

SOLUTION BRIEF • CA SPECTRUM® NETWORK EVENT AND FAULT MANAGEMENT

ca technologies

How Can I Ensure Our Network Delivers a Reliable User Experience?

With CA Spectrum®, you can monitor the backbone of your application innovation and user experience—the network that delivers your business-critical applications and services—and provide your business the high performance and availability it requires for success in the application economy.

Executive Summary

Challenge

In today's economy, where nearly every business is a software business, fortunes and success are becoming increasingly intertwined with application innovation and user experience. It's critical that the network that supports your business-critical applications and services delivers high performance and continuous availability.

Opportunity

Network architects, engineers and operators require visibility into a complex ecosystem: software-defined networking and virtualization, exponential growth in traffic, wide diversity of services and connections, ubiquity of wireless computing, and a multiplicity of network monitoring tools and equipment vendors. In addition to visibility, the network team needs to respond to a seemingly countless number of issues that require a world-class network monitoring solution to identify and resolve quickly.

Benefits

CA Spectrum® enables your organization to accurately monitor and manage its dynamic, complex network, including physical, virtual and converged cloud environments as well as many new software defined network (SDN) technologies. CA Spectrum is a best-in-class fault and event management platform and an essential tool for enterprises, government agencies, communications service providers and managed service providers that look to their network operations team for reliable network services and rapid problem resolution.

SECTION – 1

Your Network Is Your Backbone—How Fragile Is It?

The network is the backbone of nearly every business, and its importance is often highlighted by its fragility under extreme, constant pressure. Network architectures are more dynamic as virtualization and various forms of software-defined networking are deployed, creating multiple blind spots. The volume of network activity is growing exponentially, and, as a result, the number of events can easily overwhelm even the largest network operations teams. A diversity of networking services—from the LAN to the WAN and across multiple types of IP services—and an increasingly wireless LAN supporting a wide array of IP devices keeps the network operations team constantly on its toes. Finally, the tools required to manage a multi-vendor, multi-technology network require visibility into multiple protocols and many vendor-specific systems.

The Six Definitive Requirements for Event and Fault Management

Network event and fault management is a core component of every network monitoring solution. The ideal solution provides six key capabilities:

Discovery, Modeling and Topology Mapping

An accurate picture of the inventory provides an intuitive view of the current state of availability, issues and risks to the business. This requires the ability to automatically discover the network and device configurations, model the environment and map the topology down to individual ports and paths.

