Roger Bacalzo
IBM Content Manager Storage Team

October 22, 2014

Product Implementation Training (PIT)

IBM FileNet Content Manager 5.2.1GA

CPE Server Communication, new 5.2.1 Feature

Introduction

- Course Overview
  - 5.2.1 CPE Server Communication Feature
- Target Audience
  - Support Teams and Lab Services
- Suggested Prerequisites
  - Knowledge of P8 Administration Environment
  - Knowledge of Advanced Storage Areas
- Version Release Date: October 31, 2014

Course Objectives

After this course you will be able to:

- Explain how the CPE server communication feature is used with Advanced Storage Areas
- Configure CPE server communication between sites

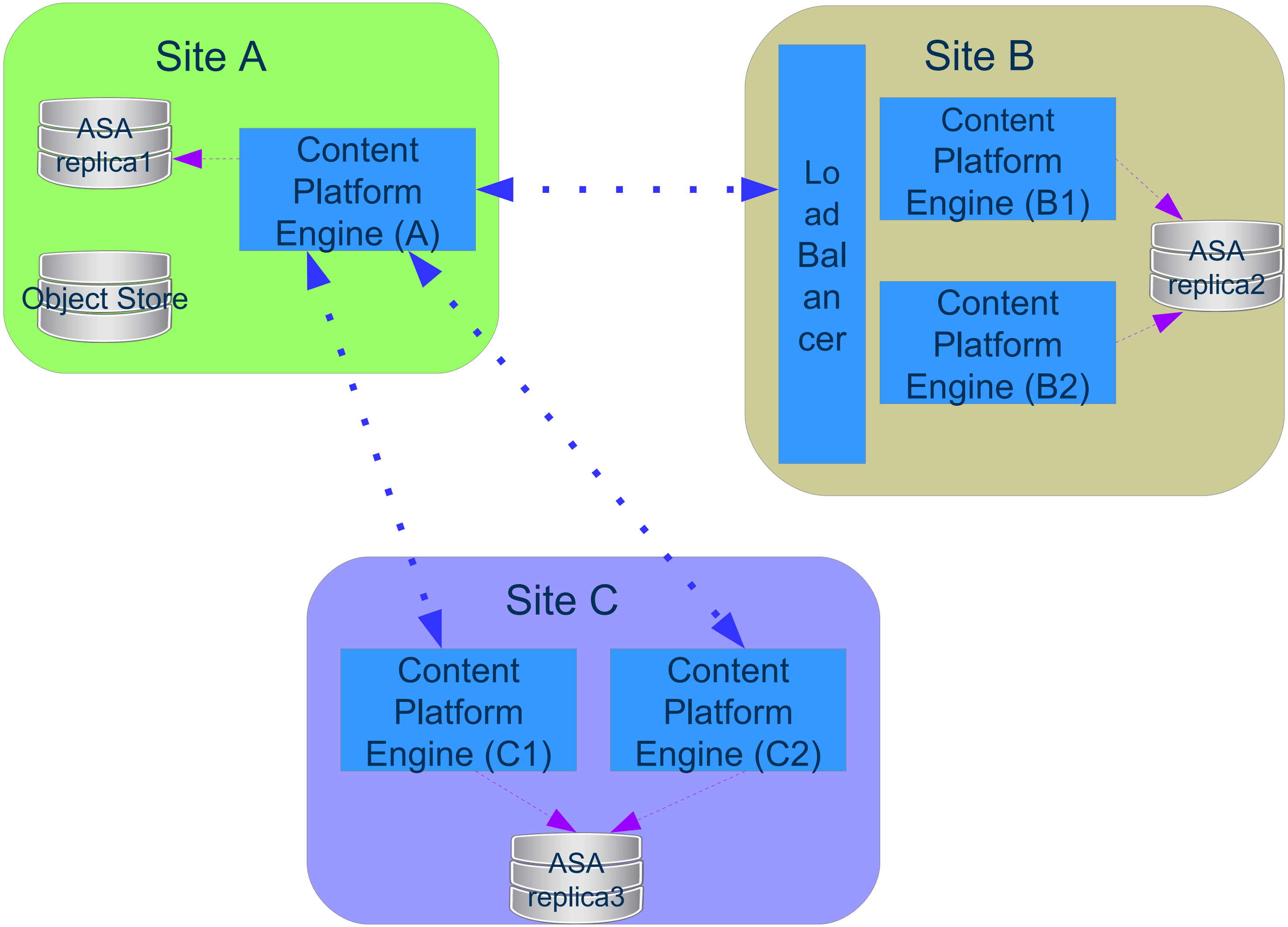
Course Roadmap

➔ Overview
- Server Communication Operations
- Authentication
- Failover
- Configuration
- Demonstration

