AUTOMATED MONITORING AND EVENT RECOVERY OF VBLOCK™ INFRASTRUCTURE PLATFORMS WITH IPSOFT MANAGED SERVICE

May 2011
# Table of Contents

Executive Summary .................................................................................................................. 3  
The Challenge .......................................................................................................................... 3  
The Solution ............................................................................................................................ 3  
Technology Overview ............................................................................................................ 6  
  Vblock™ Infrastructure Platforms ......................................................................................... 6  
  IPsoft Tools ......................................................................................................................... 7  
Solution Architecture ............................................................................................................ 9  
Hardware and Software Resources ......................................................................................... 10  
Solution Testing and Validation ............................................................................................ 11  
  Testing Objectives ............................................................................................................... 12  
  Test Results ......................................................................................................................... 13  
  Example Test Case Scenario: An FC Port on the Cisco MDS Switch was Shut Off .......... 15  
Conclusion ............................................................................................................................. 19
Executive Summary

Effectively diagnosing and resolving problems in a converged infrastructure environment can be a challenging task. When a system or process fails, the operational efficiency, productivity, security, and sometimes even the revenue of the business are impacted. Downtime impacts multiple users and services. When these failures occur, the number one priority of the Information Technology (IT) Operations team is to restore business services to normal operations as quickly as possible.

An effective incident management program records, classifies, tracks, and closes all incidents in a controlled and consistent manner. How well an IT organization manages incidents to a successful conclusion is one metric by which IT’s overall performance and value is measured. One way to address this is to have an automated system that collects the relevant infrastructure information, diagnoses the data, and correlates the potential causes before ever engaging an engineer. The benefits of automated monitoring and repairing of incidents include:

- Intelligent Root Cause Analysis (RCA) to help with service restoration and reduced redundancy events
- Accurate identification of redundancy failures
- Reduced Mean Time to Resolve and Repair (MTTR) problems
- Scalable operations
- Lowered operating expenses through reduced labor costs
- Exceeding Service Level Agreements (SLAs) to the business
- Reduced human error

The Challenge

When an incident impacts service, the IT support goal is to identify the incident and restore the service as fast as possible. In traditional data centers, the approach to incident management is essentially a sequential, labor-intensive, and time-consuming process of elimination of possible root causes through trial and error. Root cause identification and resolution usually requires IT administrators to spend hours and perform numerous checks against the various pieces of the infrastructure. Every hour spent on incident identification and triage increases the operational costs to IT. The longer it takes to filter, analyze, and correlate alerts and symptoms to find the root cause of an incident, the longer the time to resolution. The ability to quickly correlate events and alerts is critical to effective incident and problem management.

Today’s IT management leaders are facing increasing pressure to increase efficiency while decreasing total cost of ownership. Labor is one of the largest costs for most IT organizations. No IT infrastructure is ever issue free, and increased complexity makes them harder to manage. Another challenge IT operations can face during troubleshooting is determining which support engineers to engage first. With more complex infrastructure environments comes a larger range of potential causes for an incident. Resolution can involve downtime and the potential for human error. Having a central knowledge base that can quickly and accurately resolve problems is one solution to this problem.

The Solution

With Vblock™ Infrastructure Platforms, VCE delivers the industry’s first completely integrated IT offering that combines best-in-class network, compute, storage, management, virtualization, and security technologies with end-to-end vendor accountability. The converged infrastructure provided by Vblock Infrastructure Platforms offers new opportunities for IT to more consistently diagnose issues through standardized components. It enables greater use of autonomic systems to reduce or eliminate the need for human intervention for debugging and resolving infrastructure alarms and incidents.
VCE Company has teamed with IPsoft to define a solution that reduces downtime, increases recovery speed, reduces human error, and enables scale via automated monitoring and repairing of incidents on Vblock Infrastructure Platforms.

