DX Unified Infrastructure Management (DX UIM)

Reference Architecture Version 20.4

Broadcom, the pulse logo, and Connecting everything are among the trademarks of Broadcom and/or its affiliates in the United States, certain other countries, and/or the EU.

Copyright © 2021 by Broadcom. All Rights Reserved.

The term “Broadcom” refers to Broadcom Inc. and/or its subsidiaries. For more information, please visit www.broadcom.com.

Broadcom reserves the right to make changes without further notice to any products or data herein to improve reliability, function, or design. Information furnished by Broadcom is believed to be accurate and reliable. However, Broadcom does not assume any liability arising out of the application or use of this information, nor the application or use of any product or circuit described herein, neither does it convey any license under its patent rights nor the rights of others.

Change History

Date	Version	Author	Description of Change
14-Mar-2018	1.0	James Christensen	Intial Draft
15-Mar-18	1.1	James Christensen	Added port diagram, minor reevisions
02-Sep-20	2.0	UIM Team	Updated to UIM 20.3
20-Oct-21	2.1	DX UIM Team	Updated to DX UIM 20.4

Distribution List

Date	Version	Name	Company, Organizational Position

Referenced Documents

Related Project Documentation
DX Unified Infrastructure Management Product Documentation: https://techdocs.broadcom.com/content/broadcom/techdocs/us/en/caenterprise-software/it-operations-management/unified-infrastructuremanagement/20-4.html
DX Unified Infrastructure Management Probes Documentation: https://techdocs.broadcom.com/content/broadcom/techdocs/us/en/caenterprise-software/it-operations-management/ca-unified-infrastructuremanagement-probes/GA.html

1.1 Contents

1.1 Contents **5**
1.2 Table of Figures **6**
Chapter 1: Executive Summary **7**
1.2.1 How to use this document **7**
1.2.2 Target Audience **7**
Chapter 2: Functional Architecture **8**
1.2.3 Planned End State **9**
1.2.3.1 Outcomes 11
1.2.4 Solution Personas **12**
1.2.5 Interaction of Personas **13**
1.2.6 Foundation Capability DX UIM **14**
1.2.7 Foundation Functional User Stories **17**
1.2.8 Foundation Logical Architecture **19**
1.2.9 Network Context **20**
1.2.9.1 Network Diagram – Foundation Physical Architecture 21
1.2.9.2 Data Flows Explained 21
Chapter 3: Technical Architecture **24**
1.2.10 Foundation Architecture – DX UIM **25**
1.2.10.1 Architecture Commentary 26
1.2.11 Foundation System Specification Requirements **30**
1.2.12 Base System Configuration Requirements **31**
1.2.12.1 Node Configuration – DX UIM 31
1.2.12.2 Solution Component Ports – DX UIM 31
1.2.13 Operator Console Technical Architecture **32**
1.2.13.1 Deployment Model 32
1.2.13.2 Multi-Tier Architecture 33
Chapter 4: Implementation Guidance **34**
1.2.13.3 DX UIM Installation Checklist 34
Chapter 5: Integration Guidance **36**
1.2.13.4 Integration Features 36
1.2.13.5 Integration Overview 36
1.2.13.6 Integration Process Flow 40

1.2 Table of Figures

Figure 1 DX UIM Logical Architecture 10
Figure 2 DX UIM UI Interactions 10
Figure 3 Interaction of Personas 13
Figure 4 DX UIM Foundation Logical Architecture 19
Figure 5 DX UIM Port diagram..... 20
Figure 6 DX UIM Network diagram 21
Figure 7 DX UIM Robot Dataflow 22
Figure 8 DX UIM UI Data Flow 23
Figure 9 - DX UIM Medium Solution Environment 25
Figure 10 Integration of DX UIM and Email Server 37
Figure 11 Integration of DX UIM and LDAP/Active Directory 38
Figure 12 Integration of DX UIM and Service Desk 39
Figure 13 Integration Process Flow 40

Chapter 1: Executive Summary

This Reference Architecture provides information relating the baseline functional and technical architecture required to deliver the DX Unified Infrastructure solution (DX UIM).

The DX UIM architecture provides a holistic solution to manage system and network fault alarms. Configured according to this specification, the solution is capable of routing incident tickets to the right resolver.

This document can be considered as the logical and physical design, illustrating how the technical solution should be implemented to meet the architecture (non-functional and environment constraints) requirements and how it will be configured or customized to support the requirements. It is only relevant to the implementation of a foundational solution and should be superseded by more detailed design, implementation, test and operational artifacts as part of later phases or iterations of an implementation project.

All content contained in this document is based on CA Lead Practices and where necessary, it has been updated to reflect the corporate governance standards for architecture requirements.

A Reference Architecture is simply a starting point; the design for a generic solution that addresses a common set of use cases. The solution can be implemented as specified herein and will perform as described. However, it should be expected that the design may change significantly in order to meet unique client environmental and business requirements. This reference architecture makes many assumptions about what is 'common' and is based on the guidance provided at https://techdocs.broadcom.com/content/broadcom/techdocs/us/en/ca-enterprise-software/it-operationsmanagement/unified-infrastructure-management/20-4.html , which includes factors and scenarios that should be taken into consideration for any customized solution.

1.2.1 How to use this document

This document provides context and instruction. Architectural diagrams and commentary are used to explain how the solution should be deployed and configured. Where product documentation provides instruction, URL references are provided (with commentary in some cases.) The reference architecture and product documentation together form the foundation for creation of a site-specific design and deployment plan.

1.2.2 Target Audience

This reference architecture is intended for use by IT architects and systems administrators to aid in design and deployment. This document does not serve as a replacement for product training or professional services. It is assumed that the reader has sufficient training and experience with the individual products to follow product documentation and the included instructions

Chapter 2: Functional Architecture

This section contains the following topics:

Planned End State
Solution Personas
Interaction of Personas
Foundation Capability DX UIM
Foundation Functional User Stories
Foundational Logical Architecture

1.2.3 Planned End State

This reference architecture provides a solution that includes the use of DX Unified Infrastructure Management (DX UIM) for systems and network monitoring

The planned state is to provide a reference architecture to support the implementation of DX Unified Infrastructure Management (DX UIM) for systems and network monitoring. It documents the *actual* Architecture (the adoption and adaptation of the recommended architecture) that will be implemented for Agile Operations.

This document can be considered as the logical and physical design, illustrating how the technical solution will be implemented to meet the architecture (non-functional and environment constraints) requirements and how it will be configured or customized to support the requirements. The instantiation of the physical architecture can be found in the Build and Integration Handbook after the solution implementation.

The following shows the DX UIM logical system architecture. This graphic is a simple representation of a DX UIM implementation.

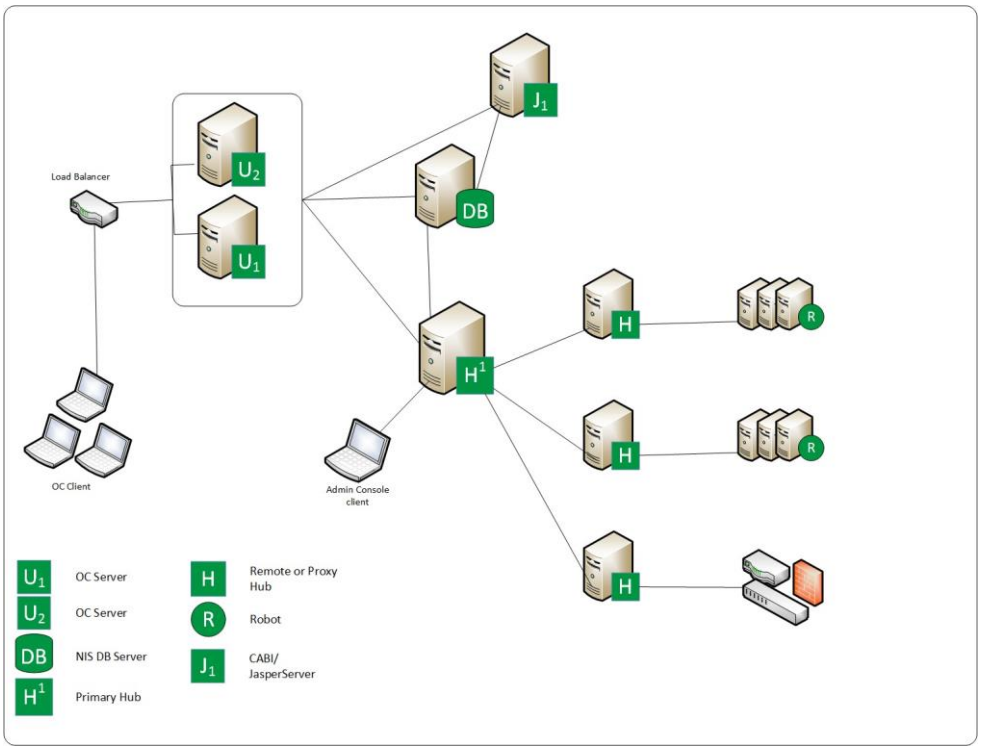


Figure 1 DX UIM Logical Architecture

This graphic is a simple representation of the UI interactions to the DX UIM core infrastructure.

