Leveraging IBM Rational ClearCase and ClearQuest CM Server to achieve a secure, centralized, and flexible deployment model in your GDD environment

Sujeet Mishra

Senior Staff Software Engineer IBM

sujmishr@in.ibm.com

Innovate2010

The Rational Software Conference

Let's build a smarter planet.

The premiere software and product delivery event.
August 16-18, Bangalore

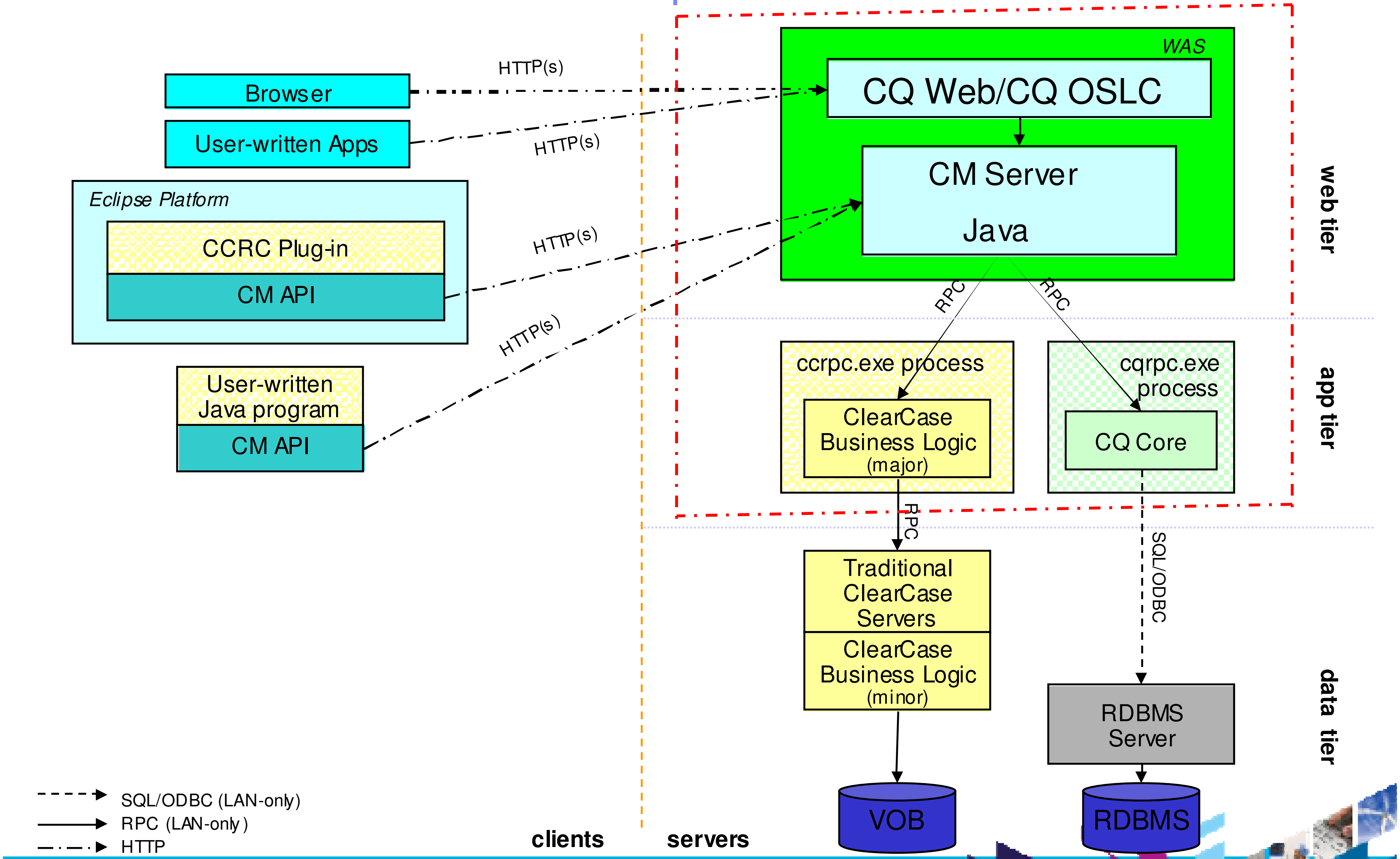
Agenda

- Introduction to CM Server
- Secure your CM Server environment
  - Enable WAS admin security
  - Control access by host name or address
  - Configure SSL with IHS
  - Use Proxy Server
- Centralized and Flexible deployment leveraging CM Server
  - Backward (cross version) compatibility and flexibility in adoption
  - Consolidate multiple sites with load balancing
  - Use region mapping
  - [New] ClearCase-ClearQuest integration option for increased flexible deployment

What is CM Server?

- CM Server stands for Configuration Management Server and/or Change Management Server.
- It is a unified (single technology stack) application server for both ClearCase and ClearQuest.
- First released in ClearCase and ClearQuest version 7.1.
- Design Goals of CM Server
  - Drive down TCO (Total Cost of Ownership)
    - Support WAN clients (CCRC, CQ Web, Full Text Search…)
    - Lower client installation and client administration costs
    - Standardize configuration and administration of servers
  - Leverage performance, security & scalability of WebSphere Application Server.
  - Lift limitations of previous CCRC Server and CQ Web Server.
  - Support a new, unified client-side Java API for custom integrations.
  - Support the new ClearQuest OSLC interface for building loosely-coupled and robust integrations.

CM Server Architecture – Component view



Agenda

- Introduction to CM Server
- Secure your CM Server environment
  - Enable WAS admin security
  - Control access by host name or address
  - Configure SSL with IHS
  - Use Proxy Server
- Centralized and Flexible deployment leveraging CM Server
  - Backward (cross version) compatibility and flexibility in adoption
  - Consolidate multiple sites with load balancing
  - Use region mapping
  - [New] ClearCase-ClearQuest integration option for increased flexible deployment

Secure your CM Server environment
* Enable WAS administrative security

- CM Server is a Websphere Application Server (WAS) Hosted J2EE application.

