

```

{
  "vendor_identifier": "Aruba ClearPass",
  "version": "4.0",
  "name": "Aruba ClearPass Assets",
  "content_type": "application/json",
  "type": "REST_EVENT",
  "event_type": [
    "LEASE",
    "FIXED_ADDRESS_IPV4",
    "HOST_ADDRESS_IPV4",
    "FIXED_ADDRESS_IPV6",
    "HOST_ADDRESS_IPV6",
    "DISCOVERY_DATA"
  ],
  "headers": {
    "Accept": "*/*"
  },
  "instance_variables": [
  ],
  "steps": [
    {
      "name": "skip object deletion",
      "operation": "CONDITION",
      "condition": {
        "statements": [
          {
            "left": "${E:A:operation_type}",
            "op": "==",
            "right": "DELETE"
          }
        ],
        "condition_type": "OR",
        "stop": true
      }
    },
    {
      "name": "assignDeviceVariables from E:",
      "operation": "NOP",
      "body_list": [
        "${XC:COPY:{L:address}:{E:values{ip_address}}}$
{XC:COPY:{L:name}:{E:values{discovered_name}}}${XC:COPY:{L:type}:
{E:values{device_type}}}${XC:COPY:{L:Location}:
{E:values{device_location}}}${XC:COPY:{L:description}:
{E:values{network_component_description}}}${XC:COPY:{L:os_version}:
{E:values{os}}}${XC:COPY:{L:model}:{E:values{device_model}}}${XC:COPY:
{L:vendor}:{E:values{device_vendor}}"
      ]
    },
    {
      "name": "assignDeviceVariables from E: model",
      "operation": "NOP",
      "body_list": [
        "${XC:COPY:{L:model}:{E:values{device_model}}"
      ]
    }
  ]
}

```

```

    },
    {
      "name": "check if managed",
      "operation": "CONDITION",
      "condition": {
        "statements": [
          {
            "left": "${E:A:values{unmanaged}}",
            "op": "==",
            "right": "true"
          }
        ],
        "condition_type": "AND",
        "eval": "${XC:ASSIGN:{L:managed}:{S:False}}",
        "else_eval": "${XC:ASSIGN:{L:managed}:{S:True}}"
      }
    },
    {
      "name": "check if discovered mac_address is present",
      "operation": "CONDITION",
      "condition": {
        "statements": [
          {
            "left": "${E:A:values{mac_address}}",
            "op": "!=",
            "right": "None"
          },
          {
            "left": "${E:A:values{mac_address}}",
            "op": "!=",
            "right": ""
          }
        ],
        "condition_type": "AND",
        "eval": "${XC:COPY:{L:mac}:
{E:values{mac_address}}}",
        "next": "assignMac from L: for fixed"
      }
    },
    {
      "name": "check if discovered vmhost_mac_address is
present",
      "operation": "CONDITION",
      "condition": {
        "statements": [
          {
            "left": "${E:A:values{vmhost_mac_address}}",
            "op": "!=",
            "right": "None"
          },
          {
            "left": "${E:A:values{vmhost_mac_address}}",
            "op": "!=",
            "right": ""
          }
        ]
      }
    }
  ]
}

```

```

        }
    ],
    "condition_type": "AND",
    "eval": "${XC:COPY:{L:mac}:
{E:values{vmhost_mac_address}}}",
    "next": "assignMac from L: for fixed"
}
},
{
present",
    "name": "check if discovered vport_mac_address is
present",
    "operation": "CONDITION",
    "condition": {
        "statements": [
            {
                "left": "${E:A:values{vport_mac_address}}",
                "op": "!=",
                "right": "None"
            },
            {
                "left": "${E:A:values{vport_mac_address}}",
                "op": "!=",
                "right": ""
            }
        ],
        "condition_type": "AND",
        "eval": "${XC:COPY:{L:mac}:
{E:values{vport_mac_address}}}",
        "next": "assignMac from L: for fixed"
    }
},
{
    "name": "Stop if no mac",
    "operation": "CONDITION",
    "condition": {
        "statements": [
            {
                "left": "1",
                "op": "==",
                "right": "1"
            }
        ],
        "condition_type": "AND",
        "stop": true
    }
},
{
    "name": "assignMac from L: for fixed",
    "operation": "NOP",
    "body_list": [
        "${XC:COPY:{L:Mac1}:{L:mac}}${XC:FORMAT:TRUNCATE:
{L:Mac1}:{2t}}",
        "${XC:COPY:{L:Mac2}:{L:mac}}${XC:FORMAT:TRUNCATE:
{L:Mac2}:{5t}}${XC:FORMAT:TRUNCATE:{L:Mac2}:{-2f}}",

