CA Unified Infrastructure Management

Reference Architecture

Revised October 2018

ca technologies

Referenced Documents

Related Project Documentation
CA Unified Infrastructure Management Product Documentation: https://docops.ca.com/ca-unified-infrastructure-management/9-0-2/en
CA Unified Infrastructure Management Probes Documentation: https://docops.ca.com/ca-unified-infrastructure-management-probes/ga/en/alphabetical-probe-articles

Copyright © 2018 CA. All rights reserved. All trademarks, trade names, service marks, and logos referenced herein belong to their respective companies.

Contents

Contents 3

Table of Figures 4

Chapter 1: Executive Summary 5

How to use this document 5
Target Audience 5

Chapter 2: Functional Architecture 6

Planned End State 7
    Outcomes 9
Solution Personas 9
Interaction of Personas 10
Foundation Capability CA UIM 13
Foundation Functional User Stories 15
Foundation Logical Architecture 17
Network Context 18
    Network Diagram – Foundation Physical Architecture 19
    Data Flows Explained 20

Chapter 3: Technical Architecture 22

Foundation Architecture – CA UIM 23
    Architecture Commentary 24
Foundation System Specification Requirements 28
Base System Configuration Requirements 29
    Node Configuration – CA UIM 29
    Solution Component Ports – CA UIM 29

Chapter 4: Implementation Guidance 30

CA UIM Installation Checklist 30

Chapter 5: Integration Guidance 32

Integration Features 32

Copyright © 2018 CA. All rights reserved. All trademarks, trade names, service marks, and logos referenced herein belong to their respective companies.

Integration Overview 33
Integration Process Flow 37

Table of Figures

Figure 1 CA UIM Logical Architecture 7
Figure 2 CA UIM UI Interactions 8
Figure 3 Interaction of Personas 11
Figure 4 CA UIM Foundation Logical Architecture 17
Figure 5 CA UIM Port diagram 18
Figure 6 CA UIM Network diagram 19
Figure 7 CA UIM Robot Dataflow 20
Figure 8 CA UIM UI Data Flow 21
Figure 9 - CA UIM Medium Solution Environment 23
Figure 10 Integration of CA UIM and Email Server 34
Figure 11 Integration of UIM and LDAP/Active Directory 35
Figure 12 Integration of UIM and Service Desk 36
Figure 13 Integration Process Flow 37

Chapter 1: Executive Summary

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

The CA 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 implmentation 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://docops.ca.com/ca-unified-infrastructure-management/9-0-2/en, which includes factors and scenarios that should be taken into consideration for any customized solution.

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.

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

Copyright © 2018 CA. All rights reserved. All trademarks, trade names, service marks, and logos referenced herein belong to their respective companies.

Chapter 2: Functional Architecture

This section contains the following topics:

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

Copyright © 2018 CA. All rights reserved. All trademarks, trade names, service marks, and logos referenced herein belong to their respective companies.

Planned End State

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

The planned state is to provide a reference architecture to support the implementation of CA Unified Infrastructure Management (CA 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 CA UIM logical system architecture. This graphic is a simple representation of a UIM implementation.

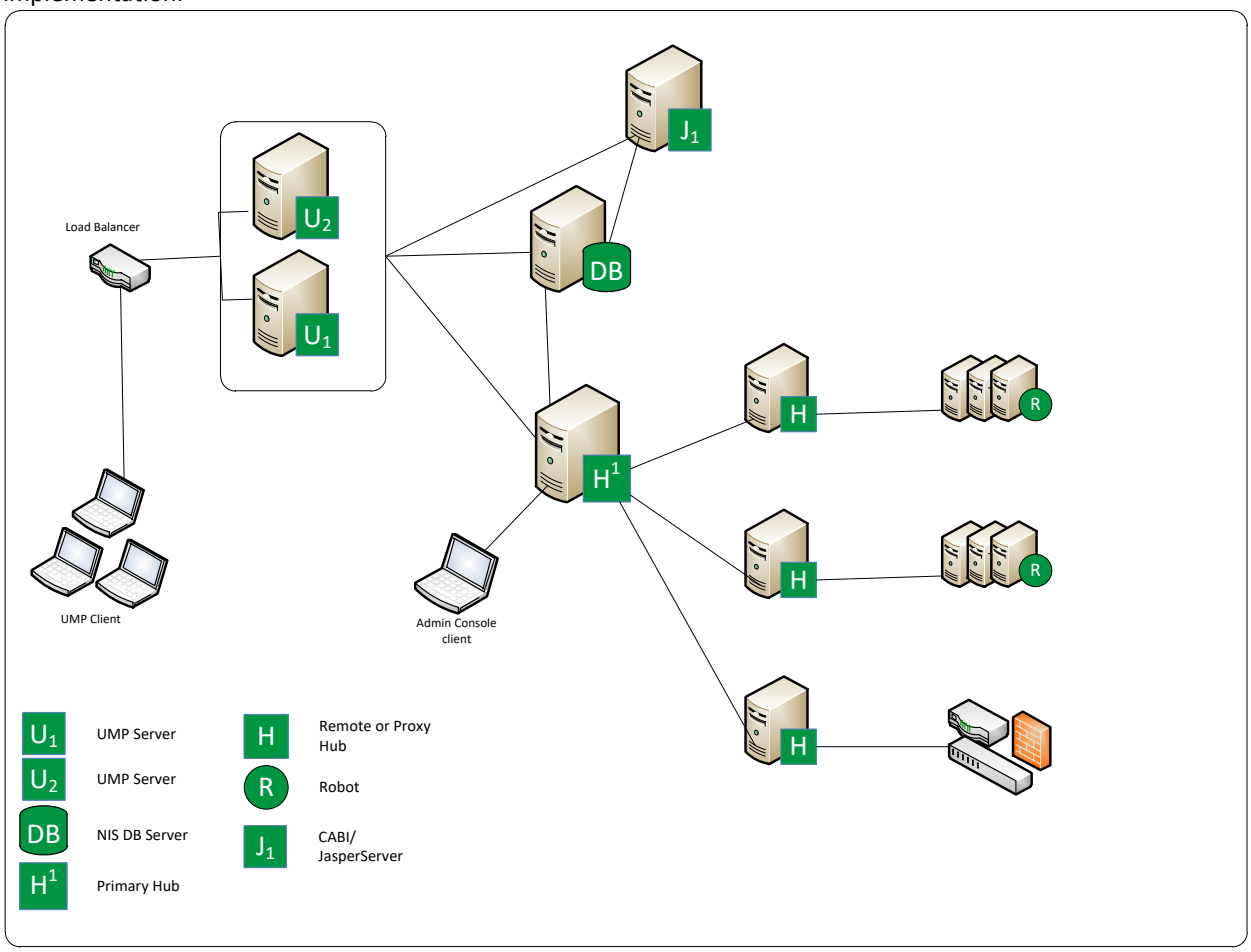


Figure 1 CA UIM Logical Architecture

Copyright © 2018 CA. All rights reserved. All trademarks, trade names, service marks, and logos referenced herein belong to their respective companies.