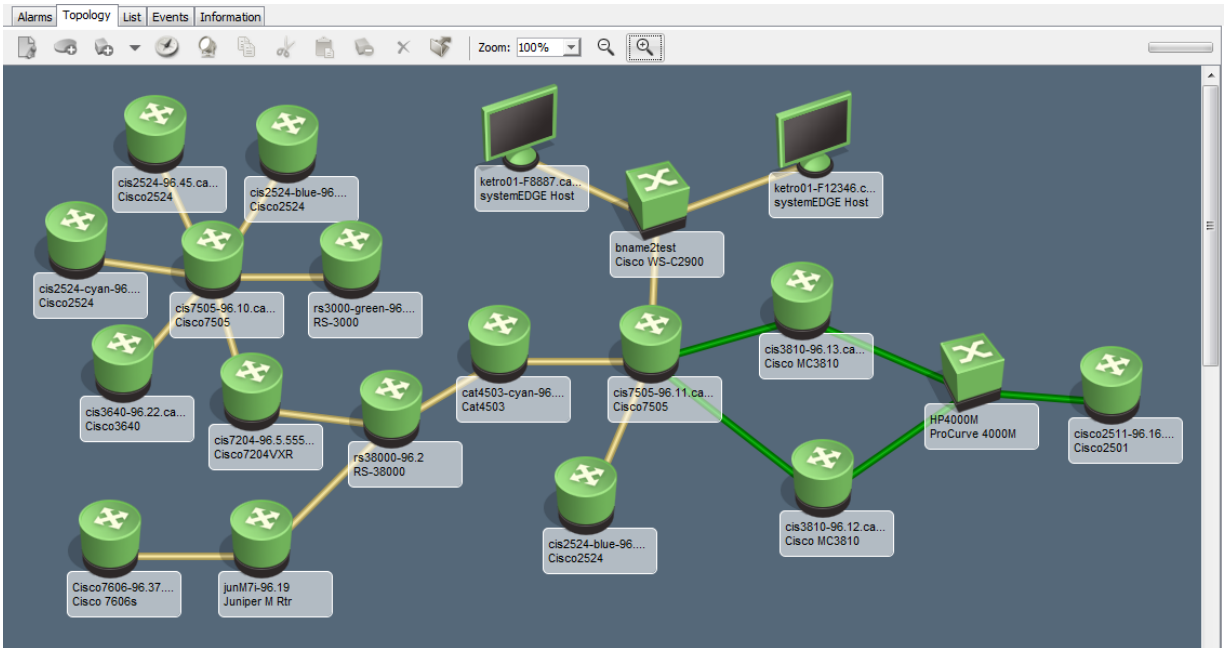


FIGURE 1.
Modeling technology creates an accurate topology map

- Modeling technology creates an accurate topology map that is automatically updated as devices are changed, added or deleted, including the highly dynamic nature of hypervisor-based virtual machines (VMs) and SDN-based entities, endpoints and VMs
- Capturing device configurations allows network operators to use change awareness as an aspect of root cause analysis, helping identify when incorrect network change and configuration management (NCCM) updates cause outages or performance issues

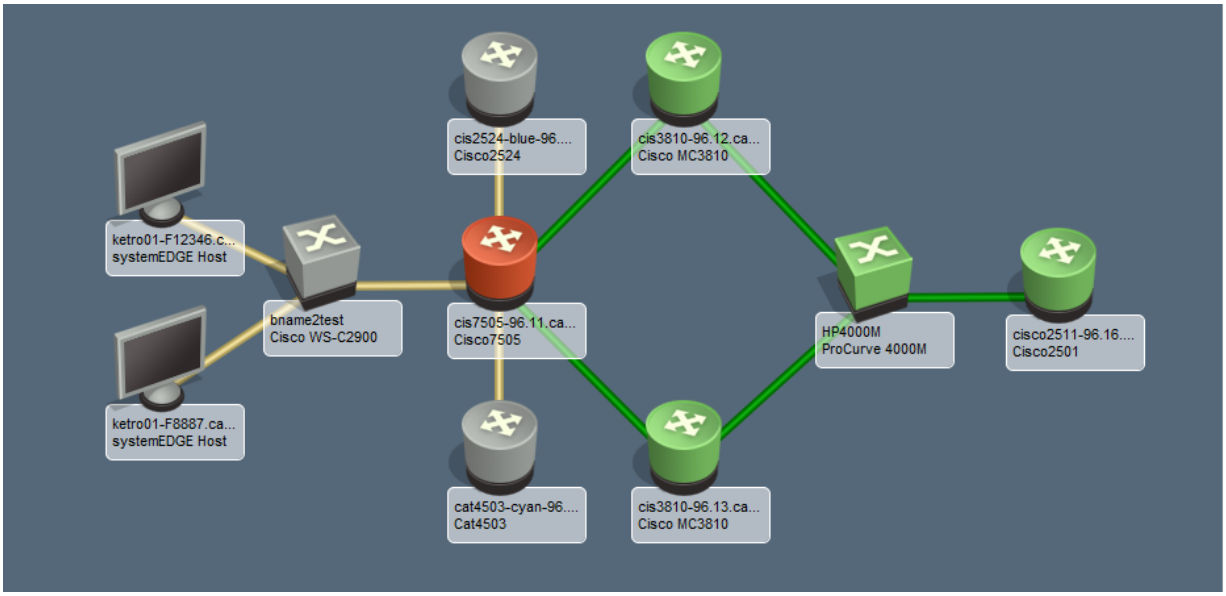
Intelligent Fault Detection, Isolation and Root Cause Analysis

IT operations teams that can focus on the root cause and the most business-critical problems are highly productive. To assist problem resolution, an intelligent model of the network can help isolate an issue down to its root cause, suppress symptomatic alarms and provide actions to take to resolve the issue.

By mapping the relationship between the network connections and network resources, administrators can pinpoint the root cause of service problems for faster resolution.

FIGURE 2.