IPsoft is a managed services provider delivering IT outsourcing solutions to enterprise customers and service providers worldwide. IPsoft’s web-based integrated IT service management platform manages complex infrastructures for production operations. This platform combines ITIL best practices for IT service delivery and support with the Six Sigma methodology for defect reduction and continuous quality improvement, enabling autonomic operational delivery engines and support tools. IPsoft’s IPcenter suite of tools detects and resolves anomalies in complex IT systems with virtual engineers. Detection, resolution, and escalation take place at machine speed. A virtual engineer knows when to take action and when to escalate to a human engineer for assistance.

Through this solution, the IPsoft managed service can help detect and mitigate incidents, such as an infrastructure failure on Vblock Infrastructure Platforms with minimal, if any, personnel interaction needed. The test cases described below have been validated for the compute, storage, network, and virtual machine components of Vblock Infrastructure Platforms.

Assumptions
While it is possible to implement this solution without the VCE Advanced Management Pod (AMP), the solution described below assumes that it is in use. AMP is a self-contained management infrastructure for Vblock Infrastructure Platforms that runs infrastructure management software such as EMC Unified Infrastructure Manager (UIM) and VMware vCenter.

Scope
This paper demonstrates how the IPsoft managed service automates and reports on monitoring and repairing of incidents on Vblock Infrastructure Platforms. The validation tests documented in this paper address a specific set of use cases for automated monitoring and repair of level 1 and 2 support infrastructure incidents. The specific goals of this paper are to:

- Describe how IPsoft performs automated remediation of incidents on Vblock Infrastructure Platforms
- Define the core metrics most useful for monitoring a Vblock platform environment
- Provide setup and configuration information for the solution
- Provide sample output showing IPsoft capabilities

Audience
This paper is intended for enterprise customers (CIOs) who are interested in and/or working with managed services. In addition, Infrastructure and Operations VPs, Directors, and Managers, and any technical management responsible for defining IT strategy will benefit from reading this paper. Sales engineers, field consultants, professional services, IT managers, infrastructure architects, partner engineers, and customers may also find the content useful.
## Terminology

<table>
<thead>
<tr>
<th>Term</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Autonomics</td>
<td>Algorithms designed to mirror the standard operating procedures performed by IT services personnel. Autonomic computing reduces the need for human intervention and eliminates having to resolve the same issue manually more than once. Detection, resolution, and escalation take place at machine speed.</td>
</tr>
<tr>
<td>Converged Infrastructure</td>
<td>A converged infrastructure packages multiple information technology (IT) components into a single, optimized computing solution. Components of a converged infrastructure solution include servers, data storage devices, virtualization, networking equipment and software for IT infrastructure management, automation and orchestration.</td>
</tr>
<tr>
<td>IT as a Service</td>
<td>IT as a Service (ITaaS) refers to a method by which an IT organization or service provider delivers well-defined services delineated at a clear business interface, usually to multiple consumers and/or different business units. Delivering services in this manner, as opposed to operating as pure infrastructure administrators, allows an IT organization to increase underlying resource utilization and reduce associated operational costs. It also enables IT to offer pay-per-use business consumption.</td>
</tr>
<tr>
<td>Level 1 Support Incident</td>
<td>Level 1 incidents are handled by Level 1 support. The responsibility of Level 1 support is to register and classify received incidents and undertake an immediate effort to restore a failed IT service as quickly as possible. If no solution can be achieved, Level 1 support will transfer the incident to Level 2 support.</td>
</tr>
<tr>
<td>Level 2 Support Incident</td>
<td>Level 2 support takes over incidents that cannot be solved immediately by Level 1 support. If necessary, it requests external support from hardware or software manufacturers.</td>
</tr>
<tr>
<td>Managed Service</td>
<td>Managed Service refers to the assumption of a customer’s 24x7 IT and/or business process environment and operations by a third-party service provider, under the governance of a Service Level Agreement (SLA) agreed upon by both parties. A Managed Service may also involve the transfer of IT assets, staff, or service to an outsourced location.</td>
</tr>
<tr>
<td>Principle of Least Privilege</td>
<td>The principle of least privilege is the practice of limiting access to the minimal level that will allow normal functioning. Applied to users, the principle of least privilege translates to giving people the lowest level of user rights that they can have and still do their jobs. The principle is also applied to things other than people, including programs and processes.</td>
</tr>
</tbody>
</table>
Technology Overview

Working with IPsoft, VCE has validated the IPsoft managed service tool for automated monitoring and repairing of IT services and support incidents in a Vblock platform converged infrastructure environment.

