Hotspot Diagnosis on Logical Level

Bo Yang
IBM China Research Lab
Beijing, China
yangbbo@cn.ibm.com

Jeff Kephart
IBM Thomas J. Watson Research Center
Hawthorne, NY, USA
kephart@us.ibm.com

Hendrik Hamann
IBM Thomas J. Watson Research Center
Yorktown, NY, USA
hendrikh@us.ibm.com

Stephan Barabasi
IBM Green Innovations Data Center
Southbury, CT, USA
barabasi@us.ibm.com

Abstract—**Hotspots in data center have been attributed to an increase in equipment failures, which causes system down time and business loss. In maintenance of IT equipment, removing hotspot with minimal cooling power cost is both ecological and financial benefits. Thus, identifying root cause of hotspots in data center is essential. A variety of factors can cause the issue, and therefore, diagnosing root cause of hotspot for removing and preventing it becomes complicated. This paper proposes a technique which supports diagnose the hotspot from logical level relative to physical conditions. In the proposed technique, performance and configuration data of each potential factor are analyzed with hotspot trochoid automatically. Effect and impact of the factor are synthesis evaluated for each component to diagnose whether it is related to the hotspot emerging or not. The diagnosis results are collected for suspects of creating hotspot in the target ambient, and then, the suspects in the whole system can be ranked for helping to identify the root cause. Hotspot diagnosis from the logical level is also useful to improve the hotspot diagnosis on other external physical conditions factors, when the logical causes are excluded by the proposed approach.**

Keywords- Hotspot Diagnosis, Green Data Center, Correlation Analysis, Monitoring, Root Cause Analysis

I. INTRODUCTION

Hotspots in data center refer to server input air conditions that are either too hot or too dry, according to the American Society of Heating, Refrigerating and Air-Conditioning Engineers (ASHRAE) TC 9.9 guidelines[1].

The recently revised ASHRAE environmental guidelines recommend the input air environment with temperature limits from 18 degrees Celsius (64.4 degrees Fahrenheit) to 27 degrees Celsius (80.6 degrees Fahrenheit), and humidity limits to less than 60% with the lower and upper dew point temperatures of 5.5 degrees Celsius (41.9 degrees Fahrenheit) and 15 degrees Celsius (59 degrees Fahrenheit). Hotspots occur when the environment at the air input to the server, storage device, communications router or other computer equipment is higher in temperature (above 27 degrees Celsius) or lower in moisture content than recommended (below 5.5 degrees Celsius Dew Point).

Major equipment manufacturers that helped to create these new guidelines have agreed that they're acceptable for the long-term reliability and performance of their equipment. One side, it is the hardware manufacturer's responsibility to ensure the equipment properly works with recommended air environment. On the other side, it's the user's responsibility to maintain the proper environment at the intake of the computer equipment.

However, IT infrastructure in data center is highly complex and dynamic with business changing, there are a large number of factors that may cause hotspots such as air-leakage through holes in the raised access floor, the lay-out of the computer equipment, air-conditioning system used. Therefore, diagnosis and removal of the hotspots become complicated. Due to the increasing complexity and scale of data center, hotspot diagnosis that relies on the expert's experiences has been facing the limit. The automated support for hotspot diagnosis is necessary.

Comparing with traditional analysis on physical root cause of hotspot based on data center architecture design, this paper proposes a technique which supports identifying the logical root cause of hotspot. Causes on logical level are easy to be removed for the data center maintenance with less hardware or ambient reconstruction. In the proposed technique, each factor on component in the target system is automatically evaluated by analyzing relationships with temperature change. The correlation coefficient of each component is individual assessed, and the analysis results of components are collected and synthesized analysis for the host equipment of components to diagnose whether the suspect is related to the hotspot emerging or not.