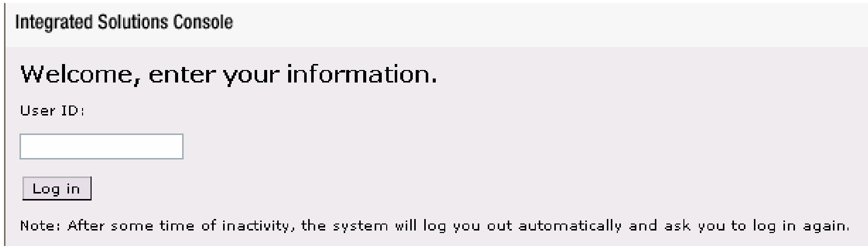
- Administrative security protects the CM Server from unauthorized access to the WAS administrative functions e.g.
  - WAS administrative console.
  - Modifications to WAS configuration.
  - Stopping the WAS instance.

- Administrative security not enabled by default
  - When a WAS profile created, the administrative security is disabled by default.
  - Security could be enabled by default in the future based on customer feedback.

- **It is very important to enable WAS administrative security.**

Secure your CM Server environment
* Enable WAS administrative security

- **Enable WAS administrative security**
  - Login to WAS admin console via http://cmserver:12060/ibm/console



Integrated Solutions Console

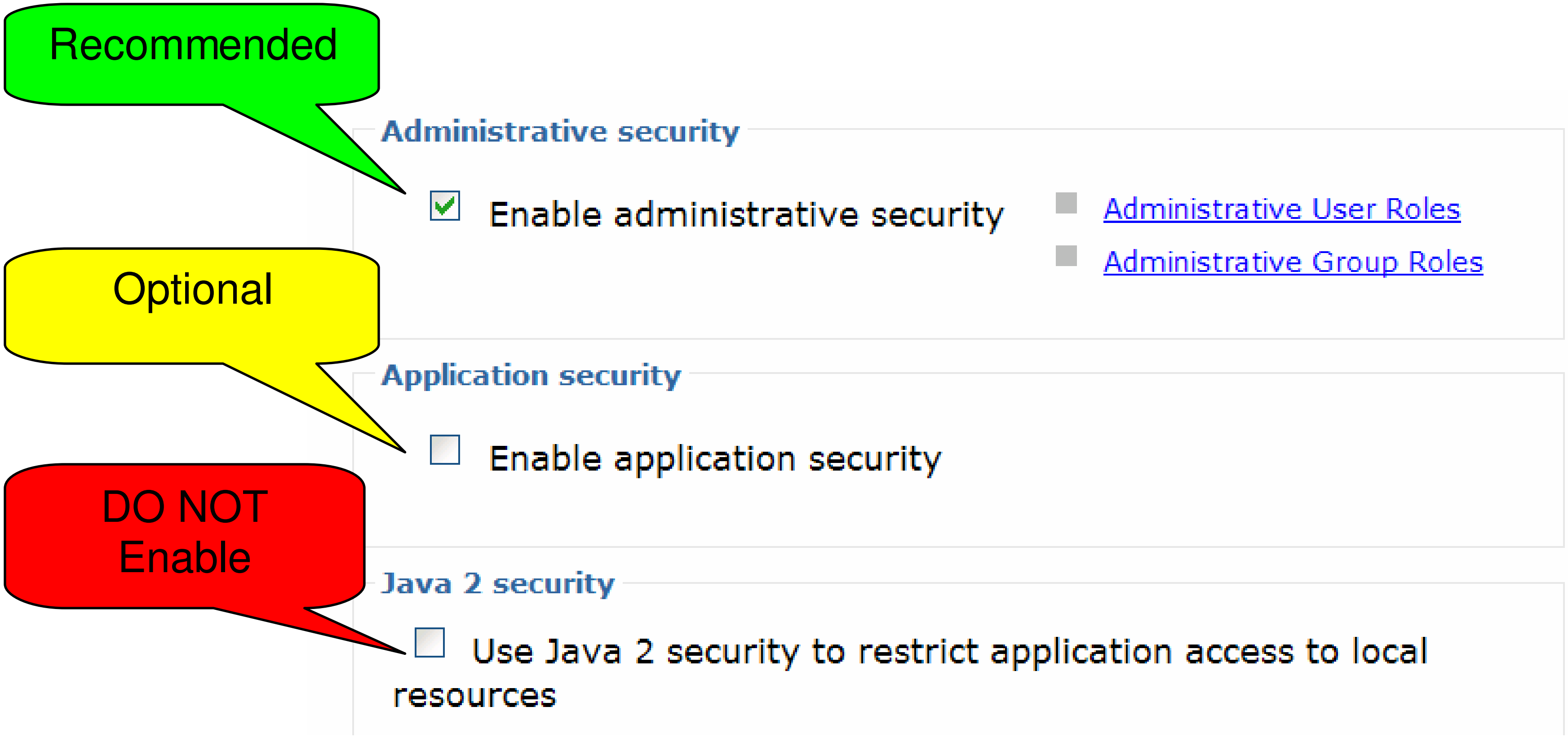
Welcome, enter your information.

User ID:

Note: After some time of inactivity, the system will log you out automatically and ask you to log in again.

- Follow Security > Secure administration, applications, and infrastructure.
  - Use the Security Configuration wizard to configure security
    - In step 1 of the wizard, select a security level. Ensure that **Java 2 security** is disabled.
    - In step 2, select a user repository. Choose one of federated or LDAP repositories. For more information, see the WebSphere Application Server v6.1 Information Center.
    - In step 3, enter the administrative user name and password. The user name must be different from the user name that is running WebSphere Application Server.
    - In step 4, confirm your selections and click **Finish**.
    - Click **Apply**.

