

ca World[®]'14

ca Opscenter

Pre-Con Education: What Is CA Unified Infrastructure Management (formerly known as CA Nimsoft Monitor) and what's new in version 8.0

Tim O'Connor, Kurt Spence, Robert Vacante

CA Technologies

UIM Product Management

OCX33E

#CAWorld

Invent Tomorrow

Abstract

Tim
O'Connor
Kurt Spence
Robert
Vacante

CA Technologies
Product Management

If you are new to CA Unified Infrastructure Management (formerly known as CA Nimsoft Monitor), please join us for this introductory session to learn more about this comprehensive monitoring solution. This session will cover the “basics” of CA Unified Infrastructure Management to help you build your knowledge on the general concepts, components and features that CA UIM offers. We will also cover the major features that are now available within our recent 8.0 release, including new analytics (“time to threshold” and “time over threshold”), reporting improvements (TopN and “At A Glance” reports) and more.

Agenda

MODULE 1: DESCRIBE CA UNIFIED INFRASTRUCTURE MANAGEMENT

MODULE 2: CONFIGURE BASIC DATA MONITORING

MODULE 3: EXAMINE MONITORED DATA

MODULE 4: ADVANCED CONFIGURATIONS

Class Question

Show of hands – how do you classify your business?

A SMB

B Large Enterprise

C Communication provider

D Managed Service Provider

Class Question

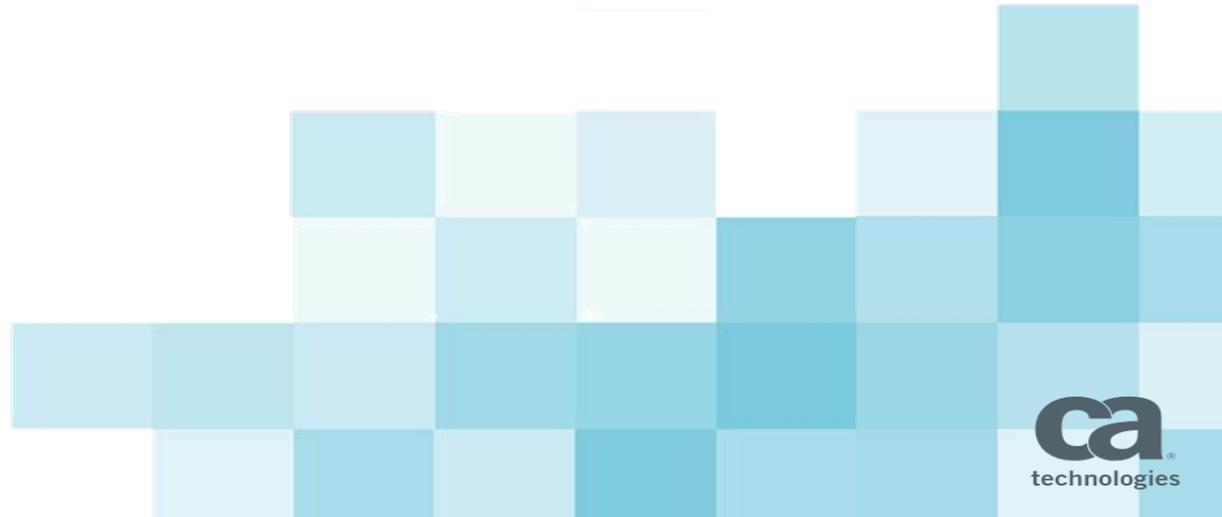
Show of hands – who is currently using UIM for monitoring, or other tools?

A UIM

B Other

C None

Module 1: Describe CA Unified Infrastructure Management



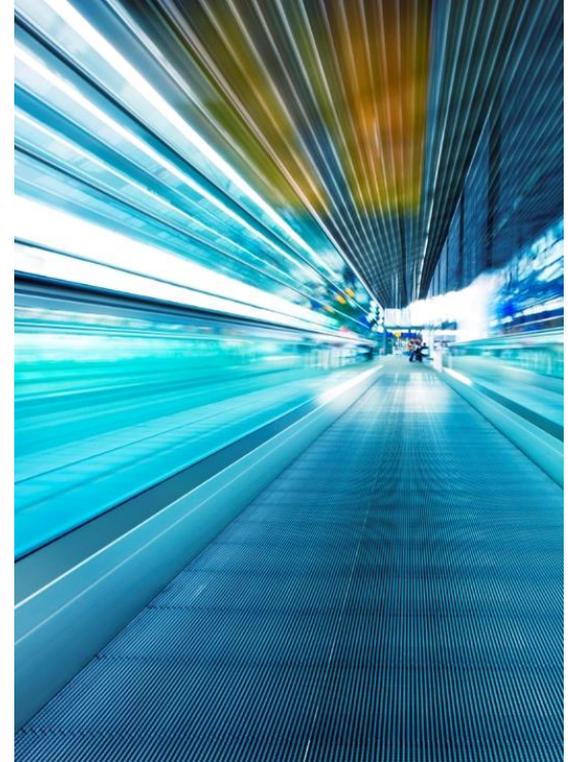
Module Objectives

After completing this module, you will be able to:

- Consider monitoring governance to fulfill your monitoring requirements
- Identify the key components of CA Unified Infrastructure Management
- Perform a network discovery

Why you need to know:

- By understanding the application of monitoring governance, you can optimally configure CA Unified Infrastructure Management to meet your specific business monitoring requirements.
- By identifying the key components, you will gain a high-level understanding of how the CA Unified Infrastructure Management logical and technical architecture is implemented, and then be enabled to quickly begin to collect performance data and events—QoS and alarms—from your environment



Monitoring Governance

By understanding the application of monitoring governance, you can optimally configure CA Unified Infrastructure Management to meet your specific business monitoring requirements.

Any monitoring deployment solution presents a number of challenges.

What Do I Monitor?

What Is Alarm Worthy?

- Notification
- Escalation
- Remediation

What Data do I Collect?

- Frequency
- Retention

How Do I Manage All This?

Monitoring Governance Approach

Monitoring governance is a disciplined approach to what has all too often been an un-disciplined activity.

- Start to think of monitoring as a service, whether it be for internal customers or the external customers of a service provider.
- Stop relying on the out-of-the-box (OOTB) approach of simply turning on all thresholds and hoping to capture something meaningful.
- Follow an intentional workshop-driven process to consider and plan the service that will be offered by monitoring.
- The resultant monitoring should be specific, focused, and discrete.

Prioritize customer value.

- Align your approach with a service offering and service catalog.
- Make it simple and easy to understand.
 - Good, better, best
 - Basic, advanced
 - Bronze, silver, gold

Focus on the value the customer gets from what you are monitoring, and not simply on what you are monitoring.

Monitoring Governance Approach Continued

- **Monitoring governance specifies the:**
 - Resources that need to be monitored
 - Probes to use
 - Individual checkpoints to enable, and which metrics you will collect for that checkpoint
 - Alarm thresholds
 - Alarm management rules to enforce, if any

Monitoring Best Practices

Do not “boil the ocean” by drifting into an unnecessarily difficult approach.

Avoid the temptation to use the full capabilities available if you do not need them.

Instead:

- Take an iterative product-release approach
- Increase customer value
- Focus on what is actionable
- Use a baseline approach to monitoring instead of randomly-determined thresholds

Adherence to the principles of monitoring governance will help to mitigate disastrous long-term effects, such as:

- Large databases
- Alarm floods
- Users losing trust
- Overall unmanageability of the system

Stakeholders

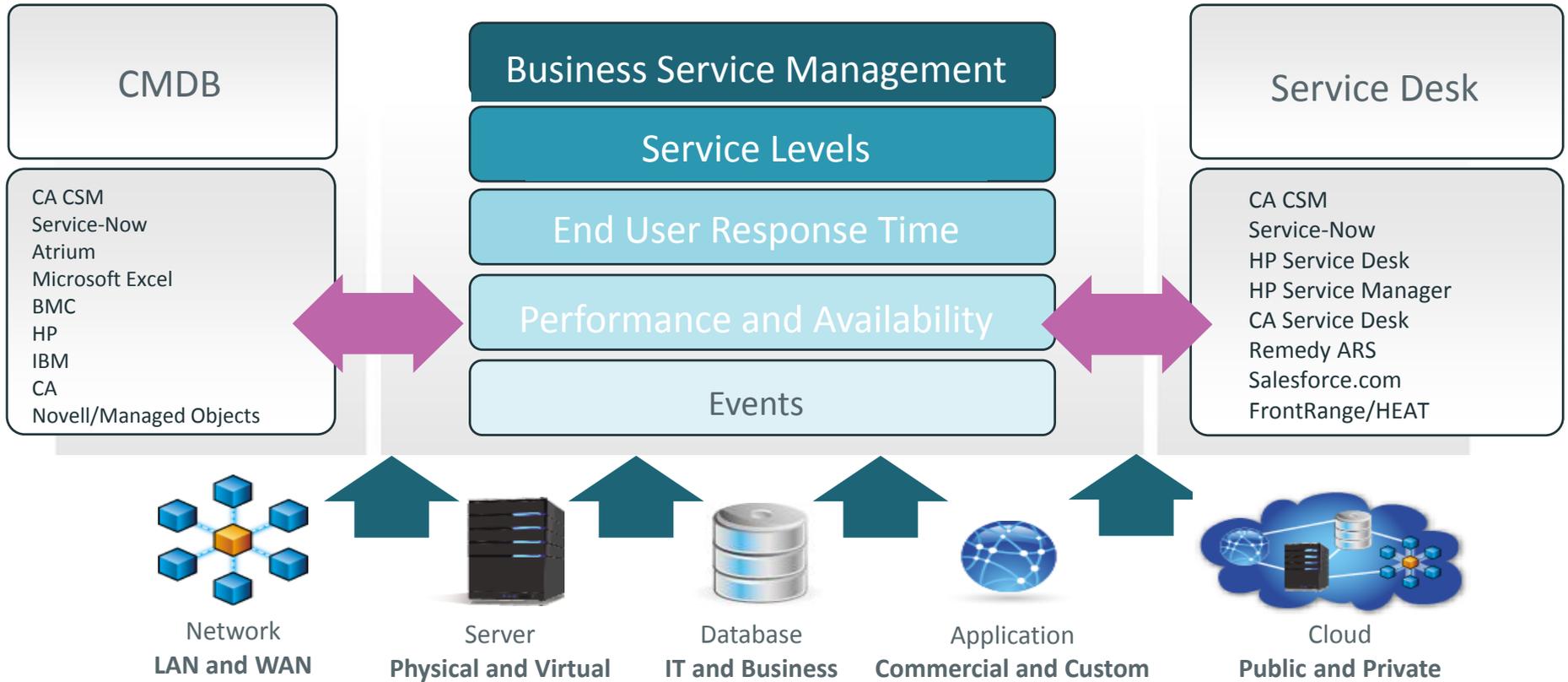
There are a number of roles with a stake in the monitoring governance framework:

Each role benefits when you apply best practices.

