
ror Member Status												
Member Name	Member Type	Status	Journal Transfer	Dejourn	naling	X.509 DN						
WIN7-64-BAS-001/PRIM	Failover	Primary	N/A	N/A		N/A						
rrored Databases												
rrored Databases Filter: Page	e size: 0	Мах гол	vs: 1000 Resu	ults: 0 P	age:	: << 1 >> >	of 1					
rrored Databases Filter: Pag Name Directory	e size: 0 Status Next Re	Max rov ecord To	vs: 1000 Resu Dejournal (Time, F	ults: 0 P	age:	: « <mark>1</mark> » >	of 1	]				
Filter: Page Name Directory No Results	e size: 0 Status Next Re	Max rov ecord To	vs: 1000 Resu Dejournal (Time, F	ults: 0 P ilename,	age:  -	:	) of 1					
Filter: Page Name Directory No Results	e size: 0 Status Next Re	Max rov ecord To	vs: 1000 Resu Dejournal (Time, F	ults: 0 P	'age: ∣₁ Offse	: « <b>1</b> » >	of 1					
Filter: Page Page Name Directory S No Results Click 'Go' to perform an a	e size: 0 Status Next Re	Max rov cord To databa	vs: 1000 Resu Dejournal (Time, F ses	uits: 0 P	age:  -	: « <b>1</b> »> > D	of 1					

If you see that it 's still in a 'Transition' status, wait a few seconds and refresh the page. Note that these statuses were enhanced in 2016.2. You can see what they look like in the latest released version <u>here</u>.

Step 4: Generate Key/Certificate For Second Failover Mirror Member

This is the same process as step 2, but I ' II replace anything with ' MachineA ' in the name with ' MachineB ' . As I mentioned before, make sure you change at least 1 of the fields in the Distinguished Name section from the CA certificate. You also need to be sure you get the correct certificate in the Get Certificate step, as you may see more than one option.

Step 5: Join Mirror as Failover Member

Just like you did for the first mirror member, you need to start the ISCAgent and enable the mirror service for this instance (refer to step 3 for details on how to do this). Then, you can join the mirror as a failover member at [System Administration -> Configuration -> Mirror Settings -> Join as Failover].

		Configuration »	System Configuration »	Enable Mirror Service
	Home	Security »	Connectivity »	Create a Mirror
		Licensing »	Mirror Settings »	Edit Mirror
	DeepSee	Encryption »	Database Backup »	Edit Async
	recharge		CSP Gateway	Join as Failover
			Management	Join as Async
	Ensemble		SQL and Object Settings »	_
000			Device Settings »	
	System Operation		National Language Settings »	
	System Operation		Zen Reports »	
			Additional Settings »	
	System Explorer			
-	System Administration			

You ' II need the ' Mirror Name ', ' Agent Address on Other System ' (the same as the one you configured as the Superserver address for the other member), and the instance name of the now-primary instance.

Mirror Name	PKIMIRROR					
	Required.					
Other Mirror	Failover Member's Info	1				
Agent Addı	ess on Other System	192.168.2.100				
		Required.				
	Mirror Agent Port	2188				
		Required.				
	Caché Instance Name	PRIM				
		Required.				

After you click 'Next', you should see a message indicating that the mirror requires SSL, so you should again use the 'Set up SSL/TLS' link. As in step 3, you' Il need the CA Server certificate (same file we used in step 3, refer to that step for how to retrieve it), and you' Il replace machine A's files and password with machine B's for this dialog.