Secure your CM Server environment
* Enable WAS administrative security



Recommended

Administrative security

☑ Enable administrative security

- Administrative User Roles
- Administrative Group Roles

Optional

Application security

□ Enable application security

DO NOT Enable

Java 2 security

□ Use Java 2 security to restrict application access to local resources

Secure your CM Server environment
* Enable WAS administrative security

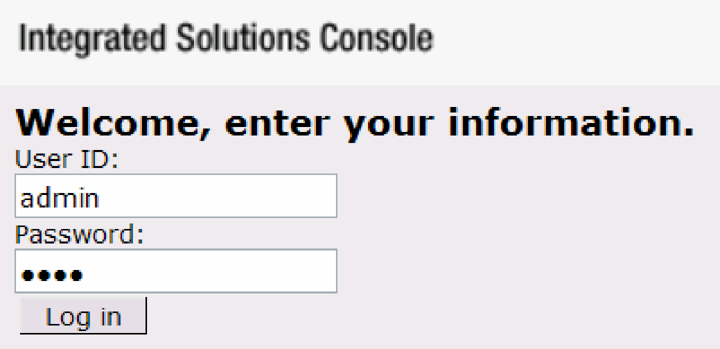
Enable ClearQuest Web for CM Server administrative security.

- Edit the file CqServerConn.properties. The location of the file is:
  - On Windows:
    <*drive*>:\install_dir\common\CM\profiles\cmprofile\installedApps\node-name\RationalClearQuestWeb.ear\CQWebModule.war\WEB-INF\classes\CqServerConn.properties
  - On UNIX system and Linux:
    install_dir/common/CM/profiles/cmprofile/installedApps/*node-name*/RationalClearQuestWeb.ear/CQWebModule.war/WEB-INF/classes/CqServerConn.properties
- Add the administrative user name and password to the following lines
  TEAM_SERVER_ADMIN_AUTHENTICATION_KEY=
  TEAM_SERVER_ADMIN_AUTHENTICATION_VALUE=
- Restart CM Server for the administrative security changes to take effect.

Secure your CM Server environment
* Enable WAS administrative security

After administrative security is enabled …

- The administrative user name and password must be provided when:
  - Log into the WAS administrative console
    - – http://server:12060/ibm/console



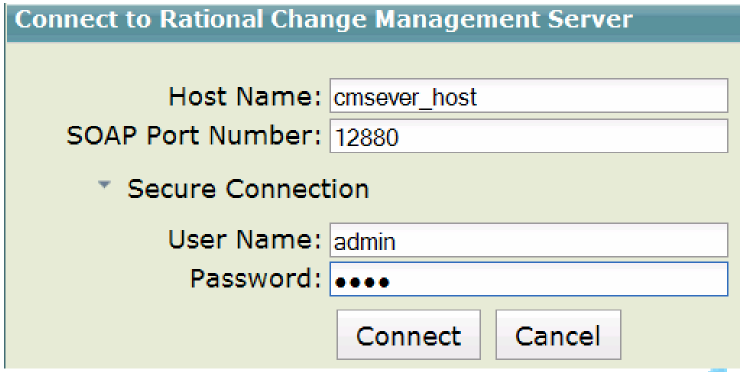
Integrated Solutions Console

Welcome, enter your information.

User ID: admin

Password: ●●●●

  - Log into the CM Server administration utility (technote # **1377925)**
    - – http://server/TeamAdminWeb



Connect to Rational Change Management Server

Host Name: cmsever_host

SOAP Port Number: 12880

Secure Connection

User Name: admin

Password: ●●●●

Secure your CM Server environment
* Enable WAS administrative security

After administrative security is enabled (contd.) …

- **Stop the CM server**.
  - (Windows Only) If *stopServer* script is used, the user and password arguments must be provided as command line arguments:

    $install_dir\common\eWAS\bin stopServer.bat -user <*admin-user-name*> -password <*admin-password*>

  - (Unix and Linux): The *cmserver_shutdown* and *cmserver_restart* scripts also accept the -user and -password arguments.
    - /opt/IBM/RationalSDLC/common/CM/bin/cmserver_shutdown/restart

- **Update the WAS Service on Windows**
  - CM Server runs as a Windows service. Update the service with additional arguments for the administrative user name and password used when stopping/starting the CM Server.
  - Run the following commands in a command prompt window, substituting <*admin-user-name*> and <*admin-password*> with the administrative user name and password, respectively.
    - Step 1: cd *$install_dir*\common\eWAS\bin
    - Step 2: **WASService.exe** -add "cmprofile" -serverName server1 -profilePath "$*install_dir*\common\CM\profiles\cmprofile" -stopArgs "-user <*admin-user-name*> -password <*admin-password*>" -encodeParams

Secure your CM Server environment

* Enable WAS administrative security

Security Considerations for Unix and Linux

- Passing the administrative user name and password to the *stopServer.sh* script exposes the user name and password to anyone who issues the ps -ef command.

- To avoid specifying the -user and -password options for commands, configure the settings as properties:
  - cd /opt/rational/common/CM/profiles/cmprofile/properties
  - Edit the file **soap.client.props** and change the values of the following properties:
    - com.ibm.SOAP.securityEnabled=true
    - com.ibm.SOAP.loginUserid=<*admin-user-name*>
    - com.ibm.SOAP.loginPassword=<*password*>
  - Encode the property value com.ibm.SOAP.loginPassword by running the following script:
    - opt/rational/common/eWAS/bin/PropFilePasswordEncoder.sh soap.client.props com.ibm.SOAP.loginPassword
    - Verify that the password is encoded and then remove the file soap.client.props.bak.