Vblock™ Infrastructure Platforms

Vblock Infrastructure Platforms provide pre-engineered, production-ready (fully tested) virtualized infrastructure components, including the best of breed technologies from Cisco, EMC, and VMware. Vblock Infrastructure Platforms are designed and built to satisfy a broad range of specific customer implementation requirements. The current Vblock platforms include:

- **Vblock Series 700**: Designed for deployments of very large numbers of virtual machines and users. Ideally suited to meet the higher performance and availability requirements of an enterprise’s business critical applications.
- **Vblock Series 300**: Designed to address a wide spectrum of virtual machines, users, and applications. Ideally suited to achieve the scale required in both private and public cloud environments.

The table below lists components of each Vblock platform.

<table>
<thead>
<tr>
<th>Category</th>
<th>Vblock Series 300</th>
<th>Vblock Series 700</th>
</tr>
</thead>
<tbody>
<tr>
<td>Compute</td>
<td>Cisco UCS&lt;br&gt;• B200M2&lt;br&gt;• B250M2&lt;br&gt;• B440M1&lt;br&gt;• B230M1</td>
<td>Cisco UCS&lt;br&gt;• B200M2&lt;br&gt;• B250M2&lt;br&gt;• B440M1&lt;br&gt;• B230M1</td>
</tr>
<tr>
<td>Storage</td>
<td>&lt;ul&gt;&lt;li&gt;300 HX&lt;br&gt;EMC VNX 7500&lt;/li&gt;&lt;li&gt;300GX&lt;br&gt;EMC VNX 5700&lt;/li&gt;&lt;li&gt;300FX&lt;br&gt;EMC VNX 5500&lt;/li&gt;&lt;li&gt;300 EX&lt;br&gt;EMC VNX 5300&lt;/li&gt;&lt;/ul&gt;</td>
<td>700MX&lt;br&gt;EMC Symmetrix VMAX&lt;br&gt;&lt;ul&gt;&lt;li&gt;Drive Types&lt;/li&gt;&lt;li&gt;EFD&lt;/li&gt;&lt;li&gt;SATA&lt;/li&gt;&lt;li&gt;NL-SAS&lt;/li&gt;&lt;/ul&gt;</td>
</tr>
<tr>
<td>Virtualization</td>
<td>VMware vSphere 4 Enterprise Plus Suite</td>
<td></td>
</tr>
<tr>
<td>Compute/Networking</td>
<td>Cisco UCS Manager/Cisco Fabric Manager</td>
<td></td>
</tr>
<tr>
<td>Storage Management</td>
<td>EMC Unisphere&lt;sup&gt;®&lt;/sup&gt;</td>
<td>EMC Symmetrix Management Console</td>
</tr>
<tr>
<td>Category</td>
<td>Vblock Series 300</td>
<td>Vblock Series 700</td>
</tr>
<tr>
<td>---------------</td>
<td>-------------------------------------------------------</td>
<td>-------------------------------------------------------</td>
</tr>
<tr>
<td>Orchestration</td>
<td>EMC Ionix Unified Infrastructure Manager (UIM) 2.1</td>
<td>Advanced Management Pod (AMP) (optional)</td>
</tr>
<tr>
<td>Security</td>
<td>Individual component security tools and protocols</td>
<td>RSA enVision, RSA SecurID® (both optional)</td>
</tr>
</tbody>
</table>

**IPsoft Tools**

IPsoft provides managed infrastructure service and enterprise applications support through a catalog of proprietary monitoring and autonomic service management components that conform to the ITIL v3 standard.

