Quick Reference Guide

netwrix

# VMware Auditing

VMware vCenter Server 4.1-6.0

## VCenter Events View

- Run vSphere Web Client on your vCenter server > Navigate to “Events” Tab > Event Console will open where you can find all events happened with your virtual machines

## vSphere Events View

- Run vSphere Client on your computer > Select a Host > Navigate to “Events” Tab > “Event Console” will open where you can find all events happened with your virtual environment

## PowerCLI Events View

- Run VMware PowerCLI connect to your vCenter using  command:
- *Connect-VIServer –server servername*
- Execute command *Get-VIEvent*
- You can get more information by executing: *Get-Help Get-VIEvent*
- You can specify parameters by adding the monitored event from the Common VM Events list into this script (save this script in txt file with .ps1 extension) and run this script in PowerCLI console:

```
Get-VIEvent -Start (Get-Date).adddays(-120) | `
  where {$_.gettype().Name -eq "add event here” -
and $_.CreatedTime -lt (Get-Date).adddays(1)} | `
  select @{N="VMname"; E={$_.Vm.Name}},
      @{N="OccuredTime"; E={$_.CreatedTime}},
      @{N="Hostname"; E={$_.Host.Name}},
     @{N="Username"; E={$_.UserName}}
```

- You can also select different date range by changing “*adddays*” parameter.

## Common VMware Events:

- VmPoweredOffEvent – VM powered off
- VmPoweredOnEvent – VM powered on
- VmSuspendedEvent – VM suspended
- AccountCreatedEvent – Account created
- AccountRemovedEvent – Account removed
- AccountUpdatedEvent – Account updated
- EnteredMaintenanceModeEvent – Entered maintenance mode
- ExitMaintenanceModeEvent – Exit maintenance mode
- PermissionAddedEvent – Permission added
- PermissionRemovedEvent – Permission removed
- PermissionUpdatedEvent – Permission updated
- UserLoginSessionEvent – User login
- UserLogoutSessionEvent – User logout
- UserPasswordChanged – User password changed
- AlarmAcknowledgedEvent – Alarm acknowledged
- BadUsernameSessionEvent – Invalid user name
- ClusterCreatedEvent – Cluster created
- ClusterDestroyedEvent – Cluster deleted
- You can find full list of events here – url2open.com/vmevents

**Gain #completevisibility into all activity in your VMware environment for free with Netwrix Auditor for VMware: netwrix.com/go/trial-vm**