Overview

- CPE server communication is used to send messages from one CPE server to another CPE server
- Used by Advanced Storage Area to access replicas in remote sites without requiring direct connectivity (e.g. file system mount) to replica.
- Messages only sent between sites. Message are not sent between CPE servers in the same site
- Messages secured using an authentication token sent with each request.
- Uses WSI transport to the Server Communication URL specified as property on Virtual Server
  - HTTP traffic more suited for a WAN environment in terms of speed and ease of configuration
- To properly load-balance message handling at the destination site, the Server communication URL should either:
  - Reference a HTTP load balancer or
  - Reference a comma-separated list of CPE servers

Overview


Site A
ASA replica1
Content Platform Engine (A)
Object Store
Site B
Lo ad Bal an cer
Content Platform Engine (B1)
Content Platform Engine (B2)
ASA replica2
Site C
Content Platform Engine (C1)
Content Platform Engine (C2)
ASA replica3

Course Roadmap

- Overview
- ➔ Server Communication Operations
- Authentication
- Failover
- Configuration
- Demonstration

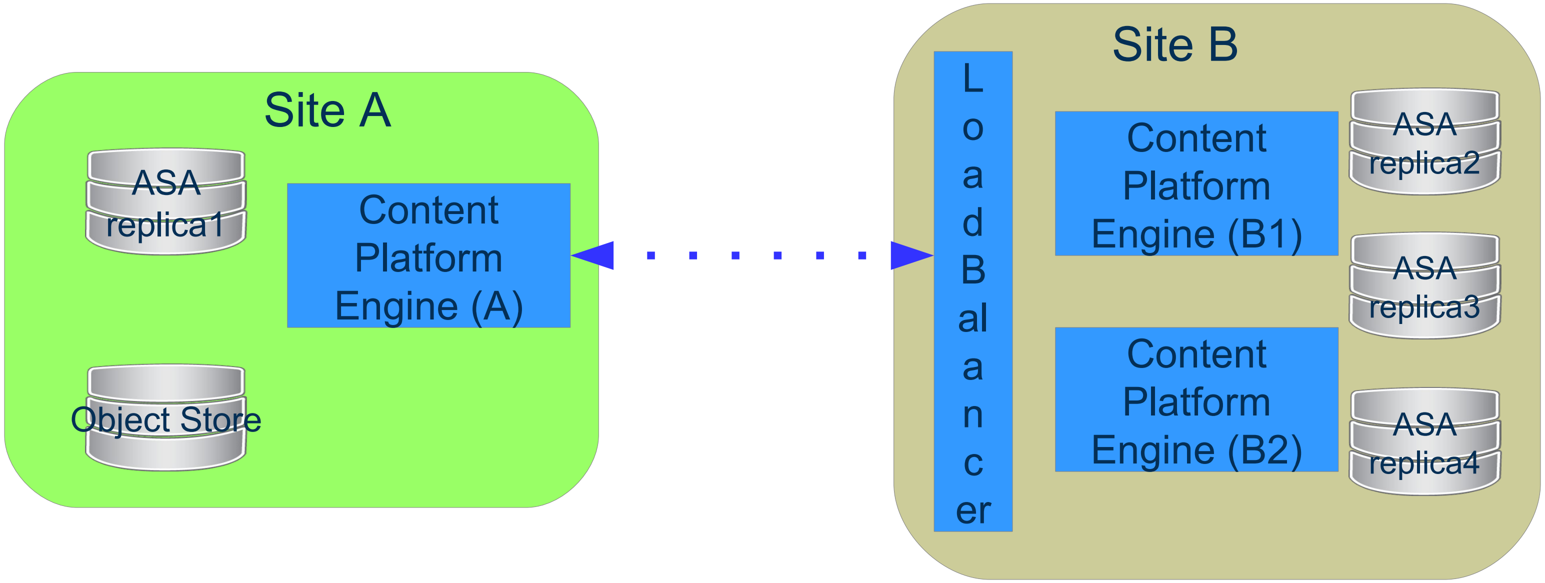
Server Communication Operations

- **Create Replica**
  - Create a replica at remote site
- **Test Replica Access**
  - Verify that replica is accessible by CPE servers at remote site
- **Create Content** (on a replica at a remote site)
- **Retrieve Content** (from a replica at a remote site)
- **Delete Content** (from a replica at a remote site)
- **Backout Abandoned Content** (from a replica at a remote site)
- **Validate Content** (in a replica at a remote site)