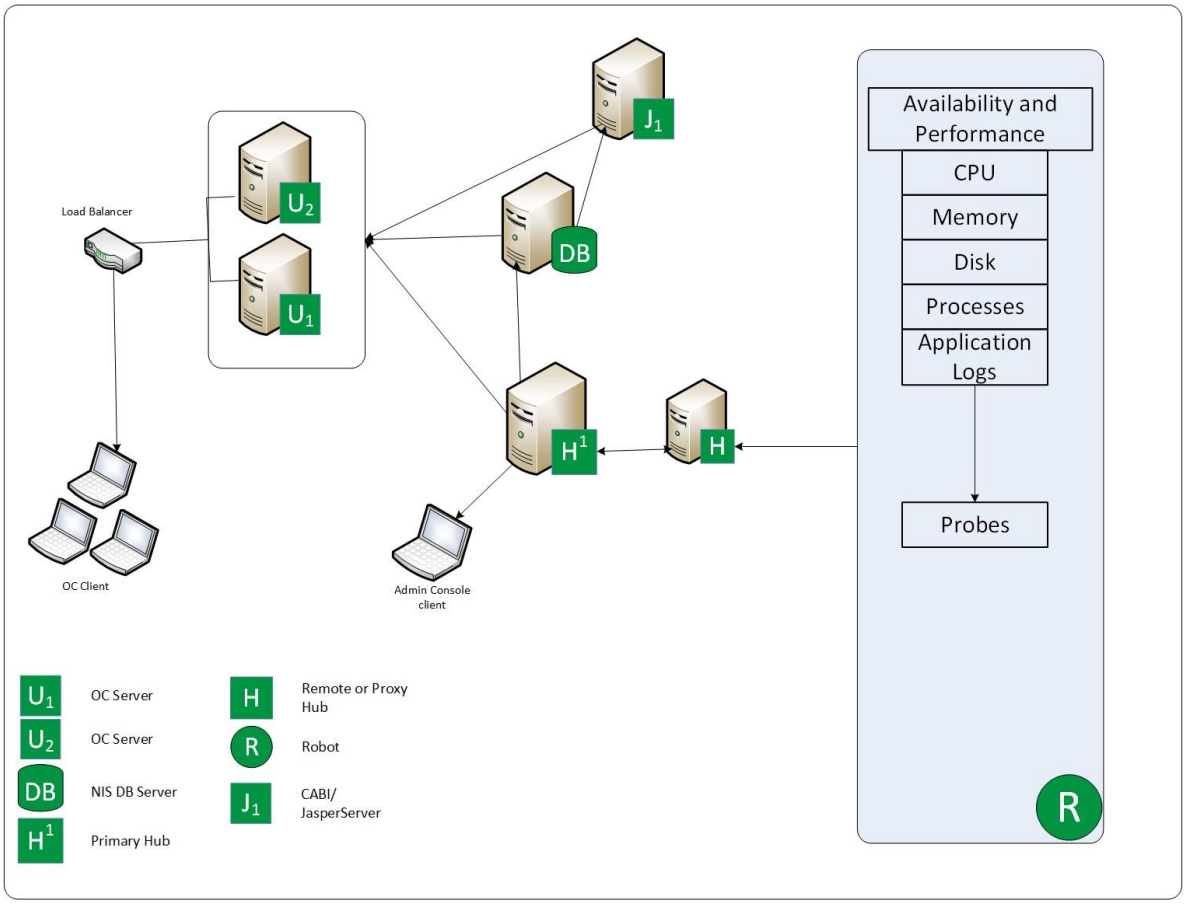


Figure 2 DX UIM UI Interactions

An overview and discussion of the DX UIM architecture can be found at https://techdocs.broadcom.com/us/en/ca-enterprise-software/it-operations-management/unified-infrastructure-management/20-4/getting-started/ca-uim-overview/ca-uim-architecture.html

1.2.3.1 Outcomes

The planned end state should provide the following outcomes:

- Network and system alarms are portrayed.
- Pertinent alarm details provide situational awareness for operational triage.
- Persona relevant dashboards display appropriate performance and alarm data.
- Administrators are able to deploy the required monitoring components and configurations
- Alarm/event management automation
  - Email notifications
  - Service Desk incident creation

1.2.4 Solution Personas

The following table summarizes the solution personas and how they can use in the integrated SOI+DX UIM+DX NetOps Spectrum solution. Where applicable, the personas are grouped by the capability in which they play a role:

Persona	Description	DX UIM Foundation
Executive	The executive persona could be the IT executive (such as CIO or CDO) or the business leader who the IT executive is sharing an update with. They want a high level view of the IT infrastructure to know whether or not the IT infrastructure underpinning the business is impaired or in jeopardy of being impaired so that they have confidence that they can meet the business objectives that the infrastructure supports or investigate any necessary remediation.	Supports the system management component (application, compute, CPU, memory) as well as storage, etc on premise and in the clouds. May also support network management for customers not using CA Performance Manager
Operations Manager	The IT Operations Manager is responsible for the team monitoring and remediating impacts to the health of the IT infrastructure. They are interested in several aspects of the IT infrastructure: • Current state - Outages impairments etc. • Resource consumption trends – Network bandwidth, storage capacity, compute (CPU, memory, disk) • Impacts to business – What is impacted if a particular application is unavailable? • Status of issues being worked	
Operator/Analyst	The operator analyst is responsible for any alarms in their area of responsibility and/or tickets assigned to them for investigation and remediation. The operator/analyst is the technical expert who will be assigned to one or more technology silos.	
NOC Operations	This is the team who is responsible for monitoring the overall IT infrastructure and is responsible for identifying alarms and ensuring that tickets are opened and routed to the appropriate operator/analyst queue for resolution.	
Administrator	The Administrator is responsible for installing, configuring, upgrading and maintaining the monitoring applications and the environment in which the run. They work hand in hand with the other personas to ensur that those other personas have the capabilities available to perform their role.	

1.2.5 Interaction of Personas

The personas defined will typically sit in an organizational hierarchy something like the one shown in Figure 4.

The Executive will be fully responsible for ensuring that all business services are delivered in a manner by which end users can realize full value from the applications they are interacting with. They will want a qualitative view by which they can validate that all key applications are in good working order. If they are not, then understanding which business group(s) is affected.

The Operations Manager will usually collaborate with the Operator/Analysts and ensure that the services provided are operating at expected levels by comparing them against baselines and, where applicable,

SLAs. If a service indicates in problem state, the Executive, he/she will turn to the Operations Manager to provide status and resolution of any issues.

The Operator/Analyst is often responsible for parts or all of the application delivery system depending on the size of the business service they support. The focus may be on applications themselves, the systems that host the applications, the networks that connect the application system components or the storage devices that host application data. They will be responsible for getting to root cause and remediating any issues identified business service and the supporting components.

The NOC Operator will be responsible for constant monitoring of issues and to identify the proper course of action to take based on problem type. This may include opening service desk tickets and routing them to the appropriate Operator/Analyst and copying the Operations Manager or Executive depending on the severity and impact to business processes as defined by the IT organization.

The Administrator(s) will be responsible for providing ongoing operational and routine maintenance to keep the management systems aligned with changes in business monitoring requirements. Additionally, the Administrator(s) will work all Personas to adjust monitoring and notification policy, dashboards, reporting as required to stay relevant.

.

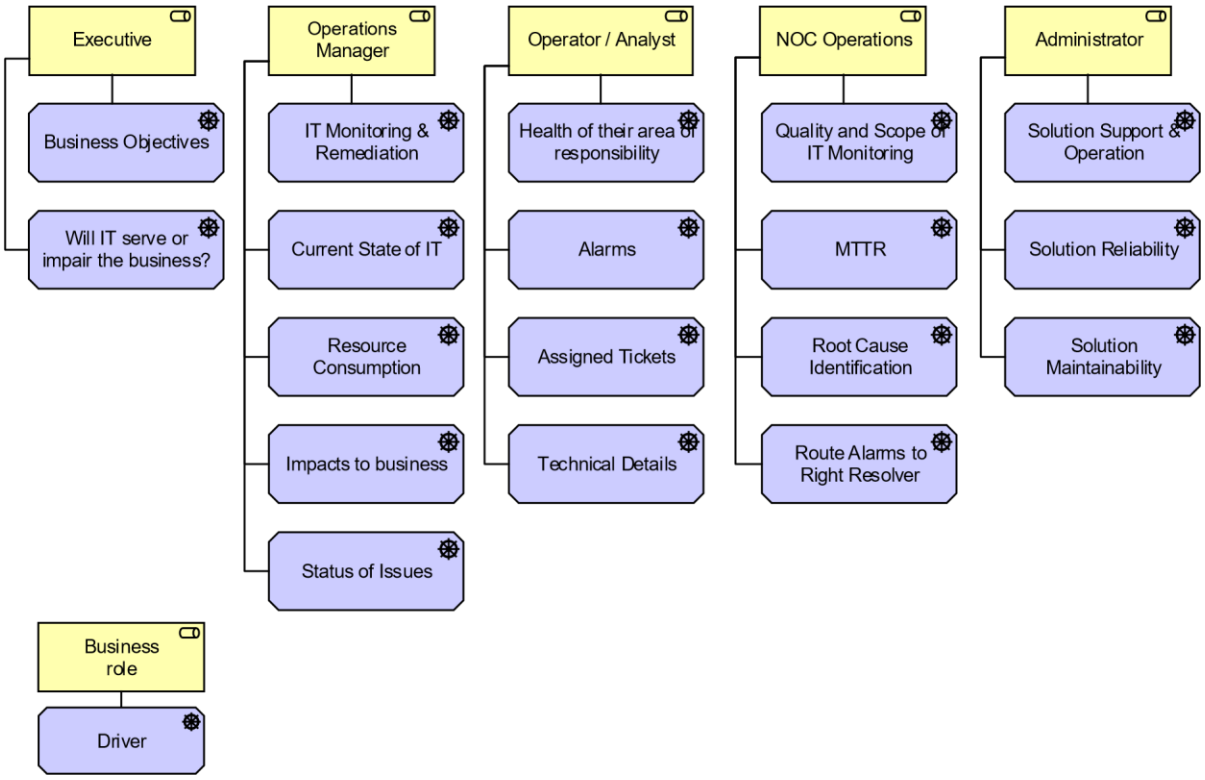


Figure 3 Interaction of Personas

1.2.6 Foundation Capability DX UIM

The following table summarizes the foundational capability, technology, and primary user stories for DX Unified Infrastructure Management.

Aspect	Description
SR1: Problem Identification	Real time status information is collected from DX UIM Agents (e.g. *Robot*); This component reports status changes and sends alarms and data metrics to the primary DX UIM server for processing and storage. DX UIM monitors its own infrastructure and supports alert identification of a component fails DX UIM allows the extraction of metric data using APIs and web services
SR2:	IT to business alignment will be achieved through configuring SLA/SLO definitions for specific IT Services and the servers /

Business Impact services upon which they rely.	The business impact of an IT “event” is now determined through assignment of a weight value to the originating device or service
SR3: Effective Prioritization of Events	DX UIM determines what events to turn into alarms and what severity level is assigned. DX UIM determines the impact of events on particular services and generates alarms at designated severity levels
SR4: Reduced Resource Requirements	Centralized and consolidated monitoring reduces the complexity and effort to manage the environment Automated notification eliminates manual effort Business impact information helps Operations staff focus on the most important events
SR5: Reduction of DX UIM Monitoring Environments	DX UIM Solution is scalable to support additional growth. Additional agents can be added as business demands change to support future growth
SR6: Centralized View of DX UIM Performance and Availability Monitoring	A centralized instance provides one environment for alert management, application discovery, event gathering, reporting, and notification services.

Aspect	**Description**
SR7: Event Management	Defined thresholds are triggered to alert Operations staff to potential problems before they become critical Metrics trending statistics are gathered for customer analysis; alarm suppression and de-duplicatioin algorithms are applied in order to reduce the number of alarms.
SR8: Automated Notification	IT support staff is automatically notified of high impact events through selected notification methods, including pager, email and (optional) service desk integration.
SR9: Reduced Mean Time to Repair	Metrics trending statistics are gathered for customer analysis; alarm suppression and de-duplicatioin algorithms are applied in order to reduce the number of alarms.

SR10: High Availability	The DX UIM solution can be deployed in a fault tolerant, highly available and/or disaster recovery environment to provide greater uptime and resiliency.
SR11: User Management, Security, and Retention	The DX UIM solution provides specific access based on user role and credentials. DX UIM supports Active Directory integration DX UIM software supports configurable port assignments DX UIM Supports configurable and user-defined data retention with separate configurations for metric and alarm data.
SR12: Usability	The DX UIM solution provides end user management to determine user impact. The DX UIM solution supports encrypted and unencrypted packet traffic. The DX UIM solution provides meaningful and actionable patterns and will provide improved alert quality.
SR13: Performance and Scalability	DX UIM supports physical and virtual instances. The DX UIM agent provides a non-intrusive footprint on the server layer and can be configured to have minimal impact. The DX UIM solution can scale as the business needs grow.

