

Top 5 VMware Incidents You Need Visibility into



Table of Contents

| | |
|---|---|
| #1: Changes to Virtual Machine Configurations | 2 |
| #2: Snapshot Creations and Deletions | 3 |
| #3: Host System Changes | 4 |
| #4: Changes to Virtual Machine Permissions | 5 |
| #5: Resource Pool Changes | 6 |
| About Netwrix Auditor | 7 |



#1: Changes to Virtual Machine Configurations

Unauthorized changes in the configurations of virtual machines can cause business-critical applications and systems - such as Exchange, SharePoint, SQL or even file servers that run in a virtualized environment - to become unavailable. Therefore, it is important to keep an eye on the configurations of virtual machines to make sure that only authorized and proper changes are made. Netwrix Auditor reports on changes made to virtual machine configurations, providing answers to the following questions:

- ❖ **Who** changed a virtual machine's configuration?
- ❖ **What is the name** of each machine whose configuration was modified?
- ❖ **Where** is each machine located?
- ❖ **When** did each change take place?

VMware Virtual Machine Changes

Shows changes to the configuration of virtual machines, such as virtual hardware, settings, and permissions.

| Action | What | Who | When |
|--|--|---------------------|--------------------------|
| ■ Added | \ha-folder-root\ha-datacenter\vm\ ProdDB Where: https://atlmktvms01.enterprise.com:443 | ENTERPRISE\J.Carter | 10/12/2016 4:36:28 PM |
| ■ Modified | \ha-folder-root\ha-datacenter\vm\ Prod-DC1 Where: https://atlmktvms01.enterprise.com:443 Added Advanced Configuration (MIGRATE.HOSTLOG): ./FS1 Enterprise-82eeac4a.hlog Advanced Configuration (TOOLS.REMINDINSTALL) changed from "true" to "false" Added Advanced Configuration (VMOTION.CHECKPOINTSVMGASIZE): 8323072 IP Address changed from "192.168.10.16" to "172.17.6.22" Added Network adapter 2 Connect at power on: True Added Network adapter 2 Connected: True Advanced Configuration (VMOTION.CHECKPOINTSVMGASIZE) changed from "7340032" to "8323072" Name changed from "ProdDC-2" to "Prod-DC1" | ENTERPRISE\J.Carter | 10/12/2016 4:36:38 PM |

#2: Snapshot Creations and Deletions

The creation and deletion of snapshots of the state and the data of the virtual machine are critical events in the VMware environment. Because each snapshot can take gigabytes of space, storing too many simultaneously can cause system performance to degrade massively. And deleting snapshots can leave you without a critical restore point. Netwrix Auditor reports on all added or deleted snapshots and provides the answers to the

- ❖ **Who** created or deleted or a snapshot?
- ❖ **Which** snapshots were created or deleted?
- ❖ **Where** was the created or deleted snapshot located?
- ❖ **When** was a snapshot created or deleted?

VMware Snapshot Changes

Shows creation, modification, and deletion of virtual machine snapshots. This report can be used to control changes to snapshots and prevent loss of important data and settings.

| What | Who | When |
|--|---------------------|---------------------------|
| \ha-folder-root\ha-datacenter\vm\DC1 Where: https://atlmktvms01.enterprise.com:443 Added Current Snapshot: After update Added Snapshot Name: After update Added Snapshot Name: Before update | ENTERPRISE\j.Carter | 11/14/2016 12:56:49 PM |
| \ha-folder-root\ha-datacenter\vm\ Netwrix Change Notifier AD | ENTERPRISE\j.Carter | 11/14/2016 1:01:20 PM |
| Where: https://atlmktvms01.enterprise.com:443 Added Current Snapshot: Preparation stage 1 Added Snapshot Name: Preparation stage 1 | | |

#3: Host System Changes

All changes to host systems should be carefully reviewed because they can negatively affect the entire virtual infrastructure. For example, a change could degrade server performance or even cause downtime across the entire virtual environment. Netwrix Auditor shows details about every change in host systems and helps answer the following questions:

- ❖ **Who** made host system changes?
- ❖ **Which** host system was affected?
- ❖ **What kind** of changes were made?
- ❖ **When** were the changes made?