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

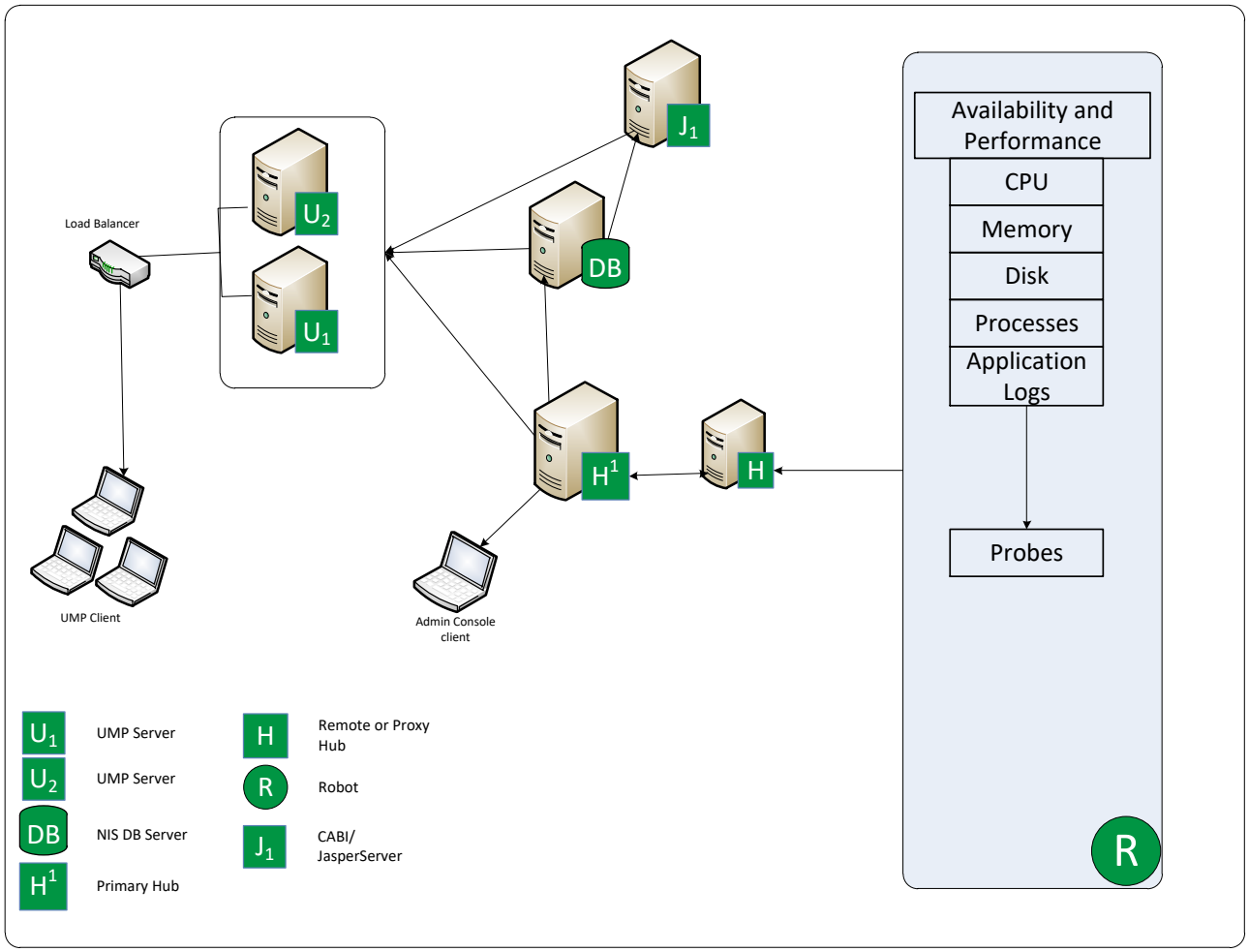


Figure 2 CA UIM UI Interactions

An overview and discussion of the CA UIM architecture can be found at: https://docops.ca.com/ca-unified-infrastructure-management/9-0-2/en/getting-started/ca-uim-reference-architecture

Copyright © 2018 CA. All rights reserved. All trademarks, trade names, service marks, and logos referenced herein belong to their respective companies.

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

Solution Personas

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

Persona	Description	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.	

Copyright © 2018 CA. All rights reserved. All trademarks, trade names, service marks, and logos referenced herein belong to their respective companies.

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 understand which business group(s) is affected.

The Operations Manager will usually collabortate 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

Copyright © 2018 CA. All rights reserved. All trademarks, trade names, service marks, and logos referenced herein belong to their respective companies.

Administrator(s) will work all Personas to adjust monitoring and notification policy, dashboards, reporting as required to stay relavent.

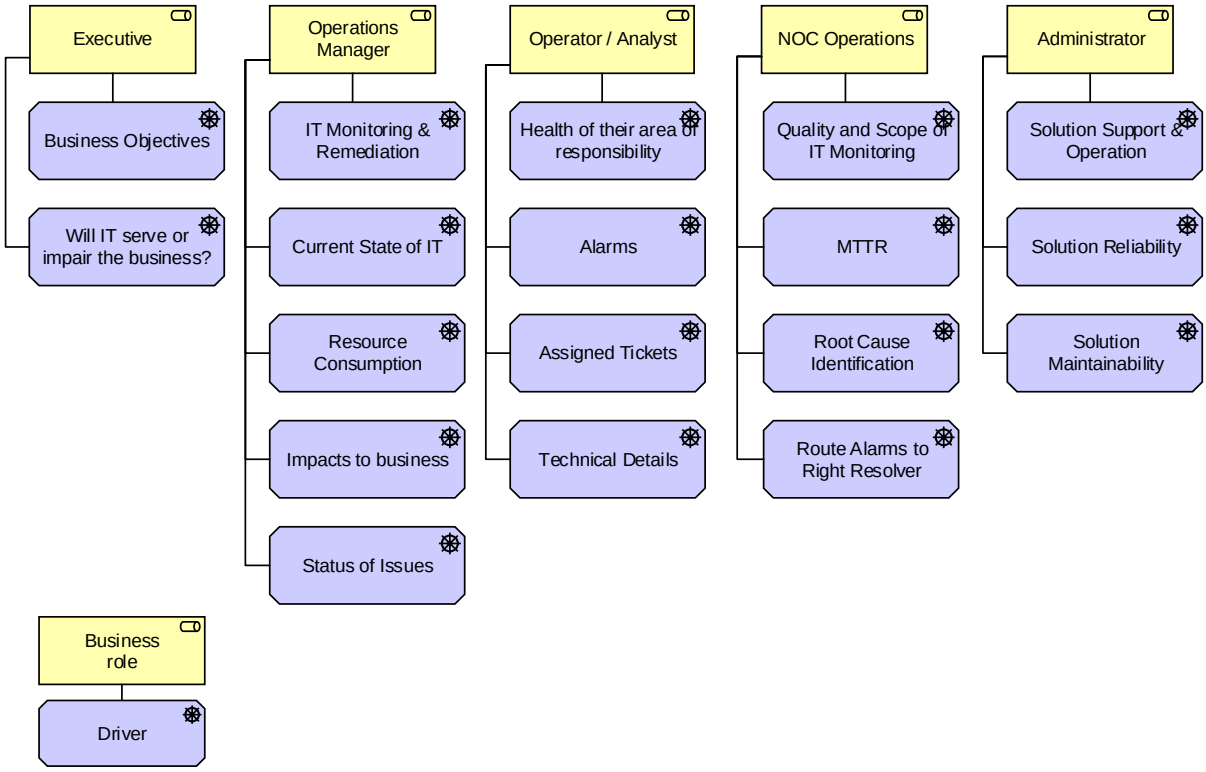


Figure 3 Interaction of Personas

Copyright © 2018 CA. All rights reserved. All trademarks, trade names, service marks, and logos referenced herein belong to their respective companies.