Aspect	Description
Capability	Model an infrastructure or network device, application, databases, cloud etc., manually or automatically. Configure sampling profiles of the network health and alerting to the problem management systems on requested health/state changes.

Aspect	Description
Content/Enabling Technology	▪ DX UIM Manager ▪ Unified Infrastructure Manager ▪ Operator Console ▪ CA Business Intelligence (CABI)
Integrations	▪ Email Gateway ▪ LDAP/Active Directory for user authentication ▪ Service Desk Gateway

1.2.7 Foundation Functional User Stories

The following section summarizes the functional user stories and the personas that participate in them.

As a/an	I want	So that
IT Executive	visibility of the health (performance and availability) of the IT services that support the business	I have knowledge of issues with the IT infrastructure supports oversight that will help lead to faster resolution
IT Executive	visibility of the health of the IT underpinnings (application, compute, storage, network) that support the business	I understand the nature of identified problems and can follow up with the responsible resolver teams
Operations Manager	visibility of the top 'N' underperforming IT underpinnings (applications, compute, storage, network) and trends	I can support the monitoring of SLAs and assess, plan and address issues before impacting their business
Operations Manager	visibility of the details of issues by specific areas (applications, compute, storage, network)	I can see trending over a period of time that will aid in identifying and preventing problems before they happen
Operator/Analyst	visibility of all alarms from IT underpinnings (application, compute, storage, network)	I can support the prioritization of issues to remediate.
Operator/Analyst	visibility of component level alarms by severity of each area (application, compute, storage, network)	I can identify the root cause and so facilitate remediation
NOC Operator	visibility of the summary view of business services (RYG) indicators and alarms	I have real time view of performance and availability of IT underpinnings that support the business.
NOC Operator	visibility of the breakdown of IT underpinnings (RYG) by geography or business group	I can see which part of the business is experiencing issues

As a/an	I want	So that

DX UIM Administrator	visibility of all alarms for IT underpinnings (application, compute, storage, network)	I can create monitoring coverage/usage reports
DX UIM Administrator	to configure DX UIM	I can verify that the tool that monitors the business infrastructure is operating as designed
DX UIM Administrator	alarm and notification management	network environment can be monitored with realtime status polling, incoming traps/events and root cause analysis
DX UIM Administrator	to configure DX UIM	IT infrastructure can be monitored with fault management

1.2.8 Foundation Logical Architecture

The following architecture illustrates the required application component packaging for the DX UIM foundation solution:

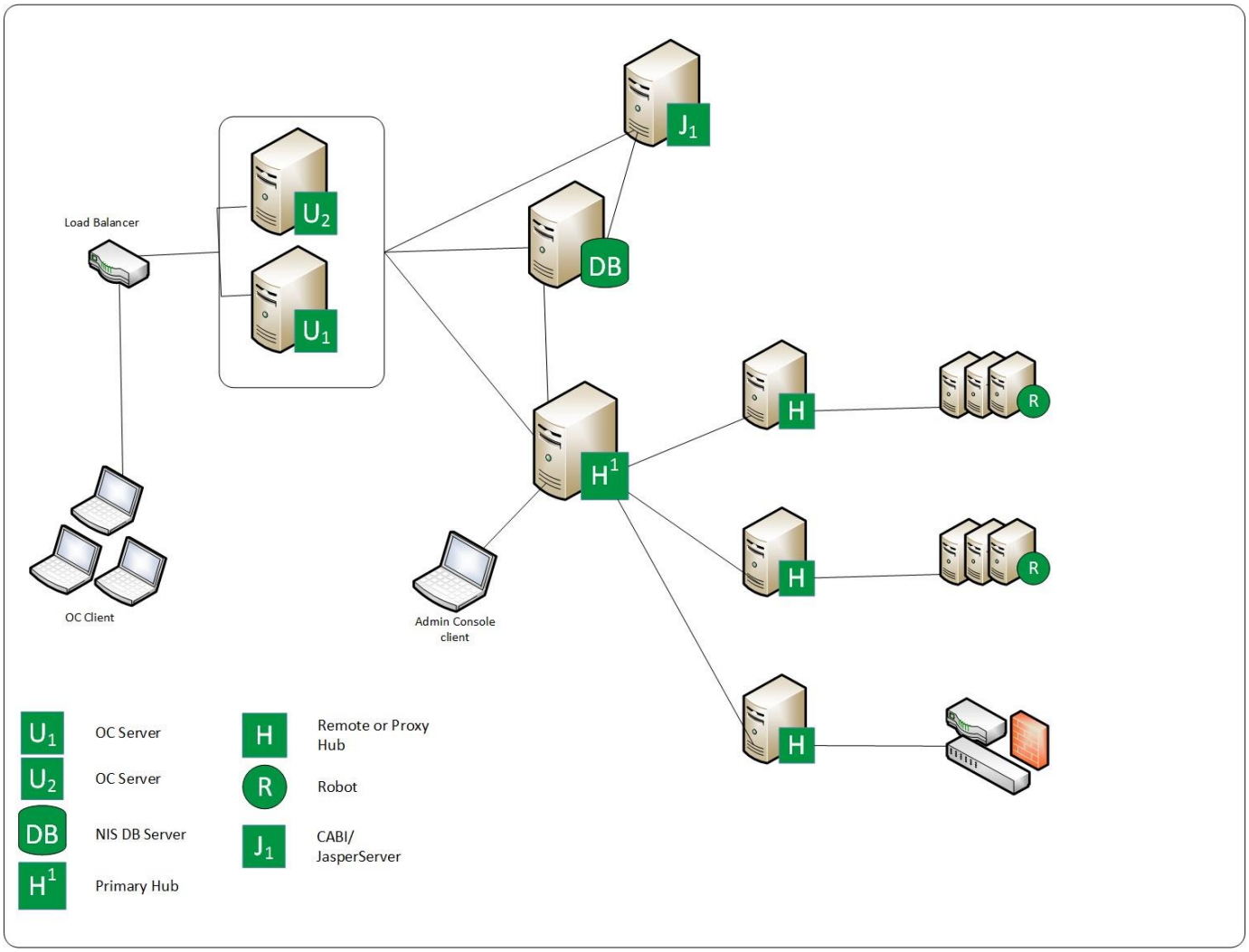


Figure 4 DX UIM Foundation Logical Architecture

1.2.9 Network Context

The following series of diagrams provide a reference implementation architecture design for the deployment of the DX UIM solution.

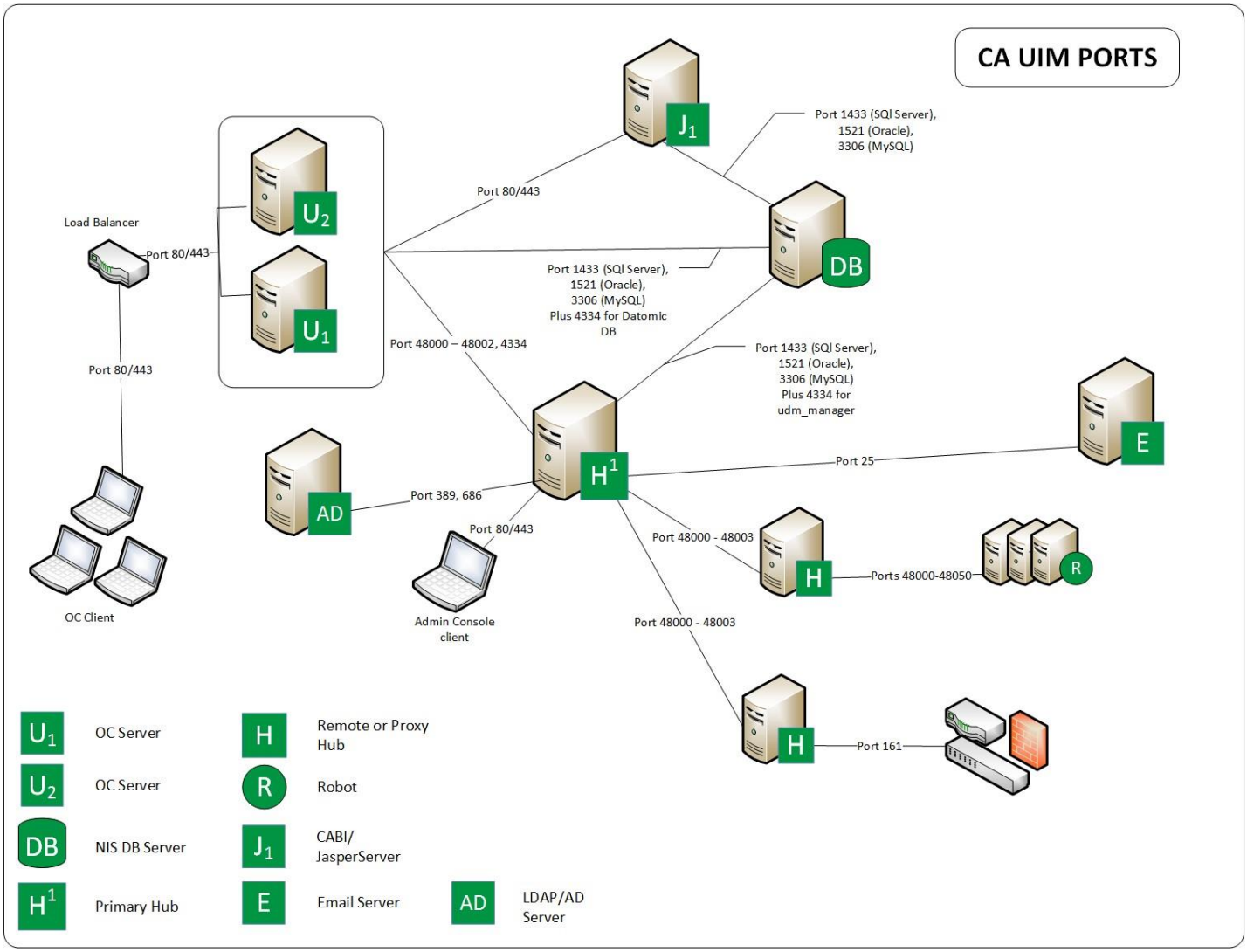


Figure 5 DX UIM Port diagram

Diagram Notes:

- Default Ports in Use: 80, 48000 (controller), 48001 (spooler), 48002 (hub), 4334 (udm_manager)
- Probe ports: 48000-48050; Ports are assigned to probes sequentially as available beginning with the first probe port number.
- Database port is dependent on the database vendor chosen - See the section Solution Component Ports for a comprehensive list.

1.2.9.1 Network Diagram – Foundation Physical Architecture

This section contains one or more views for the DX UIM solution which shows the physical/virtual instantiation of the solution for the Foundation Physical Architecture environment.