Root cause analysis pinpoints problems for faster resolution



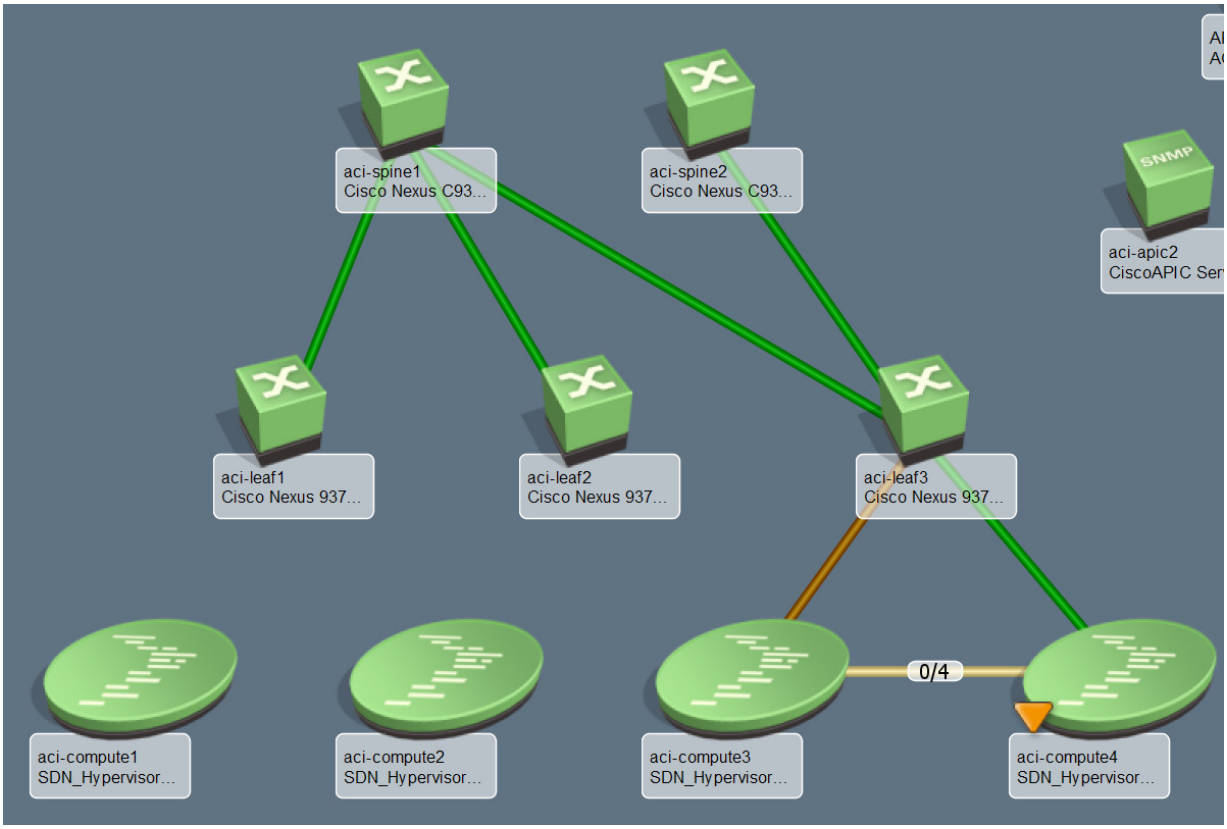
- Out-of-the-box rules for event correlation and root cause analysis reduce the manual effort associated with alternative, script-based fault and event management solutions; customization of condition correlations and actions to take allows engineers to tailor the solution for specific business requirements
- Visibility into port-to-port connections allows network administrators to pinpoint the root cause for fault isolation, suppress the alarms that are symptomatic to the root cause and improve staff productivity

Comprehensive Technology Support for End-to-End Visibility

End-to-end visibility of the LAN-to-WAN and across multiple types of IP services (SD-WANs, MPLS, VPNs, BGP, multicast, etc.) is critical for reliable service delivery.

To provide end-to-end fault and event management across most networks today requires a solution that supports the many vendors involved as well as the multitude of operating systems and vendor-specific management information available from the device. Comprehensive device discovery and support for dozens of vendors and thousands of device types provides the end-to-end visibility required to manage today's large and sprawling networks.

