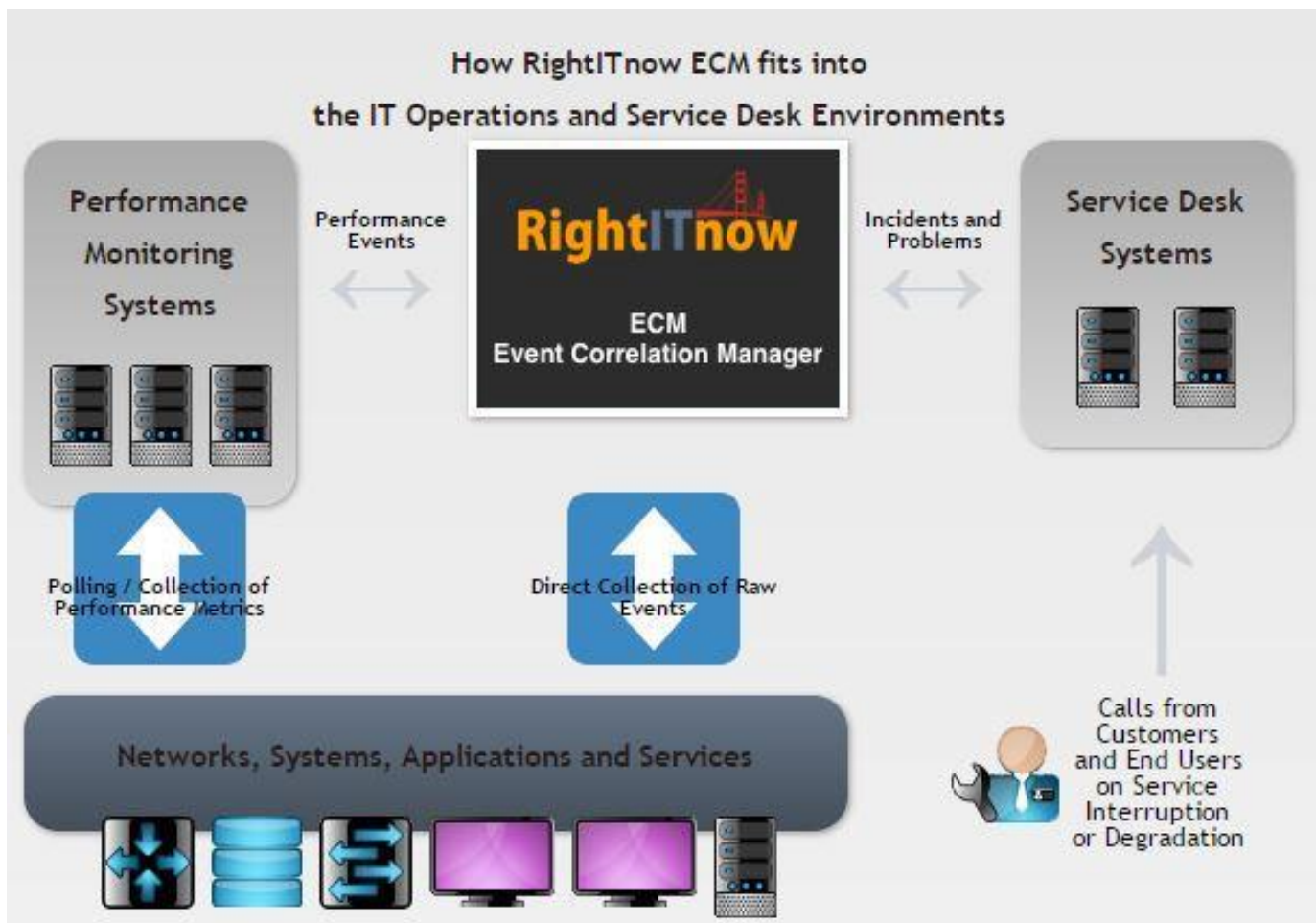


Overview

RightITnow ECM (Event Correlation Manager) is a multi-source event correlation and IT operations management solution that aggregates, filters and correlates a high-volume of infrastructure and application events into a streamlined number of actionable alerts in real-time. This enables IT operations staff to proactively detect, isolate and respond to infrastructure issues before they impact customers.

RightITnow ECM also automates the event management workflow and facilitates incident and problem management by bridging the gap between IT Operations and the Service Desk.

FIGURE 1: How RightITnow ECM fits into the IT Operations & Service Desk Environment



Key Features

Extensive IT Event Collection

RightITnow ECM supports event collection across a wide range of industry standard protocols and message formats including SNMP and Syslog that address most network devices, systems and application environments. In addition, ECM provides a SOAP/XML API and a REST API to inject any type of event stream into the system.

RightITnow ECM easily integrates with EMS's (Element Management Systems) and monitoring tools, enabling single platform consolidation of all infrastructure, application and business service events. Out-of-the-box integrations include monitoring solutions like SolarWinds Orion NPM, SCOM, Nagios, VMware vCenter and Amazon AWS CloudWatch.

Web 2.0 Interface and User Admin

RightITnow ECM's Web 2.0 interface is incredibly easy to use, configure, and administer. With its feature rich UI and flexible controls, operators can customize views, displets and rules associated with categorizing, filtering, assigning or correlating alerts. No programming required.

And with RightITnow ECM's role-based administration of customer and infrastructure data, you can manage access to data and process elements, in line with your organizational compliance policies.

IT Operations Process Automation

Using event, entity and topology collection; correlation rules; and a library of configurable internal and external actions, RightITnow ECM makes it easy to automate IT operations processes. For example, with RightITnow ECM you can automatically escalate certain alerts to the Service Desk for incident (trouble ticket) creation. Or you could automate actions including running custom scripts to perform problem resolution – for example, rebooting a server or initiating a batch process. With RightITnow ECM, it's easy to streamline your existing IT Operations workflows by automating routine or repeated operator actions.

RightITnow ECM's workflow automation capabilities extend to integrations with other management systems. For example, RightITnow ECM can be configured for closed-loop removal of alerts when linked incidents or trouble tickets are 'closed' in the Service Desk. It can also communicate alert acknowledgement and closure to monitoring systems like SolarWinds Orion NPM. RightITnow ECM's bi-directional automation of the event-to-alert-to-incident process plays a key role in optimizing IT operations and streamlining costs.

| Entity Name | Severity | Description | Count | Last Occurred | Owner |
|---|---------------|--|--------------------|---------------------|------------------|
| + Abbas Abacha (1 entities - 1 alerts - 17 events - 1 sources) | | | | | |
| + Admin (3 entities - 3 alerts - 42 events - 3 sources) | | | | | |
| - Alan Rid (5 entities - 9 alerts - 1781 events - 4 sources) | | | | | |
| 192.168.12.101 | Minor | Node 192.168.12.101 has an average response time of 303 ms which... | 10 | 24/08/2011 17:57:58 | Alan Rid |
| 192.168.12.95 | Critical | Node 192.168.12.95's packet loss has risen above 40% to 50 %. | 47 | 08/11/2011 18:08:54 | Alan Rid |
| vmcube | Warning | ACPI: APIC 00000000b780390 000D8 (v01 032009 APIC1650 200903... | 2 | 10/07/2012 13:43:43 | Alan Rid |
| Unknown | Informational | Core Service [SOLARWINDSVM-1] Started | 24 | 12/12/2013 02:11:26 | Alan Rid |
| nagios | Clear | DISK CRITICAL - free space: / 4757 MB (61% inode=77%): | 167 | 21/08/2012 05:13:16 | Alan Rid |
| nagios | Clear | PROCS CRITICAL: 68 processes with STATE = RSZDT | 1361 | 31/05/2013 05:51:11 | Alan Rid |
| nagios | Warning | DISK CRITICAL - free space: / 4329 MB (56% inode=68%): | 40 | 29/10/2012 05:27:59 | Alan Rid |
| Unknown | Informational | SQS: Queue Metrics test alarm (s) Alarm updated from INSUFFICIENT... | 6 | 29/04/2016 00:02:01 | Alan Rid |
| Unknown | Informational | HighCPURDS (CPU > 80% for 5 minutes) Alarm updated from ALARM ... | 124 | 26/07/2016 23:55:55 | Alan Rid |
| + Anna McIntyre (10 entities - 11 alerts - 81920 events - 6 sources) | | | | | |
| + Bob Smith (9 entities - 12 alerts - 86328 events - 5 sources) | | | | | |
| - Clarissa Johnson (4 entities - 4 alerts - 1036 events - 3 sources) | | | | | |
| 192.168.12.4 | Warning | alarm canceled: GW_WAN(81.148.64.1) *** delay *** | 80 | 05/03/2012 05:20:49 | Clarissa Johnson |
| 192.168.12.223 | Warning | Invalid query packet. | 820 | 07/08/2012 07:08:43 | Clarissa Johnson |
| nagios | Clear | DISK CRITICAL - free space: / 4622 MB (59% inode=77%): | 92 | 27/08/2012 05:13:40 | Clarissa Johnson |
| DBServer | Clear | Server UP | 44 | 16/02/2017 11:10:29 | Clarissa Johnson |
| + David Trend (3 entities - 3 alerts - 11980 events - 3 sources) | | | | | |
| + Joe Pie (3 entities - 3 alerts - 51 events - 3 sources) | | | | | |
| - Julia Mannick (3 entities - 4 alerts - 30 events - 2 sources) | | | | | |
| 192.168.12.101 | Informational | Node 192.168.12.101 has an average response time of 294 ms which... | 14 | 18/08/2011 00:03:14 | Julia Mannick |
| beer | Critical | pam_unix(sudo:auth): auth could not identify password for [jose] | 5 | 11/12/2012 11:09:48 | Julia Mannick |
| vmcube | Warning | ACPI: XSDT 00000000b780100 00064 (v01 032009 XSDT1650 20090... | 2 | 10/07/2012 13:43:43 | Julia Mannick |
| beer | Warning | pam_unix(sudo:auth): conversation failed | 9 | 11/12/2012 11:09:48 | Julia Mannick |
| | | | 26 entities | 50 alerts | 18318 |
| Change Severity Change Priority Assign To Close Alert Acknowledge | | | | | |
| Additional Details | | | | | |

FIGURE 2: RightITnow ECM's Alert Console

Powerful Event Correlation and Analysis

RightITnow ECM's correlation mechanisms enable IT Operations staff to consolidate, manipulate and isolate alerts as well as determine follow-on actions. The system facilitates the creation of simple to advanced rules in an intuitive graphical environment.

- ▶ **Create Rule on the Fly** – directly from the alert console, lets the operator create a rule based on the values on an coming alert and automatically triggers a series of actions to remediate an issue on the fly or set a rule to perform forward alert suppression, i.e an immediate alert flooding prevention. This helps streamline and clear IT operator consoles and put the focus on real critical situations.
- ▶ **Generic and Reverse X in Y** – detecting events within a specific window that meet specified alert conditions, such as multiple spikes in CPU utilization in a server or the absence of a heartbeat event over a set number of counts.
- ▶ **Topology Based** – With the knowledge of device, system, interface, and port connectivity, inferring and suppressing downstream alerts. For example, when a network switch fails all downstream alarms from connected devices are suppressed.
- ▶ **Custom Correlation** – Easily configurable advanced rules with multiple variables and conditions make it simple to track virtually any set of alert conditions within the IT infrastructure.

IT Management System Interoperability

RightITnow ECM integrates with all the major incident management systems, such as ServiceNow and BMC Service Desk.

User Authentication can also be delegated to Microsoft Active Directory or OpenLDAP to ensure a much faster and seamless deployment.

Management Dashboards

RightITnow ECM's dashboards make it easy to assess the efficiency of IT operations and plan for improvement. For example, productivity metrics could include the number of events, alerts and incidents that are consolidated, correlated or closed at an individual device, operator, service or customer level. Process oriented metrics could include the relative application of different correlation mechanisms across the alert spectrum; frequency of changes in alert severity levels; average time to close and ratios of resolved alerts to escalated incidents across a business or service group. And all metrics can be tracked in near real-time to effect immediate changes, or over time to measure and drive long term operational improvements.

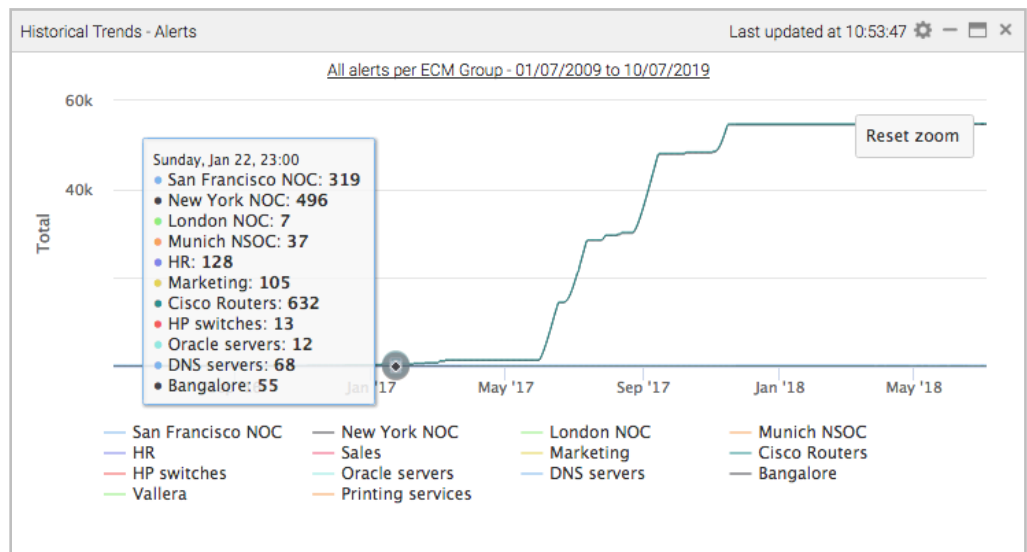


FIGURE 3: RightITnow ECM's Historical Alert Trends

RightITnow ECM: How It Works

Step 1: Event Capture and Categorization

Raw events injected into the RightITnow ECM system are normalized and de-duplicated according to user defined rules – dramatically reducing the overall signal to noise ratio. Events that turn into alerts are then automatically enriched with contextual information that includes entity (i.e. Configuration Item) attributes such as maintenance schedule, default owner, entity group and service tags etc., all of which are critical to decision making and escalation in the following stages.

Step 2: Alert Correlation and Isolation

Once alerts have been created they are immediately displayed in the alert console and evaluated against all the correlation rules. In addition to a set of predefined rules provided by ECM, there is no limit in the number and complexity of the rules that an administrator can define and deploy, using the same graphical metaphor throughout the system. In addition to triggering rules on alert creation or modification, the correlation engine supports the execution of periodic rules on a user-defined interval.

Step 3: Remediation and Escalation

Once alerts are prioritized, correlated and displayed in the alerts console, IT operations staff can initiate a variety of remedial actions and escalation processes. These include both automated and manual mechanisms.

The screenshot displays the 'Correlation Rules' interface. On the left, a table lists various rules with columns for Name, Status, Rule Type, and Owner. On the right, a configuration panel for the 'DNS Service Down' rule is shown, including fields for Name, Description, Owner, and Run actions on, along with a condition builder and action settings.

| Name | Status | Rule Type | Owner |
|-----------------------------------|--------------------------------------|------------------------|----------------|
| Maintenance | 1 rules : 1 deployed, 0 undeployed | | |
| Close Maintenance | 1 rules : 0 deployed, 1 undeployed | | |
| Tag | 8 rules : 7 deployed, 1 undeployed | | |
| Periodic | 12 rules : 1 deployed, 11 undeployed | | |
| Timed Condition (XinY) | 5 rules : 4 deployed, 1 undeployed | | |
| SSH auth failure | Undeployed | Timed Condition (XinY) | robert baritum |
| LinkUpDown | Deployed | Timed Condition (XinY) | robert baritum |
| VCenter Alarm | Deployed | Timed Condition (XinY) | robert baritum |
| Invalid Packet | Deployed | Timed Condition (XinY) | robert baritum |
| Timed checks for flapping | Deployed | Timed Condition (XinY) | Admin |
| Upon Event Arrival | 10 rules : 6 deployed, 4 undeployed | | |
| 1 Set Alert Severity | Undeployed | Upon Event Arrival | |
| 2 Set Alert Description | Deployed | Upon Event Arrival | |
| 3 RaiseSeverity Web Server Down | Deployed | Upon Event Arrival | |
| 4 Minor HR Nagios | Undeployed (Schedu... | Upon Event Arrival | Julia Mannick |
| 5 alert flood description | Undeployed | Upon Event Arrival | Alan Rid |
| 6 Open alert | Undeployed | Upon Event Arrival | david |
| 7 DNS Service Down | Deployed | Upon Event Arrival | |
| 8 VMware Alarm Status | Deployed | Upon Event Arrival | |
| 9 VMware out of disk space urgent | Deployed | Upon Event Arrival | Admin |
| 10 VMware out of disk space | Deployed | Upon Event Arrival | Admin |

1. Name and describe the rule

Name: DNS Service Down

Description: If the service tag of the alert is 'DNS' and message contains 'Server Down', raise an incident.

Owner: Nobody

Do not apply rule to alerts where the incoming event has been processed out of order.

Run actions on: Alerts not in Maintenance

Create Deploy Schedule

1.1 Choose alert's connectors to show relevant variables

2. Define the condition

Match All

- Description contains Server Down
- Tag equals DNS

Also check if the following alerts exist

3. Set the actions

For the incoming alert

If the condition is true: Insert Incident

If the condition is false: <No Action>

For the following alerts

FIGURE 4: RightITnow ECM's Correlation Console

Why RightITnow?

RightITnow ECM lowers your IT operations costs by reducing the volume of alerts and incidents your operations and Service Desk teams need to process.

Cost Effective and Easy to Use

RightITnow ECM's intuitive user interface combined with its real-time, centralized management deliver a dramatically lower cost of ownership compared to legacy event management systems. RightITnow ECM offers in one feature-packed product what legacy systems barely deliver in a convoluted suite of components.

More Productive

With RightITnow ECM, your IT Operations and Service Desk staff can stop wasting time fire fighting and instead focus on a manageable number of service impacting alerts.

Faster Problem Resolution

With ECM's contextual/enriched alerts, and linked incident/trouble ticket records, your IT Operations and Service Desk staff can solve problems faster. The contextual knowledge of underlying foundational events, correlation results and link backs to performance data (say, from an original monitoring source) where applicable – all contribute to faster problem resolution.

Improved Service Level Delivery

Since RightITnow ECM captures all events from all sources at all times, problems relating to undetected or "silent failures" are eliminated. As a result, customers and end users gain from increased availability and uptime and assured performance against service levels.

About RightITnow

RightITnow delivers real-time, cross-domain event correlation software that enables enterprises to optimize IT Operations processes so they can drive down costs, resolve problems faster and assure end user services. It achieves this by automating the event to alert to incident life cycle and bridging the gap between IT Operations center and the Service Desk – driving higher productivity and effectiveness. For more information, please visit www.RightITnow.com.

Contact us at info@RightITnow.com

US Office 101A Clay Street, #150, San Francisco, CA 94111 USA +1 415 350 35 81



FIGURE 5: RightITnow Before & After

RightITnow ECM Cloud

NO Prerequisites: Just register and login using your browser

RightITnow ECM On-Premise supported environments and platforms

Prerequisites

Before attempting to install and configure RightITnow ECM, ensure that you satisfy the following requirements:

Hardware Requirements

- A server with dual quad-core processors and 64GB of RAM

Operating Systems

- Red Hat Enterprise Linux 6 or later
- CentOS 6 or later
- Ubuntu 14.04 LTS or later
- Microsoft Windows 7/8/10 or Microsoft Windows Server 2008/2012/2016
- Mac OS X 10.6 (Snow Leopard) or later

Software Requirements (64-bit where possible)

- Oracle JRE/JDK 8 or Oracle JDK 11 LTS or OpenJDK 11
- MySQL Standard Edition 5.6 or 5.7 (or MySQL Cluster NDB 7.5.5+)

User data stores

RightITnow allows you to import and synchronize your user data from the following repositories:

- Microsoft Active Directory
- OpenLDAP

Event sources

RightITnow accepts and processes events from the following sources:

- Amazon AWS CloudWatch, Microsoft Azure and Google Cloud Logging
- InfoVista
- ManageEngine APM
- Nagios, Nagios XI, Groundwork, Icinga & Naemon
- SCOM 2012 & 2016
- ServiceNow® CMDB
- SNMP Traps
- Solarwinds Orion NPM & SAM
- Syslog
- VMware
- Zabbix
- Zenoss

To create your own event source you can use the SOAP API and to integrate with other applications, you can use the REST API.

Incident management systems

Automatically log incidents based on RightITnow Alerts on the following systems:

- Atlassian JIRA
- BMC Service Desk
- ManageEngine ServiceDesk Plus
- Salesforce Service Cloud
- Serena BSM
- ServiceNow®
- Zendesk

To interface with another Incident system, please inquire about the Incident Connector API.