VMware Host System Changes

Shows changes to host systems (ESX and ESXi servers). Such changes must be carefully reviewed because they usually affect the entire virtual infrastructure.

| Action | What | Who | When |
|---|---|--------------------|--------------------------|
| ■ Modified | \ha-folder-root\ha-datacenter\host \ATLMKTVMS01.enterprise.com | ENTERPRISEJ.Carter | 4/20/2016 3:09:37 PM |
| Where: https://atlmktvms01.enterprise.com:443 Datastore 0 accessible to Host changed from "SYS_" to "Storage for VM's" Datastore 1 accessible to Host changed from "Storage for VM's" to "SYS_" | | | |
| ■ Modified | \ha-folder-root\ha-datacenter\host \ATLMKTVMS01.enterprise.com | ENTERPRISEJ.Carter | 10/13/2016 4:50:06 PM |
| Where: https://atlmktvms01.enterprise.com:443 Added Port Group: Cluster Network Added Port Group: Datastore Network | | | |

#4: Changes to Virtual Machine Permissions

To ensure the availability of critical systems running in virtual environments, you need to ensure that only authorized users have access to the virtual machines. This requires complete visibility into all changes to virtual machine permissions. Netwrix Auditor gives you control over changes to virtual machine permissions and provides detailed answers to the following questions:

- ❖ **Who** changed virtual machine permissions?
- ❖ **Where** is each virtual machine with changed permissions located?
- ❖ **When** was the change made to each virtual machine's permissions?
- ❖ **What** exactly was changed in the virtual machine's permissions?

| Action | What | Who | When |
|---|---|---------------------|-------------------------|
| ■ Modified | \ha-folder-root\ha-datacenter\vm\ RedHat666 Where: https://atlmktvms01.enterprise.com:443 Added Permission 0 Group: False Added Permission 0 Principal: ENTERPRISE\N.Key Added Permission for user ENTERPRISE\N.Key: Administrator Added Permission Propagate for user ENTERPRISE\N.Key: True | ENTERPRISE\J.Carter | 4/20/2016 3:06:44 PM |
| ■ Modified | \ha-folder-root\ha-datacenter\vm\ Prod-DC1 Where: https://atlmktvms01.enterprise.com:443 Removed Permission 0 Group: False Removed Permission 0 Principal: ENTERPRISE\T.Simpson Removed Permission for user ENTERPRISE\A.Terry: Read-Only Removed Permission Propagate for user ENTERPRISE\A.Terry: True | ENTERPRISE\J.Carter | 11/7/2016 4:46:10 PM |

#5: Resource Pool Changes

Resource pools control resource allocation for virtual machines. If a share allocated to virtual machines is insufficient or a resource pool is deleted, the virtual machines may perform badly or stop functioning altogether. Since virtual machines often host critical business applications, ongoing monitoring of resource pool changes is essential to ensuring application availability and user productivity. Netwrix Auditor tracks every change made to resource pools and gives answers to the following questions:

- ❖ **Who** changed a resource pool?
- ❖ **Which** resource pools were changed?
- ❖ **Where** is each changed resource pool located?
- ❖ **When** did each change take place?
- ❖ **What** exactly was changed in each resource pool?

VMware Resource Pool Changes

Shows changes to resource pools. Because resource pools control resource allocation, changes to them usually affect the entire virtual infrastructure.

| Action | What | Who | When |
|--|---|--------------------------|-------------------------|
| ■ Removed | \ha-folder-root\ha-datacenter\host\ ATLMKTVMS01.enterprise.com\ Resources\John Carter\Enterprise\QA | ENTERPRISE\ T.Simpson | 2/27/2016 3:35:14 AM |
| Where: https://atlmktvms01.enterprise.com:443 | | | |
| ■ Modified | \ha-folder-root\ha-datacenter\host\ ATLMKTVMS01.enterprise.com\ Resources\JohnCarter\Enterprise | ENTERPRISE\ T.Simpson | 11/7/2016 4:31:20 PM |
| Where: https://atlmktvms01.enterprise.com:443 CPU Shares Level changed from "Normal" to "High" | | | |




About Netwrix Auditor

Netwrix Auditor is a **visibility and governance platform** that enables control over changes, configurations and access in hybrid cloud IT environments to protect data regardless of its location. The unified platform provides security analytics for detecting anomalies in user behavior and investigating threat patterns before a data breach occurs.

Netwrix Auditor includes applications for Active Directory, Azure AD, Exchange, Office 365, Windows file servers, EMC storage devices, NetApp filer appliances, SharePoint, Oracle Database, SQL Server, VMware and Windows Server. Empowered with a RESTful API, Netwrix Auditor provides **endless integration, auditing and reporting capabilities** for security and compliance.

Unlike other vendors, Netwrix focuses exclusively on providing complete visibility and governance for hybrid cloud security. The sharp focus enables us to offer much more robust functionality than legacy change auditing solutions. Netwrix Auditor has been already honored with more than **100 awards** and recognized by almost **160,000 IT departments** worldwide.

Deploy Netwrix Auditor Wherever You Need It

-  Free 20-Day Trial for On-Premises Deployment: netwrix.com/freetrial
-  Free Virtual Appliance for Hyper-V and VMware Hypervisors: netwrix.com/go/appliance
-  Free Cloud Deployment from the AWS, Azure and CenturyLink Marketplaces: netwrix.com/go/cloud



netwrix.com/social

Netwrix Corporation, 300 Spectrum Center Drive, Suite 1100, Irvine, CA 92618, US

Toll-free: 888-638-9749

Int'l: +1 (949) 407-5125

EMEA: +44 (0) 203-318-0261