```

```

        "${XC:COPY:{L:Mac3}:{L:mac}}${XC:FORMAT:TRUNCATE:
{L:Mac3}:{8t}}${XC:FORMAT:TRUNCATE:{L:Mac3}:{-2f}}",
        "${XC:COPY:{L:Mac4}:{L:mac}}${XC:FORMAT:TRUNCATE:
{L:Mac4}:{11t}}${XC:FORMAT:TRUNCATE:{L:Mac4}:{-2f}}",
        "${XC:COPY:{L:Mac5}:{L:mac}}${XC:FORMAT:TRUNCATE:
{L:Mac5}:{14t}}${XC:FORMAT:TRUNCATE:{L:Mac5}:{-2f}}",
        "${XC:COPY:{L:Mac6}:{L:mac}}${XC:FORMAT:TRUNCATE:
{L:Mac6}:{-2f}}",
        "${XC:COPY:{L:MacFull}:{L:mac}}"
    ]
},
{
    "name": "Get Check if duplicate endpoint with Fixed",
    "operation": "GET",
    "parse": "JSON",
    "headers": {
        "Authorization": "Bearer ${S:A:SESSID}"
    },
    "transport": {
        "path": "/api/endpoint/mac-address/${L:A:Mac1}$
{L:A:Mac2}${L:A:Mac3}${L:A:Mac4}${L:A:Mac5}${L:A:Mac6}"
    },
    "result": [{
        "codes": "200,201,202,203,204,404,405",
        "next": "Skip if modify event and no mac address
with Fixed"
    ]
},
{
    "name": "Skip if modify event and no mac address with
Fixed",
    "operation": "CONDITION",
    "condition": {
        "statements": [
            {
                "left": "${P:A:mac_address}",
                "op": "!=",
                "right": ""
            }
        ],
        "condition_type": "AND",
        "next": "check for Threat Category"
    }
},
{
    "name": "Stop everthing if duplicate is found and it
didn't skip in previous step",
    "operation": "CONDITION",
    "condition": {
        "statements": [
            {
                "left": "${P:A:mac_address}",
                "op": "!=",
                "right": ""
            }
        ]
    }
}

```

```

        }
    ],
    "condition_type": "OR",
    "stop": true
}
},
{
    "name": "Add an endpoint from a Fixed",
    "operation": "POST",
    "parse": "JSON",
    "headers": {
        "Authorization": "Bearer ${S:A:SESSID}"
    },
    "transport": {
        "path": "/api/endpoint"
    },
    "body_list": [
        "{",
        "\"mac_address\": \"${L:A:MacFull}\"",
        "\"status\": \"${L:A:managed}\"",
        "\"description\": \"Added via API at ${UT:A:TIME}\"",
        "\"attributes\": {",
            "\"client_hostname\": \"${L:A:name}\"",
            "\"Device Type\": \"${L:A:type}\"",
            "\"Device Vendor\": \"${L:A:vendor}\"",
            "\"Location\": \"${L:A:Location}\"",
            "\"Model\": \"${L:A:model}\"",
            "\"Infoblox DHCP Fingerprint\":",
            "\"Infoblox Managed\": \"${L:A:managed}\"",
            "\"Infoblox Last Known IP\": \"${L:A:address}\"",
            "\"OS Version\": \"${L:A:os_version}\"",
        },
    ]
},
{
    "name": "Testing fixed",
    "operation": "POST",
    "parse": "JSON",
    "headers": {
        "Content-Type": "application/json",
        "User-Agent": "Infoblox Security Integration",
        "Accept": "*/*"
    },
    "transport": {
        "path": "/async_netd/deviceprofiler/endpoints"
    },
    "body_list": [
        "{",
        "\"mac\": \"${L:A:MacFull}\"",
        "\"ip\": \"${L:A:address}\"",

