SOLUTION BRIEF

How to Achieve Operational Assurance in Your Private Cloud

As enterprises implement private cloud and next-generation data centers to achieve cost efficiencies and support business agility, operational assurance becomes paramount. The most modern, robust hardware and software will still go down if process failure or administrator "pilot error" leads to mistakes in data center operations. And since enterprise IT performance is often compared to public cloud providers, maintaining availability at the highest level is absolutely essential.

Ironically, the risk to availability from operational issues is worse in virtual and private cloud architectures than with traditional, hardware-centric designs. Physical systems are natural silos, with built-in segregation of duties, and dedicated staff per function. Virtualization and cloud concentrate risk in the virtualization administrators, who have broad responsibilities. Virtual admins need to wear many hats and may not be expert in everything they are responsible for, making mistakes more likely. Furthermore, malicious compromise of a single admin account can lead to catastrophic outage and data loss. Finally, auditing of virtual admin activity is usually weak, making it difficult to troubleshoot problems after they occur.

HyTrust can become a cornerstone to ensure operational assurance in the virtualized data center and private cloud, introducing a number of key benefits.

Reduce Data Center Downtime

As anyone who has worked in IT operations for any length of time will tell you, human error is the most common source of downtime. In fact, a recent Gartner study concluded that "**Through 2015, 80% of outages impacting mission-critical services will be**

With HyTrust, You Can:

- Reduce downtime by preventing accidental misconfiguration
- Prevent large scale errors introduced through automation
- Achieve faster remediation and recovery with platform hardening, alerts, and actionable log data
- Free up headcount required for compliance through automation

caused by people and process issues, and more than 50% of those outages will be caused by change/configuration/release integration and hand-off issues." Even if strong change control procedures exist, there is usually nothing to prevent a simple "fat finger" mistake when the change is actually performed.

Configuration errors happen all the time. Here are just a few examples HyTrust has come across:

- A vCenter admin "drag and dropped" a set of sensitive virtual workloads into the wrong place in the virtual network, leaving them exposed to attack and unauthorized access, and bringing the company out of compliance.
- A virtualization administrator accidently misconfigured a virtual switch, which dropped connectivity for a number of key virtual servers.
- An admin accidentally suspended a virtual machine responsible for hosting the organization's credit card processing application, taking it offline for 4 minutes – and resulting in significant lost revenue.

IT administration accounts can also be leveraged for truly malicious activity. At Shionogi Pharmaceuticals, a disgruntled former employee was able to remotely access a VMware vCenter admin account and use it to delete 80 production VMs, causing substantial downtime. In another event, an employee deleted the primary vCenter admin account itself, causing downtime in multiple international datacenters. And in a well-publicized incident in San Francisco, a former government employee locked out network administrative access for everyone except himself, causing massive financial and reputational damage to the city's government. All of these events were possible because of the poor level of controls placed on IT administrators.

> "As with years past, errors made by internal staff, especially system administrators who were the prime actors in over 60% of incidents, represent a significant volume of breaches and records, even with our strict definition of what an "error" is."
>
> – Verizon 2015 Data Breach Investigations Report

Prevent Large Scale Errors Introduced by Automation

The promise of private cloud is an agile, self-service model enabled by new management tools for orchestration and automation. But this automation can also produce undesirable consequences, including VM sprawl, sensitive workloads being accidentally moved to untrusted locations, or even large scale outages. Consider the situation of a large financial institution where an admin made a typo in a script and then executed it, only to find that the script accidentally powered off over 30,000 VMs, instead of powering them on.

As you'll learn in Section 2, HyTrust solutions can uniquely provide controls to prevent actions by unauthorized administrators, provide the right controls to keep administrators in their 'swim lanes', and enable secondary approval to further protect sensitive operations.

Faster Remediation and Recovery

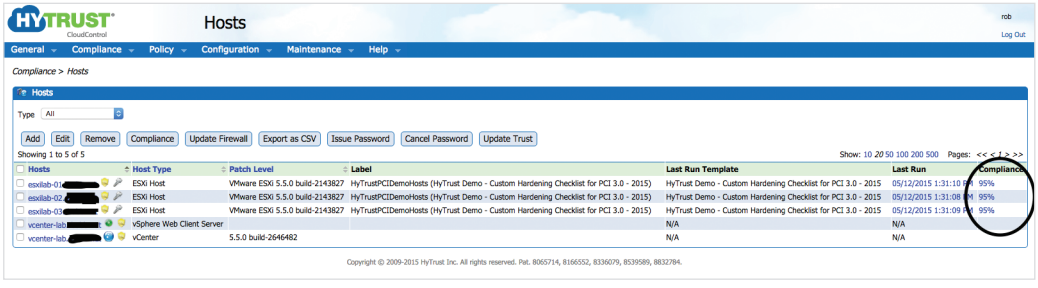
The costs of downtime will vary greatly depending on the mistake and environment. A Ponemon Institute survey of 450 data center professionals estimated that a two hour data center outage costs an average of just over $900,000 or more than $7900 per minute. Partial outages, which were defined as the outage of one or more racks within the datacenter, had an average recovery time of less than one hour with an associated cost of about $350,000. To that must be added the cost of lost reputation, both for the organization and the IT team itself.

