UCS Manager KVM Troubleshooting TechNote

Document ID: 115958

Contributed by Andrew Kelly and Andreas Nikas, Cisco TAC Engineers.
Feb 28, 2013

Contents

Introduction

The keyboard, video, mouse (KVM) console on the Cisco Unified Computing System Manager (UCS Manager) allows access to video output for a particular blade or service profile. This document provides the troubleshooting methodology to examine failed KVM sessions on Cisco Unified Computing System (UCS) B−Series servers.

Prerequisites

Requirements

The scenarios, symptoms, and steps listed in this document are written for troubleshooting issues after the initial setup is already completed. For initial configuration refer to this document: Unified Computing System KVM Console Access to Blade Server Configuration Example.

Components Used

The information in this document is based on the Cisco UCS Manager and Cisco UCS B−Series Blade Servers.

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, make sure that you understand the potential impact of any command.

Conventions

Refer to Cisco Technical Tips Conventions for more information on document conventions.

Troubleshooting Methodology

Although there are many sources for KVM failure, mis−configurations and Java issues are among the most

common failure points. While this document assumes the configuration was functional at one time, it focuses on troubleshooting the components involved in a successful KVM launch. Failure points include:

- Network connectivity for the entire path of the blade Cisco Integrated Management Controller (CIMC) to client browser.
- Java complications on the client in an attempt to access the KVM.
- UCS Manager failures and defects, which impact KVM/CIMC.

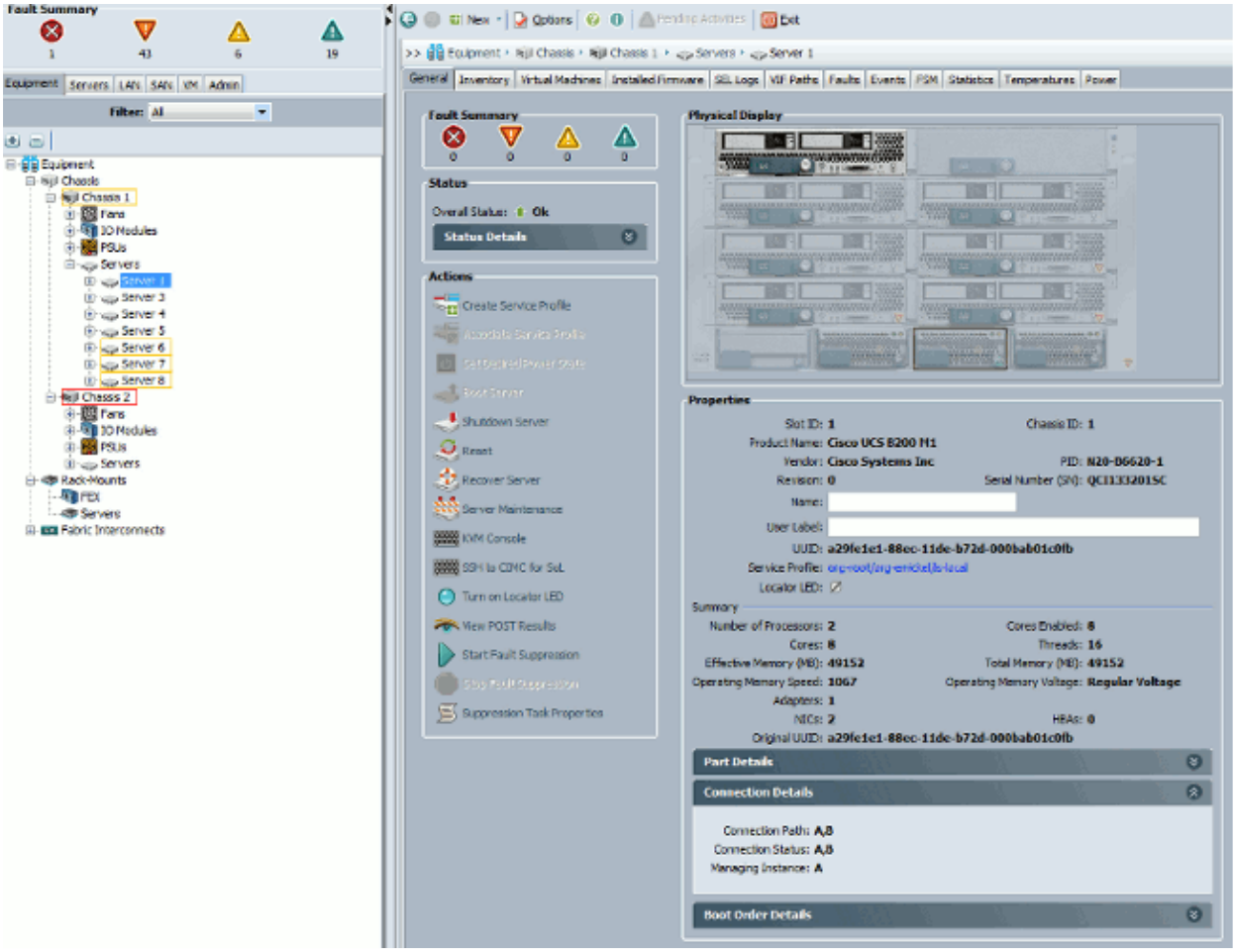
Prior to troubleshooting these failure points, it is best to first examine the scope of the problem:

- Has a single KVM failed, or are all KVMs in the system affected?
- Can the KVM be accessed from another machine in the network, or do all work stations exhibit the same behavior?

Network Connectivity

1. If you are unable to ping the KVM IP address, which was assigned from the management (MGMT) IP pool, you must verify that the IP pool addresses are within the same subnet as the management IP address assigned to the fabric interconnect. If the pool does not match, all KVMs that receive IP addresses from this pool are impacted.
2. Verify TCP port 2068 is not blocked by the access control list (ACL) or firewall between client and blade CIMC. With this port closed, it results in failure to connect to any UCS KVM.
3. Verify browser configuration to ensure HTTP proxy does not break communication.
4. If you are unable to ping the KVM IP address, check which fabric interconnect manages the instance for the blade and verify if it responds. If a fabric interconnect suffers from a failed/down mgmt0 interface, all blades that are managed by it experience KVM accessibility issues.

   To verify the management instance of the blade, choose the blade from **Equipment** > **General** > **Connection Details**.



5. If you are able to ping the KVM IP address, but still not able to connect to the KVM, you may have a duplicate IP address in the network. One way to verify this is to statically assign a new IP address that you know is not in use to the blade. If the host can be taken down, decommission the blade in question and then try to ping the KVM IP address again. If it is still successful, that IP is duplicated in the network. Remove the IP from the other device, or adjust the UCS MGMT IP Pool to not include that address.

Java Complications

1. Verify that the proper Java version is installed. The UCS Manager web page lists the requirements and links for tested java versions.
2. Monitor and collect Java logs from the Java Control Panel when you launch KVM. Click **Start** > Enter **Run** > Enter **javaws −viewer**.
3. Clear Java cache In the Java Control Panel > Click **General** > **Temporary Internet Files** > Click **View**. It launches a Java Cache Viewer. Delete all the **KVM Viewer**.
4. Does the standalone KVM launcher work? You can bypass the KVM launcher and UCS Manager with the kvm.zip.

    a. First, you must create an Intelligent Platform Management Interface (IPMI) policy/user and add this to the affected blades service profile (this is under policies).
    b. Go to http://<ucs manager ip address>/kvm.zip to download the kvm.zip file.
    c. Unzip and run the launchkvm.bat file. It then prompts you for an IP address of the server (KVM address found in UCS Manager), and the IPMI user name and password you configured.

UCSM Failures and Defects

There are very few defects related to KVM connectivity on the UCS Manager, however, to investigate anomalies on the UCS, use these commands and log files:

1. Verify Fabric Interconnect IP Tables:

```
UCS-A# connect local-mgmt
UCS-A(local-mgmt)# show mgmt-ip-debug ip-tables
```

2. Monitor blade CIMC messages file:

```
connect cimc [x/y]           (where x is the chassis and y is the server)
UCS-A# connect cimc 2/1
Trying 127.5.2.1...
Escape character is '^]'.
CIMC Debug Firmware Utility Shell [ support ]
[ help ]# messages
```

3. Use the tail command to review the Port to Application Mapping (PAM) proxy file from UCS Manager. This can be done live or from technical support files.

```
UCS-A# connect local-mgmt
UCS-A(local-mgmt)# tail-mgmt-log svc_sam_pamProxy
```

Related Information

- **Unified Computing System KVM Console Access to Blade Server Configuration Example**
- **Cisco UCS B−Series Blade Servers**
- **Cisco UCS Manager**
- **Cisco Unified Computing System**
- **Cisco UCS Manager Configuration Examples and TechNotes**
- **Technical Support & Documentation − Cisco Systems**

Updated: Feb 28, 2013 Document ID: 115958