IPcenter, IPsoft’s management portal, transforms businesses through automation. IPcenter is a service delivery portal that manages client technology environments. It provides tactical and strategic views of each managed component across all layers, in real-time, through a single, customizable Web-based portal. Features include:

- System monitoring - proactively detects system and network problems and initiates intelligent agents to automatically correct problems. It issues automatic alerts when automatic resolution is not possible.
- Problem reporting – logs all problems into a single problem report and ticket management function; problems can be reported by a hotline, email, or direct Web entry.
- Asset management – provides a central Configuration Management Database (CMDB) that stores all information about installed hardware and software assets. Most assets can be drilled down to check current and historical performance
- Network status utilization – network maps are available for real-time views of status and use, with the ability to drill down on components for more information.

IPcenter is an ITIL v3-aligned service portal, meaning it is aligned to the key services of an IT operation, including service design, service transition, service operation, continual service improvement, service delivery management, and service technology. It has operational processes embedded within it, ensuring processing adherence and execution, including the following ITIL service operation and service transition activities: incident management process, change management process, event management process, and problem management process.
IPcenter provides through its tools a consolidated end-to-end automation framework that encompasses level 1 and level 2 support activities. Even when automation cannot completely remediate a problem, it gathers information to facilitate IT support personnel activities. The complete IPcenter kit contains over 40 ITIL-aligned components that can be used to help the Vblock administrator manage their systems. The diagram below highlights key IPcenter components used in this validation test:

**IPmon**
IPmon provides monitoring, embedded intelligence, system, and network management capabilities. It monitors network services and host resources through a simple plug-in design and enables development of customer service checks. The checks run in parallel mode to allow optimal scalability for a growing infrastructure.

**IPim**
IPim is IPsoft’s incident management application. It tracks incidents through the integrated IPradar workflow system, ensuring the progression of an incident from inception to satisfactory resolution in the shortest possible time. It provides abilities for complete audit and transparency into how events are handled.

**IPradar**
IPradar is IPsoft’s workflow/queue management system. It provides you with control of your entire operations as you can view, in a consolidated framework, all exceptions, events, alerts, trouble tickets, and project tasks in your system. This helps ensure all tasks are executed within committed timelines.

**IPautomata**
IPautomata is IPsoft's toolkit for building intelligent software agents to facilitate data gathering, management, and remediation of detected issues. It learns about your systems and networks and can generate autonomic agents that self-correct exceptions in your environment. You can view automata tasks assigned to you, search for particular automata, view automata details, and – if you have permissions – design custom automata.

IPautomata is a “state space engine” that learns and executes remediation sequences in response to an incoming event. Execution can be automatic or manually triggered by an engineer. All IPautomata executions are fully logged and can be viewed, or exported as text, through the Web user interface. IPautomata provides a framework that enables all internal and external components to interface with each other. It logs the following for each execution:

- Start and end time of execution
- User who initiated the process (if manual)
- All variable values
- All connection information
- Status, including reason for failure
- Associated IPsoft ticket/event
- The command for each state
Solution Architecture

This paper demonstrates how IPsoft automates and reports on monitoring and repairing of incidents on Vblock Infrastructure Platforms. Although the solution was tested specifically on Vblock 700, it applies to all Vblock Infrastructure Platforms.

IPsoft manages and monitors Vblock Infrastructure Platforms with IPcenter v3, IPsoft's operational service delivery portal. IPcenter includes IPmon, a monitoring appliance that incorporates features of a proxy for automation initiated by IPcenter. IPmon can be an appliance or, in this case, a virtual machine running Red Hat Linux installed on the Vblock Platform Advanced Management Pod (AMP). The core of the IPcenter portal typically resides elsewhere on the other end of a virtual private network (VPN) tunnel. This segregation requires bi-directional communication between IPcenter and IPmon and a VPN connection must be established.

The diagram below shows an example of traffic flow. The main design principals are to ensure enforcement of the principle of least privilege and to maximize the efficiency of all communications while ensuring security.

Note: Although there was one IPmon server used in this validation test, there may be multiple IPmon servers involved in other configurations for scalability purposes.