The unique network requirements placed on the DX UIM solution are summarized in the following diagram:

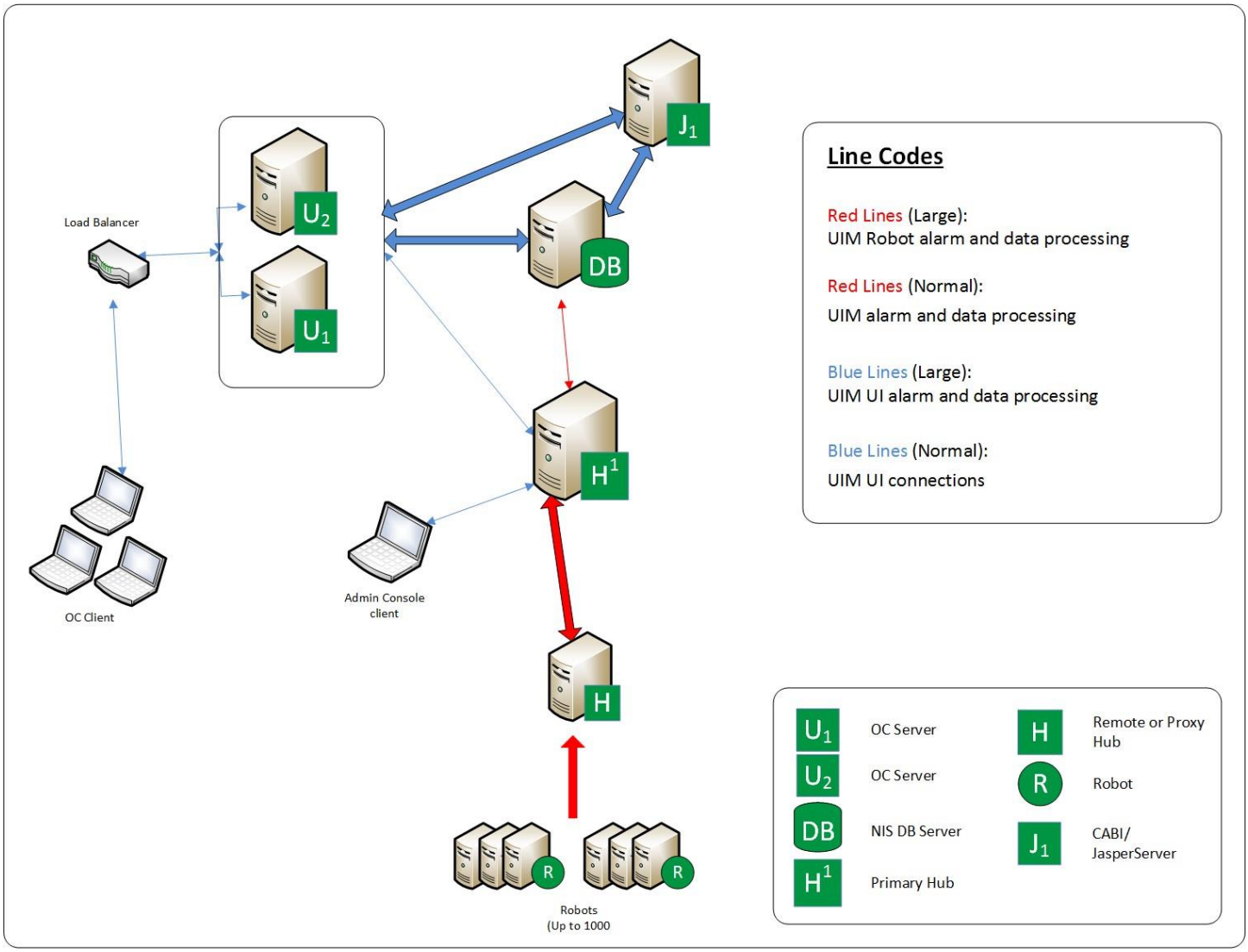


Figure 6 DX UIM Network diagram

1.2.9.2 Data Flows Explained

Data flow are detailed and explained in more detail below, including external components such as SMTP.

Thicker flow lines in the diagrams denote larger data volume.

1.2.9.2.1.1 Robot Data Flow

Robot data flow is a depicted in this diagram:

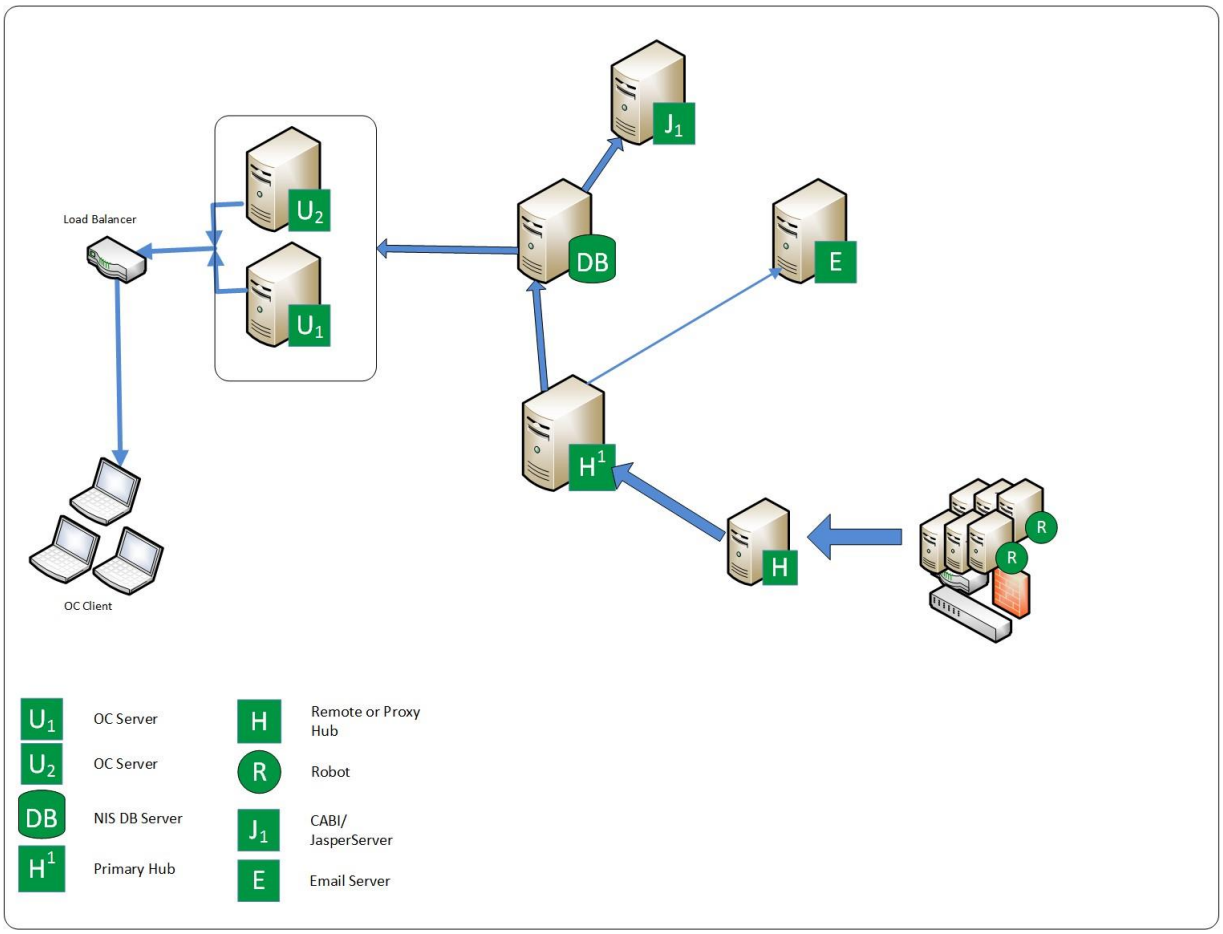


Figure 7 DX UIM Robot Dataflow

- Secondary hubs employ a store and forward methodology. Metric and alarm data are placed in queues which are underpinned by physical data files (proprietary format). As items are pulled and acknowledged from the queue by the subscribing component, they are deleted from the data file.

- All collected metric and alarm data is sent to the Primary hub for processing

- Email alarm actions are sent to the external email server (SMTP and IMAP/Exchange are supported)

- Metrics and alerts are pulled to the UI reports and displays based on the current context.

1.2.9.2.1.2 UI data flow

UI data flow is a depicted in this diagram:

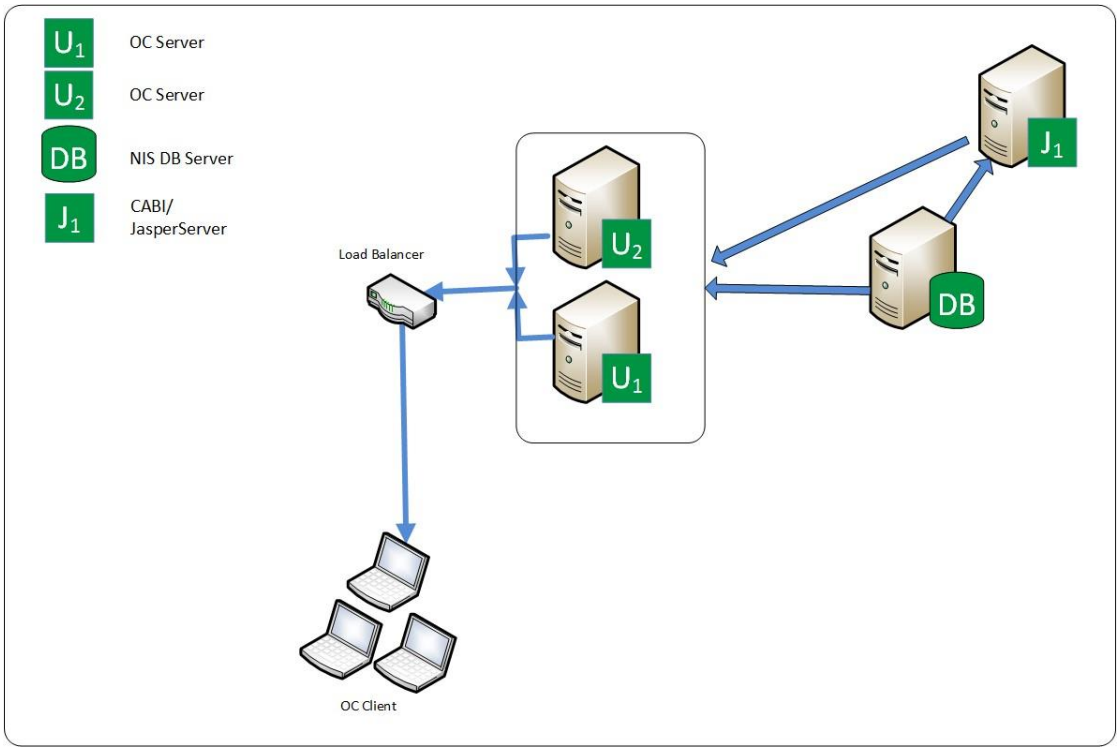


Figure 8 DX UIM UI Data Flow

- Operator Console Server(s) query the DX UIM database based on the current context of the end user browser page
- The CABI/JasperServer queries the DX UIM database for the data needed to populate the dashboard and/or report that is currently being viewed
- The Operator Console servers and the CABI use JDBC interfaces to the query the database.