- Check permissions on sensitive WAS files e.g properties and executables. Permissions should limit access to WebSphere administrators.

Secure your CM Server environment

* Enable WAS administrative security

Upgrading CM Server

- Administrative security **must** be temporarily disabled prior to upgrading the CM Server .

- Disabling and Administrative Security
  - Start the WebSphere Application Server administrative console by entering the following URL in your browser window: http://localhost:12060/ibm/console
  - Log in by using the administrative user name and password.
  - Click **Security > Secure administration, applications, and infrastructure**.
  - Clear **Enable administrative security**.
  - Click **Apply** to save your changes
  - Restart CM Server to effect the changes.

Additional Resources

Refer to technote **#1386762** for additional information on managing WAS administrative security.

Secure your CM Server environment
* Control Access by host name or address

- Access to the CM Server can be controlled via an access list including the name or address of the host to be included or excluded.
  - This can be done by configuring the Websphere Application Server web container transport chain.
    - Login to http://server:12060/ibm/console
    - Follow Server → Application Servers → server1
    - Access the **Configuration** tab. In the **Container Settings** section, expand **Web Container Settings**.
    - Click on **Web container transport chains**
    - Click on **WCInboundDefault**
    - Add the host name or address to the exclude or include list.
    - Click “Apply” and restart CM Server
- Technote #**1397016** discusses steps to secure the WAS profile used by ClearQuest Full-Text Search service. These steps can be applied to other WAS profiles, such as CM Server “cmprofile” with variation in ports used.

Secure your CM Server environment
* Configure SSL access using IBM HTTP Server (IHS)

- It is highly recommended to configure CM Server to use the Secure Socket Layer (SSL) protocol for secure communication with ClearCase Remote Client (CCRC) and ClearQuest Web.

- The current version (7.1.x) of CM Server does not support Open SSL.
  - A previously created Open SSL certificate must be converted to IBM SSL certificate for use with the CM Server.
  - See the InfoCenter contents on steps to convert Open SSL to IBM SSL.

Secure your CM Server environment
* Configure SSL access using IBM HTTP Server (IHS)

Steps to configure SSL using IHS

- Uncomment the line “Include conf/ssl.conf” in the file %RATIONAL_COMMON%\IHS\conf\httpd.conf.

- Create %RATIONAL_COMMON%\IHS\key.kbd and %RATIONAL_COMMON%\IHS\key.sth using the IHS Key Management utility.
  - Refer to Creating HTTP server keys.

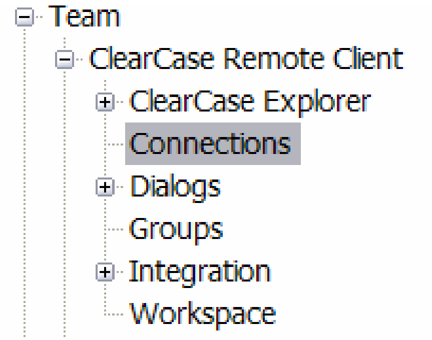
- Create the IBM SSL certificate.
  - Refer to Creating a self-signed certificate for the HTTP server.

- Redirect non-SSL requests as SSL requests.
  - Refer to Forcing an SSL connection with CM Server.

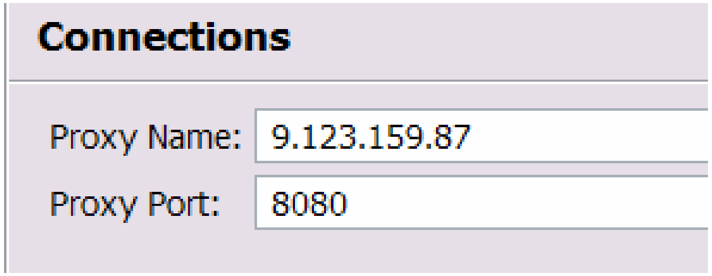
Secure your CM Server environment

* Use Proxy Servers in CCRC/CM Server environment

- **Reverse proxy**
  - User connects / authenticates using URL to proxy server.
- **Forward proxy**
  - CCRC user specifies proxy information in CCRC preferences page.



- Team
  - ClearCase Remote Client
    - ClearCase Explorer
    - Connections
    - Dialogs
    - Groups
    - Integration
    - Workspace

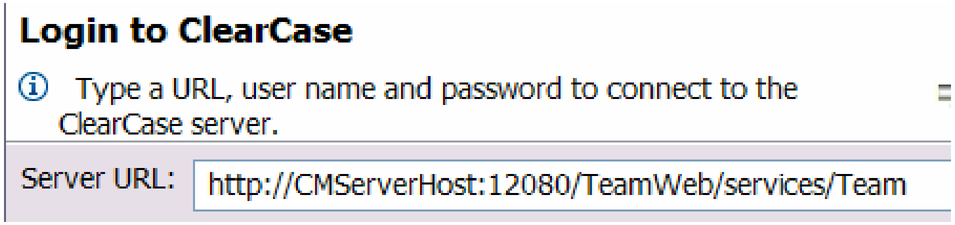


Connections

Proxy Name: 9.123.159.87

Proxy Port: 8080

  - CCRC user connects using CM Server URL



Login to ClearCase

ⓘ Type a URL, user name and password to connect to the ClearCase server.