Stakeholder	Benefits Provided
CA UIM administrators	<ul style="list-style-type: none">– Reduced overall effort required to maintain the solution
Service providers	<ul style="list-style-type: none">– Increased product confidence– Scalable service catalog-based monitoring infrastructure– Quicker time to market
Infrastructure owner	<ul style="list-style-type: none">– Quality information regarding their infrastructure– Timely notices about issues and outages

Logical Architecture

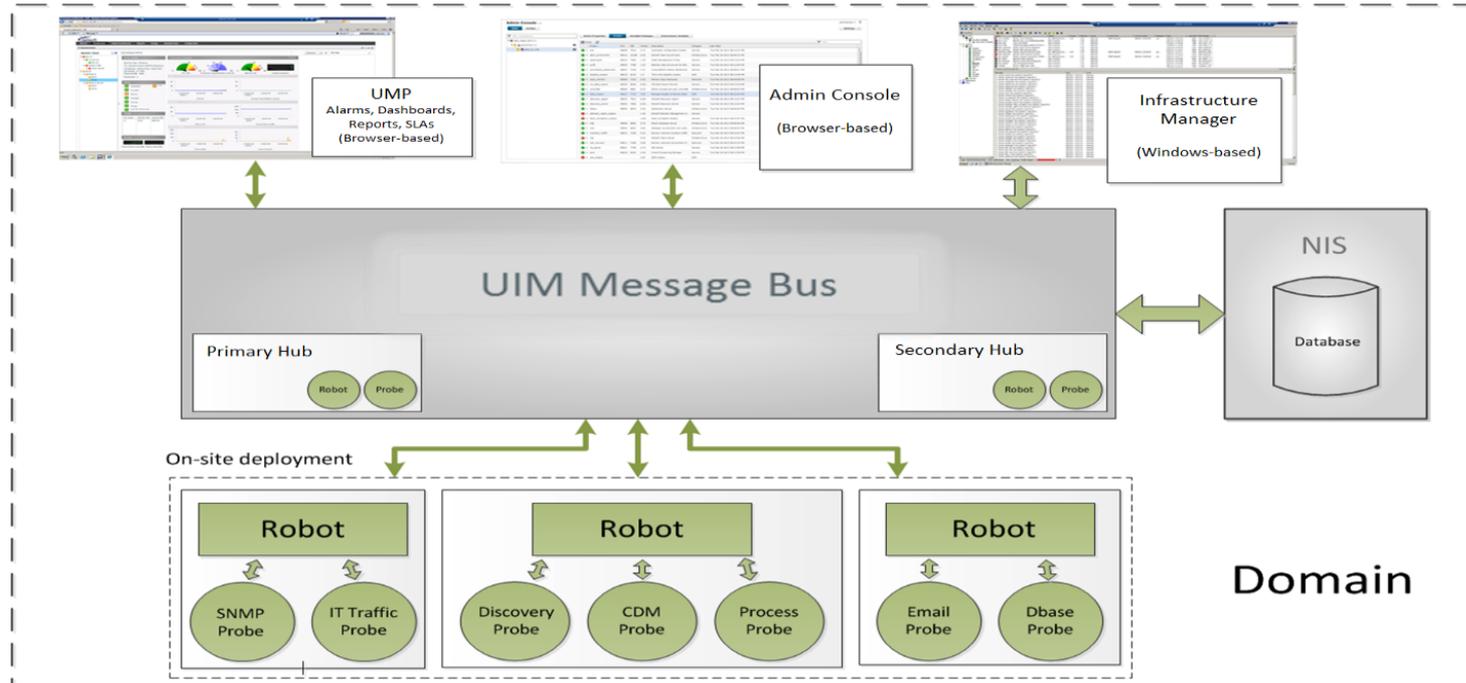
Hierarchy of Business Requirements and Inputs



Technical Architecture

System Architecture for an On-site Deployment

The following diagram represents the implementation of the CA Unified Infrastructure Management system architecture to meet your on-site monitoring requirements.

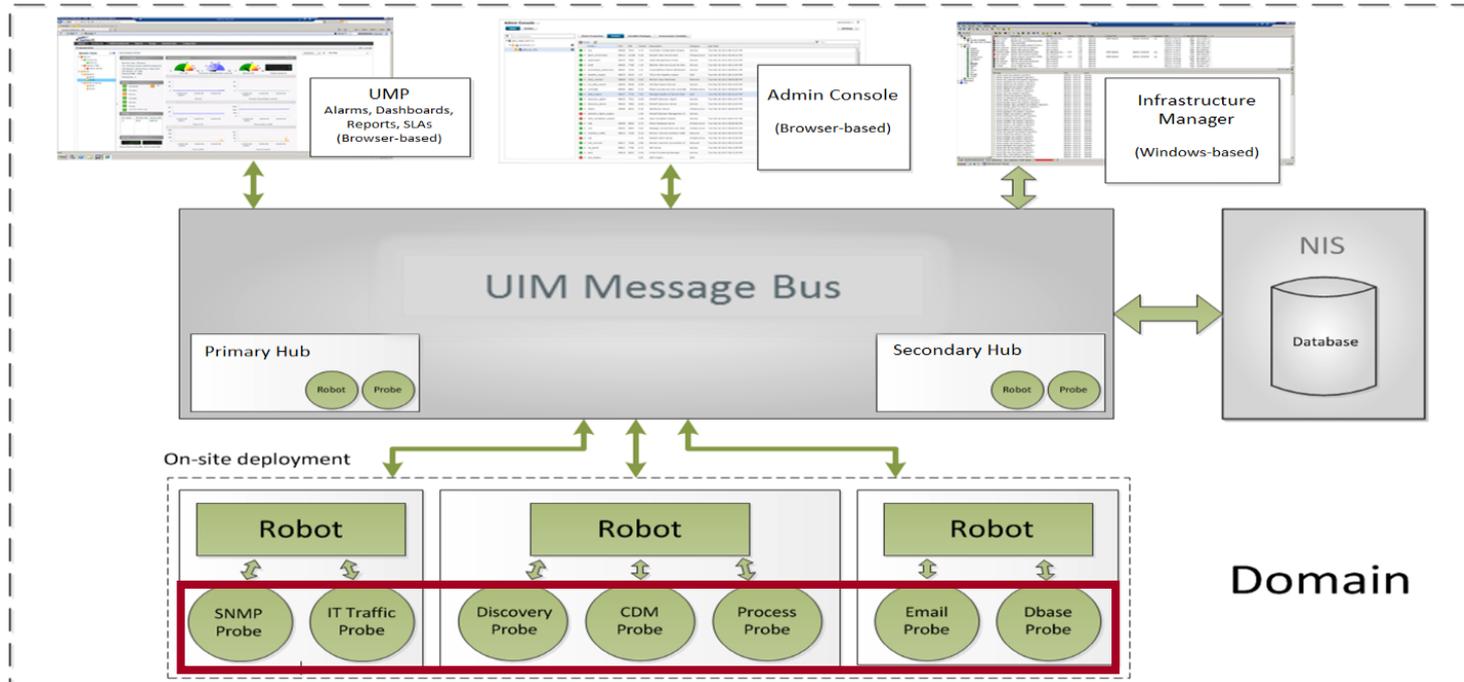


Technical Architecture

Probes

A probe is software that performs a dedicated task at the bottom of the hierarchy.

- A probe must be deployed to a robot.

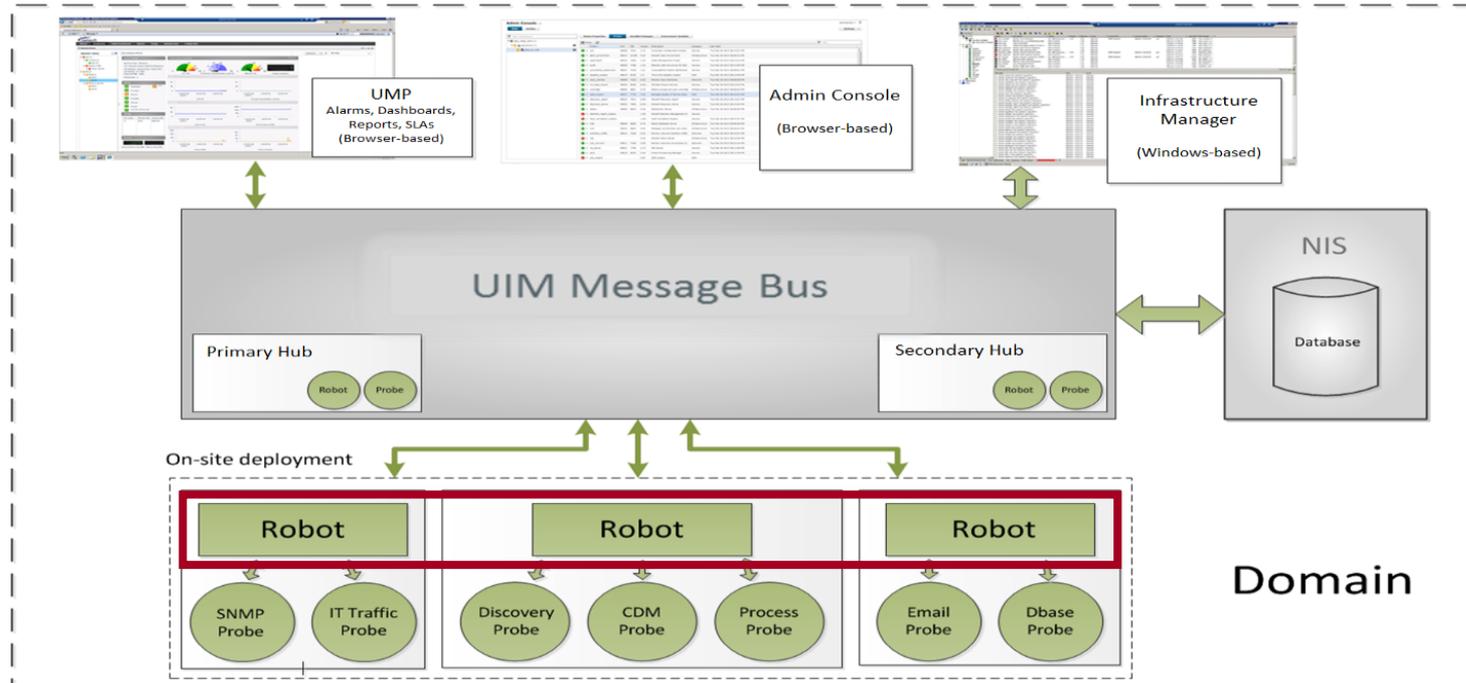


Technical Architecture

Robots

A robot is installed on each computer you want to monitor and manages probes.

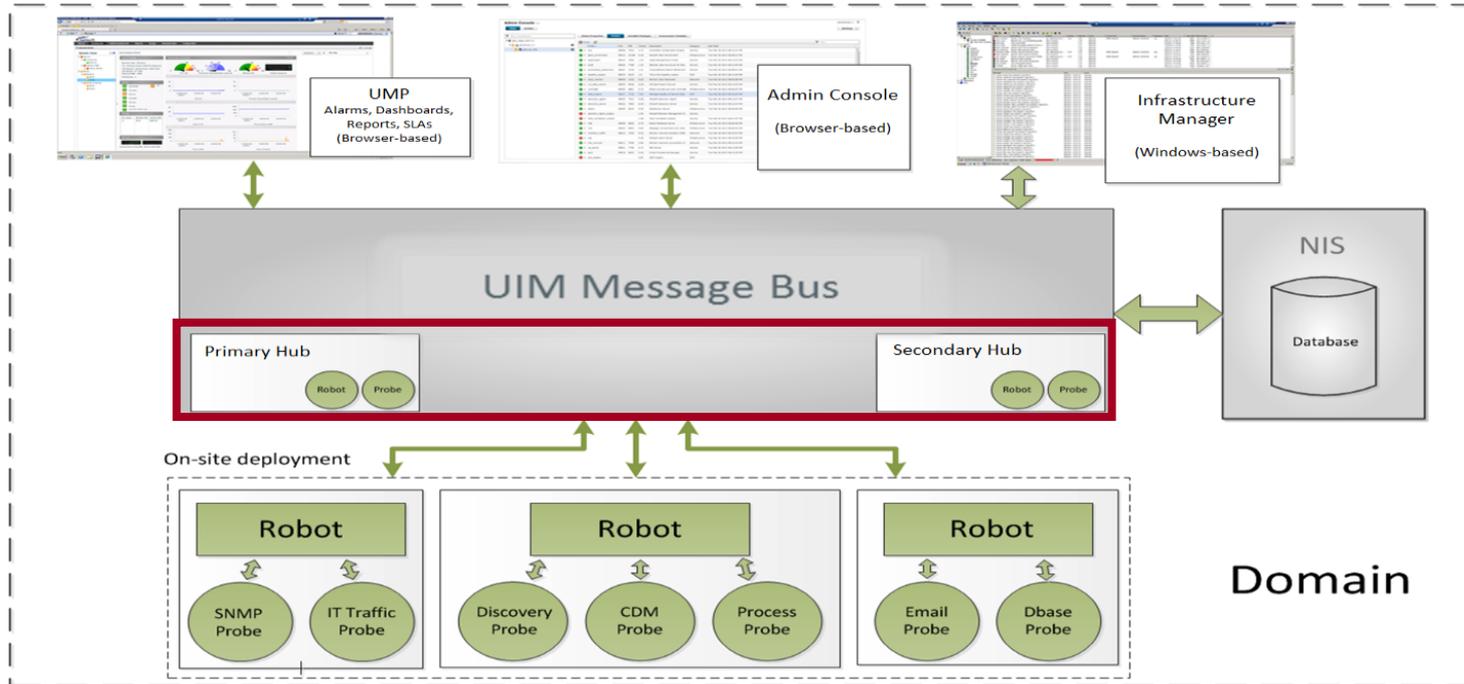
- A robot is known in other monitoring solutions as an agent.