Batched Operations

Operations that apply to multiple replicas in a site are sent in a single request

- Create Content
- Delete Content
- Backout Content
- Validate Content



Course Roadmap

- Overview
- Server Communication Operations

➔ Authentication

- Failover
- Configuration
- Demonstration

Authentication

- Each message sent between CPE servers has a one-time-use authentication token
- Token is used to ensure validity of CPE server sending the message
- Validation performed at the CPE server receiving the message
- Authentication token constructed at sending CPE server using:
  - Server id
  - Nonce (unique for each message)
  - Timestamp
  - SHA-256 hash based on P8 domain master key

- Receiving CPE server validates the token by:
  - Re-computing SHA-256 hash to verify it is identical to the one in the token
  - Ensuring the token hasn't been seen before by this server by checking a Nonce cache of recently received tokens
  - Verifies timestamp is within allowed time-to-live interval (60 second default)

Server Clock Skew

- Since authentication token has a timestamp component, it's possible to get authentication failure if the destination CPE server's system time is not in sync with the sending CPE server's time

- Recommend that all CPE server machines utilize a Network Time Protocol (NTP) service to keep all server clocks in sync

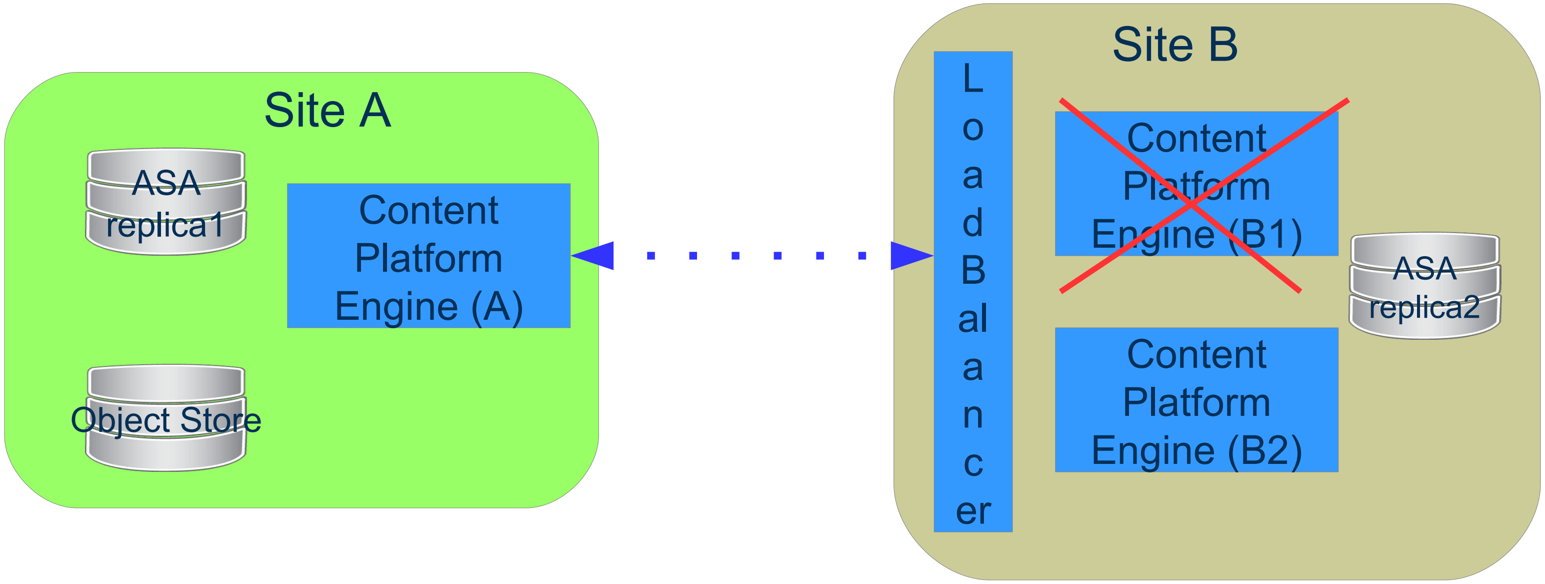
- Sending CPE server can detect authentication failures due to clock skew and resend message

Course Roadmap

- Overview
- Server Communication Operations
- Authentication
- → Failover
- Configuration
- Demonstration