Server URL: http://CMServerHost:12080/TeamWeb/services/Team

Agenda

- Introduction to CM Server
- Secure your CM Server environment
  - Enable WAS admin security
  - Control access by host name or address
  - Configure SSL with IHS
  - Use Proxy Server
- Centralized and Flexible deployment leveraging CM Server
  - Backward (cross version) compatibility and flexibility in adoption
  - Consolidate multiple sites with load balancing
  - Use region mapping
  - [New] ClearCase-ClearQuest integration option for increased flexible deployment

Centralized Flexible deployment using CM Server

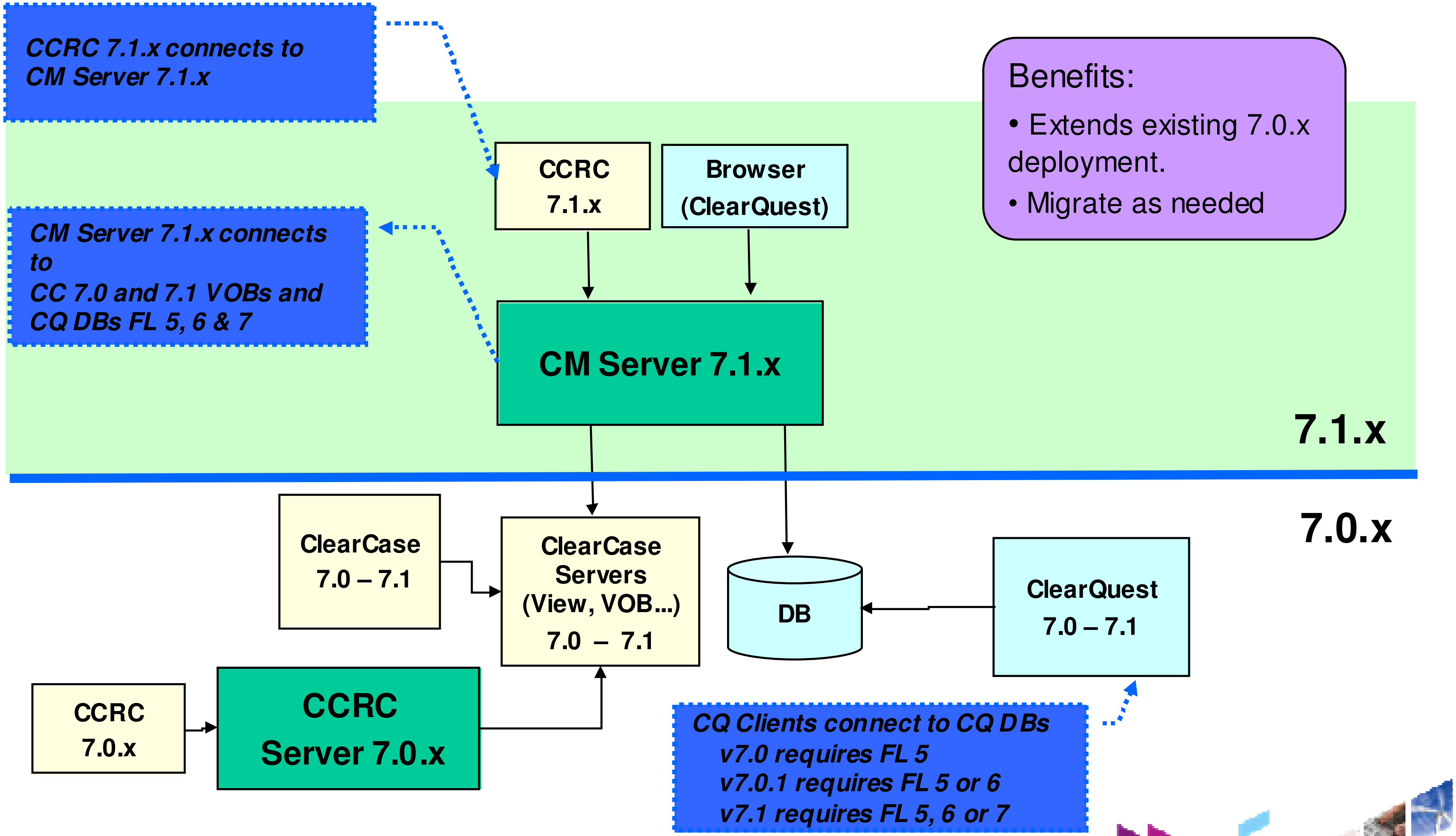
* Backward compatibility and flexibility in adoption

- ClearCase
  - v7.1.x CM Server is compatible with v7.0.x VOB servers
  - Once v7.0.x CCRC server is upgraded to v7.1 CM Server, CCRC client connecting to this CM Server must be upgraded to v7.1 version.
  - V7.0.x CCRC server and v7.1.x CCRC Server (CM server) can access the same v7.0.x VOB servers.

- ClearQuest
  - v7.1 CM Server supports Feature Level 5, 6 and 7 CQ databases
  - CQ Full-Text Search support requires ClearQuest Feature Level 7. However, this is not required for MultiSite'ed CQ DB.

Centralized Flexible deployment using CM Server

* Backward compatibility and flexibility in adoption


CCRC 7.1.x connects to CM Server 7.1.x
CM Server 7.1.x connects to CC 7.0 and 7.1 VOBs and CQ DBs FL 5, 6 & 7
CCRC 7.1.x
Browser (ClearQuest)
CM Server 7.1.x
7.1.x
7.0.x
ClearCase 7.0 – 7.1
ClearCase Servers (View, VOB...) 7.0 – 7.1
DB
ClearQuest 7.0 – 7.1
CCRC 7.0.x
CCRC Server 7.0.x
CQ Clients connect to CQ DBs
v7.0 requires FL 5
v7.0.1 requires FL 5 or 6
v7.1 requires FL 5, 6 or 7

Benefits:

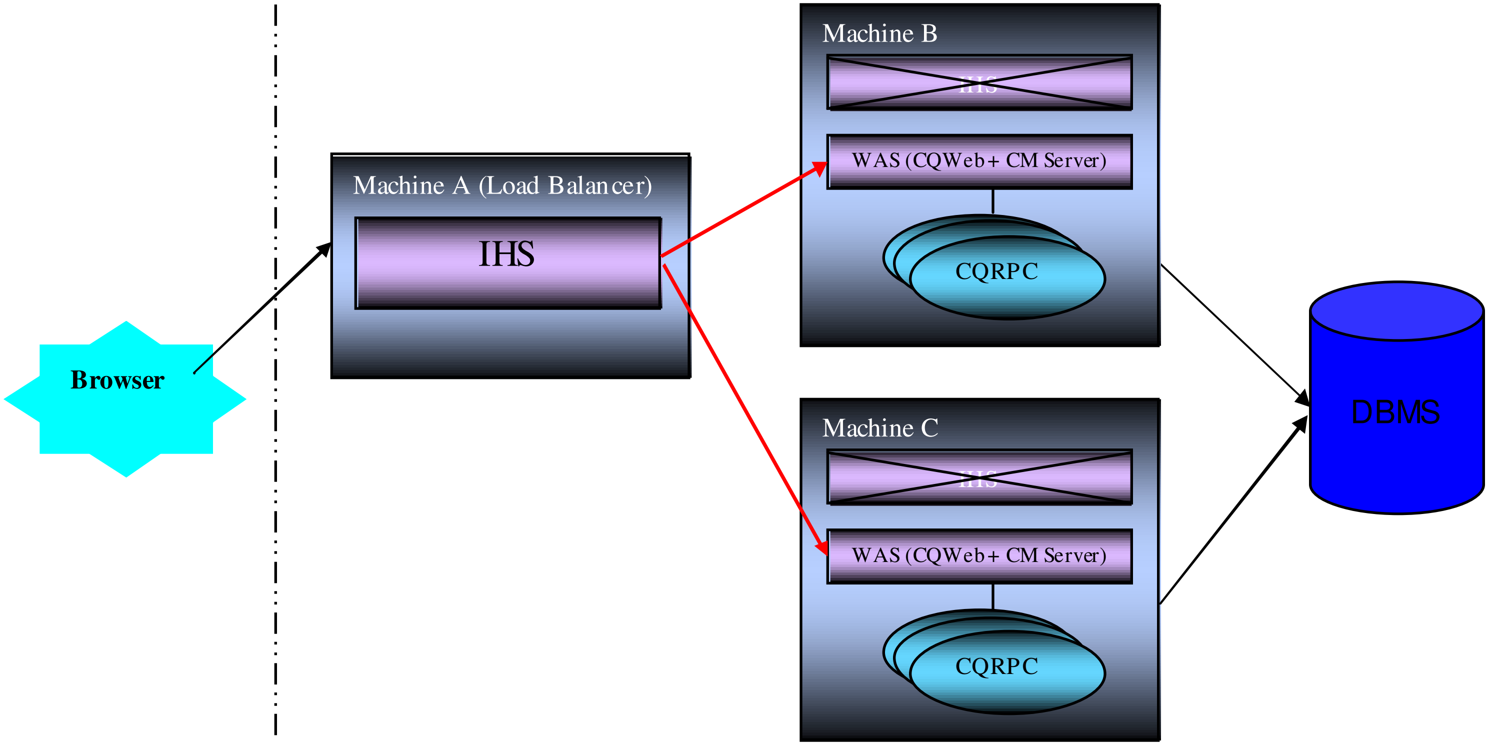
- Extends existing 7.0.x deployment.
- Migrate as needed

Centralized Flexible deployment using CM Server
* Consolidating multiple sites with load balancing

- CM server load balancing options provided with 7.1.x
  - Using IBM HTTP Server – Out of the Box option
    - Provides random / round robin load distribution
    - Configuration technote for CCRC: #**1377474**
    - Configuration technote for CQWeb: #**1377478**
  - Using WebSphere Edge Component (see InfoCenter for details)
    - Edge Component Load Balancer – True Load Balancing
      - Monitors load on CM Server and distributes accordingly
      - Administration Console to monitor load
- Both options provide backup/failover capability.

Centralized and Flexible deployment leveraging CM Server

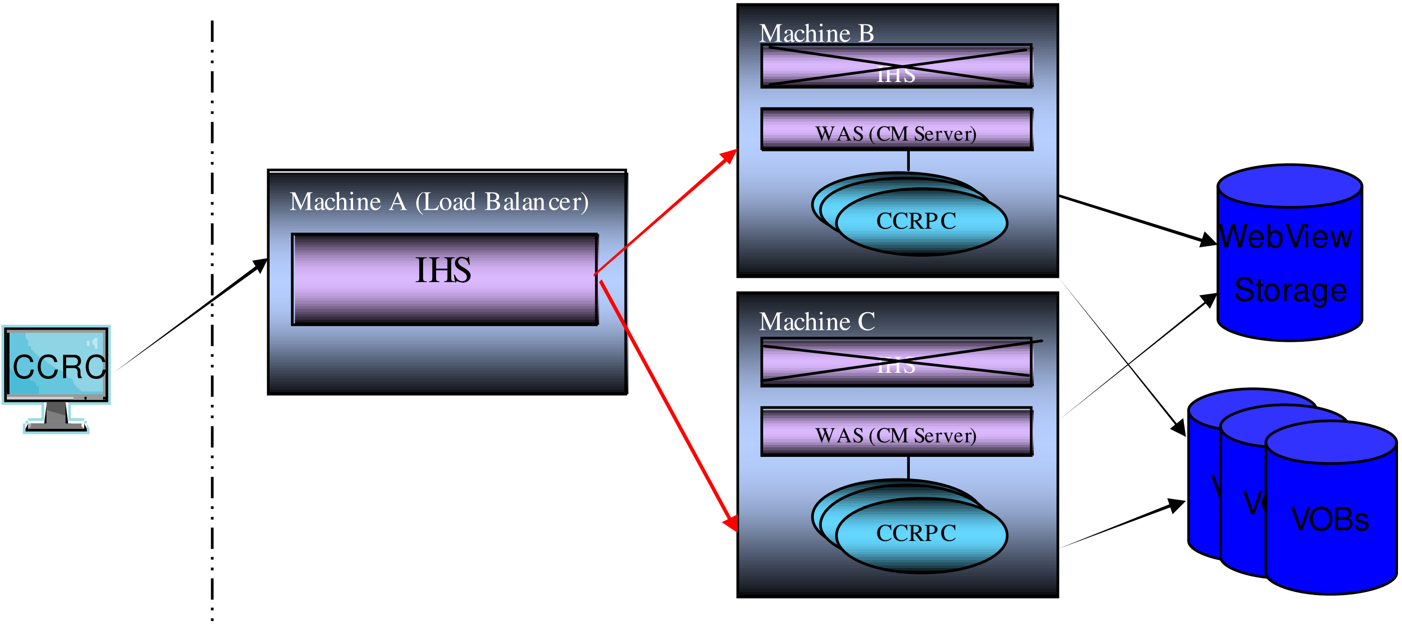
* Consolidating multiple sites with load balancing