```

```
        "\hostname\": \"${L:A:name}\",",
        "\device\":{",
            "\family\": \"${L:A:vendor}\",",
            "\category\": \"${L:A:type}\",",
            "\name\": \"${L:A:name}\"",
        },
    ]
},
{
    "name": "end of adding a Fixed",
    "operation": "CONDITION",
    "condition": {
        "statements": [
            {
                "left": "1",
                "op": "==",
                "right": "1"
            }
        ],
        "condition_type": "AND",
        "stop": true
    }
},
```

```

    {
      "name": "check for Threat Category",
      "operation": "CONDITION",
      "condition": {
        "condition_type": "AND",
        "statements": [
          {
            "left": "${P:A:attributes{Infoblox Threat
Category}}",
            "op": "==",
            "right": ""
          }
        ],
        "eval": "${XC:ASSIGN:{L:ThreatCategory}:
{S:Unknown}}",
        "else_eval": "${XC:COPY:{L:ThreatCategory}:
{P:attributes{Infoblox Threat Category}}}"
      }
    },
    {
      "name": "check for Threat Detection Device IP",
      "operation": "CONDITION",
      "condition": {
        "condition_type": "AND",
        "statements": [
          {
            "left": "${P:A:attributes{Infoblox Threat
Detection Device IP}}",
            "op": "==",
            "right": ""
          }
        ],
        "eval": "${XC:ASSIGN:{L:ThreatDetection}:
{S:Unknown}}",
        "else_eval": "${XC:COPY:{L:ThreatDetection}:
{P:attributes{Infoblox Threat Detection Device IP}}}"
      }
    },
    {
      "name": "check for Threat Name",
      "operation": "CONDITION",
      "condition": {
        "condition_type": "AND",
        "statements": [

```

```

        {
            "left": "${P:A:attributes{Infoblox Threat
Name}}",
            "op": "==",
            "right": ""
        }
    ],
    "eval": "${XC:ASSIGN:{L:ThreatName}:{S:Unknown}}",
    "else_eval": "${XC:COPY:{L:ThreatName}:
{P:attributes{Infoblox Threat Name}}}"
    }
},
{
    "name": "check for Threat Severity",
    "operation": "CONDITION",
    "condition": {
        "condition_type": "AND",
        "statements": [
            {
                "left": "${P:A:attributes{Infoblox Threat
Severity}}",
                "op": "==",
                "right": ""
            }
        ],
        "eval": "${XC:ASSIGN:{L:ThreatSeverity}:
{S:Unknown}}",
        "else_eval": "${XC:COPY:{L:ThreatSeverity}:
{P:attributes{Infoblox Threat Severity}}}"
    }
},
{
    "name": "check for Threat Status",
    "operation": "CONDITION",
    "condition": {
        "condition_type": "AND",
        "statements": [
            {
                "left": "${P:A:attributes{Infoblox Threat
Status}}",
                "op": "==",
                "right": ""
            }
        ],
        "eval": "${XC:ASSIGN:{L:ThreatStatus}:{S:Other}}",
        "else_eval": "${XC:COPY:{L:ThreatStatus}:
{P:attributes{Infoblox Threat Status}}}"
    }
},
{
    "name": "Check if fingerprint is unknown",
    "operation": "CONDITION",
    "condition": {
        "condition_type": "AND",