II. HOTSPOT PROBLEM REVIEW

When a hotspot is detected, administrator in data center needs to analyze what are the causes of abnormal temperature change. The primary cause is not enough cooling capability to provide enough cold air to the cold aisle, additional cooling units are expected. Interestingly, too much cooling capacity can be a significant contributor to the existence of hotspots. If the heat load in the room requires eight cooling units and there are 10 or 12 installed, each of the 10 or 12 units is doing less work than if there were only eight. This decreases the temperature

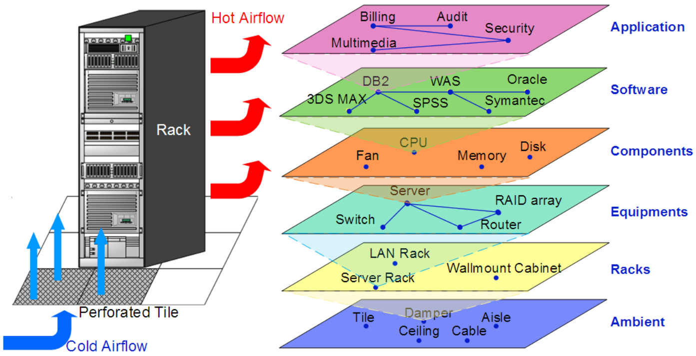

Figure 1. Six layers model for hotspot associated factors

drop across the units, and the under-floor temperature is higher, which can contribute to additional hotspots when the static pressure is also too low [2]. Even worse is the more cooling systems, the more energy cost would spend.

Figure 1 illuminates a simplified cooling system work model in data center. Cold airflow is provided to equipment from perforated tile in cold aisle, and hot air is exhausted to hot aisle. As to the simple airflow exchange system, we can divide the factors of creating hotspot into 6 levels. First level is application level that includes various applications, the workload of applications is the source to drive IT equipment work, consume energy and generate heat. Second level is software level that is the media to support application works by leveraging various components of hardware. The third level is components level, which includes atom unit of hardware. The component is the real customer of energy and producer of heat. If the generating heat allows negative, cooling unit such as Fan can be assigned in this level. The fourth level is equipments level that includes macro hardware item with independent function such as server, router, switch etc. The general management unit in data center, rack, can be classified into the fifth level, which provides the base environment and layout for IT equipment. The last level, ambient level in data center is composed with physical unit such as tile, ceiling, damper etc. With this classification, it is easy to clarify the root cause of hotspot. And it can help to design more relevant solution for diagnosing and remedying hotspot.

There are several prior works for supporting the hotspot management. These works including hotspot monitoring [3], data center reconstruct [4] and leveraging various cooling system [5].

Sharma et al. [6] report that power consumption for cooling a data center can be reduced significantly by designing the air flow path to prevent mixing of hot and cold air and present non-dimensional parameter based models of the air flow inside aisles. D. Brooks et al. [7] and M. Huang et al. [8] investigated more sophisticated dynamic thermal management (DTM) approaches to degrade performance gracefully by modulating power-intensive chip functions.

Obviously, most of them focus on the level 3~6, we can call them the physical or "hard" factor for hotspot. However, the hotspot management can not always achieve sufficient performance. If the business and its applications are dynamic changing and expanding, hotspot cannot be managed with good manner under static IT planning and data center reconstruct.

If the hot source is caused by performing extreme workload of software and application on server, it is hard to identify and remediate it with complex and dynamic IT infrastructure composed by thousands of software components in data center. A simplified solution with virtualization technology is popular in recent years [9][10]. However, this solution doesn't improve the diagnosis of hotspot, it is more like central management for distributed application on single physical host. Furthermore, when many virtualization servers host on same location, it increases the complexity for hot spot diagnosis and remediation.

RK Sharma et al [11] and M. Justin et al. [12] proposed modulating temperature by migrating workload among servers to thermally balance the load distribution across a programmable data center. It provides another solution to remove the hotspot by balance hot sources, besides enhancing cooling system efficiency.

However, excepting hotspot remediation and physical cause diagnosis, there is little work to identify the real root cause of hot source behind the phenomena of temperature change. In this paper, we are focusing on the diagnosing the "logical" or logical root cause of hotspot relative to physical condition factors in data center.

III. HOTSPOT DIAGNOSIS ON LOGICAL LEVEL

The proposed technique is designed for detected hotspot and supports the root cause diagnosis for logical factors. Each component in the target system is automatically evaluated for impact factor (IF) by correlation analysis algorithm. While the automatic evaluation which includes the IF and the ranking of the potential root causes are collected.

The diagnosis system assesses two kinds of root cause for hotspot. The first impact (IIF, Individual Impact Factor) is assessed based on the likelihood of component on server for a temperature change. The granularity of root cause is component of server, such as CPU, Memory, Disk, Software, etc.

The IIF is assessed as high when the attribute has an effect on the temperature change on a target point.