IPmon initiates monitoring. It sends back to IPcenter two types of traffic:

- Events that breach defined thresholds (alerts)
- Performance data for reporting and graphing purposes

IPcenter initiates automation, using the IPmon server as a secured proxy to initiate connections to the client environment. Connections from IPmon can be made through a number of protocols depending on the device type; Secure Shell (SSH) and IPremote are the most popular connection methods used.
IPmon requires access to all services to be monitored, from Internet Control Message Protocol (ICMP) echo request to device-specific connection protocols and command line access. Although most monitoring is accomplished through Simple Network Management Protocol (SNMP) or IPremote (IPsoft’s client-side monitoring agent), IPmon may require access to the Vblock infrastructure through any of a number of protocols required for monitoring and automation including HTTP, SSH, Telnet, SNMP, or native API ports. Traffic back to the IPsoft facility is subject to the IPsoft security specification, available separately.

Internal and external access to IPmon is restricted to IPsoft employees. It is an appliance (virtual or physical) for which only IPsoft is responsible, including remote monitoring.

Once the IPmon servers are installed and configured, IPcenter discovers all Vblock platform components and applies an element-specific monitoring template to each component. For example, there is a specific template for the VMAX storage array in a Vblock 700; there are also templates for UCS blades, Cisco switches, and so forth. Additional customization and recovery actions can be manually configured.

IPsoft’s automated repair capabilities are central to this solution and depend on IPautomata and the automation library. IPcenter creates and builds its own automation library by monitoring, tracking, and learning from human intervention. It creates automated resolutions:

- Through a manual process, where recovery action steps are created in the automation library and executed when needed
- By recording the steps followed to recover an incident and inserting the steps into the automation library
- Through a combination of both manual process and recording of steps

When an event is identified, be it from monitoring, a user request, or anything else, IPcenter leverages the automation library and CMDB to correlate events intelligently. Even when automation cannot completely remediate a problem, it supports human engineering activities by gathering information.

**Hardware and Software Resources**
The following table lists the hardware and software resources used to validate the solution:

<table>
<thead>
<tr>
<th>Resource</th>
<th>Description</th>
</tr>
</thead>
</table>
| Vblock 700 | ▪ Cisco UCS blade pack  
 ▪ Cisco Fabric Interconnect 6140  
 ▪ Cisco MDS 9506  
 ▪ EMC Symmetrix VMAX  
 ▪ VMware vSphere 4.0 U1 Enterprise plus build 208167  
 ▪ VMware vCenter Server 4.0 U1 build 186498  
 ▪ EMC PowerPath/VE |
| AMP | ▪ Red Hat Linux RHET 5.5 (64 bit)  
 ▪ IPmon |
Solution Testing and Validation

This solution demonstrates how IPcenter detects and remediates incidents on Vblock Infrastructure Platform components. The diagram below shows the Vblock platform components that can be monitored.

Note: The diagram above illustrates an example of a Vblock 700. Not all Vblock Infrastructure Platforms will look like this.
The table below shows what was monitored for the solution test environment.

<table>
<thead>
<tr>
<th>What to Monitor</th>
<th>Category</th>
<th>Vblock 700 Component</th>
</tr>
</thead>
<tbody>
<tr>
<td>Storage</td>
<td>Storage</td>
<td>EMC Symmetrix VMAX-iSCSI and SAN</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Cisco MDS Aggregation SAN switch</td>
</tr>
<tr>
<td>Network Switches</td>
<td>Network</td>
<td>Cisco Nexus 1000V</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Cisco Nexus 5020 data center switches</td>
</tr>
<tr>
<td>UCS Blades/Chassis</td>
<td>Compute</td>
<td>Cisco 6140 fabric interconnects</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Cisco UCS 5108 chassis</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Cisco UCS B-series blade server packs</td>
</tr>
<tr>
<td>Virtualization</td>
<td>Virtualization</td>
<td>VMware vSphere / vCenter</td>
</tr>
</tbody>
</table>

**Testing Objectives**

The main objective of the validation exercise was to demonstrate IPcenter monitoring of all the Vblock Infrastructure Platform components and repairing of any encountered incidents automatically.