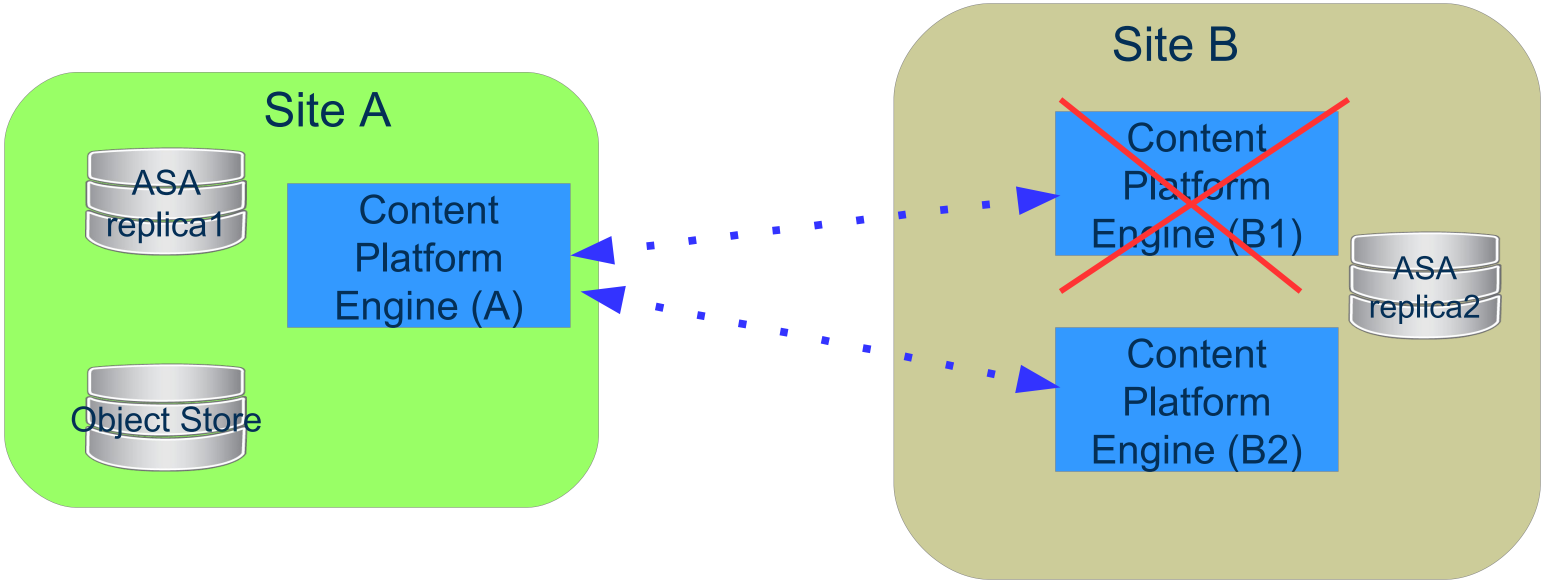
Failover

- If server communication URL specifies a load balancer to front multiple back-end CPE servers, then it is that load balancers responsibility to handle failover if one of the back-end CPE servers goes down.


Site A
ASA replica1
Content Platform Engine (A)
Object Store
Site B
Load Balancer
Content Platform Engine (B1)
Content Platform Engine (B2)
ASA replica2

Failover

- If server communication URL specifies multiple CPE serves, then each one can be tried before failing the request.


Site A
ASA replica1
Content Platform Engine (A)
Object Store
Site B
Content Platform Engine (B1)
ASA replica2
Content Platform Engine (B2)

Course Roadmap

- Overview
- Server Communication Operations
- Authentication
- Failover
- ➔ Configuration
- Demonstration