Chapter 3: Technical Architecture

This section provides information relating to default configuration requirements that apply to the applications; for example, Port numbers for Web Services, Database Configuration, OS Configuration, and Supporting Services. These requirements are described via a Reference Implementation Architecture (RIA). A Foundation Architecture is provided to express the core functionalities delivered in a Foundation deployment.

Underlying Platforms – The operating system and database platforms for the SOI/DX UIM/DX NetOps Spectrum RIA are fully documented in the Foundation System Specification Requirements section. It also indicates which servers can be deployed on virtual platforms (VMWare).

This section contains the following topics:

Foundation Architecture
Foundation System Specification Requirements
Base System Configuration Requirements
Operator Console Technical Architecture

1.2.10 Foundation Architecture – DX UIM

This section contains views for the DX UIM solution which shows the physical/virtual instantiation of the solution for the Foundation Network / Physical Architecture environment. The Foundation DX UIM reference architecture is suitable for UAT and Production environments; provides redundancy for resilience, and scales by standing up redundant hub pairs initially sized to support discovery and management of up to 2,000 endpoints per hub pair depending on the types of endpoints being managed.

The unique network requirements placed on the DX UIM solution is summarized in the following diagram:

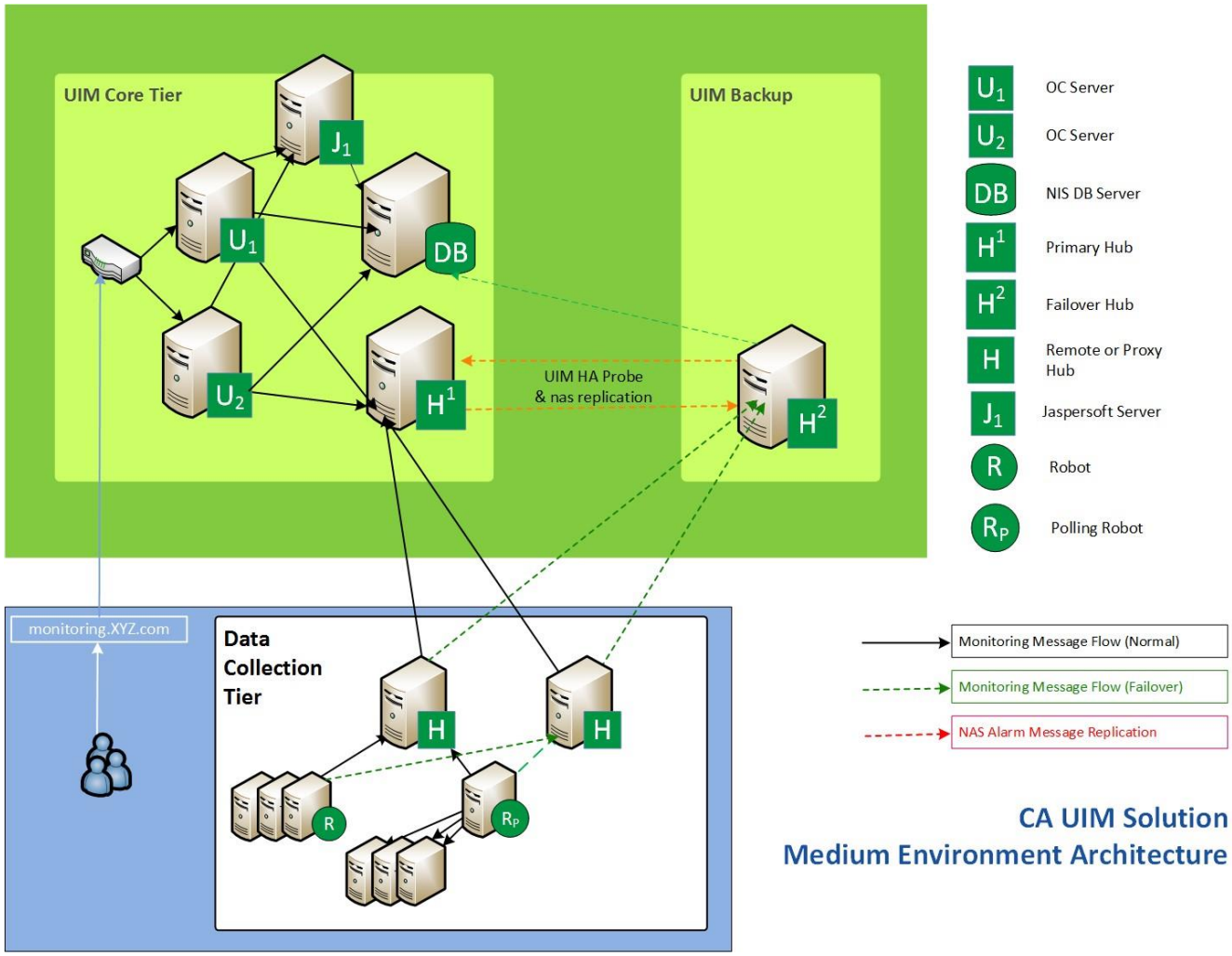


Figure 9 - DX UIM Medium Solution Environment

1.2.10.1 Architecture Commentary

1.2.10.1.1.1 DX UIM Architecture Commentary

The Foundation Architecture is a two tier design consisting of four systems at the first tier (the Primary Hub, the Operator Console, and Jaspersoft, and the database) and secondary hubs for the second tier.
The primary hub and Operator Console, working with the customer-provided database system, make up the core architecture. Every hub in the deployment that is not the Primary Hub (i.e. the first DX UIM Hub server deployed), is considered a Secondary hub. Some Secondary hubs are deployed for specific purposes, so we give them more descriptive, role-based names:

- Failover Hub – A secondary hub used to failover the message bus from another hub – usually just the Primary Hub, but you can have High Availability (HA) between any two secondary hubs.
- Scale or Proxy hub – A secondary hub that is deployed for the purposes of creating a scalable deployment
- Remote hub – A secondary hub that is physically located in a remote location

1.2.10.1.1.2 DX UIM Database

DX UIM supports using either MS SQL Server, Oracle, or MySQL for the backend database. By nature, the DX UIM solution is an OLTP (On Line Transaction Processing) system which requires a highly efficient database configuration to maintain acceptable insert and read performance. For larger implementations, it is rare that an out-of-the-box database configuration will provide the performance and efficiency that is required. There will likely need to be some tuning of the database and primary hub components to achieve optimum performance relative to the implementation size. Even smaller implementations may require some performance tuning due to the quantity and frequency of metric sampling. If Microsoft SQL Server is chosen for the DX UIM database, a document titled “DX UIM Database Best Practices for MS SQL Server” can be provided upon request.

1.2.10.1.1.3 Authentication and Authorization

DX UIM integrates with Active Directory and can be configured to use Active Directory (single-domain) for authentication. When a user logs in to DX UIM, their login credentials are passed from the web browser/UI to the Primary hub and authenticated via the integration with Active Directory. If the user passes authentication, the user is authorized to access the product based on their role/Access Control List (ACL) settings.

1.2.10.1.1.4 User Management

DX UIM User access will be provided by LDAP authentication to Active Directory. The access verification method is configured through the Settings configuration on the Primary Hub. Local accounts may also be configured for fallback in case LDAP is unavailable.

Two types of users exist in the DX Unified Infrastructure Management solution—*bus* users and *account contact* users. The permissions for both user types are set in the access control list (ACL). Administrators can create users of these two types to meet their security or multi-tenancy needs.

The following chart describes the key differences between bus users and account contact users.

Bus Users	Account Contact Users
Managed in Admin Console or Infrastructure Manager.	Managed in the Account Admin portlet.
Stored in the hub security file.	Stored in CM_ database tables.
Can see all data, systems, and alarms within DX UIM.	Can only see data, systems, and alarms with origins that match at least one of the account's origins.
Can access legacy Windows UIs.	Cannot access legacy Windows UIs.
Can access the bus, callbacks, and messages.	Cannot access the bus.

1.2.10.1.1.5 High Availability (HA)

There are two options for enabling high availability for the Primary Hub.

Option 1 – Install the DX UIM server on a Microsoft Cluster.

A cluster configuration minimizes the risk of having a single point of failure due to hardware problems or maintenance. Monitoring continues to operate even if the cluster nodes change state.

Failover is handled by the cluster when DX UIM is installed on a Microsoft Cluster.

The Windows Cluster method creates a virtual IP address for the cluster nodes running the DX UIM components. Using a virtual IP address means that none of the DX UIM components need to be reconfigured to point to the failover node.

The DX UIM Server supports failover with the following Microsoft versions:

- Windows Cluster 2012
- SQL Server Cluster 2008, 2012, 2014, and 2019

Follow the instructions found at https://techdocs.broadcom.com/content/broadcom/techdocs/us/en/ca-enterprisesoftware/it-operations-management/unified-infrastructure-management/20-4/installing/install-uim-server/installing-in-anactive-passive-microsoft-cluster.html

Option 2 - Set up failover using a primary hub and a secondary hub with the HA probe.

Failover is handled by the HA probe when DX UIM is installed on the primary and secondary hubs with the HA probe.

- One DX UIM HUB Server acts as a primary computer and the other as a secondary or backup.
- The responsibility of the secondary is to take control when the primary fails and to relinquish control when the primary recovers. This responsibility is the function of the HA probe.

With the HA probe, failover is automated, but the Operator Console components require configuration so that they point to the failover server. Use a LUA script or a probe available from DX UIM Services to configure Operator Console failover.

Secondary hubs can also be installed as high availability pairs. Use of the HA probe is dependent on the hub function/role and position in the hub hierarchy.

Secondary hubs that function as the endpoint hubs (no additional hubs downstream, only robots) are usually considered and installed as an Active/Active pair. The robots are configured with one as their primary hub connection and the other explicitly configured as the secondary. In this way, the hub pairs provide both load balancing and high availability.

Secondary hubs that function as proxy/tunnel/scaling hubs and are intermediary hubs between the Primary hub and the endpoint hubs are usually configured as an Active/Passive pair with the HA probe configured to enable/disable the downstream communication channels (queues).

