How do I securely erase VMware virtual machines from ESXi host(s)?

Introduction:

As with selecting “Delete” for a file on a standard operating system such as Windows, simply deleting a virtual machine does not securely overwrite it from its data store. A standard delete will only remove the pointer to the virtual machine and it’s data on the storage. Blancco Virtual Machine Eraser has been developed to offer secure overwriting and reporting of virtual machines on various hyper-visors.

https://download.blancco.com/Tutorials/Virtual_Machine_Data_Recovery/Virtual_Machine_Data_Recovery.mp4

There are many different integration methods and the right one for you simply depends upon your unique environment and requirements. Let’s start by establishing whether it should be a manual or automatic process.

The needs which drive secure virtual machine erasure are the same as for securely erasing physical disks and hardware. Perhaps customer demand is behind the requirement. Perhaps compliance with a security standard or recommendation such as ISO 27001, 27040, 27018, the Payment Card Industry Data Security Standard or the Cloud Security Alliance is the root cause. Finally, perhaps secure erasure has become a competitive advantage in your portfolio and a Value Added Service in a list of other possible security options (such as firewall, encryption and backup) for users to choose from when spinning up a new virtual machine or LUN. Yes, Blancco also has a product called Blancco LUN Eraser which can also be run from ESXi and is used for securely erasing entire LUNs:
https://download.blancco.com/Tutorials/Blancco_LUN_Windows/Blancco_LUN_Windows.mp4

Now comes the question:

Do your needs require you to only manually erase specific virtual machines on demand when requested to do so? In that case, see the “Manual Operation” and “Semi-Automatic” sections below.

Do your needs require you to implement the automatic erasure of all virtual machines once “Delete” has been selected for them by the end-users? If yes, see the “Automatic Operation” section below.

Manual Operation:
In brief, Blancco Virtual Machine Eraser can be run directly from a host ESXi server by establishing an SSH connection with that server, opening the CLI and manually typing the erasure commands. This is the perfect way to securely decommission particular virtual machines which for some reason or another (most likely customer demand), require secure erasure. See more information about this operation in this video:

https://download.blancco.com/Tutorials/Blancco_Virtual_On_Demand_ESXi/Blancco_Virtual_On_Demand_ESXi.mp4

Semi-Automatic:
Perhaps you still only need to erase specific machines on demand but do not wish to open an SSH tunnel and manually type commands. If you are using vCenter Server to manage multiple ESXi host servers, it is possible for you to pair your vCenter Server instance with vRealize Orchestrator and incorporate special Blancco workflows to offer the option to your administrators to simply right-click specific virtual machines in the vCenter Server GUI and choose “Blancco Secure VM Erasure”. This offers you the flexibility of handpicking which virtual machines will be securely erased without the need for any special actions taken. See more here:

https://download.blancco.com/Tutorials/Blancco_Virtual_-_vCenter_Server/Blancco_Virtual_-_vCenter_Server.mp4

For more information, read this article.

Automatic Operation:

If your goal is to automate the erasure of all virtual machines which are selected for decommission in your environment, you are in luck! Blancco has its own VIB package which can be installed on the host ESXi servers and called into action with a REST API. If you have your own portal with which your users create, use and delete virtual machines, this REST API functionality can be built directly in. Simply have your portal send XML payloads to the host ESXi servers requesting the erasure of a virtual machine whenever the user has selected it for deletion. The ongoing erasure status can also be fetched from the ESXi host server and displayed for the users in your portal’s UI. See more about the REST API here:
https://download.blancco.com/Tutorials/Blancco_vCloud_Eraser_REST_API/Blancco_Virtual_REST_API.mp4

If you are using VMware’s own portal, vCloud Director, you can integrate directly into its UI as well:
vCloud Director Part 1: https://download.blancco.com/Tutorials/Blancco_vCloud_Eraser/Blancco_vCloud_Eraser.mp4
vCloud Director Part 2: https://download.blancco.com/Tutorials/Blancco_vCloud_Eraser_Workflows/Blancco_vCloud_Eraser_Workflows.mp4

Erasure reports:

After every erasure, regardless of the implementation method, a digitally signed erasure report is automatically generated and stored on the host ESXi server. These reports can also be automatically sent to the Blancco Management Console which resides on a dedicated server with its own database in the same network, or even to Blancco Cloud if the host ESXi servers have an internet connection. See a video about the Blancco Management Console here:
https://blancco.wistia.com/medias/0u0q9tt3qv

These reports form a tamper-proof audit trail which confirm that the erasures actually happened, when it happened and with what overwriting method. They can be viewed directly in the Blancco Management Console / Blancco Cloud or exported and sent to internal users, external customers or an external database. The exporting can happen automatically via an API. See more information about the API here:
https://blancco.wistia.com/medias/oisyat9lzw

Conclusion:

More information about Blancco Virtual Machine Eraser can be found from here.

That about sums it up. If you have more questions, please be in contact with your Blancco representative and let them know that you have already read through this knowledge-base article. We look forward to serving you!