Configuration – Server Communication URL

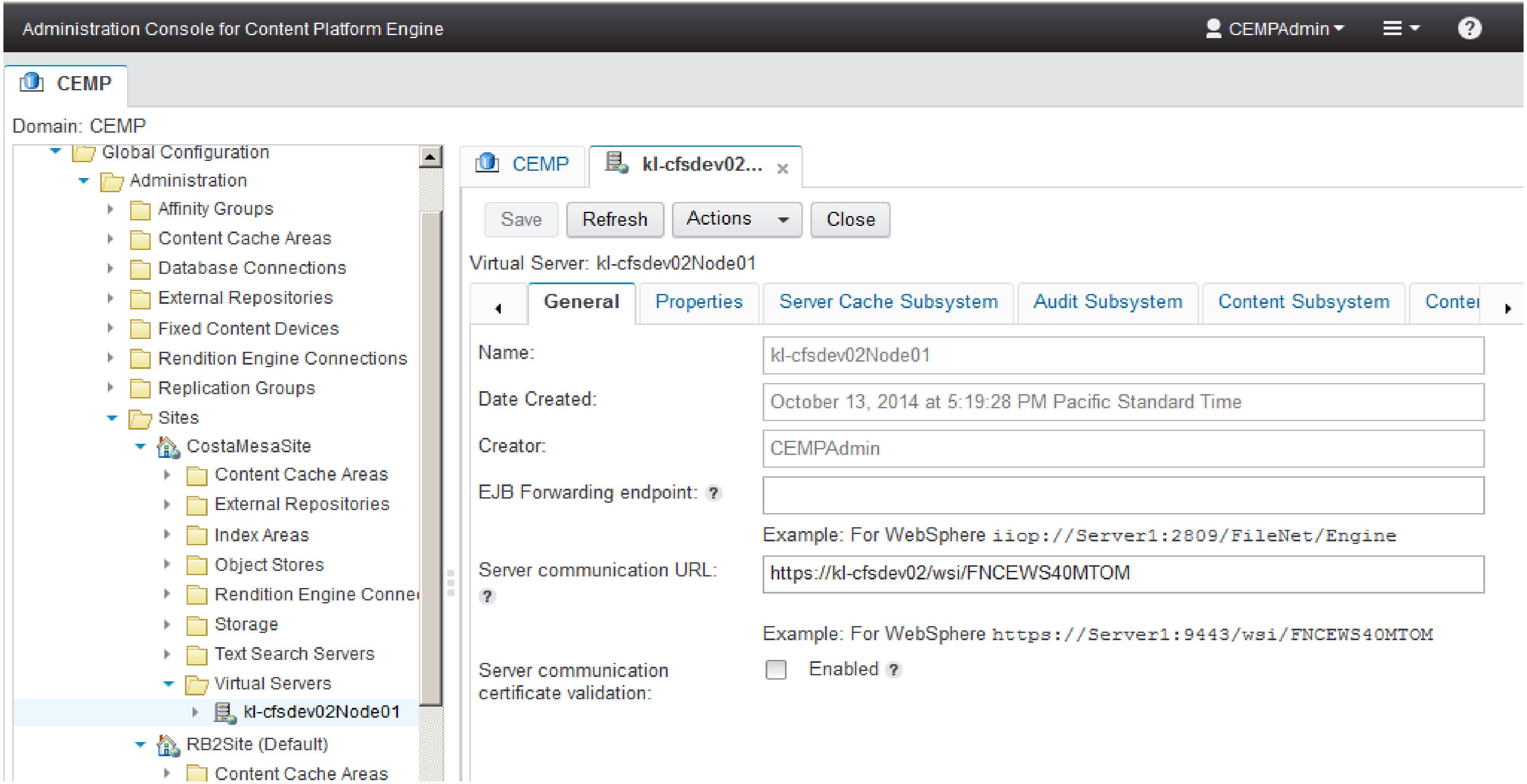
- The Server communication URL is configured at the Virtual Server node for the site that is receiving the messages (i.e. the destination site).

- On ACCE, this can be found under:
  - {domain} > Global Configuration > Administration > Sites > {site name} > Virtual Servers > {virtual server node}

- The Server communication URL should always use **https** to ensure that the messages are encrypted during transport

- If a load balancer is not being used, then specify the Server communication URL as a comma-separated list of the WSI URLs for each CPE server at the destination site.

Configuration – Server Communication URL referencing load balancer



Virtual Server: kl-cfsdev02Node01

Name: kl-cfsdev02Node01

Date Created: October 13, 2014 at 5:19:28 PM Pacific Standard Time

Creator: CEMPAdmin

EJB Forwarding endpoint: ?