1.2.10.1.1.6 Virtualization

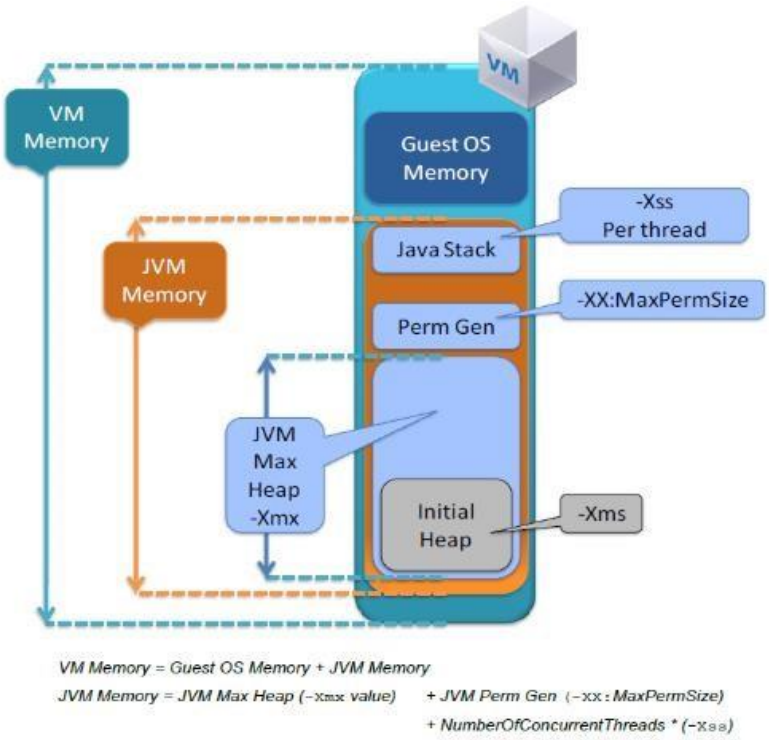
In a virtual environment, you can share resources to maximize your return on hardware investment or provide higher availability. However, because most of the CA software (APM, Performance Manager, Spectrum, DX UIM, etc.) will need to react to changing environmental conditions in real-time.

The CA software requires CPU resources, memory resources, and disk speeds to be running at optimal capacity. If any one of these resources is impacted because of another virtual machine or the virtual infrastructure places false limits on the resources available to the CA software, the performance of software will negatively be affected. Therefore, we recommend that you run CA software with CPU and memory resources that are dedicated 100 percent of the time. If you are using a storage area network (SAN), it is important to match the SAN performance requirements to be equivalent or better than those recommended in our hardware specifications.

The best practice recommendation is to fully dedicate resources that are equivalent to what would be provided by a physical system, these are specified in the hardware specifications, for Virtual Machines (VMs) being used for the CA software. Specifically, for Vmware environments, we recommend:

- Dedicated (reserved) resource group(s) should be assigned to the CA software virtual machines(s) to ensure required resources are always made available (e.g. reserved) regardless of the state of any other VMs running on the same server. The specific resource group allocations should be based on the sizing information from provided by the CA.
- Specific RAID volumes or LUN should be created with dedicated disks/spindles for the CA software to avoid disk I/O contention from other applications which may be sharing the same RAID or storage array. The greater the volume of disks/spindles allocated to the RAID volume or LUN will provide greater IO distribution and will maximize read/write times for the processes.
- Ensure that the size the virtual machine memory leaves adequate space for the Java heap, the other memory demands of the Java virtual machine code and stack, and any other concurrently executing process that needs memory from the guest operating system.
- Set the memory reservation value in the Vmware Infrastructure Client to the size of memory for the virtual machine. As any type of Memory Swapping (physical or virtual) is detrimental to performance of JVM heap especially for Garbage Collection.

- If your ESX host is overcommitted, ensure that the Balloon Driver is running within the virtual machine so that memory is optimally managed.
- There is no protection for the JAVA process memory. Therefore, it is recommended that the following calculation is used:



VM Memory = Guest OS Memory + JVM Memory

JVM Memory = JVM Max Heap [-Xmx value]

+ JVM Perm Gen [-xx: MaxPerSize]

+ Number of Concurrent Threads * Memory Per Thread [-Xss]

Note: ESX Server version 5 does not allow for I/O load balancing across HBA cards.

By following the lead practices of dedicating necessary resources to the CA software, you will limit the issues that are caused by lack of resource availability.

Due to the nature of the CA software and how can be negatively affected by CPU, memory and disk resource constraints, great care should be taken to ensure that the software can effectively share resources based on the above requirements.

1.2.11 Foundation System Specification Requirements

The hardware requirements for the solution are defined in the following table. Note that these are specific to a Reference Implementation Architecture based on average (Small) environments. Product documentation should be consulted for latest sizing estimates or engage CA Services for assistance with system sizing. Please see the Hardware Overview - https://techdocs.broadcom.com/content/broadcom/techdocs/us/en/ca-enterprise-software/itoperations-management/unified-infrastructure-management/20-4/installing/pre-installation-planning/prepare-yourserver-hardware.html

CA Reference Implementation Architecture					
Systems	**Servers**	**CA Recommended**			
	Total	**CPU (Cores)**	**Memory (GB)**	**Disk (GB)**	**Backup (GB)**
DX Unified Infrastructure Management	7	80	112	1624	1624
Solution Totals	**7**	**80**	**112**	**1624**	**1624**

DX Unified Infrastructure Management					
Server Role	**Type**	**CPU (Cores)**	**Memory (GB)**	**Disk (GB)**	**Backup (GB)**
DX UIM Primary Hub	VIRT	16	16	100	100
DX UIM Primary Hub, HA	VIRT	16	16	100	100
DX UIM Database	VIRT	16	16	1024	1024
DX UIM Operator Console	VIRT	16	16	100	100
DX UIM CABI	VIRT	8	16	100	100
DX UIM Remote Hub	VIRT	4	16	100	100
DX UIM Remote Hub (Backup)	VIRT	4	16	100	100
Total	**7**	**80**	**112**	**1624**	**1624**

1.2.12 Base System Configuration Requirements

1.2.12.1 Node Configuration – DX UIM

System configuration must comply with product documentation, located at the following URL: https://techdocs.broadcom.com/content/broadcom/techdocs/us/en/ca-enterprise-software/it-operationsmanagement/unified-infrastructure-management/20-4/installing/pre-installation-planning/ca-uim-sizingrecommendations.html

Refer to https://techdocs.broadcom.com/content/broadcom/techdocs/us/en/ca-enterprise-software/it-operationsmanagement/unified-infrastructure-management/20-4/installing/pre-installation-planning/configure-your-operatingsystems.html for information on general operating system prerequisites.

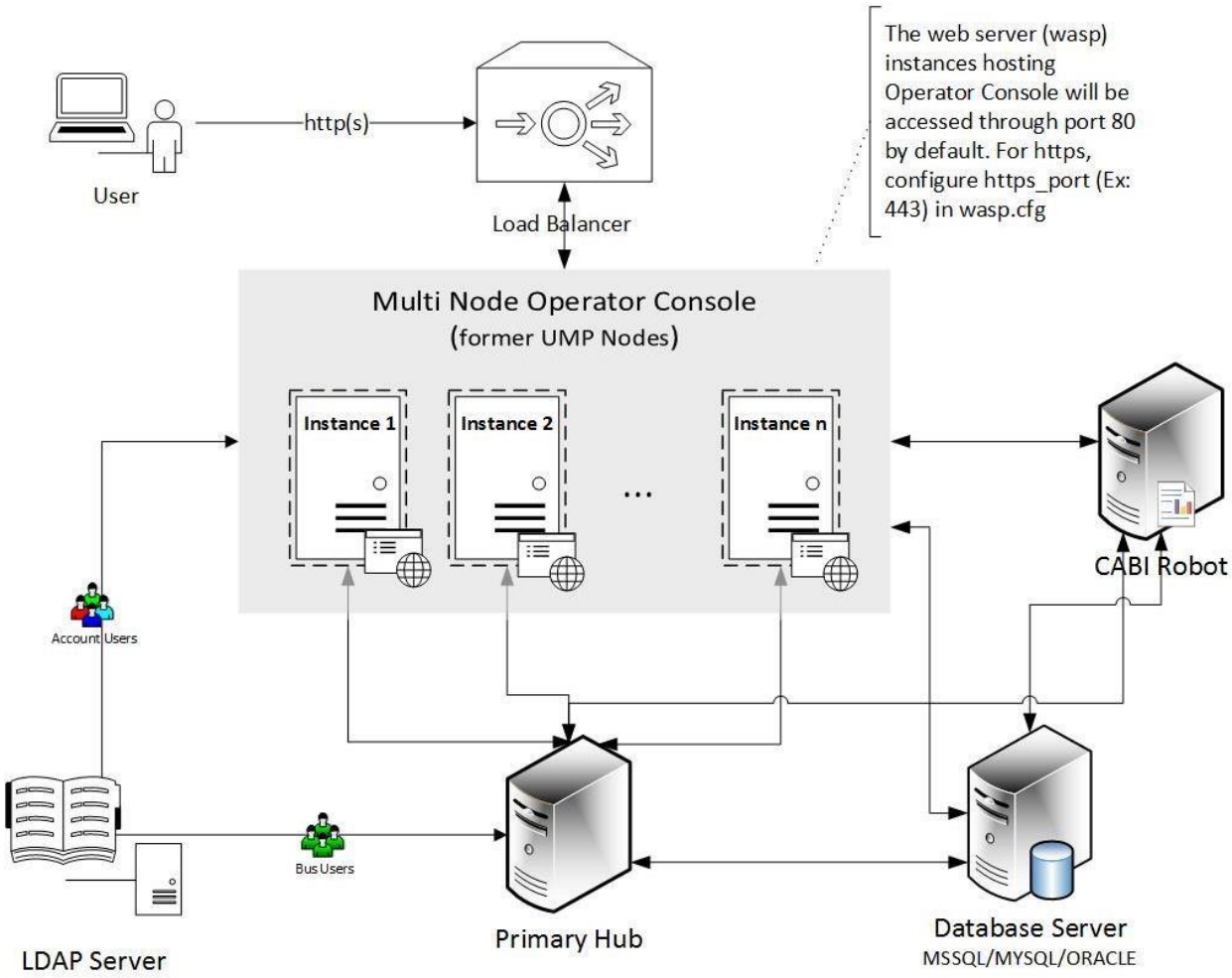
For Operating System support questions, refer to the Compatibility Support Matrix.

1.2.12.2 Solution Component Ports – DX UIM

Refer to https://techdocs.broadcom.com/content/broadcom/techdocs/us/en/ca-enterprise-software/it-operationsmanagement/unified-infrastructure-management/20-4/installing/pre-installation-planning/firewall-port-reference.html for a list of current communication ports for DX UIM.

