Cisco APIC Server Data Sanitization

Contents

Cisco APIC server data sanitization

The Cisco Integrated Management Controller (IMC) 4.3.1.230097 release and later supports the data sanitization feature, which erases all sensitive data in a Cisco UCS server. This makes the extraction or recovery of customer data impossible. In general, you would use this process before returning the server due to a return merchandize authorization (RMA) process.

As the Cisco IMC progresses through the erase process, the Cisco IMC updates a status report. You can check the status of the data sanitization process for each individual device erase from the report, then identify and rectify any issues, if required.

After the sanitization process completes, the server goes offline and is unusable because all your data, including server settings, is erased. If you want to reuse the server, you must set up the server as though this was your first time configuring it.

Supported server components for data sanitization

This feature is supported on the following server components in Cisco UCS C-series M5 (APIC-L3/M3) and M6 (APIC-L4/M4) servers:

- Board domain components (BMC, BIOS)
- Host domain components (VIC, storage, NVDIMM)

Beginning with Cisco IMC release 4.3.2.230207, this feature is supported on the following server components of Cisco UCS S-series M5 (APIC-L3/M3) servers:

- Board Domain components (BMC, BIOS)
- Host domain components (VIC, NVDIMM)

Data sanitization erase process

The erase process for data sanitization is performed in the following order on the server components:

1. NVDIMM
2. Storage
3. VIC
4. BIOS
5. Cisco IMC

You can choose to either perform data sanitization on all server components or choose only VIC and Storage components for data sanitization. The Cisco IMC reboots when the data sanitization process is completed and generates a report.

After the process is complete, the password is reset to the default. You can then change the password and perform a full component firmware update using the latest firmware.

Sanitize data in a Cisco UCS server

This procedure uses the following UCS M6 (APIC-L4/M4) server in the example commands:

```
server1:
  name: server1
  type: ifc
  model: M6
  role: active
  id: 1
  serialnumber: ABC123456DE
  platform:
    cimc:
      address: 192.168.141.201
      username: admin
      password: MyCIMCPassword
      name: server1-cimc
  users:
    admin:
      username: admin
      password: MyAdminPassword
  networks:
    mgmt:
      address: 192.168.141.200
      netmask: '21'
      gateway: 192.168.136.1
    inband:
      vlan: 2
      address: 10.0.0.1
      netmask: '16'
```

Follow these steps to sanitize data in a Cisco UCS server.

Step 1. Download the HUU ISO, then copy it to the build machine:

```
scp ~/Downloads/ucs-c225m6-huu-4.3.2.240009.iso user1@system1.local:/data/ssd
```

Step 2. From the build machine, mount 192.168.125.200:/home/nfsshare and copy the HUU ISO to the share:

```
user1@system1:/data/ssd$ mkdir /data/ssd/ucs_share
user1@system1:/data/ssd$ sudo mount -t nfs 192.168.125.200:/home/nfsshare
/data/ssd/ucs_share
user1@system1:/data/ssd$ cp ucs-c225m6-huu-4.3.2.240009.iso ucs_share/
```

Step 3. Mount the HUU ISO to vmedia0.

```
user1@system1:/vol/apicbin$ curl -k -u admin:MyCIMCPassword
https://192.168.141.201/redfish/v1/Managers/CIMC/VirtualMedia/0/Actions/VirtualMedia.In
sertMedia -XPOST -d '{"Image":"192.168.125.200:/home/nfsshare/ucs-c225m6-huu-
4.3.2.240009.iso","WriteProtected":true,"TransferProtocolType":"NFS","TransferMethod":"
Stream","Inserted":true}'
{
    "Messages":     [],
    "Id":           "16",
    "Name":         "Vmedia insert monitor",
    "StartTime":    "2024-03-26T16:48:47+00:00",
    "TaskState":    "Running",
    "@odata.id":    "/redfish/v1/TaskService/Tasks/16",
    "@odata.type":  "#Task.v1_4_0.Task"
}user1@system1:/vol/apicbin$ user1@system1:/vol/apicbin$ curl -k -u
admin:MyCIMCPassword https://192.168.141.201/redfish/v1/Managers/CIMC/VirtualMedia/0
```

Step 4. Get the status of vmedia0.

```
user1@system1:/vol/apicbin$ curl -k -u admin:MyCIMCPassword
https://192.168.141.201/redfish/v1/Managers/CIMC/VirtualMedia/0
{
```

```
    "@odata.id":         "/redfish/v1/Managers/CIMC/VirtualMedia/0",
    "@odata.type":       "#VirtualMedia.v1_4_0.VirtualMedia",
    "@odata.context":    "/redfish/v1/$metadata#VirtualMedia.VirtualMedia",
    "Description":       "Virtual Media Settings",
    "Image":             "192.168.125.200:/home/nfsshare/ucs-c225m6-huu-
4.3.2.240009.iso?nolock",
    "TransferMethod":    "Stream",
    "TransferProtocolType": "NFS",
    "WriteProtected":    true,
    "Inserted":          true,
    "ImageName":         "ucs-c225m6-huu-4.3.2.240009.iso",
    "Status": {
        "State":         "Enabled",
        "Health":        "OK"
    },
    "Id":                "0",
    "Name":              "Virtual CD",
    "MediaTypes":        ["CD", "DVD"],
    "Actions":           {
        "#VirtualMedia.EjectMedia":     {
            "target":
"/redfish/v1/Managers/CIMC/VirtualMedia/0/Actions/VirtualMedia.EjectMedia"
        },
        "#VirtualMedia.InsertMedia":    {
            "Image@Redfish.AllowableValues":        ["This parameter shall specify the
string URI of the remote media to be attached to the virtual media. (Required)"],
            "UserName@Redfish.AllowableValues":     ["This parameter shall contain a
string representing the username to be used when accessing the URI specified by the
Image parameter."],
            "Password@Redfish.AllowableValues":     ["This parameter shall contain a
string representing the password to be used when accessing the URI specified by the
Image parameter."],
            "WriteProtected@Redfish.AllowableValues":       ["true"],
            "TransferProtocolType@Redfish.AllowableValues": ["CIFS", "HTTP", "HTTPS",
"NFS"],
            "TransferMethod@Redfish.AllowableValues":       ["Stream"],
            "Inserted@Redfish.AllowableValues":     ["true"],
            "target":
"/redfish/v1/Managers/CIMC/VirtualMedia/0/Actions/VirtualMedia.InsertMedia"
        }
    }
}
```


Step 5. Sanitize the data.

```
user1@system1:/vol/apicbin$ curl -k -u admin:MyCIMCPassword
https://192.168.141.201/redfish/v1/Managers/CIMC/Actions/Oem/CiscoUCSExtensions.DataSan
itize -XPOST -d '{"HostSoftwareImage":"/redfish/v1/Managers/CIMC/VirtualMedia/0",
"SanitizeTargets":[ "HostDomainComponents","BoardDomainComponents"]}'
{
    "Messages":     [{
        "@odata.type":  "#Message.v1_1_1.Message",
        "MessageId":    "CiscoUCS.1.3.0.DataSanitizationOK",
        "Message":      "Performing data sanitization of targets Storage, VIC, BIOS,
CIMC on product APIC-SERVER-L4T serial number ABC123456DE.",
        "MessageArgs":  ["Performing data sanitization of targets Storage, VIC, BIOS,
CIMC on product APIC-SERVER-L4T serial number ABC123456DE."],
        "Severity":     "OK",
        "Resolution":   "No resolution is required."
    }, {
        "@odata.type":  "#Message.v1_1_1.Message",
        "MessageId":    "CiscoUCS.1.3.0.DataSanitizationOK",
        "Message":      "Performing storage drive data sanitization.",
```

```
            "MessageArgs":  ["Performing storage drive data sanitization."],
            "Severity":     "OK",
            "Resolution":   "No resolution is required."
        }],
        "Id":   "17",
        "Name": "Data Sanitization",
        "StartTime":    "2024-03-26T16:57:39+00:00",
        "TaskState":    "Running",
        "PercentComplete":      8,
        "@odata.id":    "/redfish/v1/TaskService/Tasks/17",
        "@odata.type":  "#Task.v1_4_0.Task"
}
```

Step 6. Get the status again to see the progress of the data sanitization process.

```
user1@system1:/vol/apicbin$ curl -k -u admin:MyCIMCPassword
https://192.168.141.201/redfish/v1/TaskService/Tasks/17 -XGET
{
    "@odata.id":    "/redfish/v1/TaskService/Tasks/17",
    "@odata.type":  "#Task.v1_5_0.Task",
    "@odata.context":       "/redfish/v1/$metadata#Task.Task",
    "Id":   "17",
    "Name": "Data Sanitization",
    "StartTime":    "2024-03-26T16:57:39+00:00",
    "PercentComplete":      8,
    "TaskState":    "Running",
    "Messages":     [{
        "@odata.type":  "#Message.v1_1_1.Message",
        "MessageId":    "CiscoUCS.1.3.0.DataSanitizationOK",
        "Message":      "Performing data sanitization of targets Storage, VIC, BIOS,
CIMC on product APIC-SERVER-L4T serial number ABC123456DE.",
        "MessageArgs":  ["Performing data sanitization of targets Storage, VIC, BIOS,
CIMC on product APIC-SERVER-L4T serial number ABC123456DE."],
        "Severity":     "OK",
        "Resolution":   "No resolution is required."
    }, {
        "@odata.type":  "#Message.v1_1_1.Message",
        "MessageId":    "CiscoUCS.1.3.0.DataSanitizationOK",
        "Message":      "Performing storage drive data sanitization.",
        "MessageArgs":  ["Performing storage drive data sanitization."],
        "Severity":     "OK",
        "Resolution":   "No resolution is required."
    }],
    "TaskMonitor":  "/redfish/v1/TaskService/Oem/TaskMonitor/17"
}
```

After the sanitization process completes, the server goes offline and is unusable because all your data, including server settings, is erased.

Americas Headquarters
Cisco Systems, Inc.
San Jose, CA

Asia Pacific Headquarters
Cisco Systems (USA) Pte. Ltd.
Singapore

Europe Headquarters
Cisco Systems International BV Amsterdam,
The Netherlands

Cisco has more than 200 offices worldwide. Addresses, phone numbers, and fax numbers are listed on the Cisco Website at **https://www.cisco.com/go/offices**.

Printed in USA Cxx-xxxxxx-xx 01/21