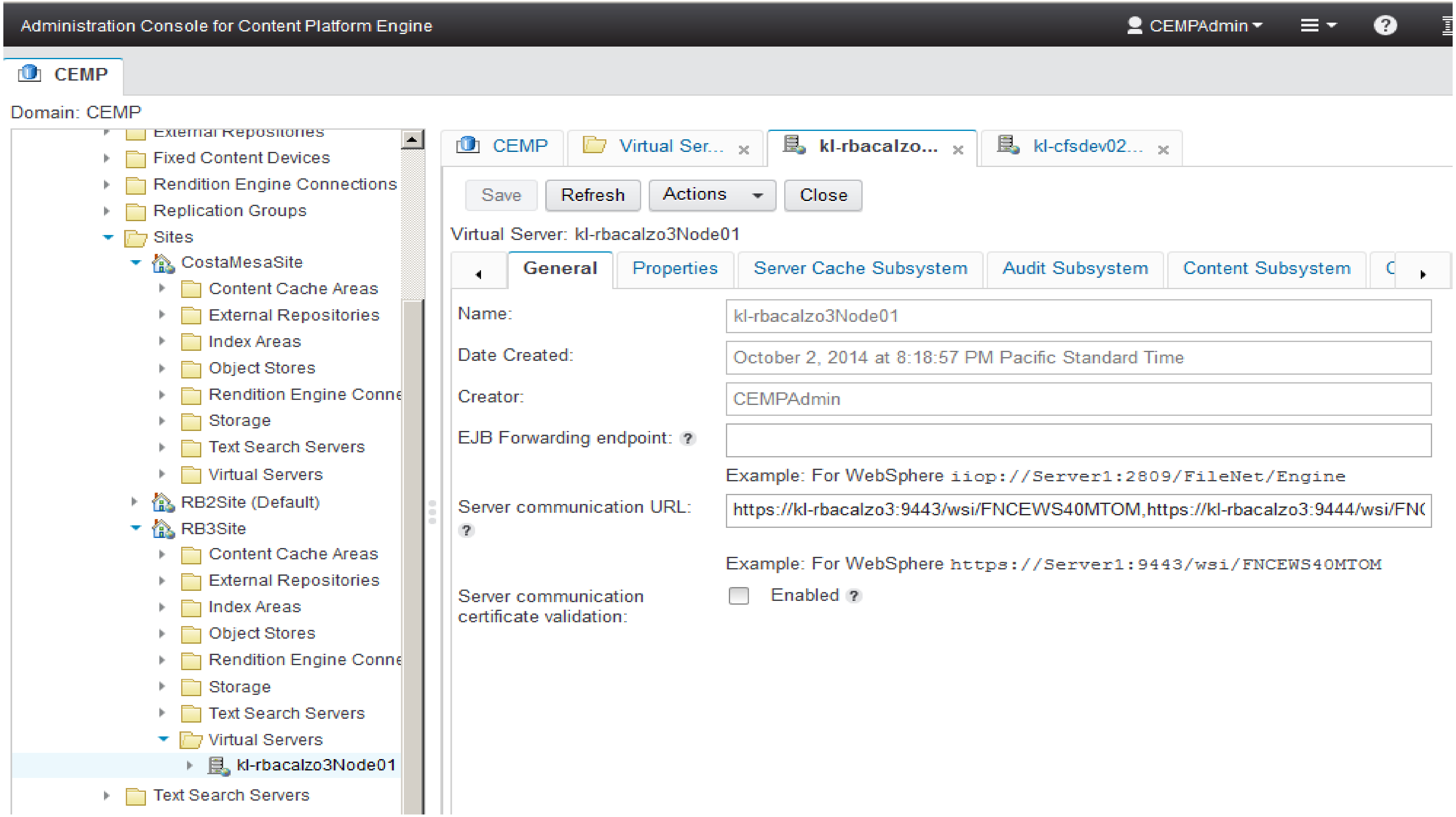
Example: For WebSphere `iiop://Server1:2809/FileNet/Engine`

Server communication URL: ? https://kl-cfsdev02/wsi/FNCEWS40MTOM

Example: For WebSphere `https://Server1:9443/wsi/FNCEWS40MTOM`

Server communication certificate validation: ☐ Enabled ?

Configuration – Server Communication URL referencing multiple CPE servers



Virtual Server: kl-rbacalzo3Node01

Name: kl-rbacalzo3Node01

Date Created: October 2, 2014 at 8:18:57 PM Pacific Standard Time

Creator: CEMPAdmin

EJB Forwarding endpoint: ?

Example: For WebSphere `iiop://Server1:2809/FileNet/Engine`

Server communication URL: ? https://kl-rbacalzo3:9443/wsi/FNCEWS40MTOM,https://kl-rbacalzo3:9444/wsi/FN(

Example: For WebSphere `https://Server1:9443/wsi/FNCEWS40MTOM`

Server communication certificate validation: □ Enabled ?