The second impact (MIF, Multiple Impact Factor) is assessed based on the likelihood of several components of server for a temperature change. It is useful to identify the hotspot caused by the server, which is server-granularity diagnosis. The MIF is assessed as high when several components co-contribute effect on the temperature change on a target point.

The two kinds of impact are collected from each of the servers and are used to rank the root cause for a hotspot. Additionally, the likelihoods can support deciding whether the hotspot is caused by server or other external factors.

Figure 2 illustrates how the system diagnoses root causes based on the two impacts for a detected hotspot on a heat map of data center. There is a hotspot *H1* is detected and is reported on the monitoring system (two servers, *S1* and *S2* are supposed

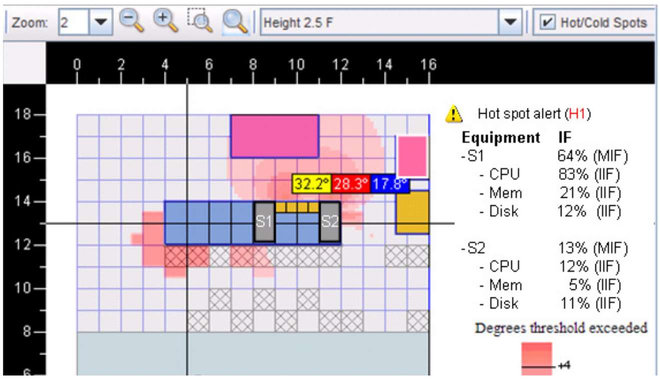

Figure 2. Diagnosing root cause based on impact factor analysis

to be suspects for hotspot *H1*. Suppose hotspot is changing with time series that indicates a consequence for a change in environment, and Distance *D* will affect the efficiency of hot source for a hotspot.

The right side of figure 2 shows a situation where the CPU-utilization, Memory availability and Disk activity underlying *S1* are analyzed as suspects with IIF evaluation respectively. Based on the atom-analysis, the IIF of components is synthesis analyzed to assess the MIF of *S1*. In this case, high CPU-utilization is diagnosed as the main root cause for hotspot *H1*. As hot source, *S1*'s contribution for *H1* based on MIF evaluation is diagnosed as the No.1 suspect in the ranking of all candidates. When drill down the configuration items on *S1*, a process "cidaemon.exe" is detected who occupying 98% CPU and its changing profile has high IIF value 83% to the hotspot than other processes. Thus, the real root cause of hotspot behind the phenomenon of high CPU utilization can be locked on the software.

On the other hand, the assessment on *S2* indicates that it does not show a correlation with *H1*'s occurring effectively. Since both IIF and MIF are not assessed as high at *S2*, these likelihoods are insufficient for identifying *S2* as the root cause for *H1*.

However, the hotspot could be created by multiple factors and causes, every hot source around it should be checked before the real root causes has been identified. Therefore, we propose leverage logical-physical components mapping to help administrator to diagnose the real root cause with automatic method of analyzing and ranking suspects of root causes.

The analysis result includes how many servers will be involved to contribute the hotspot, what are the main components of equipment in the activity, where is the position of the factor in suspect list. The analysis result can be accessed by web service response and stored in diagnosis system for supporting generating report, audit and making decision.

IV. IMPLEMENTATION

In this paper, we aim at finding out root causes of hotspot from logical level with our logical-physical mapping diagnosis system. Our approach implements root cause analysis from two levels of abstraction: the logical-level and the IT infrastructure physical-level.

In the implementation, we leveraging correlation coefficient to evaluate impact of hotspot associated factors. With the history data of monitoring, individual impact factor (IIF) of factor x on hotspot y is estimated as below:

$$IIF(x,y) = \frac{Cov(x,y)}{\sqrt{Var(x)Var(y)}} \quad (1)$$

Where $Cov(x,y)$ is Covariance of x and y, $Var(x)$ is Variance of x.

As to Multiple Impact Factor (MIF) Analysis, temperature y is supposed to be "affected" not by just one cause x, but by several factors $\{x_j\}$. In this paper, we use linear regression to construct the relationship between factors $\{x_j\}$ and hotspot y. We assume that the linear relation is:

$$y\hat{} = \beta_0 + \beta_1 x_1 + \beta_2 x_2 + \ldots + \beta_p x_p + \varepsilon(x) \quad (2)$$

Where p is the number of the components on equipment, and $\varepsilon(x)$ is a random noise (*e.g.* measurement errors).