1.2.13 Operator Console Technical Architecture

1.2.13.1 Deployment Model

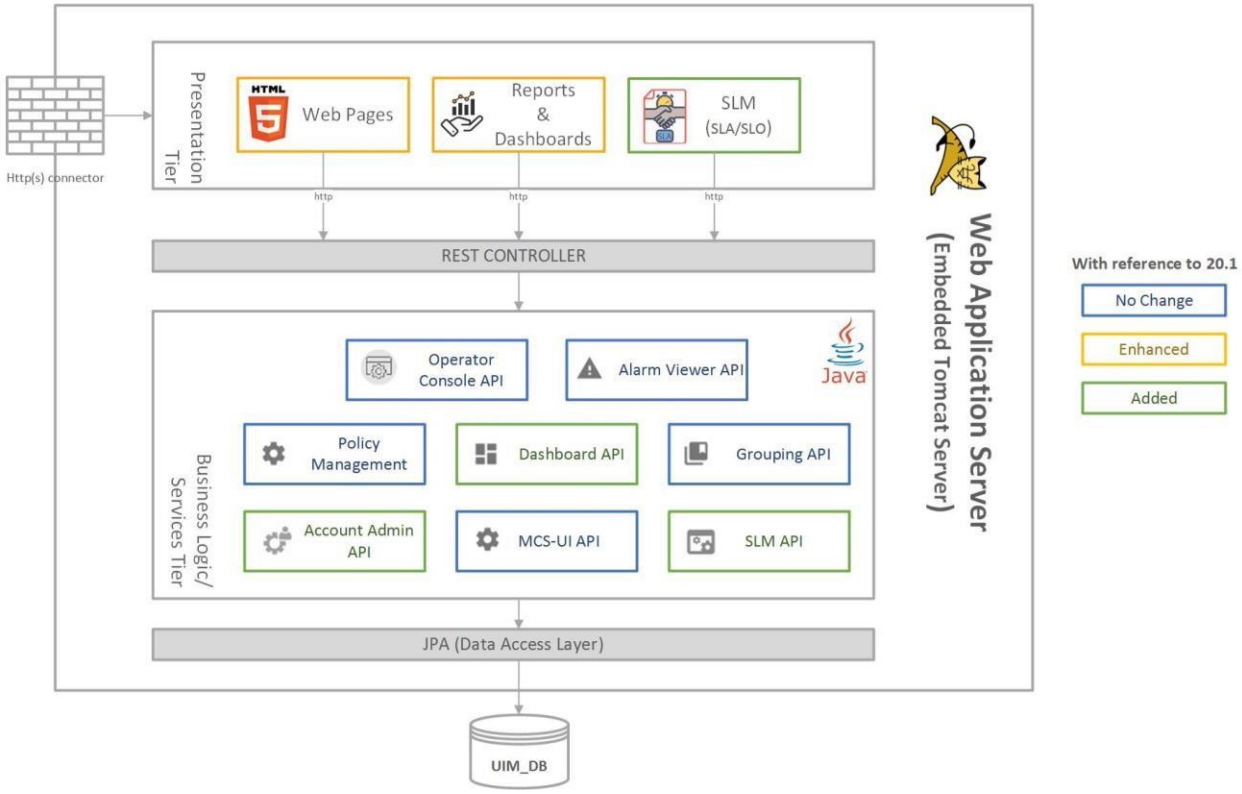


With DX UIM 20.4.0, deployment of CABI on Operator Console is supported. Refer to https://techdocs.broadcom.com/us/en/ca-enterprise-software/it-operations-management/unified-infrastructure-management/20-4/installing/ca-business-intelligence-with-ca-uim.html

For the sizing guidance when CABI is deployed on Operator Console, Refer to https://techdocs.broadcom.com/content/broadcom/techdocs/us/en/ca-enterprise-software/it-operationsmanagement/unified-infrastructure-management/20-4/installing/pre-installation-planning/ca-uim-sizingrecommendations.html

1.2.13.2 Multi-Tier Architecture

This section contains the multi-tier architectural model of the Operator Console. Operator Console deployment consists of many web applications. Operator Console has integration point for these different web apps. Each web application has its own Rest API implementation which interacts with the database for any request from the Operator Console UI. The web applications share the Session Id when these are accessed through the Operator Console UI. Operator Console uses many modern frontend frameworks for these web applications along with the Rest API for different operations.



Chapter 4: Implementation Guidance

This section contains the following topics:
DX UIM Installation Checklist

Note: The checklist links take you to the most current version of the documentation. If you are using a different version of DX UIM; select a different version of the documentation in the Versions drop-down in the upper right corner of https://techdocs.broadcom.com/ the page.

1.2.13.3 DX UIM Installation Checklist

Note: To take advantage of all the integration features that the DX UIM and DX NetOps Spectrum integration offers; 9.2.0 or greater must be installed and configured.

Steps	Resource Links
Hardware requirements, operating systems, database software.	Complete the Pre-Installation Steps (https://techdocs.broadcom.com/content/broadcom/techdocs/us/en/ca-enterprise-software/it-operations-management/unified-infrastructure-management/20-4/installing/pre-installation-planning.html)
Install DX UIM, includes the Message Bus, Domain, Primary Hub, Robot, Core Probes, and more.	Install the DX UIM Server (https://techdocs.broadcom.com/content/broadcom/techdocs/us/en/ca-enterprise-software/it-operations-management/unified-infrastructure-management/20-4/installing/install-uim-server.html)
Install DX UIM IM, a management console for some DX UIM tasks.	Install the Infrastructure Manager (https://techdocs.broadcom.com/content/broadcom/techdocs/us/en/ca-enterprise-software/it-operations-management/unified-infrastructure-management/20-4/installing/install-infrastructure-manager.html
Install Secondary HUBs, most deployments have at least one extra hub.	Install the Secondary Hubs (https://techdocs.broadcom.com/content/broadcom/techdocs/us/en/ca-enterprise-software/it-operations-management/unified-infrastructure-management/20-4/installing/install-secondary-hubs.html
Install Operator Console, presents the performance and availability data that DX UIM collects.	Install the Operator Console (https://techdocs.broadcom.com/content/broadcom/techdocs/us/en/ca-enterprise-software/it-operations-management/unified-infrastructure-management/20-4/installing/Install-Operator-Console-(OC).html/)
Install CABI, provides rich reporting and integrates in-memory analysis capabilities.	(Optional) Install CABI (https://techdocs.broadcom.com/content/broadcom/techdocs/us/en/ca-enterprise-software/it-operations-management/unified-infrastructure-management/20-4/installing/ca-business-intelligence-with-ca-uim.html)

Create and maintain an accurate list of the devices in your IT environment.	Discover the Systems to Monitor (https://techdocs.broadcom.com/content/broadcom/techdocs/us/en/ca-enterprise-software/it-operations-management/unified-infrastructure-management/20-4/installing/discover-systems-to-monitor.html)
Robots manage the probes that collect monitoring data and perform other functions.	Deploy the Robots (https://techdocs.broadcom.com/content/broadcom/techdocs/us/en/ca-enterprise-software/it-operations-management/unified-infrastructure-management/20-4/installing/deploy-robots.html)
Includes configuring a proxy server, email address login, HTTPS, SAML single sign-on, and more.	(Optional) Complete the Post-Installation Steps (https://techdocs.broadcom.com/content/broadcom/techdocs/us/en/ca-enterprise-software/it-operations-management/unified-infrastructure-management/20-4/installing/optional-post-installation-tasks.html)
Deploy and configure the monitoring probes based on your environment type.	Deploy the Monitoring Probes (https://techdocs.broadcom.com/content/broadcom/techdocs/us/en/ca-enterprise-software/it-operations-management/unified-infrastructure-management/20-4/installing/deploy-your-monitoring-probes.html

Chapter 5: Integration Guidance

There are three basic integrations included in the Foundational Capabilities:

Email notification – Email Gateway

User Authentication – LDAP/Active directory integration

Incident creation – Service Desk Gateway

You can integrate DX UIM with other products for customized monitoring solutions.

The DX Operational Intelligence Gateway (oi_connector) probe integrates DX Unified Infrastructure Management (DX UIM) and DX Operational Intelligence (DOI). You can configure the oi_connector probe to send data to DX Operational Intelligence. The CA Digital Operational Intelligence Gateway (oi_connector) achieves the following:

- Store DX UIM alarms, inventory, metrics (QoS), and DX UIM groups in DX Operational Intelligence
- Build Dashboards with the alarms, QoS and inventory information
- (Optional) Store Spectrum alarms and inventory in DX Operational Intelligence

Refer oi_connector (DX Operational Intelligence Gateway) Release Notes for more information.

For information on integrating with other CA products, see the topic "Integrating Other CA Products" in the DX Unified Management documentation.

1.2.13.4 Integration Features

This reference architecture demonstrates integration and configuration that will solve the following use cases:

- Automated email notifications for critical alarms/events
  - Attribute based matching for notification
- User authentication based on organizational user ids and policies
- Automated service desk incident creation
  - Multiple service desk support
  - Bi-directional communication for closing/resolving the alarms and incidents
  - Attribute based matching for automated incident creation
  - Manual selection capabilities

1.2.13.5 Integration Overview

Figure 10 Integration of DX UIM and Email Server provides a high level depiction of the solution. Detailed information for configuring the email gateway probe can be found in the DX Unified Infrastructure Management Probes documentation -

https://techdocs.broadcom.com/content/broadcom/techdocs/us/en/ca-enterprise-software/it-operations-management/caunified-infrastructure-management-probes/GA/alphabetical-probe-articles/emailgtw-email-gateway.html
Information regarding the Nimsoft Alarm Server (nas) probe can be found in the DX Unified Infrastructure Management Probes documentation - https://techdocs.broadcom.com/content/broadcom/techdocs/us/en/ca-enterprise-software/itoperations-management/ca-unified-infrastructure-management-probes/GA/alphabetical-probe-articles/nas-alarmserver/nas-im-configuration.html