Technical Architecture

Hubs

A hub is a robot that has additional responsibilities, which includes managing its robots.

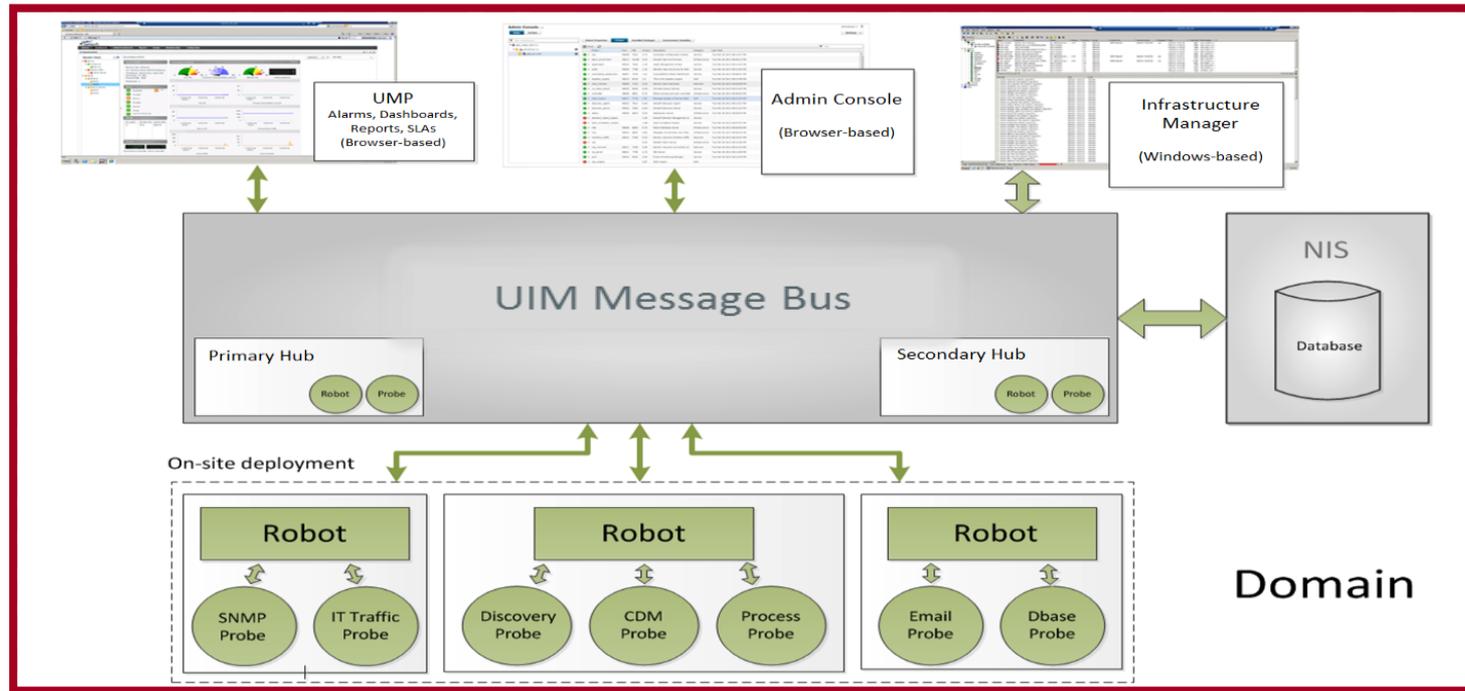


Technical Architecture

Domain

The domain is a logical set into which all infrastructure components are grouped.

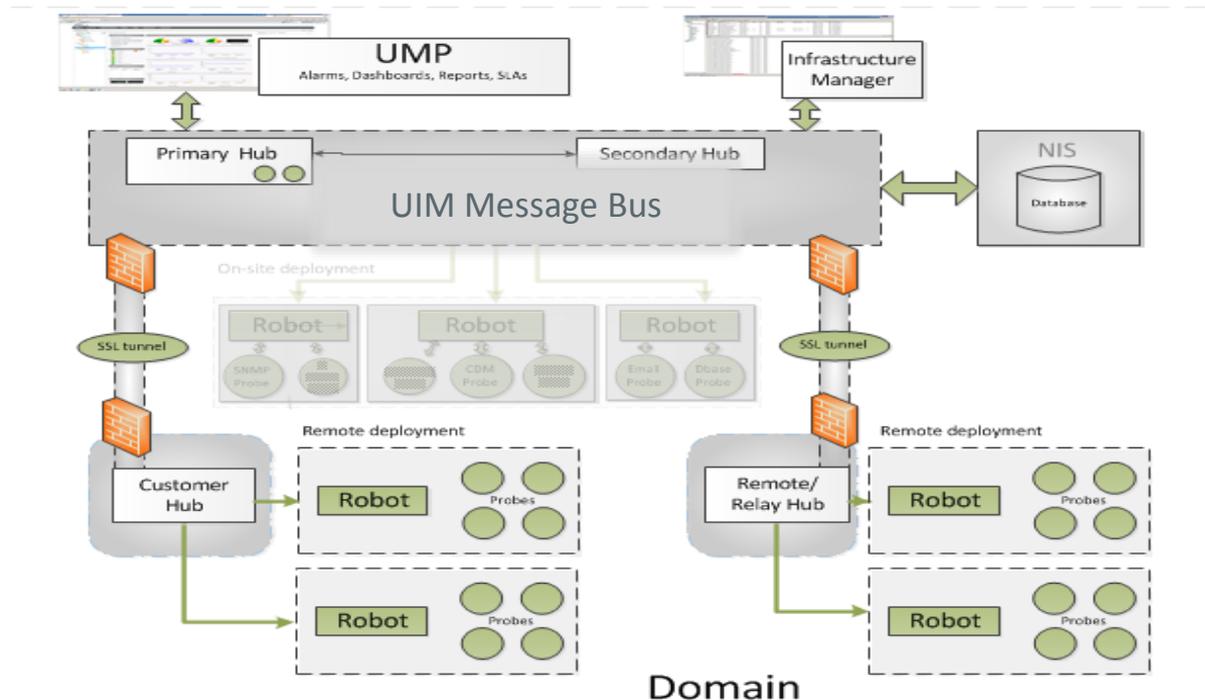
- In CA Unified Infrastructure Management, there is typically only one domain.



Technical Architecture

System Architecture for On-site and Remote Deployments

The following diagram represents the implementation of the CA Unified Infrastructure Management system architecture to meet your enterprise monitoring requirements.



Message Flow

Message Bus

The message bus provides a set of services to robots, hubs, database, and management consoles.

The message flow on the bus is managed using routing and naming schemes based on request/response and publish/subscribe models:

Request/response is the standard way of communicating over the network. A client issues a request to a server and the server responds to the request.

Publish/subscribe enables clients to send data—such as alerts, performance data, or messages targeted for gateway servers—without a designated receiver. It also enables clients to select messages based on subject.

The subscribe mechanism enables probes and robots to select messages based on subject rather than on sender address.

A client that is configured to receive messages sends a subscribe request to the hub.

The client then receives messages matching the subscribed subjects from the hub.

Message Flow

Message Queues

Message queues transfer messages to and from hubs.

Permanent queues are stored in the local hub database and survive a hub restart.

This type of queue ensures that messages are delivered even if the receiver is down when a message is generated.

Temporary queues are used for less-critical communication paths.

Queues are set up in two ways:

Automatically

Queues are often a transparent part of the infrastructure.

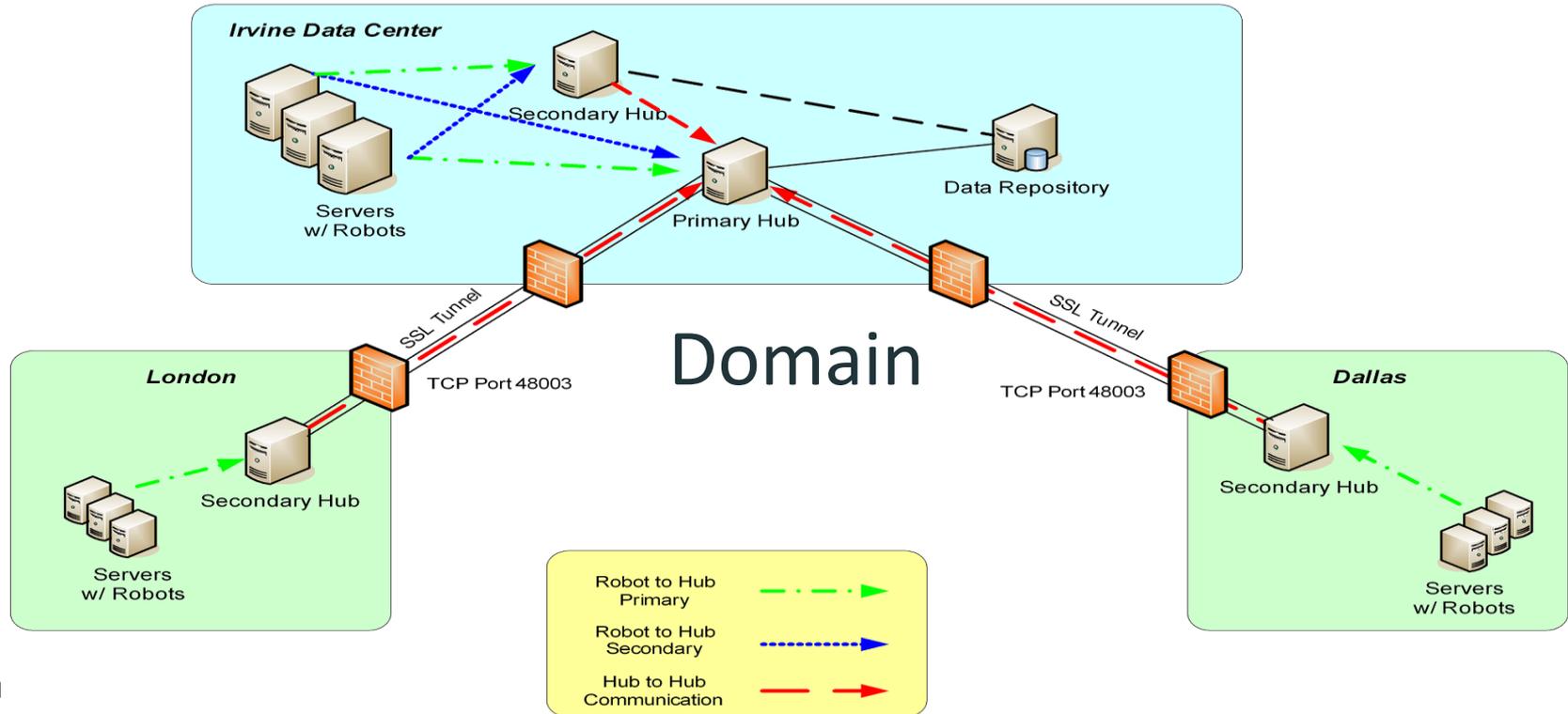
Permanent queues are set up between hubs during installation while temporary queues are created as needed.

Manually

You can create queues with Infrastructure Manager.

For example, if you have multiple secondary hubs, you need to create queues to send data to the primary hub.

CA Unified Infrastructure Management Management



Key Components of CA Unified Infrastructure Management

By identifying the key components, you will gain a high-level understanding of how the logical and technical architecture is implemented.