Specifically, these critical elements were looked at:

- How failures are detected
- Troubleshooting
- Mitigation
- Validation
- How failures are communicated
- How failures are documented
- What happens if an incident is caused by another failure
- Remediation and recovery process

During testing, each incident went through the following lifecycle in IPcenter:
These test cases were covered:

- Application/event correlation by testing an event affecting both a database and an application
- Simulate a VMware VM performance issue by testing performance with low memory
- Simulate a system crash by turning off a virtual machine
- Simulate a Symmetrix VMAX storage configuration issue by causing the VMAX dial system to malfunction
- Simulate a UCS chassis issue by shutting off a virtual network interface card (vNIC)
- Simulate a UCS blade failure by powering off a blade
- Simulate a network interface failure by shutting off a Cisco 5020 network switch
- Simulate a switch port interface failure by shutting off an FC port on a Cisco MDS switch

**Test Results**

IPcenter successfully completed all test cases and remedied all system faults as expected. The test cases demonstrated the following:

- **Monitoring:** IPcenter tool connected to Vblock platform components and monitored the devices
- **Failure handling:** Various system faults were simulated to verify that IPcenter was able to detect each fault and update device statuses accordingly.
- **Remediation:** IPcenter repaired faults, where able, and device statuses were returned to normal upon completion.

The following results were observed for each test case:

<table>
<thead>
<tr>
<th>Vblock Platform Component Monitored</th>
<th>What Was Tested</th>
<th>What IPcenter Did</th>
</tr>
</thead>
<tbody>
<tr>
<td>Application/event correlation</td>
<td>Application/event correlation was tested through an event affecting the database and an application (application/event correlation). An application required a connection to a MySQL database. The interface on which MySQL listens was taken down, breaking both the database and the application.</td>
<td>IPmon showed MySQL interface down, application down, MySQL database down, but the application server interface up. IPradar only receives a “HOST DOWN for MySQL Interface” message, which is the root cause of the issue. IPradars reacted to the alert. It identified an alternate network interface on the device and moved the IP for the MySQL server to the other interface. MySQL database recovered and the application recovered in IPmon.</td>
</tr>
<tr>
<td>VMware virtualization</td>
<td>We simulated a VMware VM performance issue by testing performance with low memory.</td>
<td>IPmon showed high memory utilization for the virtual machine. IPradar received the memory usage notification. IPradars picked up the notification and requested for approval to increase the memory. Approval was granted through a web form (could be through a telephone call or email). IPradars connected to the Virtual Center console, allocated additional memory to the machine, restarted the virtual machine, and verified that the additional memory was there.</td>
</tr>
<tr>
<td></td>
<td>We simulated a system crash by turning off a virtual machine from the Virtual Center</td>
<td>IPmon detected that the host was down. IPradar received the host down notification. IPradars picked up the notification,</td>
</tr>
<tr>
<td>Vblock Platform Component Monitored</td>
<td>What Was Tested</td>
<td>What IPcenter Did</td>
</tr>
<tr>
<td>-----------------------------------</td>
<td>---------------------------------------------------------------------------------</td>
<td>--------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Symmetrix VMAX storage</td>
<td>We simulated a Symmetrix VMAX storage physical configuration issue by causing the VMAX dial system to malfunction.</td>
<td>IPmon detected that VMAX dial system was malfunctioning. IPradar received the Symmetrix Event Notification alarm. IPautomata picked up the notification, connected to the VMAX, gathered current configuration statistics, and created a ticket detailing the error found and the details gathered in real-time from the VMAX. It submitted the ticket to EMC support.</td>
</tr>
<tr>
<td>UCS chassis</td>
<td>We simulated a UCS chassis issue by shutting off a vNIC on a UCS chassis.</td>
<td>IPmon detected that the vNIC port was down. IPradar received the vNIC port down notification. IPautomata picked up the notification, connected to the UCS blade chassis console, and re-enabled the port.</td>
</tr>
<tr>
<td>UCS blade</td>
<td>We simulated a UCS blade failure by powering off a blade.</td>
<td>IPmon detected that the host was down. IPradar received the host down notification. IPautomata picked up the notification and powered up the blade.</td>
</tr>
<tr>
<td>Network interface</td>
<td>We simulated a network interface failure by shutting off an FC port on a Cisco 5020 network switch.</td>
<td>IPmon detected that the FC port was down. IPradar received the FC port down notification. IPautomata picked up the notification, connected to the 5020 switch, and re-enabled the port.</td>
</tr>
<tr>
<td>Switch port interface</td>
<td>We simulated a switch port interface failure by shutting off an FC port on a Cisco MDS switch.</td>
<td>IPmon detected that the FC port was down. IPradar received the FC port down notification. IPautomata picked up the notification, connected to the MDS switch, and re-enabled the port.</td>
</tr>
</tbody>
</table>
Example Test Case Scenario: An FC Port on the Cisco MDS Switch was Shut Off
This section shows the detailed results.