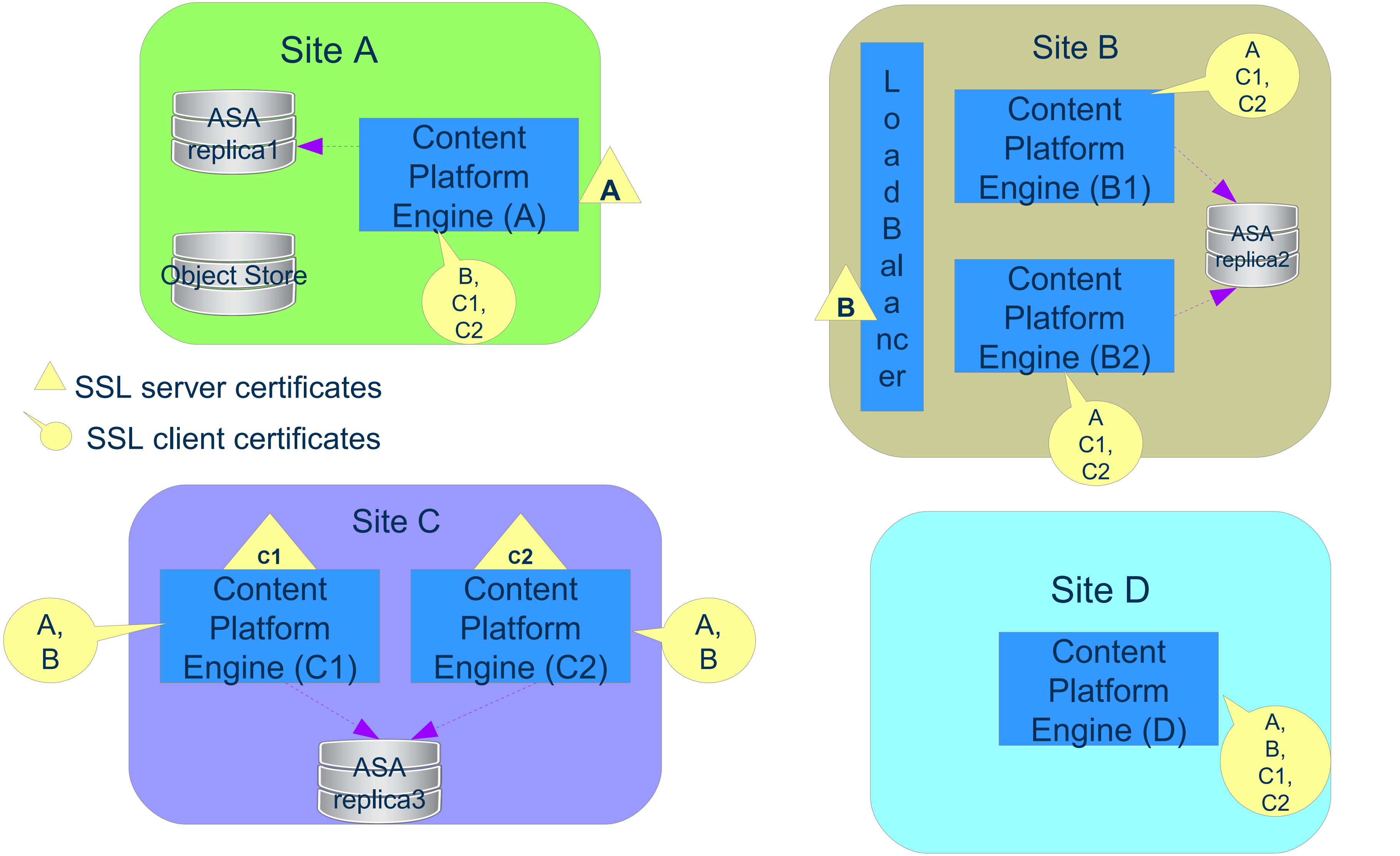
Configuration – Server communication certificate validation

- SSL certificate validation is used to prove to the sending CPE server that the destination CPE server is who it says it is ...

- Since CPE servers are typically within a company's corporate network, it is usually not necessary to perform SSL certificate validation

- If certificate validation is desired, then ensure
  - Install SSL server certificate at all CPE server communication endpoints (i.e. loadbalancer or CPE server(s))
  - Install corresponding SSL client certificate on all CPE servers

Configuration – Server communication SSL certificate configuration



Course Roadmap

- Overview
- Server Communication Operations
- Authentication
- Failover
- Configuration