And the monitoring data used to analysis is made of n measurements y_i, $i = 1,2,\ldots,n$ taken for n sets of factors $\{x_{ij}\}$ of the independent variables:

$$y_i = \beta_0 + \beta_1 x_{i1} + \beta_2 x_{i2} + \ldots + \beta_p x_{ip} + \varepsilon(x)_i \quad (3)$$

In this expression, β_i are fixed but unknown numbers, and $\varepsilon(x)_i$ are n realizations of the $\varepsilon(x)$.

When β_i is calculated with least square method, multiple correlation coefficient R will be estimated as equation (4):

$$R = \sqrt{1 - \frac{SSE}{SST}} \quad (4)$$

Where

$$SSE = \sum_{i=1}^{n}(y_i - \hat{y}_i)^2, \quad SST = \sum_{i=1}^{n}(y_i - \bar{y})^2 \quad (5)$$

And MIF is calculated with following equation:

$$MIF = W(d) \times R \quad (6)$$

Where $W(d)$ is a weight of distance affection on hotspot for the equipment.

However, not all of components are involved to contribute to the hotspot, filtering innocent components before evaluating suspect ranking can improve the analysis efficiency with computing β_i. Thus, we introduce *F*-test as filter module for filtering innocent factor. With the *F*-test, the dimension of components involved in hotspot diagnosis is reduced. It benefits to improve diagnosis efficiency and filter noise data.

In our solution, the reduced model is accumulated and reused to evaluate IIF and MIF on similar equipment as a rule in future.

V. CASE STUDY

Simulation environment includes 23 servers and 2 racks. Double-blind test is used to verify if the proposed method can find out root causes that examiner used to create hot spot.

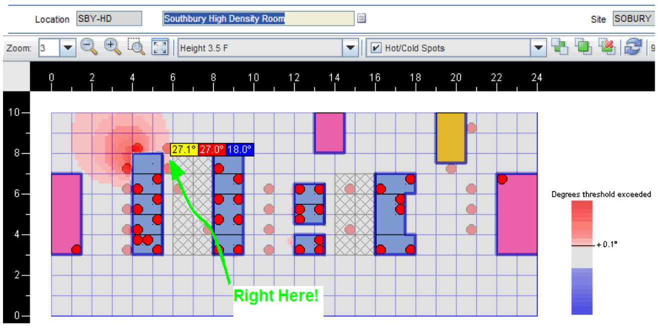

Figure 3. Hotspot crept around from the exhaust side to the cold aisle

IBM Tivoli Monitoring is used to collect the sensor data in data center, and configuration data is discovered by Tivoli Manager Application Dependency Discovery Manager.

We have been able to see a hotspot form on the air intake side of the Rack 1-5 ("Rack 1-5" refers to rack on the left-top nearby hotspot in figure 1). The hotspot crept around from the exhaust side to the cold aisle as shown in figure 3. We saw the interpolated temperature rise to 27.1 degrees Celsius on the intake side of Rack 1-5.

TABLE I. FACTOR LIST FOR HOTSPOT DIAGNOSIS

Factor No.	Name	Associated Component	Parent Rule
1	Busy_CPU	CPU	Server
2	Write_sect_per_sec	Disk	Server
3	Read_sect_per_sec	Disk	Server
4	Cpu_Util for Disk	CPU	Server

For each candidate that might be the root cause for a hotspot on Rack 1-5 sensor, the factors in table I of each server was import to the diagnosis system for analyzing the MIF with the monitoring data of temperature on sensor of Rack 1-5B, when data preprocessing is introduced to filter metrics that no correlation with the temperature changes. Suspect ranking list for the experiment that is concluded by the proposed approach is shown in table II.

TABLE II. MIF VALUE FOR EACH SERVER

Ranking No.	Server Name	MIF for hotspot nearby Rack 1-5
1	vmrhelres02	85%
2	vmrhelres08	84%
3	vmrhelres07	84%
4	vmrhelres06	84%
21	isfusio01dev	35%
22	isdirector-dev	34%
23	istdi01dev	28%

With analysis on lots of experiments, we noticed that potential root causes are always included in a subset of servers that have high correlation with hotspot change profile. When we applied cluster analysis to identify the subset in the case, 48%~80% is the margin between suspects of creating hotspot and other servers. Therefore, 80% is the suggested value for us in the paper to set up in the case study.