**Step 1:** The IPcenter main console shows the network switch port status before a fault occurred. Note that the 111 monitors are all reporting a status of green (OK):
Step 2: IPmon picked up a critical alert for the MDS port. Here is the alert for the port failure:

Step 3: A ticket was created for the alert. Detailed information about the alert appears on the right:
Step 4: IPautomata executes a successful automated recovery. Note the Success status:

Step 5: After IPautomata completes recovery, the network port state returns to a green OK status:
Step 6: IPcenter shows that the incident is completely recovered:

Step 7: The IPcenter main console shows that the error has been cleared. The port status shows a green OK status:
Conclusion

Companies are leveraging converged infrastructures for cost savings and to provide predictable, scalable, and flexible services. With this comes the abstraction of a converged infrastructure and the volume of data from the number and variety of services deployed on it.

Companies today are looking to shift from manual IT maintenance and support activities to intelligent automation. Automating common troubleshooting tasks and the steps to resolve common issues allows IT operations to focus on more complex issues and higher value services.

As companies adopt the converged infrastructure, they will have to shift from manual IT maintenance to automating whatever tasks they can. Reducing Level 1 and Level 2 support calls is a good starting point.

This solution demonstrates the simplicity and efficiency of using IPsoft’s managed service to monitor and repair incidents that occur on Vblock Infrastructure Platform. IPsoft offers unique technology that automatically detects and remediates exceptions in complex IT environments. Through several test cases, we validated the identification and resolution of internal Vblock platform incidents, and observed management of the notification and escalation processes.

Bringing network, compute, storage, virtualization, and management into one converged infrastructure with Vblock Infrastructure Platforms delivered with IPsoft’s autonomic management tools allows for significant benefits. It provides faster identification of incidents, driving quicker resolution through correlation, root cause, and impact analysis, which allows IT organizations to consistently exceed service level agreements negotiated with the customer.

Next Steps

To learn more about this and other solutions, contact a VCE representative or visit www.vce.com.

To learn more about IPsoft managed services, contact IPsoft Corporation or visit http://www.ipsoft.com.
ABOUT VCE
VCE, the Virtual Computing Environment Company formed by Cisco and EMC with investments from VMware and Intel, accelerates the adoption of converged infrastructure and cloud-based computing models that dramatically reduce the cost of IT while improving time to market for our customers. VCE, through the Vblock platform, delivers the industry's first completely integrated IT offering with end-to-end vendor accountability. VCE’s prepackaged solutions are available through an extensive partner network, and cover horizontal applications, vertical industry offerings, and application development environments, allowing customers to focus on business innovation instead of integrating, validating and managing IT infrastructure.
For more information, go to www.vce.com.

ABOUT IPSOFT
IPsoft is a next generation managed services company providing comprehensive support services to corporations worldwide. The company is headquartered in New York City, with offices in San Jose, CA; Chicago, IL; London; Frankfurt; Stockholm; Amsterdam and Bangalore.
For more information, go to www.ipsoft.com.

THE INFORMATION IN THIS PUBLICATION IS PROVIDED "AS IS." VCE MAKES NO REPRESENTATIONS OR WARRANTIES OF ANY KIND WITH RESPECT TO THE INFORMATION IN THIS PUBLICATION, AND SPECIFICALLY DISCLAIMS IMPLIED WARRANTIES OR MECHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE.