VM Host16 Failure

Problem Impact Analysis # Draft

Event Occurrence: 2018-04-06 Approx. 11:10 am
Event Resolved: 2018-04-06 Approx. 11:40 am

Background

The OIT Production Cluster consists of 16 physical servers hosting over 500 guest virtual servers and provides the vast majority of OIT's on-site hosting capacity. Mission-critical services such as Active Directory, Banner, Blackboard, Alertus, and more run on its hardware.

Break Down of the Problem

On Friday, April 4, at 11:10 am, a VM host rebooted unexpectedly which resulted in its guests hard-crashing. The host came back online then administrators ensured that the affected virtual machines were operational. This affected thirteen servers and multiple services including:

- UAS Degreeworks / Transfer Equivalency
- Kaltura SFTP
- ELMO
- www.alaska.edu

Target State / Goal

VM hosts should only be powered off or rebooted during scheduled outages and never while they are still running virtual machines.

Root Cause Analysis

During routine maintenance, an administrator using the Direct Console User Interface (DCUI) rebooted the wrong VM host.

Develop Countermeasures

1. Assign a unique root password to each VM host.
   As a safeguard, VMware prompts for the root password before rebooting a system through the DCUI. Multiple VM hosts are currently configured to use the same password so this did not have the desired effect.
2. Use the vCenter web interface instead of the DCUI whenever possible.
   The vCenter web interface has more safeguards, better visibility, and better auditing features than the DCUI. The DCUI should only be used for rebooting a host when the host is not responding to vCenter.

Implementation of Countermeasures

- Immediately - All administrators are required to use the vCenter web interface whenever possible.
- 05/01/2018 - Each host has a unique root password.

Follow Up / Review

05/08/2018 - A different administrator than the one who set the passwords tests the new passwords and validates that each VM host has an unique password.