CA Unified Infrastructure Management consists of the following interfaces:

- Admin Console: A web-based interface to distribute and configure probes
- Infrastructure Manager: The traditional CA Unified Infrastructure Management interface
- UMP (Unified Management Portal): A web interface providing a variety of portlets, reports, and dashboards for consuming data, including:
 - Unified Services Manager (USM)
 - List Views and Performance Reports
 - NetFlow
- Unified Reporter: A full-featured, embedded business intelligence (BI) tool with advanced reporting capabilities

The Admin Console

Primary interface for the management of your system.

Admin Console

administrator ▾ ?

Infrastructure

Archive

Settings ▾

Filter Hubs/Robots

- NMS (1)
 - primary (2)
 - nmserver
 - umpserver

System Information

Type: Regular
Address: /NMS/primary/nmserver
IP: 192.168.1.11

OS Major: Windows
OS Minor: Windows Server 2008 R2 Standard Edition, 64-bit
OS Description: Build 7600

[Show more](#)

Probes

Installed Packages

Environment Variables

Group	Probe	Port	PID	Version	Description	Category	Last Start
	ace	48021	4048	3.10	Automatic Configuration Engine	Service	Thu Jan 2 2014 06:17:37 PM
	alarm_enrichment	48011	2252	4.20	Nimsoft Alarm Enrichments	Infrastructure	Thu Jan 2 2014 06:16:55 PM
	assetmgmt	48019	3988	1.24	Asset Management Probe	Service	Thu Jan 2 2014 06:17:34 PM
	audit	48022	1620	1.22	Maintain data structures for Rob...	Service	Thu Jan 2 2014 06:17:40 PM
	automated_deploymen...	48008	2532	1.24	Cross-platform Robot Distribution	Service	Thu Jan 2 2014 06:16:49 PM
	cm_data_import	48012	1964	7.00	CM Data Import Service	Service	Thu Jan 2 2014 06:16:56 PM
	controller	48000	1200	7.10	Robot process and port controller	Infrastructure	Thu Jan 2 2014 06:16:37 PM

Navigation Pane

Main Window Pane

UMP

Available Portlets

Portlets are individual modular applications that are organized in the portal to present a custom view. UMP enables you to add many collaboration and monitoring portlets and other tools.

Drag a portlet from the Portlet list, such as List Viewer, and place it in the desired location on the UMP page.

The screenshot displays the UMP interface. On the left is a 'Portlet list' with a search bar and a list of applications under categories like 'Collaboration', 'Monitoring', and 'Tools'. The 'ListViewer' portlet is highlighted with a red box, and a red arrow points from it to a 'ListViewer' portlet in the main dashboard area. The dashboard has a top navigation bar with tabs: Reports, Design, Configuration, SLM, Dashboards, SLA Reports, My PRD Page, and MyCustomPage. Below the navigation bar, there are two portlets: 'SLAReports' and 'PerformanceReportsDesigner'. The 'SLAReports' portlet shows 'Critical Services SLA' with a compliance of 65.84% and a trend analysis indicating a breach. The 'PerformanceReportsDesigner' portlet shows a line graph for 'nmserver' with a y-axis labeled 'milliseconds' ranging from 3k to 7k.

UMP

Available Portlets continued

In UMP, you can configure, minimize, maximize, and remove portlets.

Search applications (searches as you type).

- Collaboration
- Monitoring
 - AccountAdmin Add
 - AdminConsole Add
 - ChangePassword Add
 - Dashboard Add
 - ListDesigner Add
 - ListViewer Add
 - MyTickets Add
 - PerformanceReportsDesigner Add
 - RelationshipViewer Add
 - ReportScheduler Add
 - Reports Add
 - SLAReports Add
 - SLM Add
 - UnifiedReports Add
 - UnifiedServiceManager Add
- Monitoring (Deprecated)
- Tools

Drag a portlet to place it on the page.

Websites	Avg Performance
Bing	
Brewers	
CA Technologies Home P	
Cubs	
Google	
packers	
Patriots	1,058.58
Yahoo	2,313.83

Showing 8/8 rows.

These tools enable you to configure, minimize, maximize, and remove a portlet.

Benefits of Discovery

CA Unified Infrastructure Management enables you to quickly begin to collect performance data and events—QoS and alarms—from your environment.

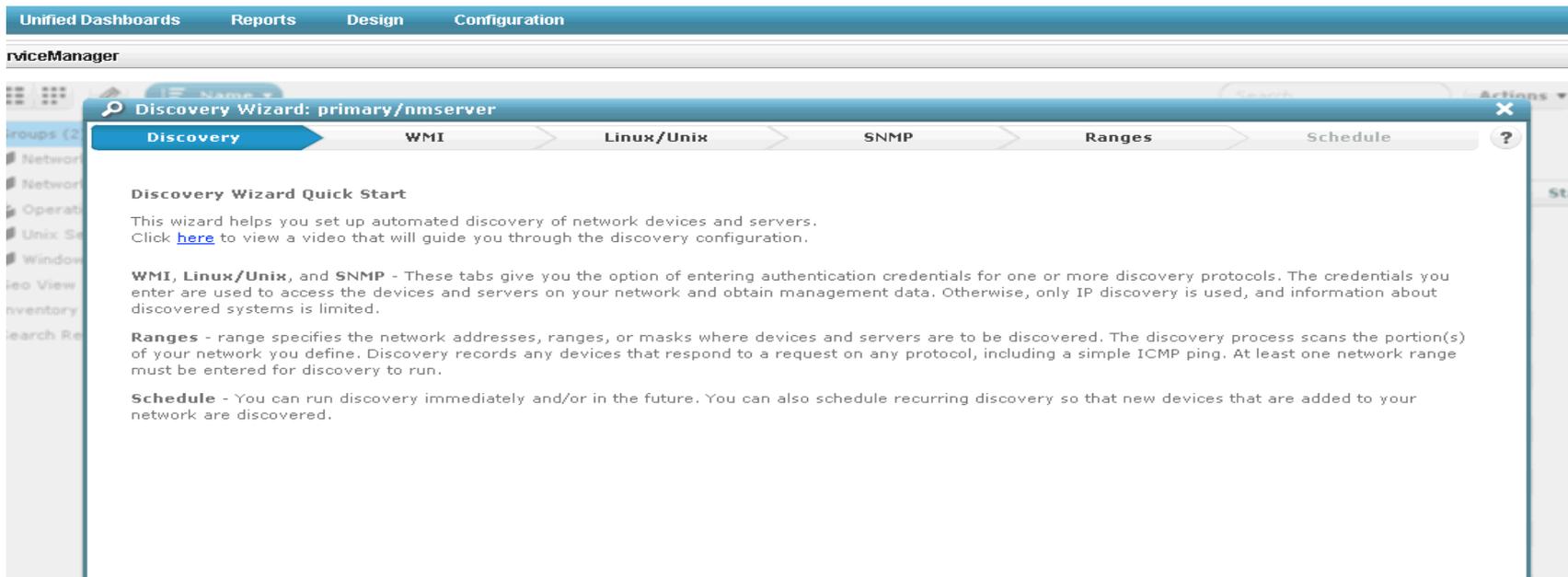
Discovery is the primary method to reduce manual effort while maintaining an inventory of devices in your managed domain.

- In CA Unified Infrastructure Management, you can enable device monitoring and management on these devices as required, engaging the broad array of probes that gather QoS data from the monitored devices and generate alarms in response to threshold breaches.
- Components in the CA Unified Infrastructure Management Server automate the discovery of hosts and devices throughout your network, recording any device within a discovery range that responds to a request on any configured protocol, including SSH, WMI, SNMP, and even a simple ICMP ping.

Discovery Wizard

Overview

Use the Discovery Wizard to set up the automated discovery of network devices.



The screenshot shows a web-based interface for a network management system. At the top, there is a navigation bar with tabs for 'Unified Dashboards', 'Reports', 'Design', and 'Configuration'. Below this, the main header reads 'DeviceManager'. A sidebar on the left contains a tree view with categories like 'Groups (2)', 'Network', 'Operat...', 'Unix Se...', 'Window...', 'leo View', 'nventory', and 'earch Re...'. The main content area displays a 'Discovery Wizard' window titled 'primary/nmserver'. The wizard has five tabs: 'Discovery' (selected), 'WMI', 'Linux/Unix', 'SNMP', and 'Ranges', followed by a 'Schedule' tab and a help icon. The 'Discovery' tab is active, showing a 'Discovery Wizard Quick Start' section. The text in this section reads: 'This wizard helps you set up automated discovery of network devices and servers. Click [here](#) to view a video that will guide you through the discovery configuration.' Below this, there are three paragraphs of explanatory text: 'WMI, Linux/Unix, and SNMP - These tabs give you the option of entering authentication credentials for one or more discovery protocols. The credentials you enter are used to access the devices and servers on your network and obtain management data. Otherwise, only IP discovery is used, and information about discovered systems is limited.' 'Ranges - range specifies the network addresses, ranges, or masks where devices and servers are to be discovered. The discovery process scans the portion(s) of your network you define. Discovery records any devices that respond to a request on any protocol, including a simple ICMP ping. At least one network range must be entered for discovery to run.' 'Schedule - You can run discovery immediately and/or in the future. You can also schedule recurring discovery so that new devices that are added to your network are discovered.'

Discovery Wizard

Authentication page

- The Authentication tabs enable you to create, edit, view, and delete authentication profiles (credentials) for discovery.
- An authentication profile contains credentials necessary for the discovery_agent probe to access and gather information about computer systems and devices in your network.
- You can define authentication profiles for the following protocols by:
 - Clicking on of the protocol tabs and clicking “New Credentials” on the left
 - Defining the credentials fields

To display online documentation about a feature or function in a particular screen, click its Help (?) icon.

Discovery Wizard: primary/nmservers

Discovery WMI Linux/Unix SNMP Ranges Schedule

Filter

- + New credentials
- 🔑 Lab

WMI (Windows Management Interface) discovery scans servers running Windows to gather system information. Click on **New credentials** to add a WMI authentication profile, or click on an existing authentication profile to make changes.

Credential name	ID
<input type="text" value="Lab"/>	<input type="text"/>
User	Password
<input type="text" value="administrator"/>	<input type="password" value="*****"/>

Discovery Wizard

Ranges page

The ranges page enables you to create or edit ranges.

A range specifies the portions of the network where you want to discover devices.

- You can also assign credentials to a range for use in discovery.
- Ranges can be defined for specific discovery_agent probes.

Discovery Wizard: primary/nmserver

Discovery WMI Linux/Unix SNMP Ranges Schedule ?

Filter

+ New range

Use the **Ranges** tab to define network addresses, ranges, or masks where devices are to be discovered. Click on **New range** to add a range. Click on an existing range to make changes. The check boxes next to authentication profiles allow you to assign any combination of SNMP, Linux/Unix, and WMI authentication profiles to a range.

Range name
Lab

Range definition
+ New IP range or single IP address

Single |
Mask
Range
Single

Credentials
Select: All None

Hide unused credentials

Filter

- Linux/Unix
- SNMP
- WMI

Discovery Wizard

Schedule page

The **Schedule** page enables you to schedule a single discovery or recurring discoveries and to perform the run immediately, in the future, or both.

A scheduled discovery does not interrupt a discovery that is already running.

- If at the time a discovery run is scheduled another discovery run is in progress, the scheduled discovery is ignored.
- If you select Run discovery now and a discovery is in progress, the current discovery run is terminated and the new run is executed.