➔ Demonstration

Demo

Create file system storage device on remote site

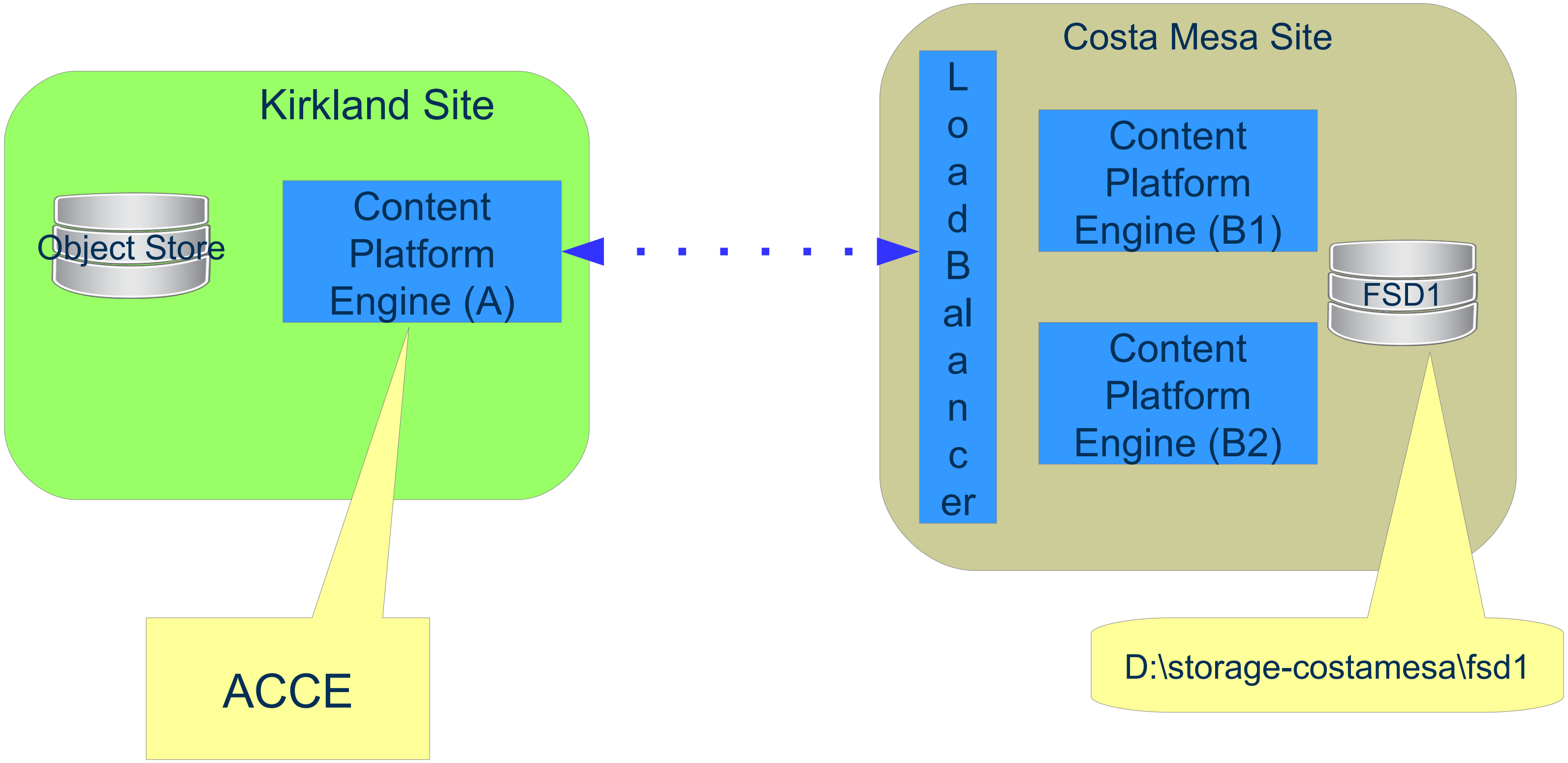
Create advanced storage area with this device

Create document

Retrieve document

Delete document

Demo


Kirkland Site
Object Store
Content Platform Engine (A)
ACCE
Costa Mesa Site
Load Balancer
Content Platform Engine (B1)
Content Platform Engine (B2)
FSD1
D:\storage-costamesa\fsd1

Best Practices

- If using Advanced Storage and have multiple sites, configure the Server Communication URL for each site
- Use **https** with Server Communication URL to ensure messages are encrypted during transport
- Do not enable certificate validation
- Use Network Time Protocol (NTP) service to ensure clocks are in sync across all sites

Course Summary

You have completed this course and can:

- *Explain how the CPE server communication feature is used with Advanced Storage Areas*
- *Configure CPE server communication between sites*

Contacts

- Product Marketing Manager:
  - Robert Finn
- Product Manager:
  - Stephen Hussy
- Subject Matter Experts (SME) / Area of Expertise:
  - Roger Bacalzo (Server Communication)
  - Bob Kreuch (Advanced Storage Area)
- Support:
  - Eric Fonkalsrud Jr (L3 Manager)

Product Help/Documentation/Resources

P8 5.2.1 Information Center (available October 31st)

http://www.ibm.com/support/knowledgecenter/SSNW2F_5.2.1/

Administering Content Platform Engine

- Defining the repository infrastructure
  - Content Platform Engine server communication
    - Configuring server communication
    - Configuring SSL for server communication