File containing trusted Certificate Authority X.509 certificate	C:\InterSystems\PRIM\mgr\CAServer\CA_Server.cer	Browse		
File containing Certificate Revocation List		Browse		
This server's credentials	File containing this configuration's X.509 certificate			
	C:\InterSystems\BACK\mgr\MachineB_client.cer	Browse		
	File containing associated private key			
	C:\InterSystems\BACK\mgr\MachineB_client.key Browse			
	Private key type       • RSA       DSA         Password:       • Enter new password       Clear password       Leave as         Private key password       • • • • • • • • • • • • • • • • • • •	is		
Cryptographic settings	Protocols SSLv2 SSLv3 TLSv1.0 TLSv1.1 TLSv1.1 TLSv1.1 TLSv1.1	3v1.2		

Again, I 'm only using TLSv1.2. Once you 've saved that, you should be able to add information about this mirror member. Again, I 'm going to change the hostnames to IP 's, but feel free to use any IP/hostname that the other member can contact this machine on. Note that the IP 's are the same for my members, as I have set this up with multiple instances on the same server.

I.

	This System	Other System
Mirror Member Name	WIN7-64-BAS-001/BACK	WIN7-64-BAS-001/PRIM
Superserver Address	192.168.2.100	192.168.2.100
Mirror Agent Port	2188	2188
SSL/TLS Requirement	The mirror requires SSL/TLS. Edit SSL/TLS	
Mirror Private Address	192.168.2.100	192.168.2.100

When you save this, you should see a message telling you not to forget to add this node to the primary 's configuration.

Step 6: Authorize 2<sup>nd</sup> Failover Member on the Primary Member

Now we need to go back to the now primary instance where we created the mirror. From the [System Administration -> Configuration -> Mirror Settings -> Edit Mirror] page, you should see a box at the bottom titled ' Pending New Members ' including the failover member that you just added. Check the box for that member and click Authorize (there should be a dialog popup to confirm).

Pending Sele	g New M ect the	<mark>lembers</mark> member(s) vou wish to authoriz	e or reiect:						
		Name	Member Type	DN					
×		WIN7-64-BAS-001/BACK	Failover	CN=MachineB,C=US					
	Authorize Reject								

Now if you go back to [System Operation -> Mirror Monitor], it should look like this (similar on both instances):

This system is a failover member in mirror PKIMIRROR

M	lirror Failover Member Inf	ormation		A	rbiter Connection St	atus
		This Failover Member	Other Failover Member		Arbiter Address	Arbiter not configured
I	Mirror Member Name	WIN7-64-BAS-001/PRIM	WIN7-64-BAS-001/BACK		Failover Mode	Agent Controlled
I	Superserver Address	192.168.2.100	192.168.2.100			
	Mirror Private Address	192.168.2.100	192.168.2.100		Connection Status	This member is not connected to the arbiter

**Mirror Member Status** 

Member Name	Member Type	Status	Journal Transfer	Dejournaling	X.509 DN
WIN7-64-BAS-001/PRIM	Failover	Primary	N/A	N/A	N/A
WIN7-64-BAS-001/BACK	Failover	Backup	Active	Caught up	N/A

Again, if you see a 'Transition' status, wait a few seconds and refresh the page.

#### Step 7: Generate Key/Certificate for Async Member

This is the same as step 2, but I ' II replace anything with ' MachineA ' in the name with ' MachineC ' . As I mentioned before, make sure you change at least 1 of the fields in the Distinguished Name section from the CA certificate. Make sure you get the correct certificate in the ' Get Certificate ' page, as you may see more than one option.

#### Step 8: Join Mirror as Async Member

This is similar to step 5. The only difference is that you may only be asked to configure 1 address (this depends what version you ' re running), and you have the added option for an Async Member System Type (I will use Disaster Recovery, but you ' re welcome to use one of the reporting options). You ' II again see a message about requiring SSL, and you ' II need to set that up similarly (MachineC instead of MachineB). Again, you ' II see a message after saving the configuration indicating that you should add this instance as an authorized async on the failover nodes.