Foundation Capability CA UIM

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

Aspect	Description
SR1: Problem Identification	Real time status information is collected from CA UIM Agents (e.g. *Robot*); This component reports status changes and sends alarms and data metrics to the primary UIM server for processing and storage. UIM monitors its own infrastructure and supports alert identification of a component fails UIM allows the extraction of metric data using APIs and web services
SR2: Business Impact	IT to business alignment will be achieved through configuring SLA/SLO definitions for specific IT Services and the servers / 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	UIM determines what events to turn into alarms and what severity level is assigned. 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 UIM Monitoring Environments	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 UIM Performance and Availability Monitoring	A centralized instance provides one environment for alert management, application discovery, event gathering, reporting, and notification services.

Copyright © 2018 CA. All rights reserved. All trademarks, trade names, service marks, and logos referenced herein belong to their respective companies.

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 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 UIM solution provides specific access based on user role and credentials. UIM supports Active Directory integration CA UIM software supports configurable port assignments UIM Supports configurable and user-defined data retention with separate configurations for metric and alarm data.
SR12: Usability	The UIM solution provides end user management to determine user impact. The UIM solution supports encrypted and unencrypted packet traffic. The UIM solution provides meaningful and actionable patterns and will provide improved alert quality.
SR13: Performance and Scalability	CA UIM supports physical and virtual instances. The UIM agent provides a non-intrusive footprint on the server layer and can be configured to have minimal impact. The UIM solution can scale as the business needs grow.

Copyright © 2018 CA. All rights reserved. All trademarks, trade names, service marks, and logos referenced herein belong to their respective companies.

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.
Content/Enabling Technology	▪ CA UIM Manager ▪ Unified Infrastructure Manager ▪ Unified Management Portal ▪ CA Business Intelligence (CABI)
Integrations	▪ Email Gateway ▪ LDAP/Active Directory for user authentication ▪ Service Desk Gateway

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

Copyright © 2018 CA. All rights reserved. All trademarks, trade names, service marks, and logos referenced herein belong to their respective companies.

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

Copyright © 2018 CA. All rights reserved. All trademarks, trade names, service marks, and logos referenced herein belong to their respective companies.

Foundation Logical Architecture

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

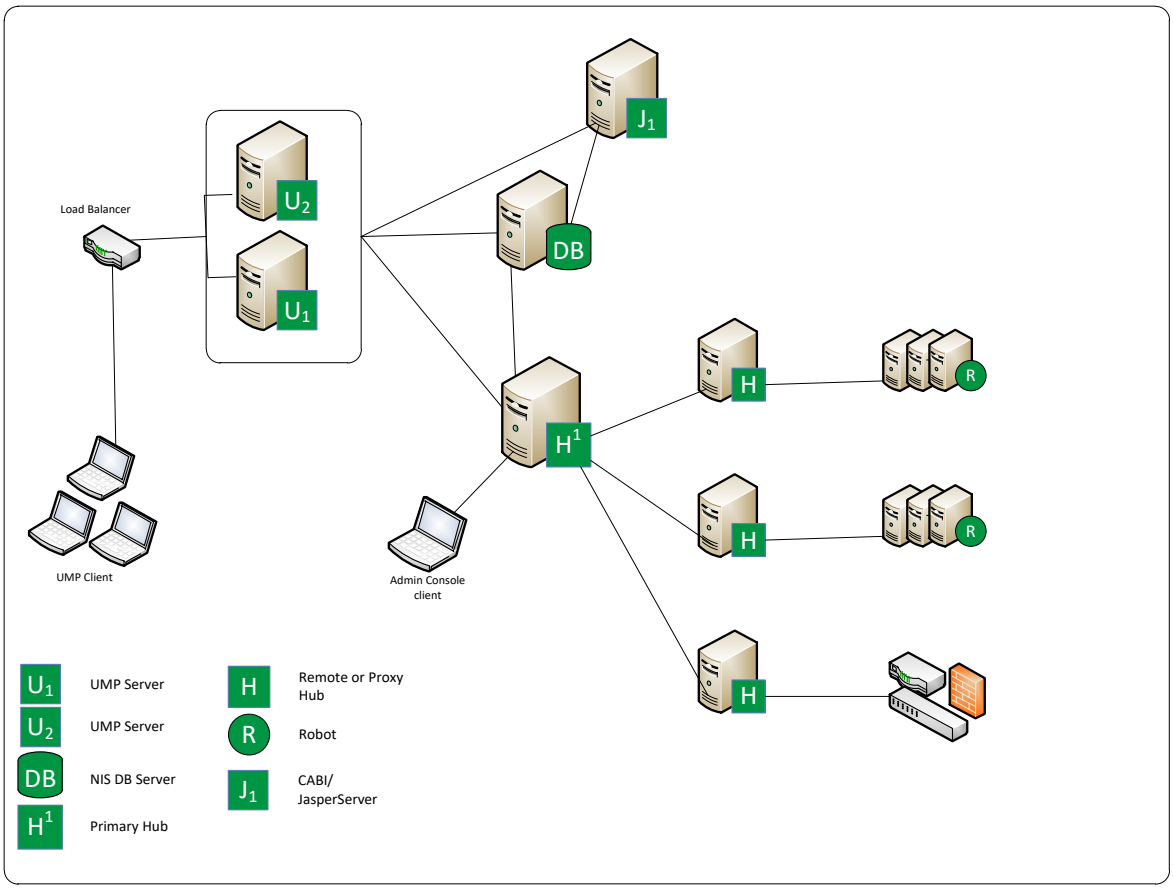


Figure 4 CA UIM Foundation Logical Architecture

Note: For more information about high availability, see the ha (High Availability) probe documentation.

Copyright © 2018 CA. All rights reserved. All trademarks, trade names, service marks, and logos referenced herein belong to their respective companies.

Network Context

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

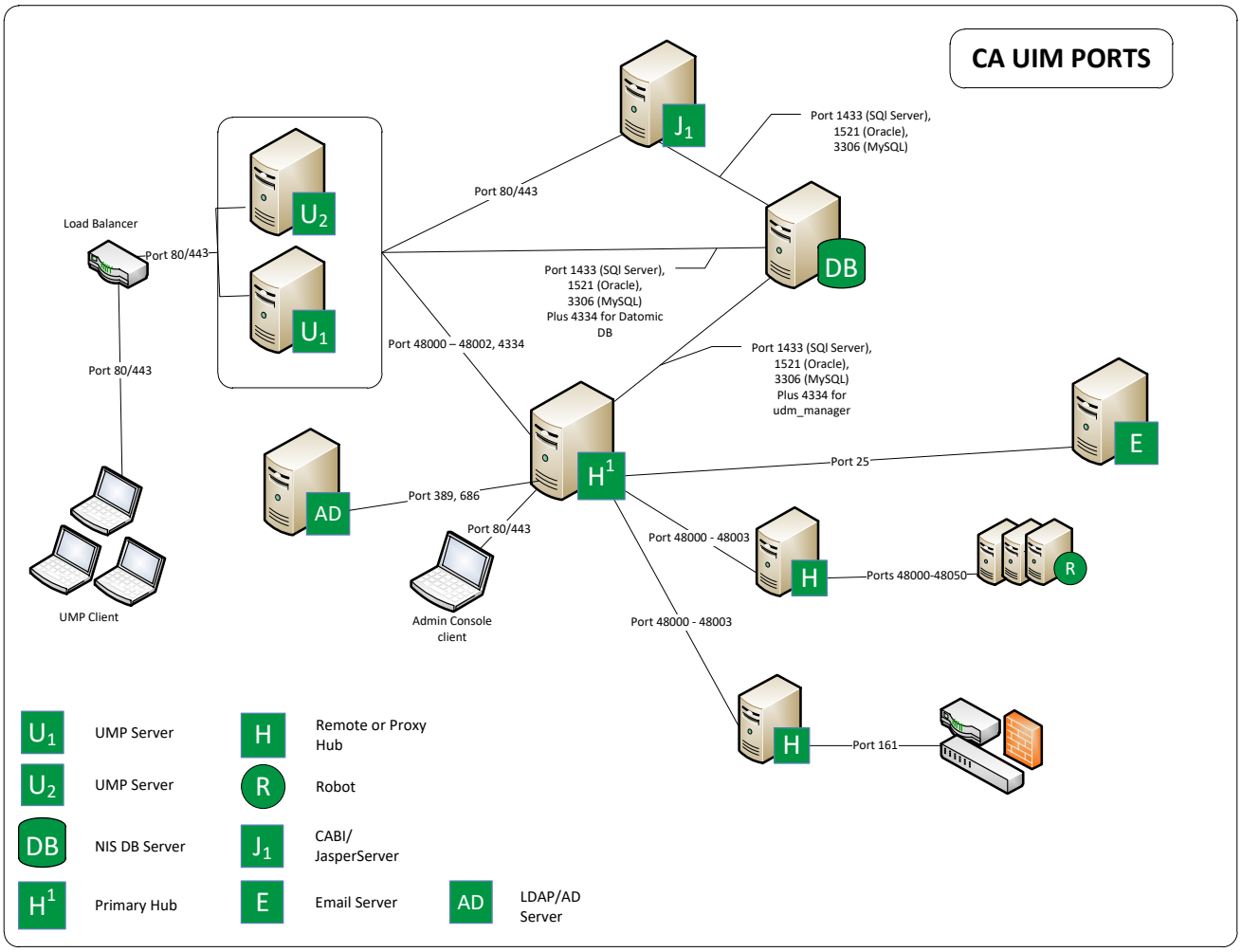


Figure 5 CA UIM Port diagram

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.

Copyright © 2018 CA. All rights reserved. All trademarks, trade names, service marks, and logos referenced herein belong to their respective companies.

Network Diagram – Foundation Physical Architecture

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

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

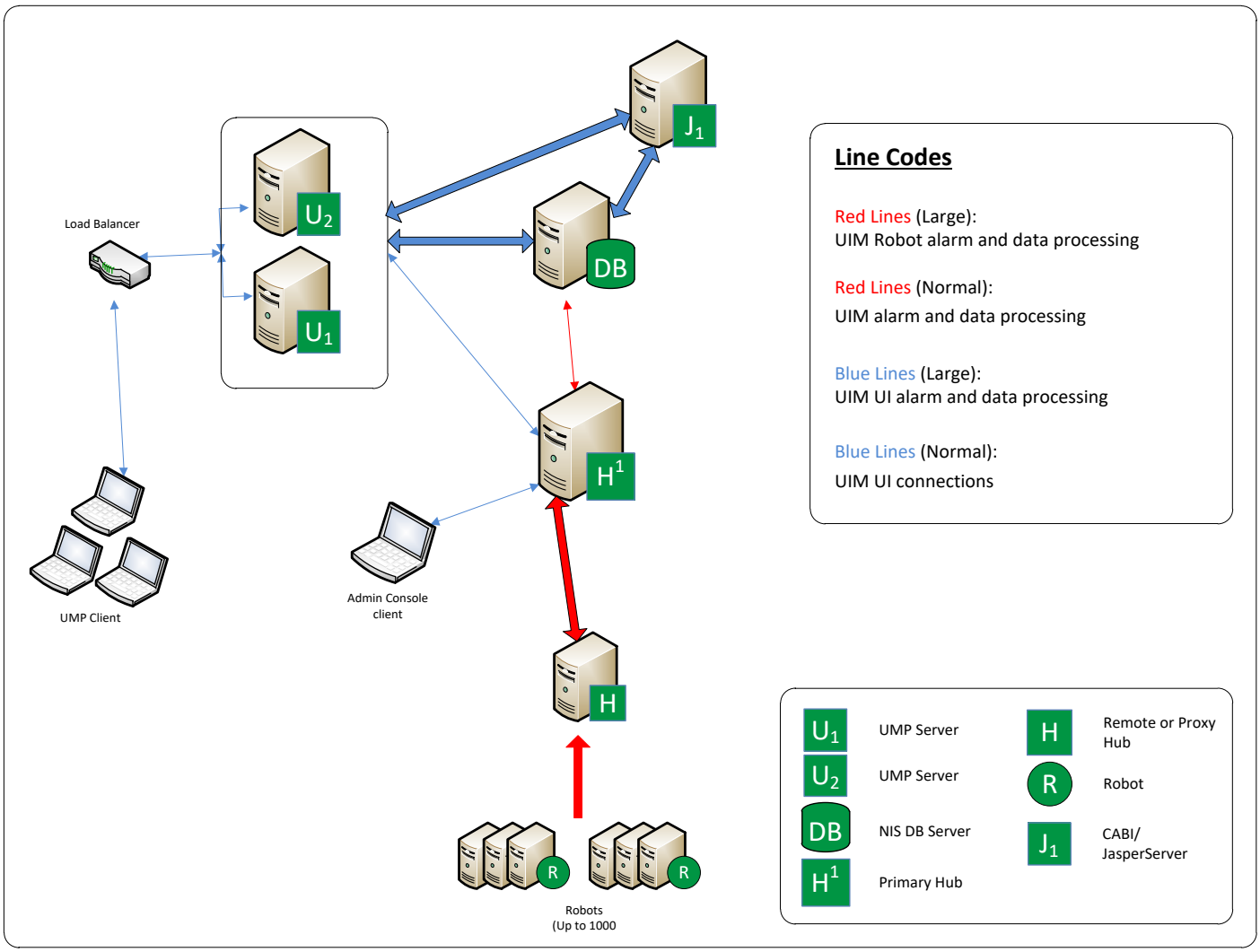


Figure 6 CA UIM Network diagram

Copyright © 2018 CA. All rights reserved. All trademarks, trade names, service marks, and logos referenced herein belong to their respective companies.

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.

Robot Data Flow

Robot data flow is a depicted in this diagram:

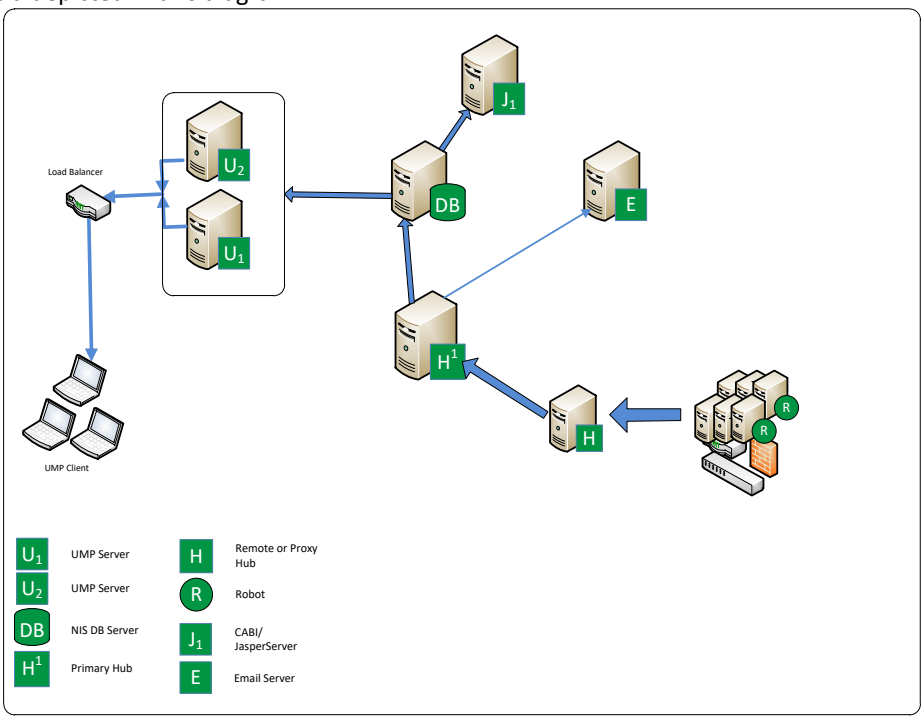


Figure 7 CA UIM Robot Dataflow

- 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.

Copyright © 2018 CA. All rights reserved. All trademarks, trade names, service marks, and logos referenced herein belong to their respective companies.

UI data flow

UI data flow is a depicted in this diagram:

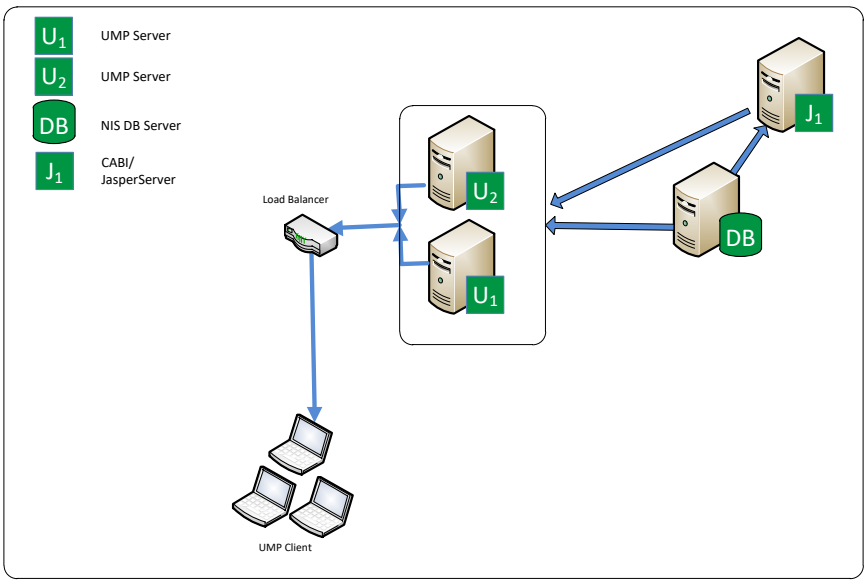


Figure 8 CA UIM UI Data Flow

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

Copyright © 2018 CA. All rights reserved. All trademarks, trade names, service marks, and logos referenced herein belong to their respective companies.

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 CA SOI/CA UIM/CA 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

Copyright © 2018 CA. All rights reserved. All trademarks, trade names, service marks, and logos referenced herein belong to their respective companies.

Foundation Architecture – CA UIM

This section contains views for the CA UIM solution which shows the physical/virtual instantiation of the solution for the Foundation Network / Physical Architecture environment. The Foundation 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 CA UIM solution is summarized in the following diagram:

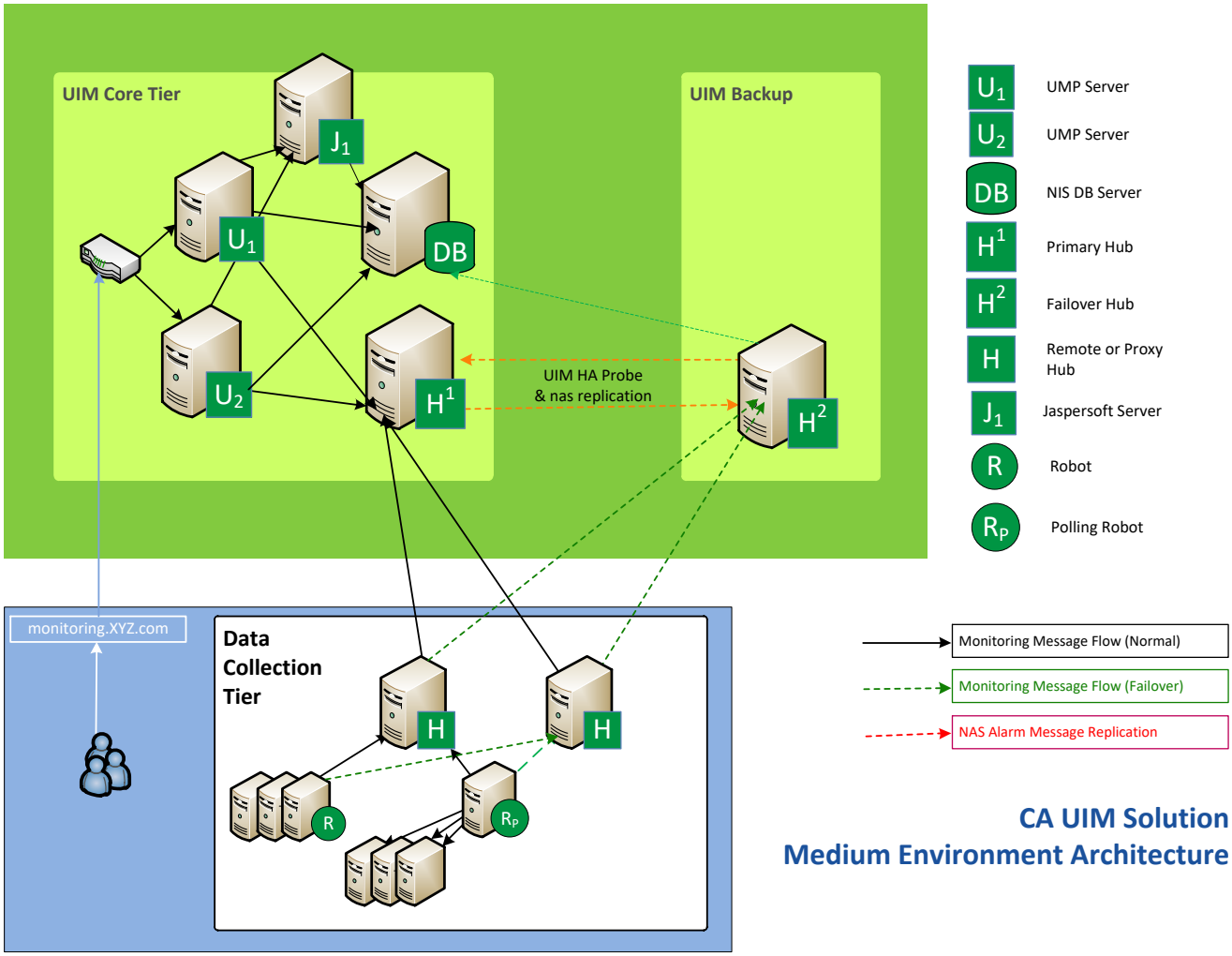


Figure 9 - CA UIM Medium Solution Environment

Copyright © 2018 CA. All rights reserved. All trademarks, trade names, service marks, and logos referenced herein belong to their respective companies.

Architecture Commentary

CA UIM Architecture Commentary

The Foundation Architecture is a two tier design consisting of four systems at the first tier (the Primary Hub, the Unified Management Portal, and Jaspersoft, and the database) and secondary hubs for the second tier.

The primary hub and management portal (UMP), 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 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

CA UIM Database

CA UIM supports using either MS SQL Server, Oracle, or MySQL for the backend database. By nature, the CA 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 CA UIM database, a document titled “CA UIM Database Best Practices for MS SQL Server” can be provided upon request.

Authentication and Authorization

UIM integrates with Active Directory and can be configured to use Active Directory (single-domain) for authentication. When a user logs in to 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.

User Management

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 CA 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.

Copyright © 2018 CA. All rights reserved. All trademarks, trade names, service marks, and logos referenced herein belong to their respective companies.

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 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.

High Availability (HA)

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

Option 1 – Install the CA UIM server on a Micrsoft 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 CA UIM is installed on a Microsoft Cluster. The Windows Cluster method creates a virtual IP address for the cluster nodes running the CA UIM components. Using a virtual IP address means that none of the CA UIM components need to be reconfigured to point to the failover node.

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

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

Follow the instructions found at https://docops.ca.com/ca-unified-infrastructure-management/9-0-2/en/installing/install-uim-server/installing-in-an-active-passive-microsoft-cluster

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 CA UIM is installed on the primary and secondary hubs with the HA probe.

- One 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 UMP components require configuration so that they point to the failover server. Use a LUA script or a probe available from CA UIM Services to configure UMP failover.

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

Copyright © 2018 CA. All rights reserved. All trademarks, trade names, service marks, and logos referenced herein belong to their respective companies.

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).

Virtualization

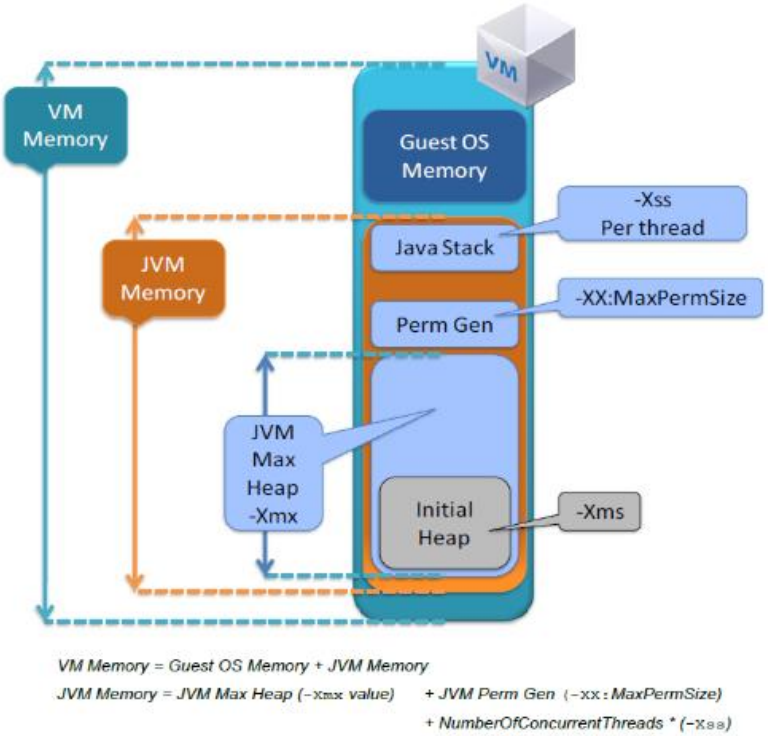
In a virtual environment, you can share resources to maximize your return on hardware investment or provide higher availability. However, because most of the CA software (APM, Performance Manager, Spectrum, UIM, etc.) will need to react to changing environmental conditions in real-time.

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:

Copyright © 2018 CA. All rights reserved. All trademarks, trade names, service marks, and logos referenced herein belong to their respective companies.



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 3.5 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.

Copyright © 2018 CA. All rights reserved. All trademarks, trade names, service marks, and logos referenced herein belong to their respective companies.

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 (Medium) 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://docops.ca.com/ca-unified-infrastructure-management/9-0-2/en/installing/pre-installation-planning/prepare-your-server-hardware

CA Reference Implementation Architecture					
Systems	**Servers**	**CA Recommended**			
	Total	**CPU (Cores)**	**Memory (GB)**	**Disk (GB)**	**Backup (GB)**
CA Unified Infrastructure Management	7	28	96	1624	1624
Solution Totals	**7**	**28**	**96**	**1624**	**1624**
CA Unified Infrastructure Management					
Server Role	**Type**	**CPU (Cores)**	**Memory (GB)**	**Disk (GB)**	**Backup (GB)**
CA UIM Primary Hub	VIRT	4	16	100	100
CA UIM Primary Hub, HA	VIRT	4	16	100	100
CA UIM Database	VIRT	4	16	1024 data	1024
CA UIM UMP	VIRT	4	8	100	100
CA UIM UMP	VIRT	4	8	100	100
CA UIM Remote Hub	VIRT	4	16	100	100
CA UIM Remote Hub (Backup)	VIRT	4	16	100	100
Total	**7**	**28**	**96**	**1624**	**1624**

Copyright © 2018 CA. All rights reserved. All trademarks, trade names, service marks, and logos referenced herein belong to their respective companies.

Base System Configuration Requirements

Node Configuration – CA UIM

System configuration must comply with product documentation, located at the following URL: https://docops.ca.com/ca-unified-infrastructure-management/9-0-2/en/installing/pre-installation-planning/prepare-your-server-hardware

Refer to https://docops.ca.com/ca-unified-infrastructure-management/9-0-2/en/installing/pre-installation-planning/configure-your-operating-systems for information on general operating system prerequisites.

For Operating System support questions, refer to the https://docops.ca.com/ca-unified-infrastructure-management/9-0-2/en/installing/product-compatibility/ca-uim-compatibility-matrix

Solution Component Ports – CA UIM

Refer to https://docops.ca.com/ca-unified-infrastructure-management/9-0-2/en/installing/pre-installation-planning/firewall-port-reference for a list of current communication ports for CA UIM.

Copyright © 2018 CA. All rights reserved. All trademarks, trade names, service marks, and logos referenced herein belong to their respective companies.

Chapter 4: Implementation Guidance

This section contains the following topics:

CA 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 CA UIM; select a different version of the documentation in the Versions drop-down in the upper right corner of http://docops.ca.com the page.

CA UIM Installation Checklist

Note: To take advantage of all the integration features that the CA UIM and CA Spectrum integration offers; CA UIM 8.4.7 or greater must be installed and configured.

Steps	Resource Links
Hardware requirements, operating systems, database software.	Complete the Pre-Installation Steps: https://docops.ca.com/ca-unified-infrastructure-management/9-0-2/en/installing/pre-installation-planning/prepare-your-server-hardware
Install UIM, includes the Message Bus, Domain, Primary Hub, Robot, Core Probes, and more.	Install the UIM Server: https://docops.ca.com/ca-unified-infrastructure-management/9-0-2/en/installing/install-uim-server
Install UIM IM, a management console for some UIM tasks.	Install the Infrastructure Manager: https://docops.ca.com/ca-unified-infrastructure-management/9-0-2/en/installing/install-infrastructure-manager
Install Secondary HUBs, most deployments have at least one extra hub.	Install the Secondary Hubs: https://docops.ca.com/ca-unified-infrastructure-management/9-0-2/en/installing/install-secondary-hubs
Install UMP, presents the performance and availability data that CA UIM collects.	Install the Unified Management Portal (UMP): https://docops.ca.com/ca-unified-infrastructure-management/9-0-2/en/installing/install-unified-management-portal-ump
Upgrade UR, Provides advanced reporting for the UMP.	(Optional) Upgrade the Unified Reporter: https://docops.ca.com/ca-unified-infrastructure-management/9-0-2/en/upgrading/ca-uim-upgrade-step-3-deploy-the-upgrade/upgrade-unified-reporter
Install CABI, provides rich reporting and integrates in-memory analysis capabilities.	(Optional) Install CABI: https://docops.ca.com/ca-unified-infrastructure-management/9-0-2/en/installing/ca-business-intelligence-with-ca-uim
Create and maintain an accurate list of the devices in your IT environment.	Discover the Systems to Monitor: https://docops.ca.com/ca-unified-infrastructure-management/9-0-2/en/installing/discover-systems-to-monitor

Copyright © 2018 CA. All rights reserved. All trademarks, trade names, service marks, and logos referenced herein belong to their respective companies.

Robots manage the probes that collect monitoring data and perform other functions.	Deploy the Robots: https://docops.ca.com/ca-unified-infrastructure-management/9-0-2/en/installing/deploy-robots
Includes configuring a proxy server, email address login, HTTPS, SAML single sign-on, and more.	(Optional) Complete the Post-Installation Steps: https://docops.ca.com/ca-unified-infrastructure-management/9-0-2/en/installing/optional-post-installation-tasks
Deploy and configure the monitoring probes based on your environment type.	Deploy the Monitoring Probes: https://docops.ca.com/ca-unified-infrastructure-management/9-0-2/en/installing/deploy-your-monitoring-probes

Copyright © 2018 CA. All rights reserved. All trademarks, trade names, service marks, and logos referenced herein belong to their respective companies.

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

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

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

Copyright © 2018 CA. All rights reserved. All trademarks, trade names, service marks, and logos referenced herein belong to their respective companies.

Integration Overview

Figure 10 Integration of CA 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 CA Unified Infrastructure Management Probes documentation - https://docops.ca.com/ca-unified-infrastructure-management-probes/ga/en/alphabetical-probe-articles/emailgtw-email-gateway

Information regarding the Nimsoft Alarm Server (nas) probe can be found in the CA Unified Infrastructure Management Probes documentation - https://docops.ca.com/ca-unified-infrastructure-management-probes/ga/en/alphabetical-probe-articles/nas-alarm-server/nas-im-configuration

Copyright © 2018 CA. All rights reserved. All trademarks, trade names, service marks, and logos referenced herein belong to their respective companies.

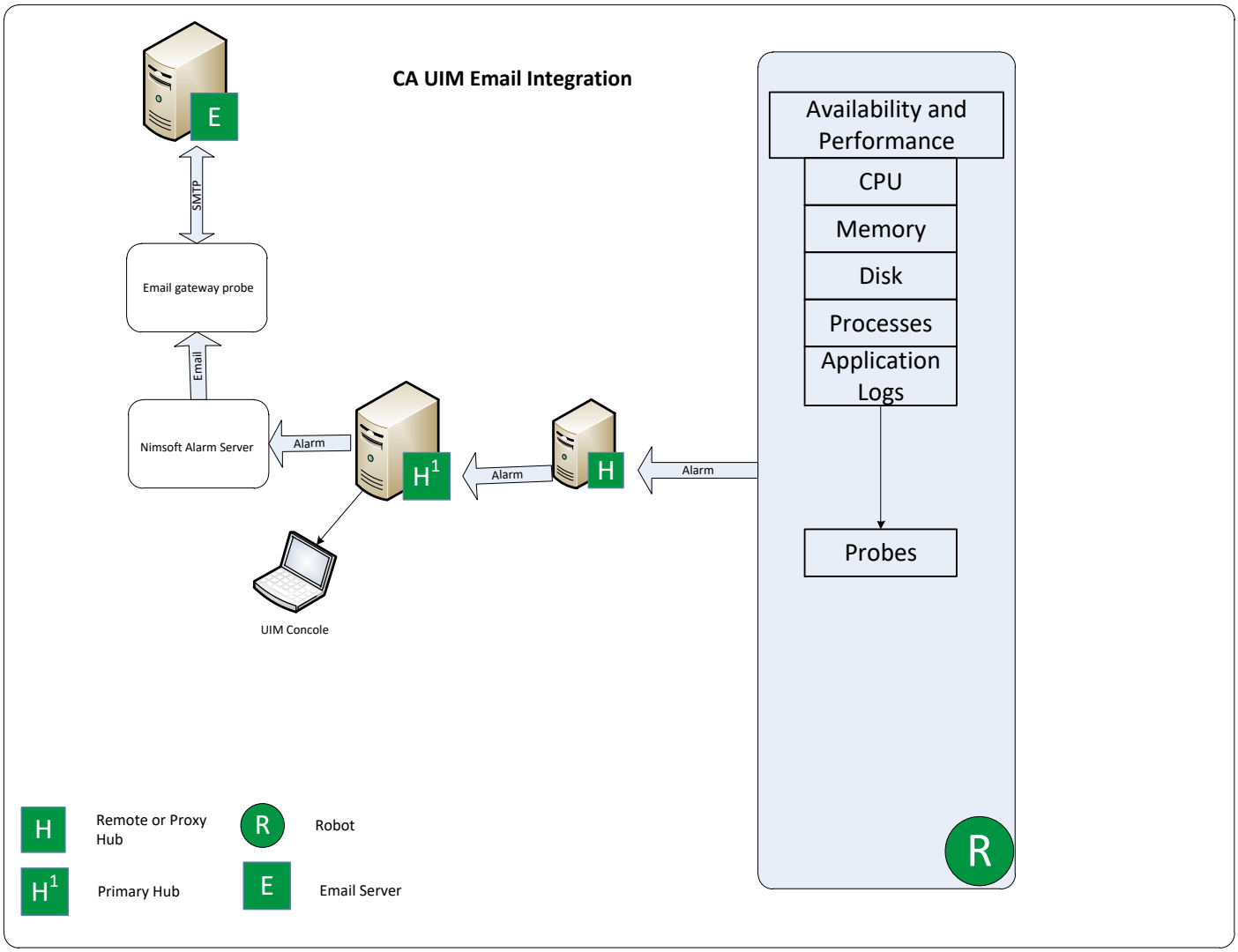


Figure 10 Integration of CA UIM and Email Server

Copyright © 2018 CA. All rights reserved. All trademarks, trade names, service marks, and logos referenced herein belong to their respective companies.

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

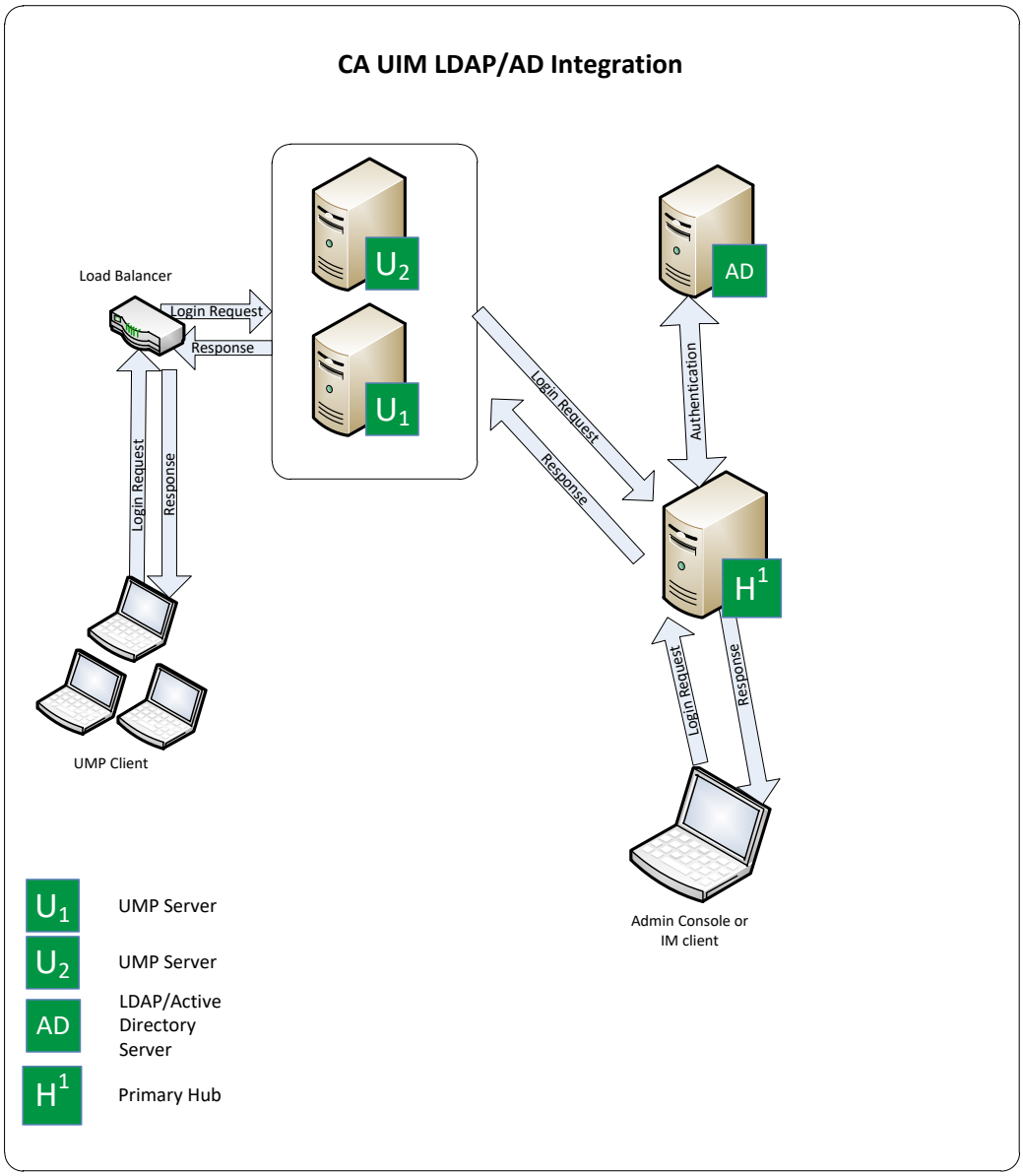


Figure 11 Integration of UIM and LDAP/Active Directory

Copyright © 2018 CA. All rights reserved. All trademarks, trade names, service marks, and logos referenced herein belong to their respective companies.

Figure 11 Integration of 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 CA Unified Infrastructure Management Probes documentation - https://docops.ca.com/ca-unified-infrastructure-management-probes/ga/en/alphabetical-probe-articles/sdgtw-service-desk-gateway

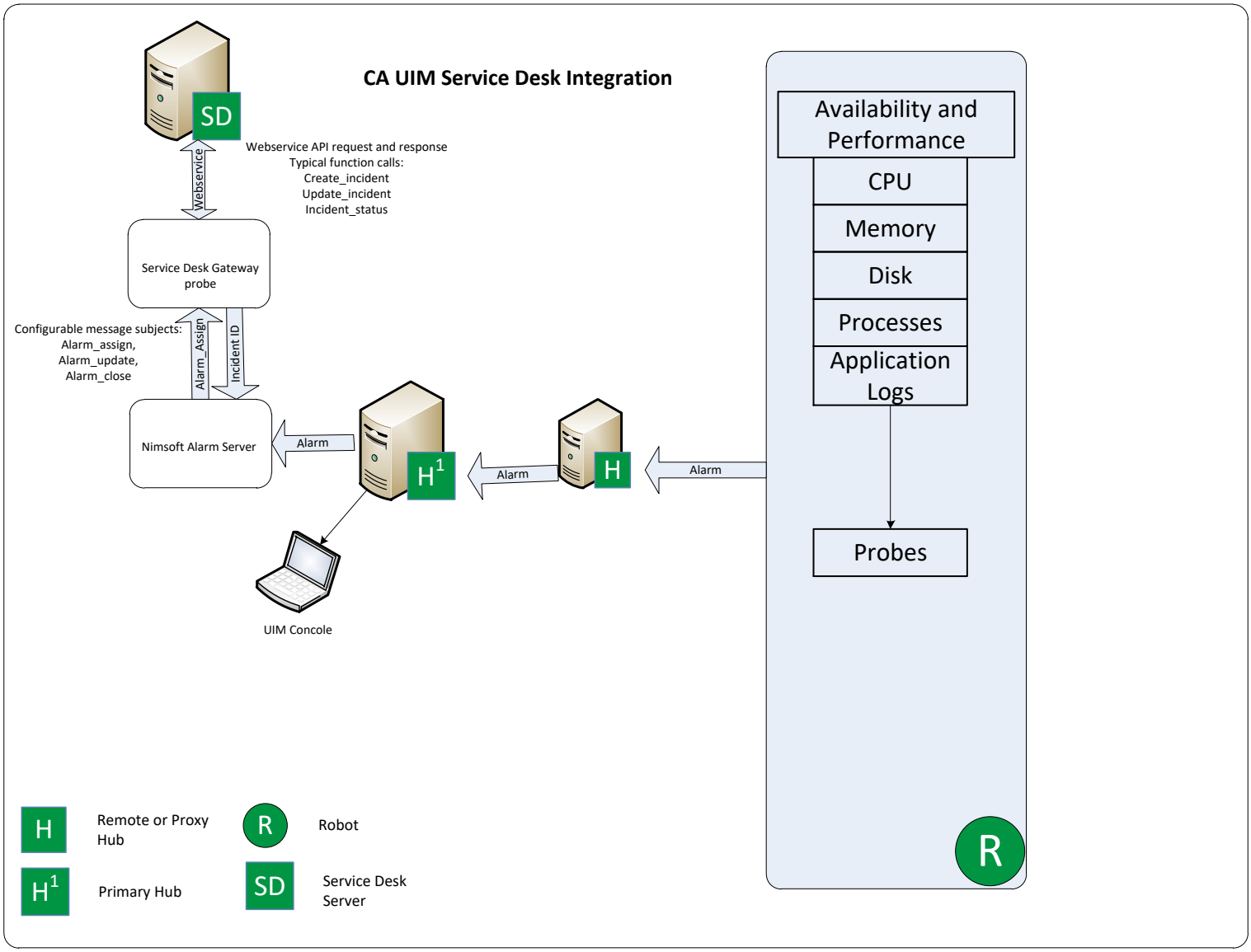


Figure 12 Integration of UIM and Service Desk

Copyright © 2018 CA. All rights reserved. All trademarks, trade names, service marks, and logos referenced herein belong to their respective companies.

Integration Process Flow

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

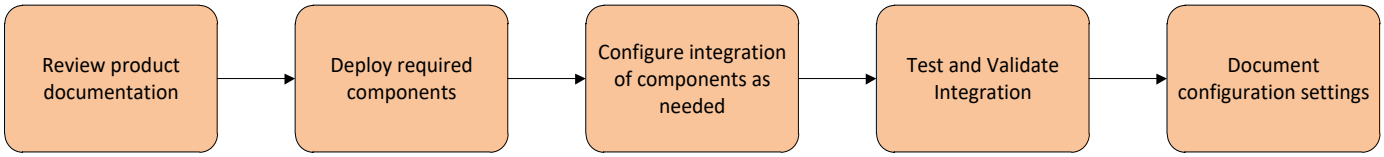


Figure 13 Integration Process Flow

1. It is important to review the appropriate product documentation to understand specific pre-requisites, 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.

Copyright © 2018 CA. All rights reserved. All trademarks, trade names, service marks, and logos referenced herein belong to their respective companies.