Consequently, speed is everything when it comes to recovering a downed system. But most virtualized infrastructure management systems don't provide the necessary granularity to determine which actions cause the downtime. The unfortunate fact is that as expectations for uptime have increased, budgets and staff levels for IT operations have declined. This means that new approaches are required to better avoid accidental downtime due to "pilot error." HyTrust provides this granular control, reporting and alerting.

Automate Compliance

Privacy regulations such as HIPAA, PCI or state disclosure laws impact almost every organization, and building a successful compliance program requires a combination of headcount, policy and technology. Further, compliance is shifting from a one time or 'once a year' scramble prior to an audit to 'continuous compliance', which requires additional effort.

HyTrust recently worked with a Fortune 50 company as part of its efforts around PCI compliance. The company recognized the need to gain better visibility and reporting for privileged admin activity in its virtualized data center in order to comply with PCI. This company was able to determine that implementing HyTrust CloudControl would automate a substantial amount of control, monitoring and reporting, enabling them to address compliance with a part time headcount, compared to the two full time employees they had previously allocated to this task, freeing them up for more strategic work.



HyTrust CloudControl automates hypervisor hardening, and provides alerts should settings deviate, allowing continuous monitoring and quick remediation

HyTrust CloudControl: Industry Leading Controls for VMware Administration

To meet security and compliance requirements for their virtualized data centers and private clouds, enterprises rely on HyTrust. HyTrust CloudControl™ offers the most complete solution available for administrator and configuration controls on VMware vSphere infrastructure (with NSX virtual networking support available soon). CloudControl supports an industry leading feature set that includes four key administrative controls:

Strong Two-Factor Authentication — CloudControl supports two-factor authentication to ensure administrators are who they say they are and prevent identity spoofing. CloudControl integrates with Active Directory, RSA SecurID, CA ArcotID, RADIUS, and Smartcards/PKI, and can also provides password vaulting to tightly secure ESXi server root access.

Role-Based Authorization & Access Control — In VMware environments, permissions are not centralized across vCenter and ESXi hosts, making them difficult to manage and resulting in a situation where companies cannot clearly see who has access to the infrastructure, or report on the actions they take. In a few mouse clicks, an admin can suspend, copy or delete a production VM, alter network configurations, or bring hypervisors out of compliance. This creates massive risks to uptime simply through administrator error. CloudControl dramatically lowers this risk by centralizing all role-based access control, ensuring consistent policies are applied regardless of whether the admin is using the web client, SSH or the CLI. Further, CloudControl provides label-based access controls to help create secure multi-tenancy in these shared cloud environments.

Secondary Approval – CloudControl supports a second level of approval for sensitive actions. An admin can attempt to perform a potentially risky action (e.g. stopping a production VM), but a second person must approve the action before it is actually executed. As with the role-based access control function, secondary approval can be tied to specific actions on specific workloads. This granular level of control makes it realistic to implement secondary approval in just the areas it is really needed – eliminating unnecessary hassles for admins as they conduct their jobs.

Forensic Quality Logging – CloudControl produces the complete, detailed activity logs that VMware vSphere and vCenter do not provide. Although VMware infrastructure is a critical component of most modern data centers and private clouds, it does not provide sufficient native logging for detailed activity forensics. If an issue arises during data center operations, detailed logs are the first tool required to troubleshoot the problem, because they will show exactly who did what to which objects.

CloudControl's logging provides that complete audit trail, both for troubleshooting and for compliance and security controls.

Log Parameter	VMware vSphere	HyTrust CloudControl
Time/Date	✓	✓
Target Object	✓	✓
Action	✓	✓
User ID	✓	✓
Source IP Address	✗	✓
Configuration Parameters	✗	✓
Secondary Approval ID	✗	✓
Denied Operation Event	✗	✓

Summary

As organizations place more and more critical and sensitive workloads on virtual infrastructure, availability of that infrastructure and the workloads it supports is paramount. HyTrust CloudControl delivers a unique and powerful set of controls on virtualization admin accounts that mitigates this risk and provides a granular activity audit trail for troubleshooting and forensics.

To learn more about HyTrust cloud security solutions, visit www.hytrust.com or join an upcoming webinar.