#### Step 9: Authorize Async Member on the Primary Member

Follow the same procedure as in step 6. Note that this procedure has been simplified in recent versions to match behavior for a 2<sup>nd</sup> failover member. Previously, you needed to manually add authorized async member information. Once this complete, there is one extra step to make sure the mirror monitors are in sync. You should go to the [System Operation -> Mirror Monitor] on the 2<sup>nd</sup> failover member (now the backup), and click 'Stop mirror'. After that 's complete, you should then click 'Start mirror'. This is just to make sure that instance retrieves the information about the async member. It should not be required in later versions. The mirror monitor should now look like this:

#### This system is a failover member in mirror PKIMIRROR

	This Failover Membe	er <u>Other</u>	Failover Member		Arbite	r Address	Arbiter not co	onfigured	
Mirror Member Name	WIN7-64-BAS-001/B	ACK WIN7	-64-BAS-001/PRIM		Failo	wer Mode	Agent Contro	helled	
Superserver Address	192.168.2.100	192.1	68.2.100						
Mirror Private Address	192.168.2.100	192.1	68.2.100		Connecti	on Status	This membe	er is not connected	i to the arbite
Mombor Nomo	Member Tree	Ctatua	Journal Transfer	Dai	ournaling	V 600 DN			
Member Name	Member Type	Status	Journal Transfer	Dej	ournaling	X.509 DN			
Member Name WIN7-64-BAS-001/PRIM	Member Type Failover	Status Primary	<b>Journal Transfer</b> N/A	Dej N/A	ournaling	<b>X.509 DN</b> N/A			
Member Name WIN7-64-BAS-001/PRIM WIN7-64-BAS-001/BACK	Member Type Failover Failover	Status Primary Backup	Journal Transfer N/A Active	Dej N/A Cat	<b>ournaling</b> ught up	<b>X.509 DN</b> N/A N/A			

#### Step 10: Add a Mirrored Database

Having a mirror is no fun if you can 't mirror any data, so we may as well create a mirrored database. We will also create a namespace for this database. Go to your primary instance. First, go to [System Administration -> Configuration -> System Configuration -> Namespace] and click 'Create New Namespace ' from that page.

View:			Search:
<b>A</b>	Configuration »	System Configuration »	Memory and Startup
Home	Security »	Connectivity »	Namespaces
	Licensing »	Mirror Settings »	Local Databases
C DeepSee	Encryption »	Database Backup »	Remote Databases
	Enterprise Manager	CSP Gateway	Journal Settings
0		SQL and Object Settings »	-
Sector Ensemble		Device Settings »	-
		National Language Settings »	
System Operation		Zen Reports »	
		Additional Settings »	
System Explorer			
System Administration			

We 'II call this 'MIRROR', and we 'II need to click 'Create New Database' next to 'Select an existing database for Globals'. You'II need to enter a name ('MIRROR') and directory for this new database. On the next page, be sure to change the 'Mirrored database?' drop-down to yes (THIS IS ESSENTIAL). The mirror name will default to the database name you chose. You can change it if you wish. We will use the default setting for all other options for the database (you can change them if you want, but this database must be journaled, as it is mirrored). Once you finish that, you will return to the namespace creation page, where you should select this new database for both 'Globals and 'Routines'. You can accept the defaults for the other options (don't copy the namespace from anywhere).

Use the form below to create a new namespace:

Name of the namespace	MIRROR Required.		
Copy from	<b>T</b>		
The default database for Globals in this namespace is a	Local Database Remote Database		
Select an existing database for Globals	MIRROR Required.	•	Create New Database
The default database for Routines in this namespace is a	<ul> <li>Local Database</li> <li>Remote Database</li> </ul>		
Select an existing database for Routines	MIRROR	-	Create New Database
Create a default Web application for this namespace	<b>e</b>		
Copy namespace mappings from	•		

Repeat this process for the backup and async. Make sure to use the same mirror name for the database. Since it 's a newly created mirrored database, there is no need to take a backup of the file and restore onto the other members.

Congratulations, you now have a working mirror using SSL with 3 members sharing a mirrored database!

Other reference documentation:

Create a mirror

Create mirrored database

Create namespace and database

Edit failover member (contains some information on adding SSL to an existing mirror)

#Best Practices #High Availability #Mirroring #SSL #System Administration #InterSystems IRIS #Caché

Source

URL: https://community.intersystems.com/post/creating-ssl-enabled-mirror-using-public-key-infrastructure-pki