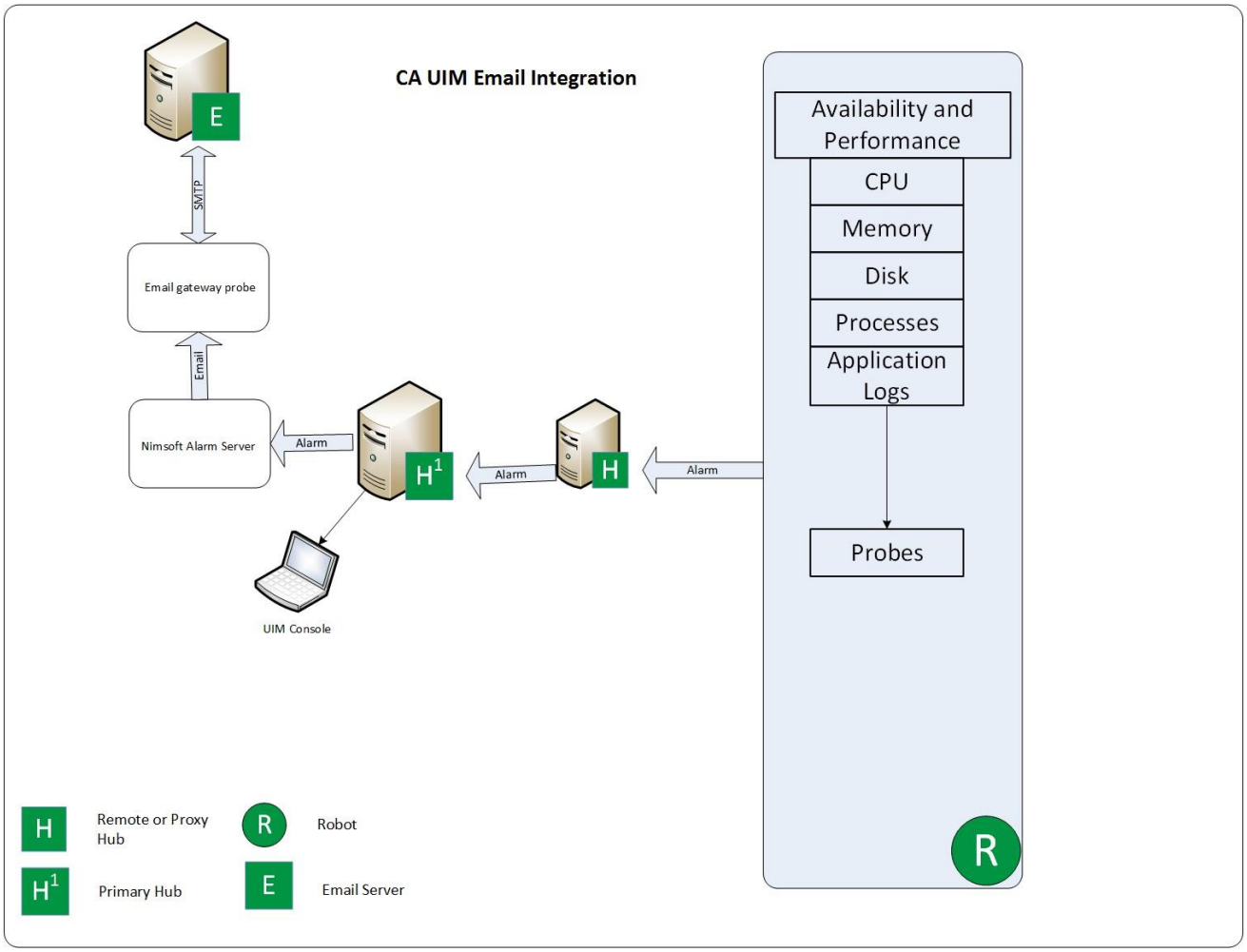


Figure 10 Integration of DX UIM and Email Server

Figure 11 Integration of DX UIM and LDAP/Active Directory provides a high level depiction of the solution. See the topic Enable Login with LDAP for detailed information.

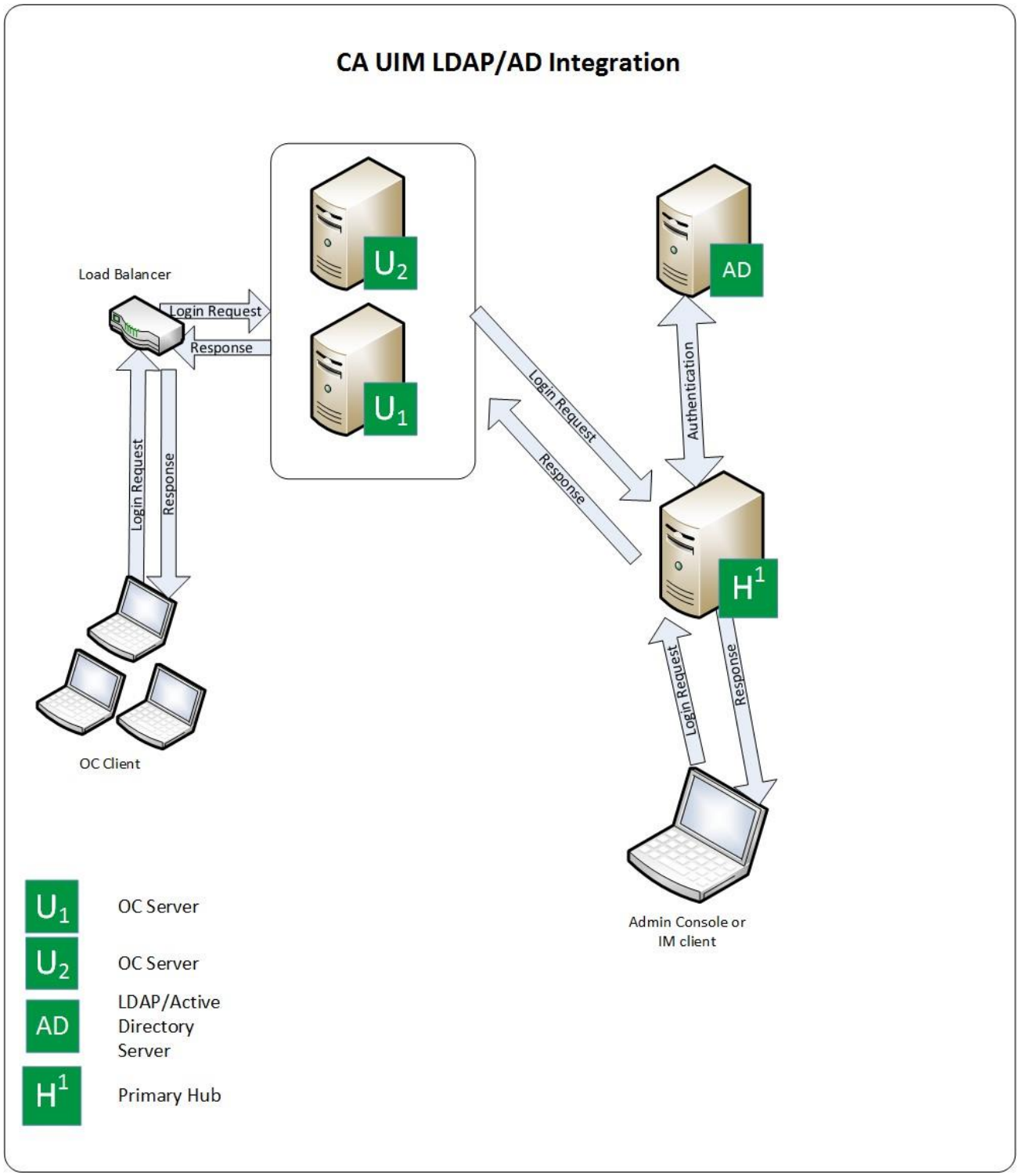


Figure 11 Integration of DX UIM and LDAP/Active Directory

Figure 11 Integration of DX UIM and Service Desk provides a high level depiction of the solution. Information regarding the Nimsoft Service Desk Gateway probe can be found in the DX Unified Infrastructure Management Probes documentation - https://techdocs.broadcom.com/content/broadcom/techdocs/us/en/ca-enterprise-software/it-operations-management/caunified-infrastructure-management-probes/GA/alphabetical-probe-articles/sdgtw-service-desk-gateway.html

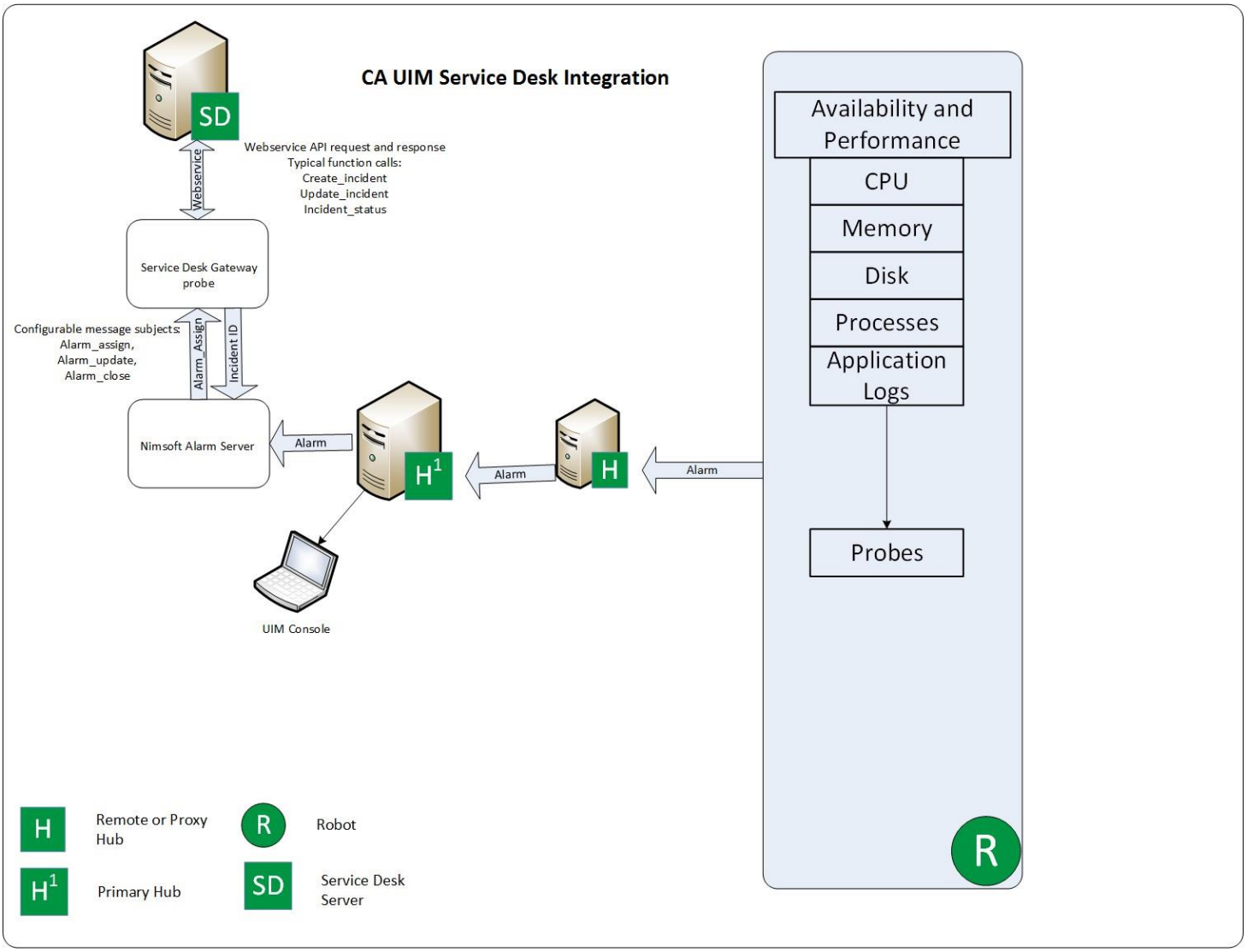


Figure 12 Integration of DX UIM and Service Desk

1.2.13.6 Integration Process Flow

Figure 13 Integration Process *Flow* describes the high level process steps to perform for integrating the solution.

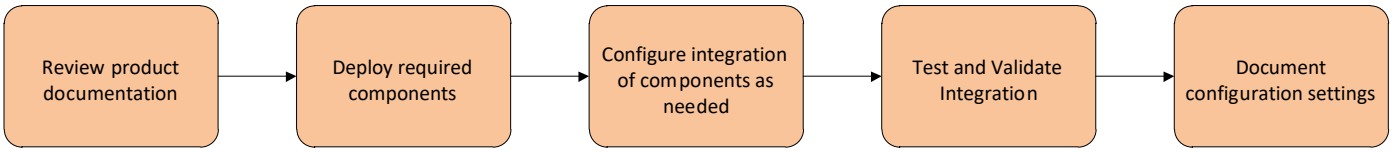


Figure 13 Integration Process Flow

1. It is important to review the appropriate product documentation to understand specific prerequisites, compatibility, and version support.
2. Install each of the components independently before integration.
3. Configure the components as needed according to the specific documentation guidelines.
4. Test and validate that the integration is working as planned.
5. Document the specific configuration settings.