- IHS will use a round-robin or random based load balancing approach in this configuration. If CQWeb/CM Server on Machine B is down, or if Machine B is down, ClearQuest web users logged to Machine B will be offloaded to Machine C.
  - For users that only have read sessions on Machine B, they won't notice anything.
  - If a user has a write session on Machine B and is in the middle of modifying a record, only non-committed data in that active session would impacted.

Centralized and Flexible deployment leveraging CM Server

* Consolidating multiple sites with load balancing



- IHS will use a round-robin load balancing approach with session affinity in this configuration.
- If both CM Servers are active, a new CCRC session will connect to the next available CM Server.
- If one of the servers is unavailable, CCRC users will be directed to the available CM Server.
- Both servers can access the same views located at a central storage location specified with CM Server MBEANs
  - ccrcViewStorage (UNC path name to storage location)
  - ccrcUseViewHostPathForGlobalPath (set to TRUE)

Centralized and Flexible deployment leveraging CM Server
* Use region mapping

- Customize/configure VOB access based on user identity
  - A user region map allows mapping of OS users and groups to ClearCase regions.
  - A user region map can be used to restrict or allow a user or a group access to a set of VOBs grouped by region.
  - A user region map is a flat file located on the CM Server. The pathname of this file is specified as a value for the MBEAN attribute “***ccrcUserRegionMapfile”.***

Centralized and Flexible deployment leveraging CM Server

* Use region mapping (an example)

- ClearCase example
  - CM Server configured with “region1” and “region2”. Either of them can be the default region.
  - “region1” contains vob1_1 and vob1_2.
  - “region2” contains vob2_1 and vob2_2.
  - Sample region mapping file

    region1 = {CMBUQE\userA }

    region2 = {CMBUQE\userB }

    – * Note: There must be a space before the final ‘}’
  - “userA” has access to vob1_1 and vob1_2 only.
  - “userB” has access to vob2_1 and vob2_2 only.

Centralized and Flexible deployment leveraging CM Server

* Use region mapping (an example)

- ClearCase/ClearQuest integration
  - Deployment configuration
    - CQ Web can be used to access multiple CC regions from a single CM Server.
    - Previous versions (v6.x and v7.0.x) allowed access only to the default CC region for the CQ Web Server.
  - Relevant use cases
    - View UCM Changeset
    - Change Headline
  - Scenario
    - User A works in CC region A
    - User B works in CC region B
    - Both users access CQ Web via http://SharedServer1/cqweb
    - User A views changeset in CQ Record A which is bound to UCM Activity in region A
    - User B views changeset in CQ Record B which is bound to UCM Activity in region B

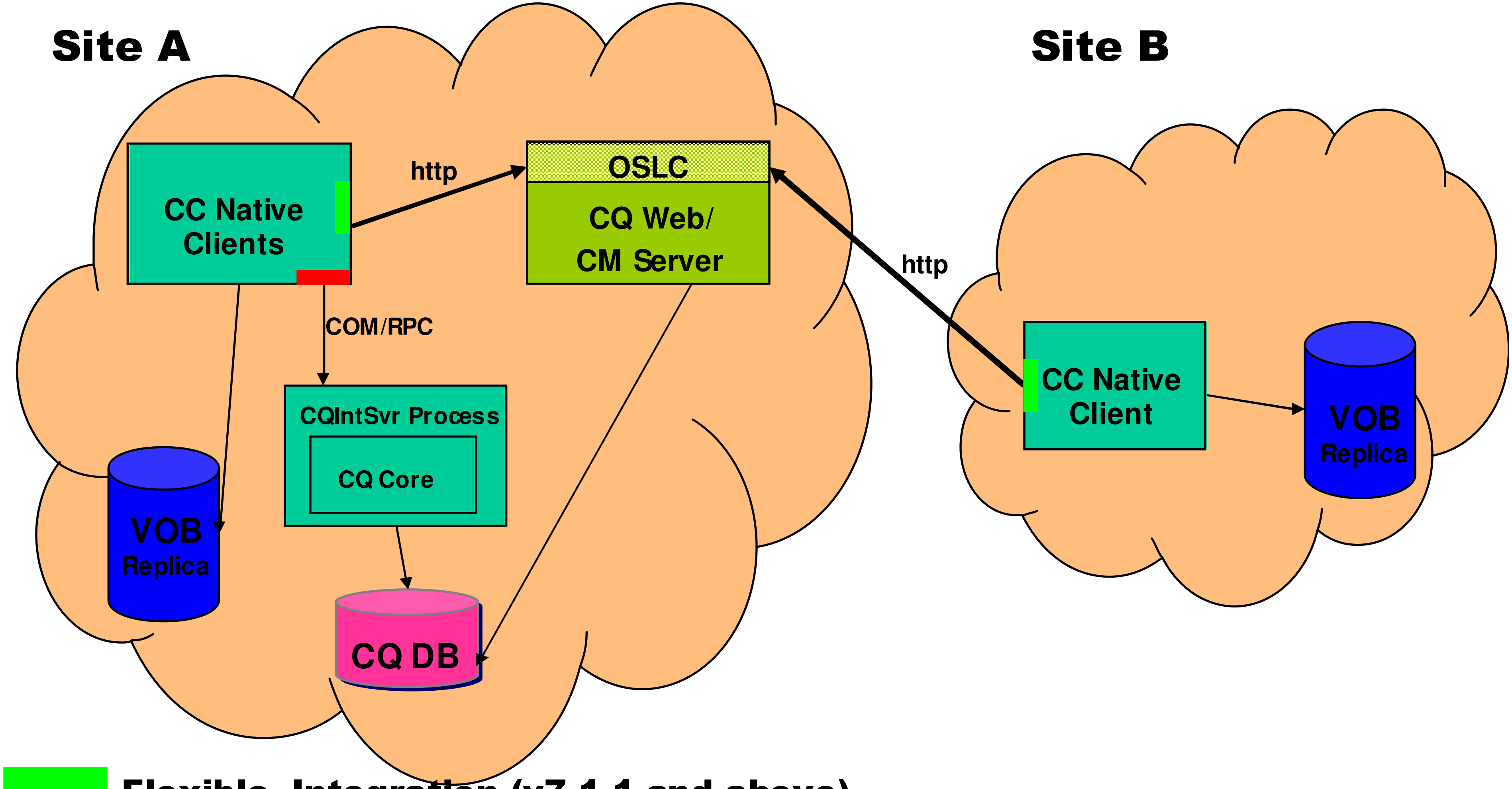
Centralized and Flexible deployment leveraging CM Server