The screenshot shows the 'Discovery Wizard: primary/nmserver' window with the 'Schedule' tab selected. The navigation bar includes 'Discovery', 'WMI', 'Linux/Unix', 'SNMP', 'Ranges', and 'Schedule'. The 'Schedule' page contains the following options and settings:

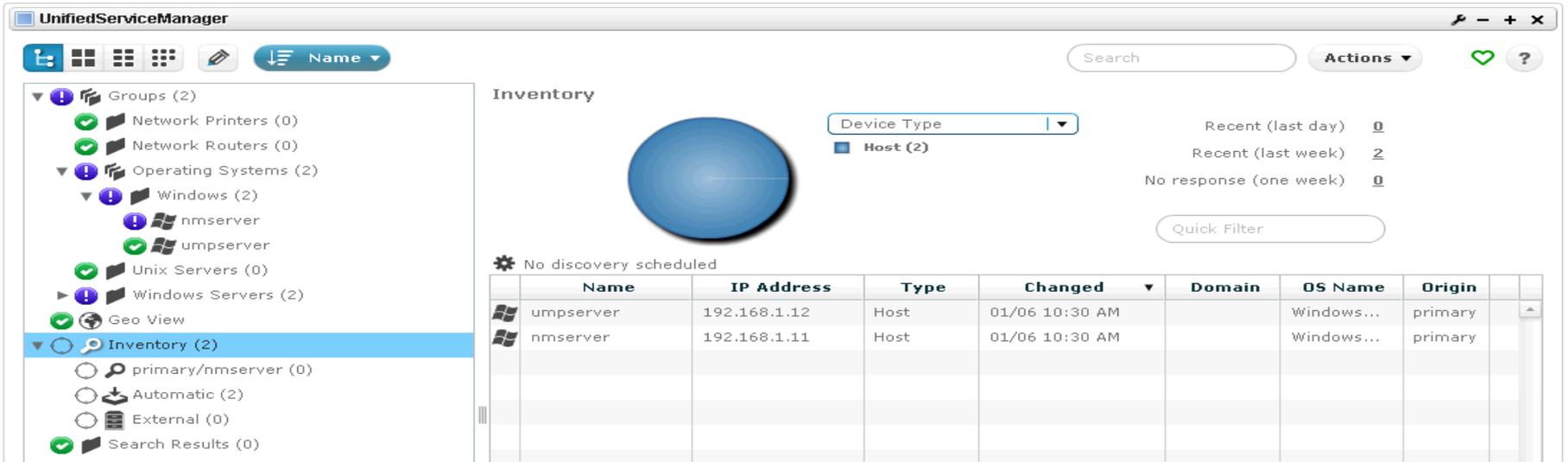
- Run discovery now
- Schedule discovery
- Starting on: 01/03/2014
- At: 00 : 00 (24 hour)
- Recurring every 24 hours

A help text box states: "You can run discovery immediately and/or in the future. A scheduled discovery does not interrupt a discovery that is already running. However, if you select **Run discovery now** and discovery is in progress, the current discovery run is terminated and the new run is executed."

Discovery Results

The Inventory node in the tree view of USM enables you to view computers and devices that have been discovered on your network

The Inventory section of the tree contains discovery agents, with network ranges under each discovery agent.



The screenshot shows the UnifiedServiceManager (USM) interface. The left sidebar contains a tree view with the following nodes:

- Groups (2)
 - Network Printers (0)
 - Network Routers (0)
- Operating Systems (2)
 - Windows (2)
 - nmserver
 - umpserver
 - Unix Servers (0)
- Windows Servers (2)
- Geo View
- Inventory (2)** (Selected)
- primary/nmserver (0)
- Automatic (2)
- External (0)
- Search Results (0)

The main area is titled "Inventory" and features a large blue sphere representing the inventory. Below the sphere, a "Device Type" dropdown menu is set to "Host (2)". To the right of the sphere, there are filters for "Recent (last day)", "Recent (last week)", and "No response (one week)". A "Quick Filter" input field is also present.

Below the sphere, a table displays the discovered hosts:

Name	IP Address	Type	Changed	Domain	OS Name	Origin
umpserver	192.168.1.12	Host	01/06 10:30 AM		Windows...	primary
nmserver	192.168.1.11	Host	01/06 10:30 AM		Windows...	primary

Lab 1 Exercise

In the following lab exercise, you will:

Discover the local subnet using the Discovery Wizard

See lab 1-1 Discover the Local Subnet Using the Discovery Wizard.



Automatic Robot Deployment

As a CA Unified Infrastructure Management administrator, you can use USM to deploy robots automatically to an individual system or group of systems.

Specifically, you can:

- Deploy robots to all or selected members of a group
- Deploy a robot to a specific system
- Do a basic or advanced search for systems to deploy robots to
- Import an XML file listing systems to deploy robots to

After you select the systems and start a deployment job, robots are automatically installed on the selected systems.



Lab 1 Exercise

In the following lab exercise, you will:

Deploy a robot using the ADE

See lab 1-2 Deploy a Robot Using the ADE.



Module 1 Summary

You should now be able to:

- Apply monitoring governance to fulfill your monitoring requirements
- Identify the key components of CA Unified Infrastructure Management
- Perform a network discovery

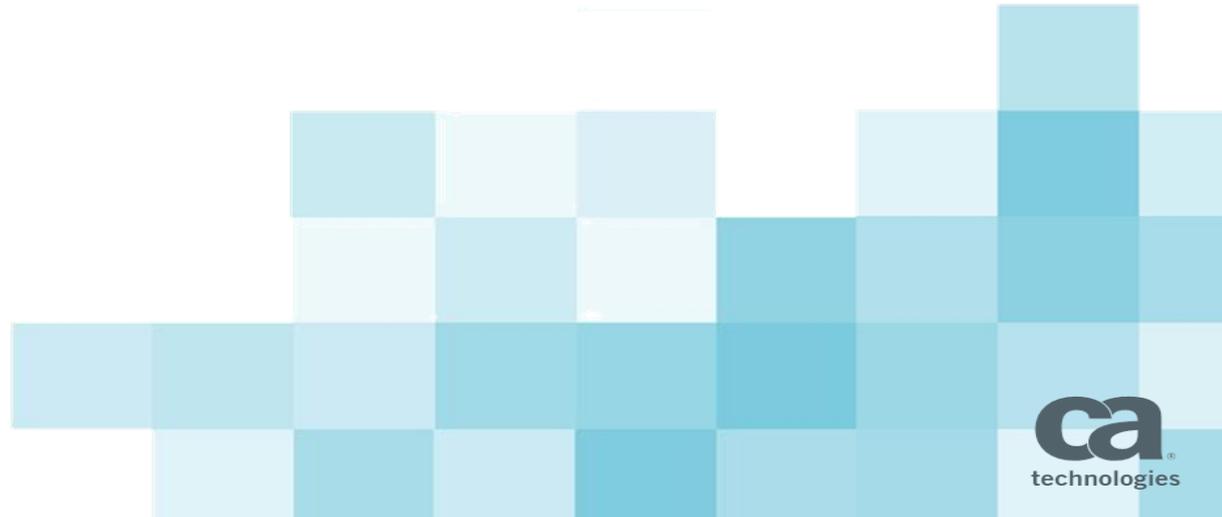
In the next module, you will:

- Configure basic data monitoring



Module 2:

Configure Basic Data Monitoring



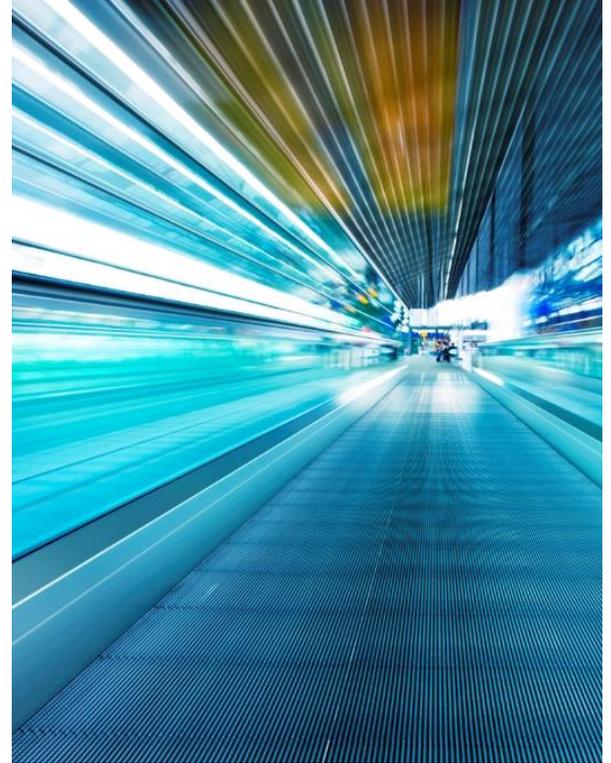
Module Objectives

After completing this module, you will be able to:

- Identify the types of data to monitor
- Complete basic probe deployment and configuration tasks
- Create USM groups

Why you need to know:

- By identifying the types of data you can monitor, you will gain a high-level understanding of the data monitoring scope of the product.
- You must deploy and configure probes to enable event and performance monitoring on robots.
- You can use groups to organize your infrastructure by location, technology, or even a service



Types of Data to Monitor

By identifying the types of data you can monitor, you will gain a high-level understanding of the data monitoring scope of the product.

You can monitor the following types of data with CA UIM:

- Performance and trend data
 - Many probes are capable of sending performance and trend data on a periodic basis in messages that are formatted and known as QoS messages.
 - These messages normally contain data—response times, network availability, CPU usage, memory usage, bandwidth utilization, and so on—used for service-level monitoring and reporting.
- Events and alarms
 - An event is a known or existing issue or the result of a failure or error in the IT object or device that causes, or might cause, an interruption or a reduction of the quality of the service.
 - You can configure events to trigger an alarm.

Class Question

A router failure has been fixed and you are now using CA UIM to track bandwidth utilization. What are you monitoring?

A Events

B Alarms

C Router failure

D Performance and trend data

Package Archive

You must deploy and configure probes to enable event and performance monitoring on robots.

The Package Archive encompasses the Local Archive and the Web Archive, from which you deploy probes to robots.

- Local Archive
 - This archive resides on the hub, therefore the list will be the same for all robots connected to the hub.
 - There can be more than one version of a package on the local archive.
- Web Archive
 - Displays the list of probe packages on the CA UIM support archive.
 - You must have a valid login and password for the CA UIM support site to download any package.

Package Archive

The Local Archive shows all of the probe packages that have been downloaded to the local hub archive.

You can deploy probes to robots from the local archive.

Admin Console

administrator ▾ | ?

Infrastructure

Archive

Settings ▾

Filter Hubs/Robots

- NMS (1)
 - primary (2)
 - nmsserver
 - umpserver

Local Archive | Web Archive | Distribution Activity

Deploy | Import | Group | [Icons] | Filter

Package	Version	Category	Description						
ace	3.10	Service	Automatic Configuration Engine						
admin_console	7.10	Service	Service Host Admin Console						
assetmgmt	1.24	Service	Asset Management Probe						
audit	1.22	Service	Maintain data structures for Robot auditing						
automated_deployment_en...	1.24	Service	Cross-platform Robot Distribution						
baseline_engine	1.10	SLM	Baseline Engine						
cdm	4.76	System	CPU, Disk and Memory performance probe						
cm_data_import	7.00	Service	CM Data Import Service						
dap	7.10	Service	Data access and collection probe						
dashboard_engine	7.10	Service	Dashboard engine						
data_engine	7.92	SLM	Manages Quality of Service Data						
discovery_agent	7.10	Service	Nimsoft Discovery Agent						
discovery_server	7.10	Service	Nimsoft Discovery Server						
distsv	5.30	Infrastructure	Distribution Server						
fault_correlation_engine	1.66	Service	Fault Correlation Engine						

0 packages selected | 87 packages

Package Archive

The Web Archive shows all of the probe packages that can be downloaded from the CA UIM Support Site.

If you deploy a package from the Web Archive, it is first automatically downloaded to the Local Archive before it is deployed to the robot.

Admin Console

administrator | ?

Infrastructure

Archive

Settings

The screenshot displays the Admin Console interface. On the left, there is a navigation pane with a search filter 'Filter Hubs/Robots' and a tree view showing 'NMS (1)' and 'primary (2)'. The main area is titled 'Web Archive' and contains a table of packages. The table has columns for Package, Version, Category, and Description. The packages listed include adevl, adogtw, ad_response, ad_server, apache, applogic_mon, applogic_ws, ARCserve_D2D, ARCserve_RHA, aws, and azure. Each row has a checkbox on the left and a 'B' icon on the right. Above the table are buttons for 'Deploy', 'Download', 'Group', and a search filter.