FIGURE 3.
End-to-end visibility across both physical and virtual environments

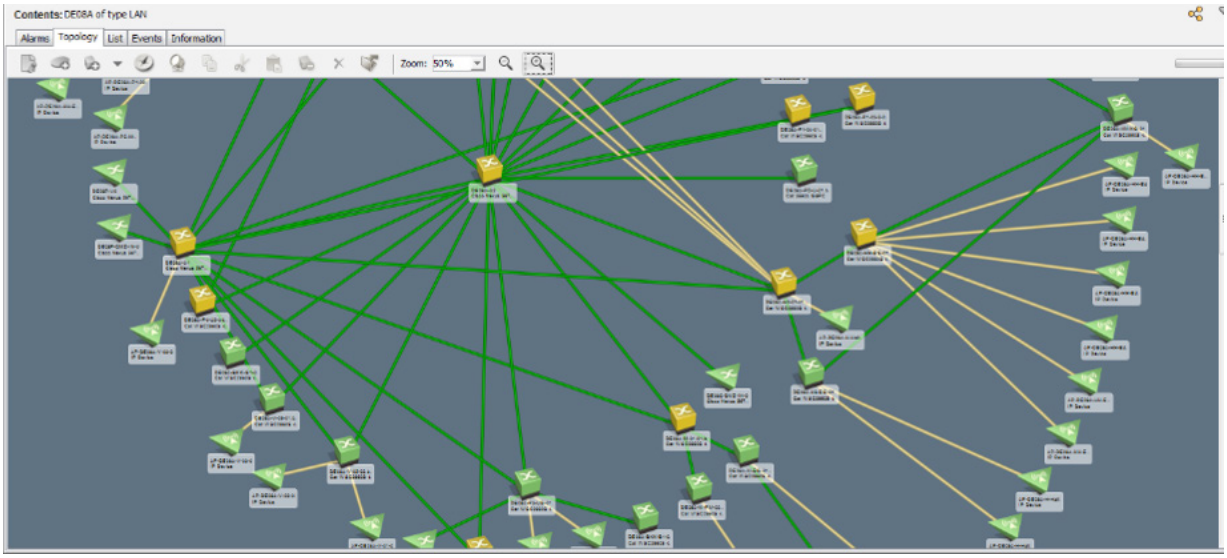


- Network monitoring must support legacy devices that are still present in many data centers and wiring closets as well as the newest virtual network and SDN-based technologies
- Device discovery must include the Layer 2 and Layer 3 physical and logical topology and trunks
- IP service overlays are required for common networking protocols and technologies like MPLS, multicast, QoS, VLANs and VPNs
- An intuitive Web client interface provides visibility into the domains, landscapes, global collections, overlays, device details, alarm summaries and alarm details
- Support for virtual networking technologies, such as Cisco® Virtual Switching Systems (VSS) and virtual PortChannel (vPC), allows organizations to more rapidly identify root cause and impact analysis with two popular networking technologies for the Cisco Nexus® product line
- Advanced systems monitoring for modern architectures, such as Cisco Unified Computing System™ servers, clusters and cloud environments

Support for Today's Wireless World

To eliminate the costly process of providing wiring to every device that needs network access, and to embrace the popularity of bring-your-own-device, organizations are increasingly turning to wireless LAN computing. Most NetOps teams today require a solution that supports both legacy wired networks as well as the faster growing wireless network for a diverse range of devices, including wearables, mobile phones, tablets, laptops, scanners, point-of-sale systems, smart meters and hundreds of styles of Internet of Things (IoT) entities.