* New CC-CQ integration option for more flexible deployment

- **Enable LAN ClearCase to communicate with WAN ClearQuest for UCM**
  - In 7.1.1 release, only ClearCase thick clients provide this support
    - Ex. Cleartool, Project Explorer, ClearCase Explorer, etc.
  - It has no impact to UCM use cases through CCRC or CQWeb
    - Plan to extend to CCRC and CQWeb
- **Uses OSLC CQ REST API**
  - Installed with 7.1.1 CQ Web
  - WAN-friendly calls over HTTP(s)
- **Advantages**
  - Removes need to deploy CQ thick clients
  - Removes dependency on CQ Multisite
  - New functionality is available on platforms not supported by ClearQuest
    - Solaris X86, Linux 390, Linux PPC, HP IA64
- See technote **#1398642** for detailed information.

Centralized and Flexible deployment leveraging CM Server

* New CC-CQ integration option for more flexible deployment



🟩 **Flexible Integration (v7.1.1 and above)**

🟥 **Native Integration**

Summary

- It is highly recommended to enable WAS administrative security for the 7.1.x CM Server (for CCRC and for ClearQuest Web).

- It is highly recommended to configure IBM Secure Socket Layer (SSL) protocol for secure communication with ClearCase Remote Client (CCRC) and ClearQuest Web. Additional security can be implemented using proxy servers.

- CM Server provides many features, options and benefits that can be leveraged to achieve a flexible, centralized deployment model for enterprise and global environments.

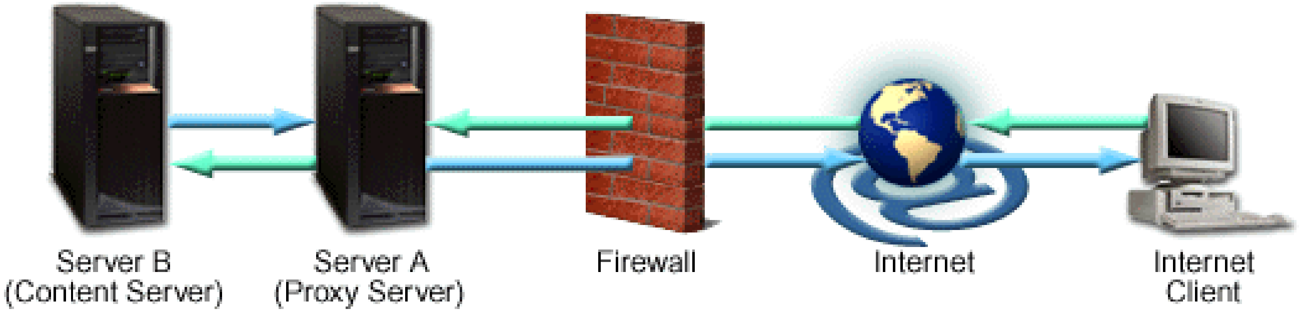
Questions

www.ibm/software/rational

The information contained in these materials is provided for informational purposes only, and is provided AS IS without warranty of any kind, express or implied. IBM shall not be responsible for any damages arising out of the use of, or otherwise related to, these materials. Nothing contained in these materials is intended to, nor shall have the effect of, creating any warranties or representations from IBM or its suppliers or licensors, or altering the terms and conditions of the applicable license agreement governing the use of IBM software. References in these materials to IBM products, programs, or services do not imply that they will be available in all countries in which IBM operates. Product release dates and/or capabilities referenced in these materials may change at any time at IBM's sole discretion based on market opportunities or other factors, and are not intended to be a commitment to future product or feature availability in any way. IBM, the IBM logo, Rational, the Rational logo, Telelogic, the Telelogic logo, and other IBM products and services are trademarks of the International Business Machines Corporation, in the United States, other countries or both. Other company, product, or service names may be trademarks or service marks of others.

Backup slides: Forward Proxy and Reverse Proxy

- Reverse Proxy



- Forward Proxy