```



```

        "statements": [
            {
                "left": "${P:A:PARSE[0]}{fingerprint}",
                "op": "==",
                "right": ""
            }
        ],
        "eval": "${XC:ASSIGN:{L:fingerprint}:{S:Unknown}}",
        "else_eval": "${XC:COPY:{L:fingerprint}:{P:PARSE[0]}
{fingerprint}}}"
    },
    {
        "name": "Check if Ruleid is unknown",
        "operation": "CONDITION",
        "condition": {
            "condition_type": "AND",
            "statements": [
                {
                    "left": "${P:A:attributes{Infoblox
RuleId}}",
                    "op": "==",
                    "right": ""
                }
            ],
            "eval": "${XC:ASSIGN:{L:RuleId}:{S:Unknown}}",
            "else_eval": "${XC:COPY:{L:RuleId}:
{P:attribute{Infoblox RuleId}}}"
        }
    },
    {
        "name": "Check if RuleCategory is unknown",
        "operation": "CONDITION",
        "condition": {
            "condition_type": "AND",
            "statements": [
                {
                    "left": "${P:A:attributes{Infoblox
RuleCategory}}",
                    "op": "==",
                    "right": ""
                }
            ],
            "eval": "${XC:ASSIGN:{L:RuleCategory}:{S:Unknown}}",
            "else_eval": "${XC:COPY:{L:RuleCategory}:
{P:attributes{Infoblox RuleCategory}}}"
        }
    },

```

```

    {
      "name": "Modify an endpoint",
      "operation": "PUT",
      "parse": "JSON",
      "headers": {
        "Authorization": "Bearer ${S:A:SESSID}"
      },
      "transport": {
        "path": "/api/endpoint/mac-address/${L:A:Mac1}${L:A:Mac2}${L:A:Mac3}${L:A:Mac4}${L:A:Mac5}${L:A:Mac6}"
      },
      "body_list": [
        "{",
        "\"mac_address\": \"${L:A:MacFull}\"",
        "\"status\": \"${L:A:managed}\"",
        "\"description\": \"Added via API at ${UT:A:TIME}\"",
        "\",",
        "\"attributes\": {",
        "\"client_hostname\": \"${L:A:name}\"",
        "\"Device Type\": \"${L:A:type}\"",
        "\"Device Vendor\": \"${L:A:vendor}\"",
        "\"Location\": \"${L:A:Location}\"",
        "\"Model\": \"${L:A:model}\"",
        "\"Infoblox Last Known IP\": \"${L:A:address}\"",
        "\",",
        "\"OS Version\": \"${L:A:os_version}\"",
        "\"Infoblox Managed\": \"${L:A:managed}\"",
        "\"Infoblox DHCP Fingerprint\": \"${L:A:fingerprint}\"",
        "\"Infoblox Threat Category\": \"${L:A:ThreatCategory}\"",
        "\"Infoblox Threat Detection Device IP\": \"${L:A:ThreatDetection}\"",
        "\"Infoblox Threat Name\": \"${L:A:ThreatName}\"",
        "\",",
        "\"Infoblox Threat Severity\": \"${L:A:ThreatSeverity}\"",
        "\"Infoblox Threat Status\": \"${L:A:ThreatStatus}\"",
        "\"Infoblox RuleId\": \"${L:A:RuleId}\"",
        "\"Infoblox RuleCategory\": \"${L:A:RuleCategory}\"",
        "\",",
        "}"
      ],
    },
    {
      "name": " modify",
      "operation": "POST",
      "parse": "JSON",
      "headers": {
        "Content-Type": "application/json",
        "User-Agent": "Infoblox Security Integration",

```

```

    "Accept": "*/*"
  },
  "transport": {
    "path": "/async_netd/deviceprofiler/endpoints"
  },
  "body_list": [
    "{",
    "\mac\": \"${L:A:MacFull}\",",
    "\ip\": \"${L:A:address}\",",
    "\hostname\": \"${L:A:name}\",",
    "\device\": {",
    "\family\": \"${L:A:vendor}\",",
    "\category\": \"${L:A:type}\",",
    "\name\": \"${L:A:name}\"",
    "}",
    "}"
  ]
},
{
  "name": "Stop Modify",
  "operation": "CONDITION",
  "condition": {
    "statements": [
      {
        "left": "1",
        "op": "==",
        "right": "1"
      }
    ],
    "condition_type": "AND",
    "stop": true
  }
}

```