FIGURE 4.
Support for wired and wireless network devices and technologies

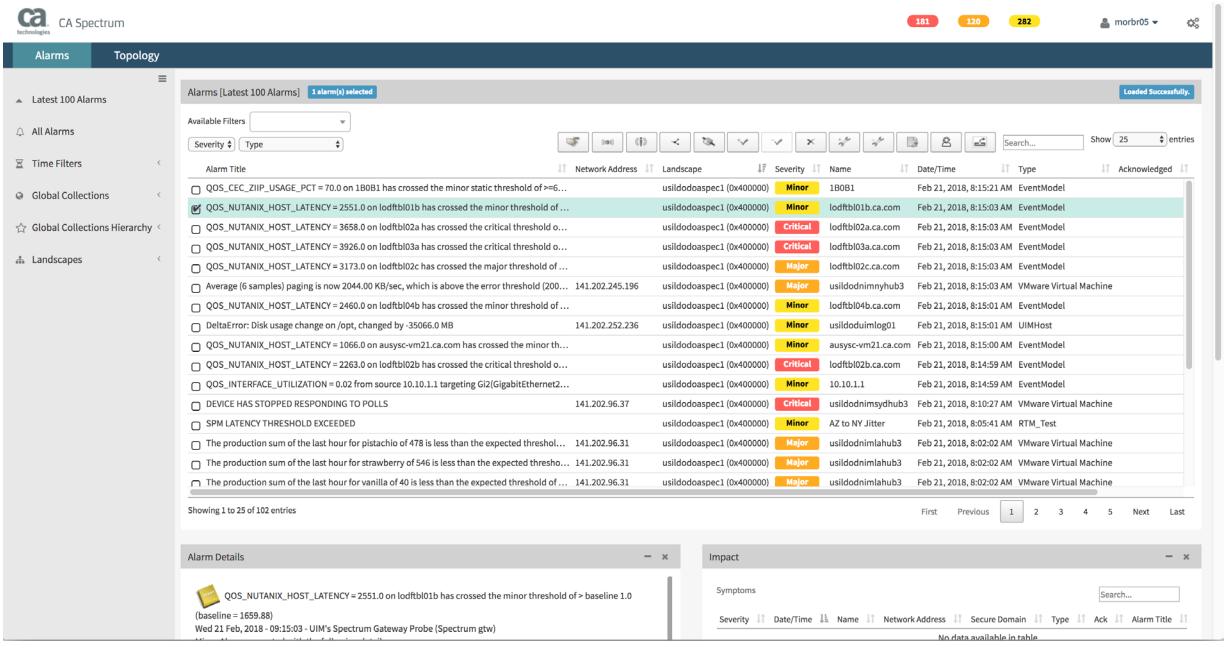


- Discovery and modeling of wireless LAN controllers (WLCs) and connected access points (APs) allows organizations to confidently deploy wireless networking as a part of adopting the consumerization of IT with a growing population of wireless wearables, mobile phones, laptops, smart meters, scanners, point-of-sale systems, IoT, etc.

Extensibility and Integration Across IT Ops Toolchain

Fault and event management is one of many elements in a modern network management toolchain. An extensible architecture and integration across the toolchain provides the means for network engineers, system integrators and managed service providers to adapt the solution for their business-specific requirements.

FIGURE 5.
Integration with multiple IT ops tools, including infrastructure management



- RESTful Web services APIs that enable customers and partners to do their own integrations and execute complex, custom workflows
- The means to push events or alarms from other devices into the solution to leverage its root cause analysis, fault isolation and alarm suppression
- A self-certification toolkit that enables support for new vendor offerings
- Support for today's most popular SDN technologies into an end-to-end monitoring solution, such as Cisco Application Centric Infrastructure (Cisco ACI™) for SD data center monitoring and fault management, SD-WAN monitoring for dynamic network connections, including the Cisco/Viptela® SD-WAN solutions, Nokia® Nuage Networks™ Virtualized Services Platform (VSP) SD-WAN solution with Network Services Gateway (NSG), and controllers supporting OpenContrail™ technology, OpenDaylight™ technology, and OpenStack® technology
- Integration with infrastructure management simplifies the discovery and synchronization of assets and alarms for comprehensive server management, log analytics and public cloud monitoring capabilities and accommodates integrated root cause analysis, fault isolation and alarm suppression
- Integration with a unified network operations portal allows you to combine fault and performance alarms and workflows with performance metrics and other essential NetOps tools for network flow analysis, application delivery and packet analysis, and unified communications management for unified event management
- Integration with business service modeling and monitoring tool enriches insight into the performance, availability and event status of the network devices that are included in the service models
- Integrations with multiple service desk solutions, out-of-the-box and bidirectional, such as the CA Service Desk Manager solution, Remedy® software from BMC®, ServiceNow® software, HPE® Service Manager and ServiceAide® Cloud Service Management allow organizations to continue leveraging prior investments or migrating to new ticketing solutions
- Support for lightweight directory access protocol (LDAP) and Microsoft Active Directory® enables the use of corporate standards for authentication and access across multiple applications

Additional Requirements

- **Multi-tenancy for enterprises and MSPs.** Many organizations require the ability to segregate different sites or customers/sites in different landscapes for secure and relevant management of enterprise locations or MSP clients. From a single console, the ability to manage multiple sites/customers and ensure each tenant's data is invisible to others is highly desirable.
- **Network service-aware management.** The ability to model the network devices supporting critical business services so that network operations can discover, model, monitor and manage the relationships between the network infrastructure and services with the business services the network supports is required by some organizations.
- **Proactive change management.** Network changes are at the heart of many issues. Integrated network change management helps minimize costly downtime and troubleshooting effort that results from ineffective network change and configuration management (NCCM). Integrated NCCM can correlate outages to configuration changes with audit trails for any network device. The solution should also offer change scheduling and automation, approval controls and detailed change reporting, enabling you to establish reference configurations, track deviations and generate alarms when deviations occur.
- **Role-based dashboards and reporting deliver powerful insights.** Pre-packaged, intuitive dashboards and reports should be easily tailored to the specific roles—administrators, enterprise-wide users, branch-office users, device-type users or tenant customers. Flexible data gathering, drag-and-drop report authoring, custom formatting, ad hoc data exploration and analysis and easy content sharing helps network operations harness data for greater insight.

SECTION 2:

CA Spectrum for Robust, Comprehensive and Sophisticated Network Event and Fault Management

CA Spectrum offers the robust, comprehensive and sophisticated capabilities IT organizations need to proactively and effectively manage the faults and events that impact their infrastructures and services.

With patented discovery and topology mapping that leads to innovative root cause analysis and fault isolation, comprehensive coverage across today's diverse network and modern SDN and wireless networking technologies, and an open architecture to extend sophisticated fault and event management across a NetOps toolchain, CA Spectrum is an essential network monitoring solution for every modern software factory.

SECTION 3:

Key Benefits/Results

With CA Spectrum, you can:

- **Speed innovation.** Capitalize on innovative technologies and approaches, such as cloud and virtualization and software-defined networks, while using a single management platform.
- **Accelerate issue resolution**. Get the practical insights you need to quickly identify and resolve problems to enable improved and organizational performances.
- **Increase IT's value.** Leverage an end-to-end view of the networking devices and services across a diverse IT services backdrop and NetOps toolchain.
- **Support consumerization of IT.** Embrace bring-your-own-device and a growing array of wireless devices with support for the most common wireless LAN controllers and access points.
- **Extend with customizations and integrations.** Get the most out of the solution with easy customization for your specific business requirements and integrations across the NetOps and IT Ops toolchain, leveraging open APIs and out-of-the-box integrations.

SECTION 4:

Next Steps

If the network is the backbone of your enterprise, government agency or portfolio of managed services, CA Spectrum should be a core component of your network monitoring toolchain. With more than 25 years of continuous innovation and development, and dozens of patents to demonstrate leadership in network event and fault management, CA Spectrum helps organizations provide the business-critical applications and improved user experiences required for success in today's application economy.

To learn more about CA Spectrum, please visit **ca.com/spectrum.**

Connect with CA Technologies

CA Technologies (NASDAQ: CA) provides IT management solutions that help customers manage and secure complex IT environments to support agile business services. Organizations leverage CA Technologies software and SaaS solutions to accelerate innovation, transform infrastructure and secure data and identities, from the data center to the cloud. CA Technologies is committed to ensuring our customers achieve their desired outcomes and expected business value through the use of our technology.
To learn more about our customer success programs, visit **ca.com/customer-success**.
For more information about CA Technologies, go to **ca.com**.

Copyright © 2018 CA. All rights reserved. Cisco, Cisco ACI, Viptela, Cisco Nexus, and Cisco Unified Computing System are registered trademarks or trademarks of Cisco Systems, Inc. and/or its affiliates in the United States and certain other countries. Nuage Networks is a trademark of the Nokia group of companies. Nokia is a registered trademark of Nokia Corporation. OpenContrail is a trademark of Juniper Networks, Inc. in the United States and other countries. OpenDaylight is a trademark of OpenDaylight Project, Inc. The OpenStack Word Mark and OpenStack Logo are either registered trademarks/service marks or trademarks/service marks of the OpenStack Foundation, in the United States and other countries and are used with the OpenStack Foundation's permission. We are not affiliated with, endorsed or sponsored by the OpenStack Foundation, or the OpenStack community. BMC, BMC Software, the BMC logo, the BMC Software logo, and other BMC marks are the exclusive properties of BMC Software, Inc., or its affiliates or subsidiaries and are registered or may be registered with the U.S. Patent and Trademark Office and in other countries. All other BMC trademarks, service marks, and logos may be registered or pending registration in the U.S. or in other countries. Microsoft and Active Directory are either registered trademarks or trademarks of Microsoft Corporation in the United States and/or other countries. All other trademarks or registered trademarks are the property of their respective owners. ServiceNow is a trademark or registered trademark of ServiceNow in the United States and other countries. All other trademarks, trade names, service marks and logos referenced herein belong to their respective companies.

200-343852_0318

ca technologies