HYTRUST
Cloud Under Control

Solution Brief

Implementing Secondary Approval, or "The Two-Person Rule"

Executive overview

Enterprises increasingly seek to virtualize their mission critical workloads in order to achieve financial objectives. At the same time, they are realizing they must monitor and control VMware privileged user access to virtual machines (VMs) in order to ensure the security and regulatory compliance of their Tier 1 applications. They also want to maintain virtualization operations productivity, so access controls must have the flexibility to fit the way the virtualization team works day-to-day.

The Secondary Approval automated workflow provided by HyTrust CloudControl™ overcomes the challenge of efficiently securing access to critical VMs. By enforcing the "two person rule" for high impact administrative operations, Secondary Approval prevents costly disruptions caused accidentally or intentionally by a VMware privileged user. The flexible, situation-specific access control enabled by Secondary Approval helps keep virtual data centers productive, secure, and compliant with regulations.

HyTrust - Cloud Under Control

HyTrust has become the de facto standard for access control, logging, and policy enforcement in VMware environments. By filling gaps in virtual infrastructure security and compliance, HyTrust gives enterprises the assurance they need to virtualize their mission critical applications, implement private clouds, pass security audits, and reap the financial benefits of increased virtualization. HyTrust CloudControl enforces role-based and asset-based policies covering VMware privileged users, virtual resources, and management interfaces. It also secures the vSphere platform and virtualized workloads by providing virtual network segmentation; comprehensive, audit-quality access logs; strong authentication; and virtual infrastructure hardening. HyTrust DataControl™ provides strong encryption and integrated key management for virtual machines from the time they are created until they are securely decommissioned.

Your challenge

Privileged users of the VMware vSphere platform typically have much greater administrative power than their counterparts who manage physical data center infrastructure. They can copy, power off, or delete a virtual machine (VM) that hosts a production application—accidentally or intentionally—with a few clicks. If the result is substantial operations downtime, a serious compliance violation, or a confidential data breach, the cost can be dramatic. Recent high profile breaches in which vSphere users destroyed production data center resources through the management interface demonstrate that the risks are real.

HyTrust access control policies based on "always on" rules provide very effective protection for critical applications and data in VMs. At the same time, data centers often want an efficient way to grant VMware users temporary administrative privileges needed to perform infrequent job duties. In other situations, managers want greater control over the use of powerful privileges by users who need those privileges to do their jobs every day.

Examples of these situations include:

- A contractor occasionally clones the virtual machine (VM) that hosts the enterprise email server in order to test patches and upgrades. The enterprise wants to ensure that the contractor cannot clone the VM for any other reason.

- A group of vSphere users conducts monthly scheduled reboots of VMs that run production workloads. Management wants to enable the reboots each month without having to approve exceptions, but also wants to require one-time approval for all other VM power-off and power-on operations.

- A virtualization operations group needs ongoing authorization to create and delete VMs used for non-production applications. However, their manager wants the ability to approve or deny any attempt to delete a production VM.

The VMware platform does not provide a viable way to enable one-time authorization of a particular operation attempted by a particular user. Consequently, many enterprises have been hesitant to virtualize their critical workloads and have missed the economic gains available from greater virtualization.

The HyTrust solution

HyTrust makes secure multi-tenancy possible by closing gaps in virtual infrastructure n addition, vSphere users can act anonymously by sharing a root account or by using a management interface that does not log their activity, such as an SSH direct-to-host connection. An administrator can clone a VM holding another tenant's sensitive data, for instance, knowing that the action can't be traced back to them. Enterprise cloud owners and CSPs must be able to monitor and record each vSphere user's activity at all times in order to ensure accountability and prove compliance with regulations.

Like the virtualization platform, traditional firewalls do not mitigate these visibility and control risks. In particular, they don't ensure tenant- level segmentation of network and other virtualized resources as well as access management.

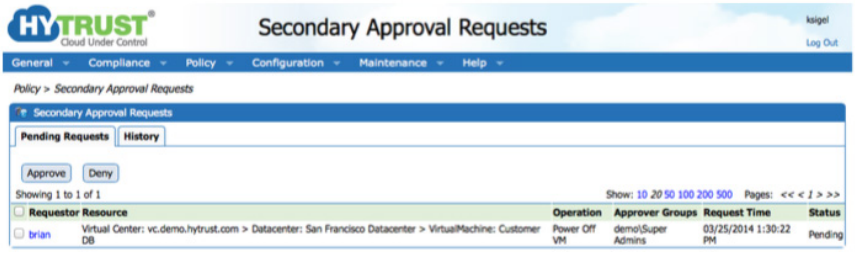
Secondary Approval workflow increases the power and flexibility of HyTrust CloudControl by enforcing the "two-person rule". According to US Air Force Instruction (AFI) 91-104, the two-person rule is designed to prevent accidental or malicious launch of nuclear weapons by a single individual. Similarly, the automated Secondary Approval process requires a designated approver to authorize an administrative operation attempted by a privileged user before the VMware platform allows the operation to proceed.

The Secondary Approval workflow is simple and efficient, making it easy for operations groups to implement. It begins when a user attempts a VMware platform operation requiring authorization, in accordance with data center policy. HyTrust CloudControl blocks execution and tells the user that Secondary Approval has been requested for the operation. HyTrust CloudControl simultaneously alerts an approver group that a user request requires review, and it provides the details of the request. When an approver makes a decision, HyTrust CloudControl notifies the user and – if the request is approved - gives the user an approver-defined window of time in which to execute the approved operation.

Examples of use cases where Secondary Approval can add value include:

- Attempts by the contractor to clone the email server VM are blocked until an approver grants permission. When a patch or upgrade has been scheduled, the approver gives the contractor a limited period of time in which to clone the VM.
- Outside of scheduled monthly reboot times, a vSphere user's attempt to reboot a production workload triggers the Secondary Approval process. A manager toggles off the rule each month while vSphere users reboot the appropriate VMs.
- Virtualization operations team members are able to create or delete a production VM only when a manager authorizes the request in HyTrust.

An attacker's attempt to use stolen log-in credentials to conduct a damaging operation is blocked, logged, and immediately reported to secondary approvers.



Approvers review the details of an attempted VMware operation and approve or deny it in seconds within a browser-based management dashboard

The HyTrust CloudControl "two person rule" workflow is not available from the VMware platform or any other source. By deploying HyTrust CloudControl with Secondary Approval, IT organizations take an essential step toward virtualizing their critical workloads and increasing their virtualization ROI without sacrificing security, compliance, or productivity.

For more information on how HyTrust enables greater virtualization of workloads that must stay compliant, visit www.hytrust.com/products/capabilities , email questions to sales@hytrust.com, or call HyTrust at 650-681-8100 for a free consultation.

HyTrust - Cloud Under Control.
1975 W. El Camino Real, Suite 203
Mountain View, CA 94040, USA
Phone: 1-844-681-8100
International: 1-650-681-8100