Table II indicates that there are 14 servers get higher MIF value than other servers distinctly. They are the top suspects for hotspot nearby Rack 1-5, if we set the threshold is 80% as confidence indicator to identify root cause. In fact, these servers are used to create the hotspot by running a CPU burning program in the experiment indeed. Therefore, the result demonstrate that analytics with MIF evaluation is workable to diagnose the logical root cause of hotspot as automatic solution.

VI. CONCLUSION

This paper has proposed the technique which supports diagnose the root cause and their internal details. The diagnosis on logical root cause is to assess the two likelihoods. The first likelihood is assessed based on the individual correlation of a single factor. The root cause by the multiple factors is identified by the second likelihood which is assessed based on the multiple impact factor analysis. The likelihoods are collected from each of the equipment and the root cause of the hotspot by other physical factor can be identified. The correlation degree between factors and hotspot is evaluated via automatic analyzing, and therefore, proper ranking of suspect for the hotspot can be obtained by the proposed technique. Additionally, actions required and ways to remedy the hotspot can be indicated.

Improving the efficiency of the technique is one of the future works. The other future work is that analysis of the affected applications, servers and business by emerging hotspot to control the risk before unexpected outage arising. We expect that such analytics are useful for reduce the cost of IT maintenance in data center.

VII. ACKNOWLEDGMENT

We acknowledge our colleagues in IBM Research for their suggestions and help on experiment for the project, especially acknowledge Suzanne McIntosh, Jonathan Lenchner, Metin Feridun, and Mike Nidd.

We also acknowledge the reviewers for their helpful comments, leading to better presentation of the paper.

REFERENCES

[1] ASHRAE TC 9.9 2008, Thermal Guidelines for Data Processing Environments, 2008, available at http://tc99.ashraetcs.org/

[2] Robert (Dr. Bob) Sullivan, How to identify and remediate data center hot spots, SearchDataCenter, Aug. 2009, available at http://searchdatacenter.techtarget.com

[3] Hamann, H.F. , A Measurement-Based Method for Improving Data Center Energy Efficiency, International Conference on Sensor Networks, Ubiquitous and Trustworthy Computing, SUTC '08, pp:312-313, 2008

[4] Robert F. Sullivan, Reducing Bypass Airflow Is Essential for Eliminating Hotspots, WHITE PAPER EXECUTIVE SUMMARY, UpsiteTechnologies, 2010, available at http://www.42u.com

[5] Fichera, R., Koetzle, L, Powell, T, “Power and Cooling Heat Up The Data Center”, Forrester Research, 2006, available at http://www.forester.com.

[6] R. K. Sharma, C. E. Bash, and R. D. Patel. Dimensionless Parameters For Evaluation Of Thermal Design And Performance Of Large-Scale Data Centers. In 8th ASME/AIAA Joint Thermophysics and Heat Transfer Conference, 2002.

[7] D. Brooks and M. Martonosi, “Dynamic Thermal Management for High-Performance Microprocessors,” Proc. 7th Int’l Symp. High-Performance Computer Architecture (HPCA 01), IEEE CS Press, 2001, p. 171

[8] M. Huang et al.,“A Framework for Dynamic Energy Efficiency and Temperature Management,” Proc. 33rd Ann. Int’l Symp. on Microarchitecture, IEEE CS Press, 2000, pp. 202–213.

[9] Ian Seaton, Hot Air Isolation Cools High-Density Data Centers, Business Management Magazine, Winter 2008, pp: 1-5. 2008.

[10] Kenneth Hess , Using Server Virtualization to Cool 4 Data Center 'Hotspots', ServerWatch 2010, June, available at http://www.serverwatch.com/

[11] Ratnesh K. Sharma, Cullen E. Bash, Chandrakant D. Patel, Richard J. Friedrich, Jeffrey S. Chase, "Balance of Power: Dynamic Thermal Management for Internet Data Centers," IEEE Internet Computing, vol. 9, no. 1, pp. 42-49, Jan./Feb. 2005.

[12] Moore, Justin and Chase, Jeff and Ranganathan, Parthasarathy and Sharma, Ratnesh, “Making scheduling "cool": temperature-aware workload placement in data centers”, ATEC '05 Proceedings of the annual conference on USENIX Annual Technical Conference, 2005