Package	Version	Category	Description
adevl	1.60	Application	Active Directory Events probe
adogtw	2.71	Gateway	ADO Database Gateway
ad_response	1.60	System	Active Directory Response Probe
ad_server	1.50	Application	Active Directory Server Monitor
apache	1.55	Application	Monitor for Apache HTTP servers
applogic_mon	1.01	Application	AppLogic Application Monitoring
applogic_ws	1.01	Application	AppLogic Grid Monitoring
ARCserve_D2D	1.00	Application	ARCserve D2D Probe
ARCserve_RHA	1.00	Application	ARCserve RHA Probe
aws	1.10	Application	Amazon AWS probe
azure	1.01	Application	Azure probe

Package Archive

The Distribution Activity tab displays a log of your probe package distributions along with the status of each distribution.

Packages can be deployed individually or in groups.

Admin Console administrator | ?

Infrastructure Archive Settings

Filter Hubs/Robots

NMS (1)

primary (2)

Local Archive Web Archive **Distribution Activity**

Task	Start Time	Stop Time
<input type="checkbox"/> <input checked="" type="checkbox"/> Installing wasp_unified_reports to /NMS/primary/umpserver	Thu Jan 2 2014 12:57:49 PM	Thu Jan 2 2014 12:58:43 PM
<input type="checkbox"/> <input checked="" type="checkbox"/> Installing 32 packages to /NMS/primary/umpserver	Thu Jan 2 2014 12:23:09 PM	Thu Jan 2 2014 12:30:06 PM
<input type="checkbox"/> <input checked="" type="checkbox"/> Installing cdm to /NMS/primary/umpserver	Thu Jan 2 2014 12:21:00 PM	Thu Jan 2 2014 12:21:03 PM
<input type="checkbox"/> <input checked="" type="checkbox"/> Installing 33 packages to /NMS/primary/nmserver	Thu Jan 2 2014 11:40:25 AM	Thu Jan 2 2014 11:46:46 AM

Probe Deployment

Deploy probes by dragging the probe from the archive to a robot.

- The target can be an individual robot, a hub, the domain, or an Infrastructure Manager group (shown in a later module).
- When a probe is dropped on a hub, domain, or group, the probe is deployed to applicable subordinate robots.

Admin Console

The screenshot shows the Admin Console interface. The 'Archive' tab is selected, and the 'Local Archive' section is active. A table lists various probes with their versions. The 'cdm' probe is selected. A callout box points to the 'cdm' probe in the table, and another callout box points to the 'primary (2)' target in the left sidebar.

Package	Version
ace	3.10
admin_console	7.10
assetmgmt	1.24
audit	
automated_deployment_en...	1.24
baseline_engine	1.10
cdm	4.76
cm_data_import	7.00
dap	7.10

You drag a probe from the local archive....

and drop it onto the target.

Probe Configuration

Once a probe has been deployed, it will need to be configured.

When a object node is selected in the left-hand pane, you can configure thresholds, severity, and enable the Publishing of QoS data on the right-hand pane.

Probe Configuration - /NMS/primary/nmserver/cdm

The screenshot displays the 'Probe Configuration' interface for the path '/NMS/primary/nmserver/cdm'. On the left, a tree view shows the following structure:

- cdm
 - NMSERVER
 - Disks
 - C:\ul> - Disk Usage
 - Disk Usage Change
 - Memory
 - Memory Paging
 - Physical Memory
 - Swap Memory
 - Total Memory
 - Processor
 - Individual CPU
 - Total CPU

The 'Total CPU' node is selected. The right-hand pane shows configuration details for two metrics:

Total CPU System	
QoS Name	QOS_CPU_USAGE
Description	Total CPU System
Units	percent
Metric Type Id	1.5:3
Publish Data	<input checked="" type="checkbox"/>

Total CPU Usage	
QoS Name	QOS_CPU_USAGE
Description	Total CPU Usage
Units	percent
Metric Type Id	1.5:1
Publish Data	<input checked="" type="checkbox"/>

USM Groups

You can use groups to organize your infrastructure by location, technology, or even a service.

Administrators can create groups—lists of computer systems—to logically manage and to assign report templates to multiple computer systems.

There are three types of groups:

- Container
 - Is a parent to other groups
- Dynamic
 - Contains the computer systems that meet a specified set of criteria
- Static
 - Contains a specified list of computer systems

USM Tree

The USM tree view displays groups in a hierarchical tree in the navigation pane on the left.

- A status icon indicates the highest severity alarm for each node in the tree.
- The number of systems in each group is indicated in parentheses after the group name.

Detailed information about groups, alarms, or systems is displayed in the pane on the right.

For more information about how to visualize and organize your infrastructure and to configure monitoring, click the ? icon.

The screenshot shows the UnifiedServiceManager interface. On the left is a navigation pane with a tree view. The tree structure is as follows:

- Groups (2)
 - Servers (2)
 - Windows (2)
 - NMSERVER (Warning icon)
 - UMPSEVER (Warning icon)
 - Discovery (4)
 - primary/nmserver (4)
 - Lab (4) (Gear icon)
 - External (0)
 - Search Results (0)

On the right, the 'Alarms' tab is active, showing a table for 'Windows Members (2)'. The table has the following data:

	Name	IP Address	Domain	Caption	Description	Dedicated	OS Type
Warning icon	NMSERVER	192.168.1.11	USEDU				Windows
Warning icon	UMPSEVER	192.168.1.12	USEDU				Windows

As you mouseover a tree item, an icon appears that enables you to add, edit, or delete groups.

Lab 2 Exercises

In the following lab exercises, you will:

- Deploy and Configure the CDM Probe
See lab 2-1 Deploy and Configure the CDM Probe.
- Create USM groups
See lab 2-2 Create USM Groups.
- Add a USM report template
See lab 2-3 Add a USM Report Template.



Module 2 Summary

This module showed you how to:

- Identify the types of data to monitor
- Complete basic probe deployment and configuration tasks
- Create USM groups

In the next module, you will:

- Examine monitored data



Module 3:

Examine Monitored Data



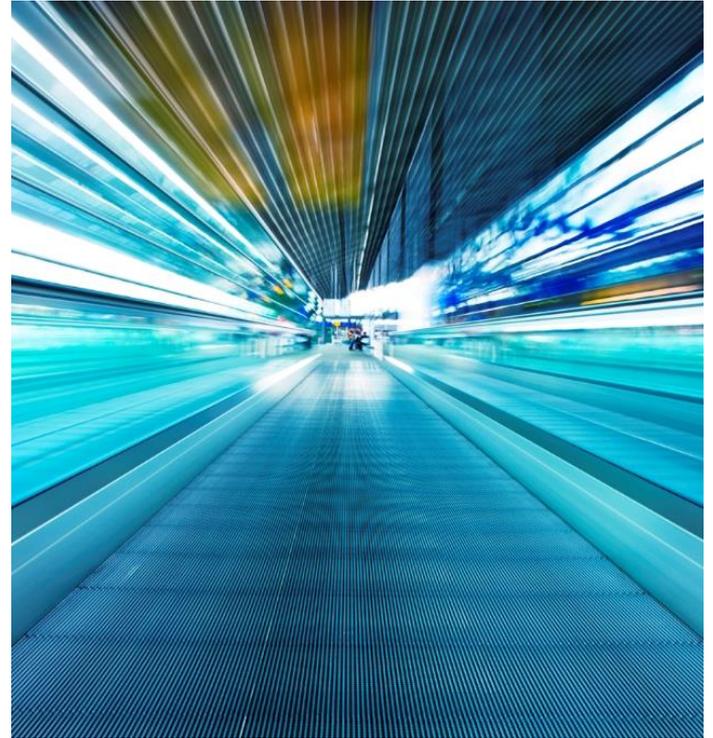
Module Objectives

After completing this module, you will be able to:

- View monitored data
- Examine monitored data in a PRD chart

Why you need to know:

- By examining monitored data in the USM and Unified Dashboards, you can understand how to view information on infrastructure objects.
- By examining monitored data in PRD charts, you can see a visual representation of QoS data.



Viewing Monitored Data

By examining monitored data in the USM and Unified Dashboards, you can understand how to view information on infrastructure objects.

CA Unified Infrastructure Management offers built-in and easily customizable views to help you spot trends, optimize resource utilization, and more.

To provide some examples of data in the UMP, you will view data in the following portlets:

- Device, alarm, metric, and group data in the USM
- Servers in the Unified Dashboards

Viewing Monitored Data

When you select a device in the navigation pane, you can view a variety of QoS data.

The screenshot displays the UnifiedServiceManager interface. On the left, a navigation pane shows a tree structure with 'NMSERVER' selected. The main area is divided into several sections:

- System Tab:** A red box highlights the 'System' tab in the top navigation bar.
- Device Details:** A central pane shows details for 'NMSERVER', including Name, IP Address (192.168.1.11), Domain (USEDU), OS Type (Windows), OS Name (Windows Server 2008 R2 Standard Edition, 64-bit), OS Version (6.1.7600), OS Description (Build 7600), Origin (primary), DNS Name (NMSERVER), NetBIOS Name (NMSERVER), NetBIOS Domain (USEDU), MAC Address (00-50-56-02-07-53), OUI Organization (VMware, Inc.), Nimssoft Type (Hub), and State (Unmanaged). A red box highlights the 'Alarms' icon and '1' alarm count below this section.
- Monitoring Charts:** On the right, three charts are displayed:
 - Total CPU Load:** A line graph showing CPU usage percentage over time (6:00 to 2:00).
 - Processor Queue...:** A bar chart showing processor queue length over time (6:00 to 6:00).
 - Total Memory Used:** A line graph showing memory usage percentage over time (6:00 to 6:00).
- Disk Usage:** At the bottom, a 'Disk Usage' section shows 'C:\' with a usage of 74.41% and a green status icon.

To view the alarm for a device, you can click the Alarms icon or the Alarms tab.

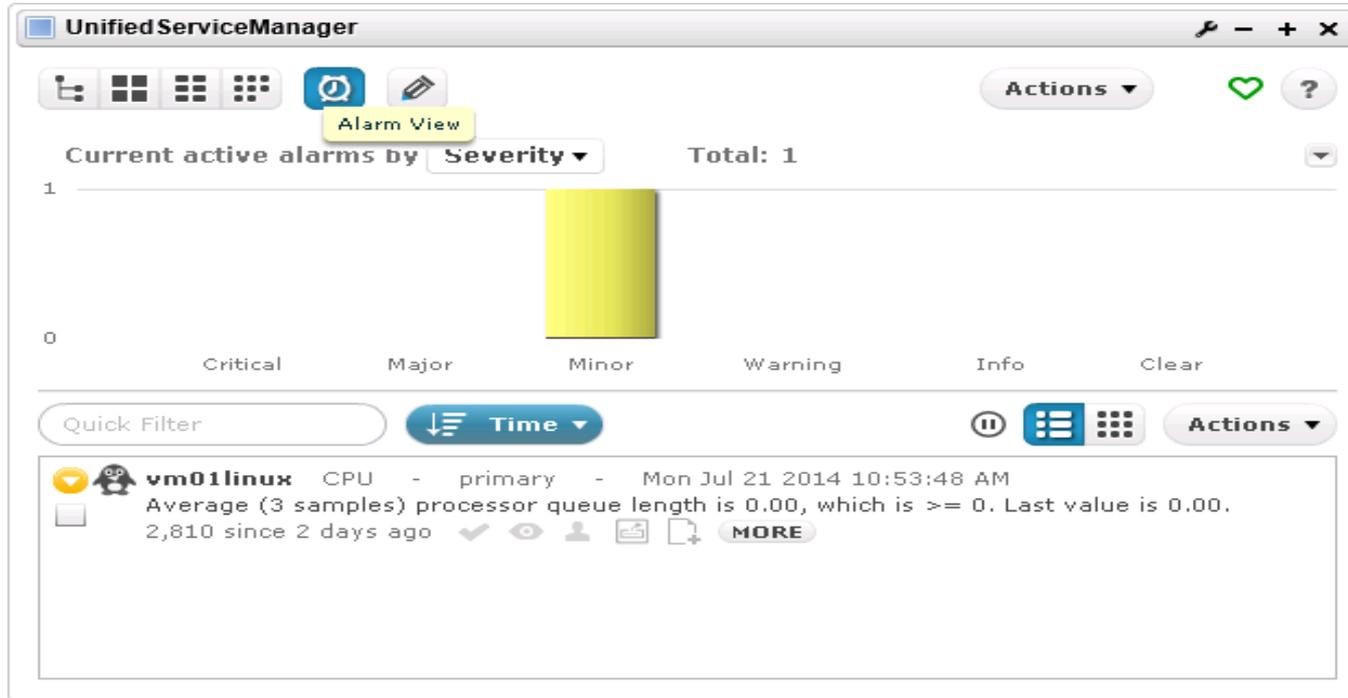
Viewing Monitored Data

The Alarms tab enables you to view the details, history, and metrics of an alarm for a device or groups of devices.

The screenshot displays the Unified Service Manager interface. On the left, a sidebar shows a tree view of groups: MyUSMGroup (4), Operating Systems (4), VMware Guests (1), and vm01linux (selected). The main area shows the 'Alarms' tab with a bar chart titled 'Current active alarms for vm01linux by Severity'. The chart shows one active alarm in the 'Minor' category. Below the chart is a table of active alarms. The first row is highlighted and has a red box around it, containing the following information: vm01linux CPU - primary - Mon Jul 21 2014 11:07:47 AM. The description is 'Average (3 samples) processor queue length is 0.00, which is >= 0.002,824 since 2 days ago'. To the right of the description is a 'MORE' button. A callout box points to this button, stating: 'To view details, history, and metrics about an alarm, you click the More button.' To the right of the table is an 'Actions' menu, also highlighted with a red box. A callout box points to this menu, stating: 'The Actions menu provides available alarm actions.' The menu items are: Clear Filters, Select All, Clear Selected, Accept, Assign..., Unassign, Acknowledge, Launch URL Action..., Set Custom..., Set Visible, Set Invisible, and Hide Invisible.

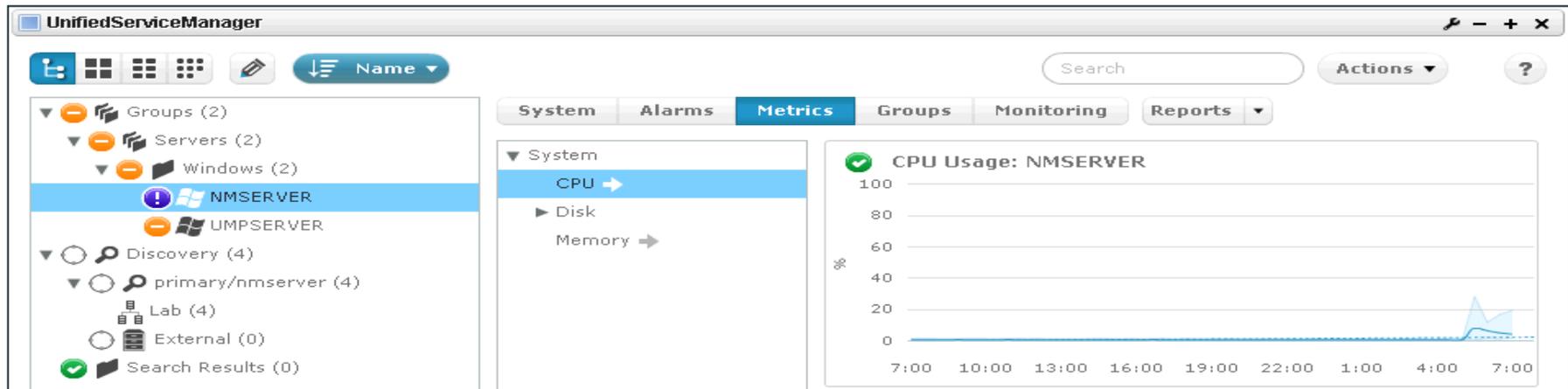
Viewing Monitored Data

The Alarm View The alarm view displays all current alarms, including those that are not associated with a group or a system.



Viewing Monitored Data

You can view additional information from the Metrics and Groups tabs.

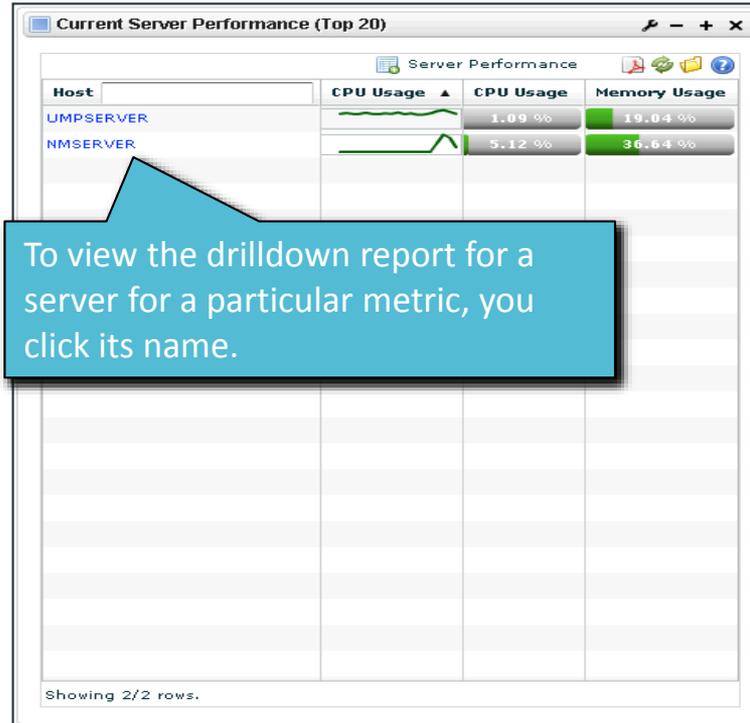


The screenshot shows the UnifiedServiceManager interface with the 'Groups' tab selected. The left sidebar shows a tree view with 'NMSERVER' selected. The main content area displays a table of monitored groups.

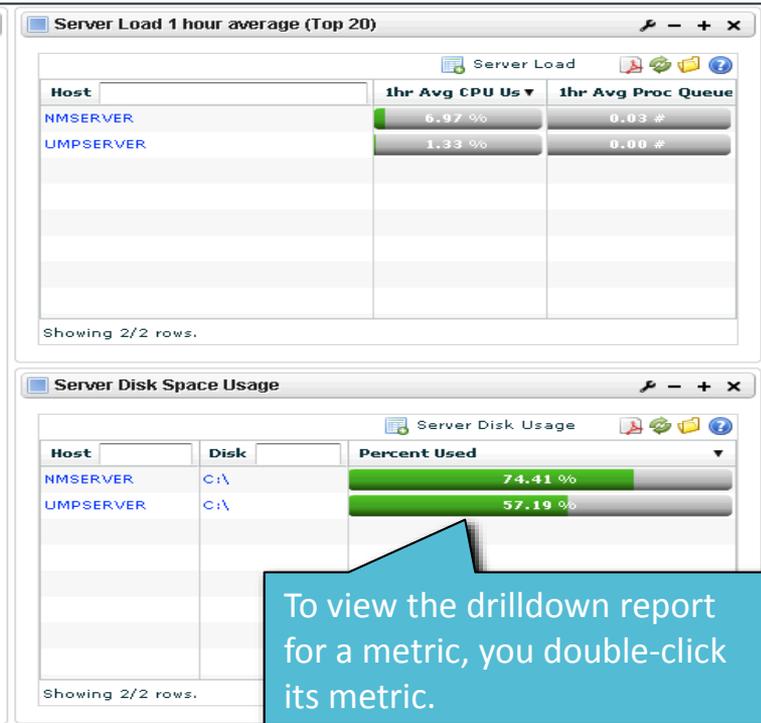
Name	Type	Priority	State
primary/nmserver	Discovery	0	Active
Windows	Dynamic	0	Active

Viewing Monitored Data

The Unified Dashboards portlets displays a variety of metrics.



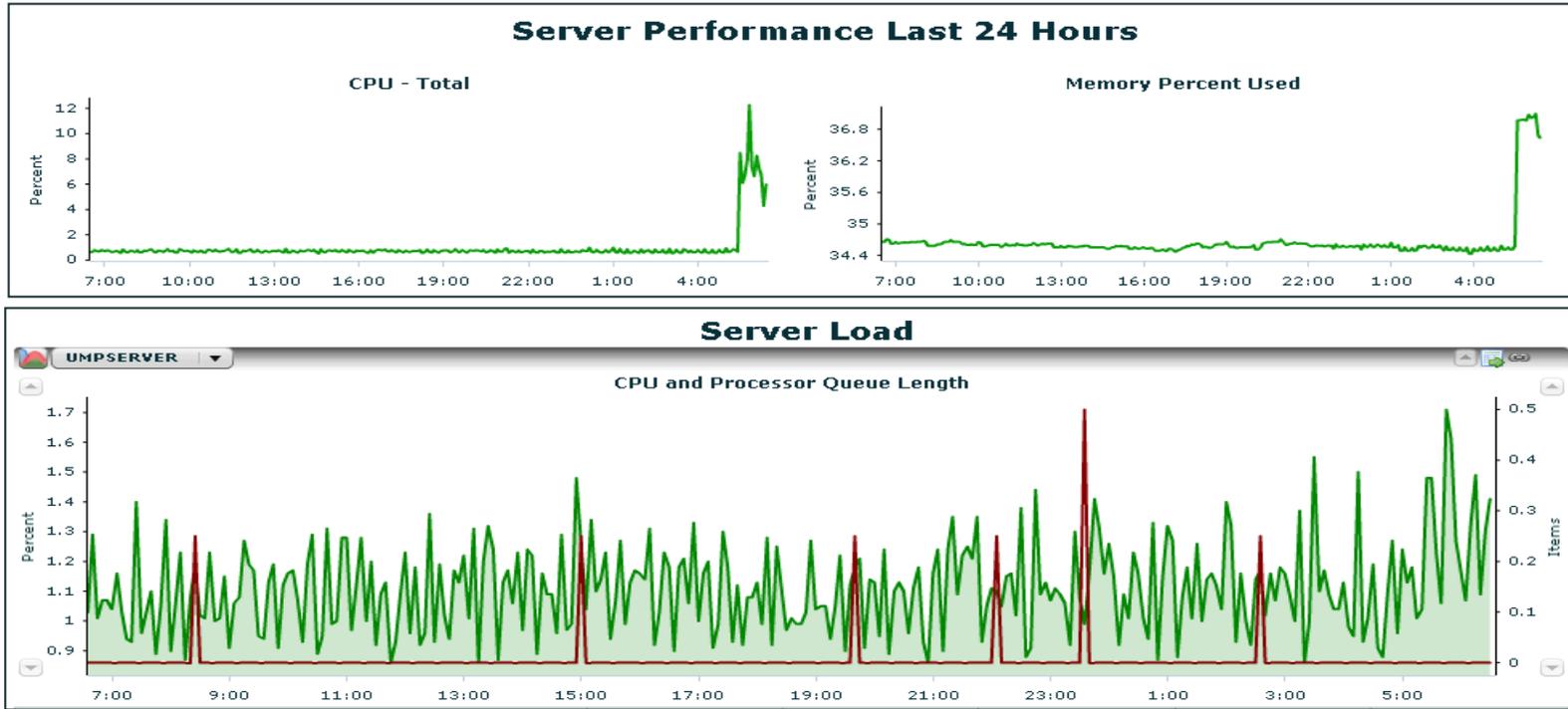
To view the drilldown report for a server for a particular metric, you click its name.



To view the drilldown report for a metric, you double-click its metric.

Viewing Monitored Data

The following screenshots are examples of drilldown reports you can generate:



Lab 3 Exercise

In the following lab exercise, you will:

- Examine monitored data
See lab 3-1 Examine Monitored Data.



PRD Chart

By examining monitored data in PRD charts, you can see a visual representation of QoS data.

With a PRD chart, you can display multiple measurements on a single chart and can view multiple charts at a time.

To begin creating a PRD chart, you click Design ► Performance Reports Designer.



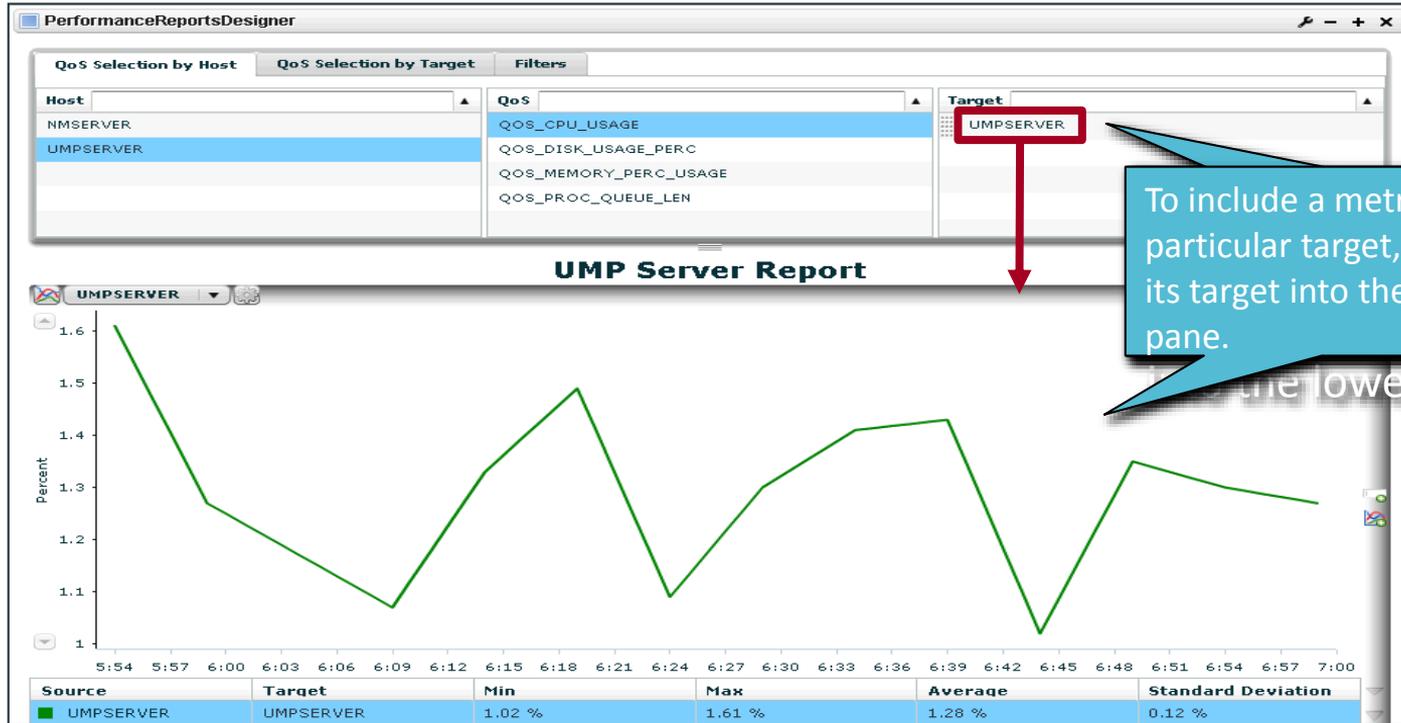
The screenshot shows a web-based monitoring interface. At the top, there is a navigation bar with 'Add' and 'Manage' buttons. Below this is a main menu with 'Home', 'Unified Dashboards', 'Reports', 'Design', and 'Configuration'. The 'Design' menu is open, showing a dropdown with three options: 'Performance Reports Designer', 'List Designer', and 'Dashboard Designer'. The background shows two performance charts for 'NMSERVER'. The left chart, 'Current Server Performance (Top 20)', shows 'CPU Usage' at 16.67% and 'Memory Usage' at 48.24%. The right chart, '1 hour average (Top 20)', shows '1hr Avg CPU Us' at 8.32% and '1hr Avg Proc Queue' at 0.08 #.

Host	CPU Usage	CPU Usa	Memory Usa
NMSERVER		16.67 %	48.24 %

Host	1hr Avg CPU Us	1hr Avg Proc Queue	
NMSERVER		8.32 %	0.08 #

Creating a PRD Chart

To create a PRD chart, you include the host, QoS measurement, target, and time range.



To include a metric for a particular target, you drag its target into the lower pane.

the lower pane.

Lab 3 Exercise

In the following lab exercise, you will:

- Create a PRD chart
See lab 3-2 Create a PRD Chart.



Module 3 Summary

This module showed you how to:

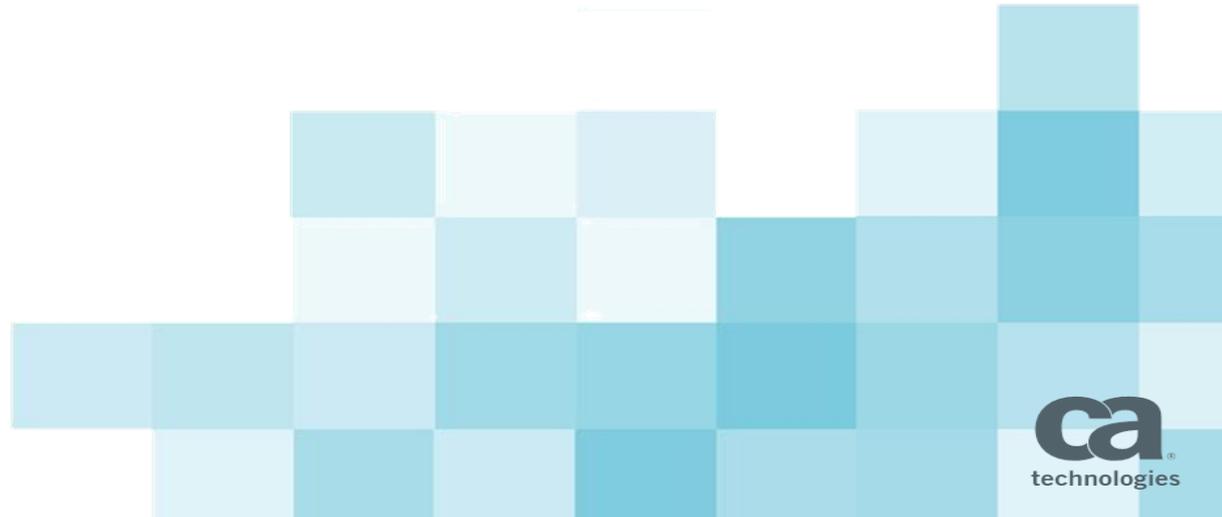
- View monitored data
- Examine monitored data in a PRD chart

In the next module, you will:

- Perform advanced configurations: secondary hub



Module 4: Advanced Configurations: Secondary Hub



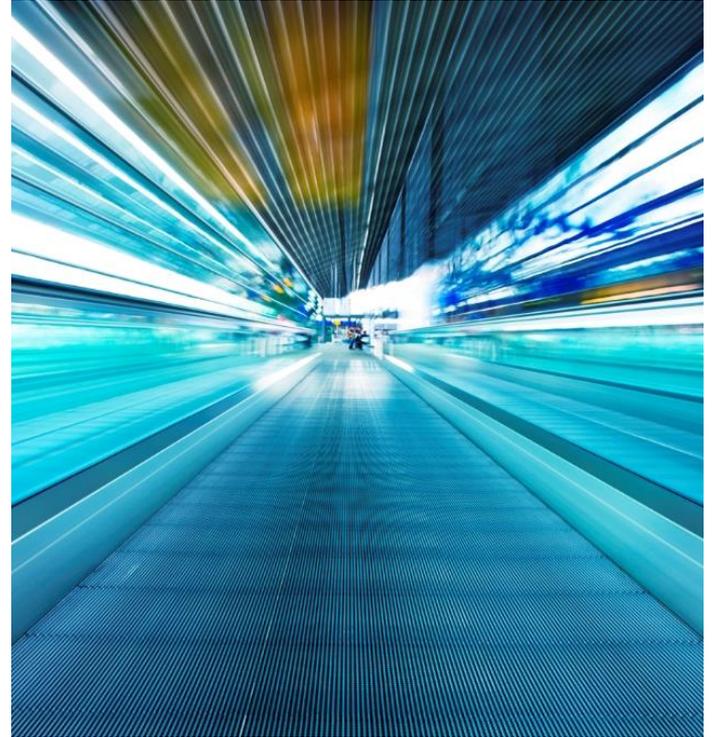
Module Objectives

After completing this module, you will be able to:

- Plan hub-to-hub communications
- Implement hub-to-hub communications

Why you need to know:

- You need to properly plan hub-to-hub communication to ensure that it fulfills the objective.
- To properly scale CA Unified Infrastructure Management, you need to deploy additional hubs and implement hub-to-hub communications.



Plan Hub-to-Hub Communications

You need to properly plan hub-to-hub communication to ensure that it fulfills the objective.

To plan hub-to-hub communications:

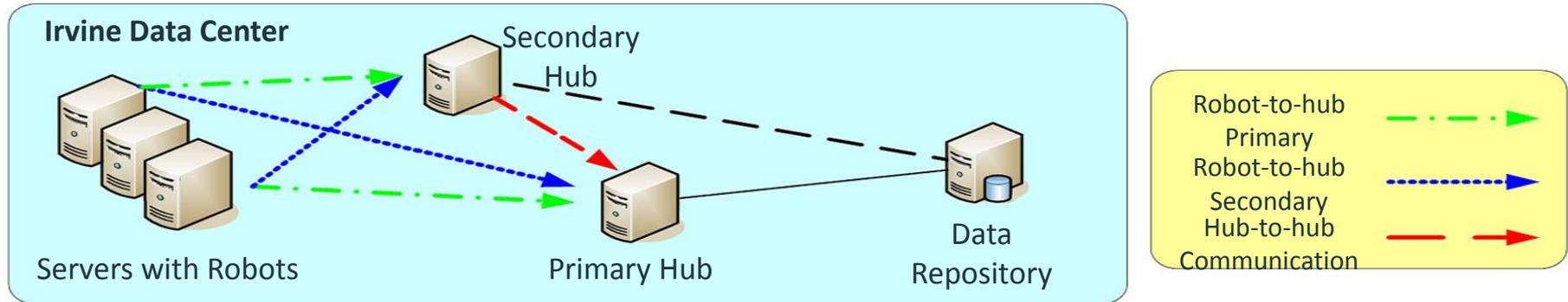
1. Decide on a network communication method:
 - Basic: Broadcast, simple network connection, no problems or block
 - Minimal: Static hubs, for traversing subnet breaks
 - Advanced: Hub-to-hub tunnels, firewalls, WAN, DMZ, and so on
2. Decide on a queue method:
 - Post: Less setup, fast and efficient, but no acknowledgment of delivery
 - Get/attach: Additional overhead, greater efficacy

Purpose of Secondary Hubs

To properly scale CA UIM, you need to deploy additional hubs and implement hub-to-hub communications.

Secondary hubs can be used to group robots according to function, geographical location, departmental code, or other criteria.

- Although secondary hubs are optional, almost all deployments have them.



Advanced deployment

Additional Hub-to-Hub Communication Factors

Hub limits for tunnels/subscribers

- We recommended 25 to 50 for Windows-based systems and 50 to 100 for UNIX- based systems
 - Subscriber limits will depend on your combination of queues and tunnels.
 - When you mix and match, you can exceed the number of queues but you need to reduce the number of tunnels, or the reverse.
 - In practice, the limits on the tunnels are most important.

Redundancy concerns

- Make sure a failover does not exceed the recommended number of subscribers.

Queue subjects/bulk sizing

- Match queue needs, whether split or combined, with subscriber limits.
- Leave bulk sizing at the default configuration until you are presented with a problem such as a queue that is not clearing.

Lab 4 Exercises

In the following lab exercises, you will:

- Deploy a secondary hub
See lab 4-1 Deploy a Secondary Hub.



Module 4 Summary

This module showed you how to:

- Plan hub-to-hub communications
- Implement hub-to-hub communications



For More Information



DevOps

To learn more about DevOps, please visit:

<http://bit.ly/1wbjjqX>

For Informational Purposes Only

© 2014 CA. All rights reserved. All trademarks referenced herein belong to their respective companies.

This presentation provided at CA World 2014 is intended for information purposes only and does not form any type of warranty. Content provided in this presentation has not been reviewed for accuracy and is based on information provided by CA Partners and Customers.

Terms of this Presentation