```
{
   "name": "DXL_RPZ/Tunnel_Event",
   "version": "3.0",
   "type": "DXL_EVENT",
   "event_type": [
      "RPZ",
      "TUNNEL"
   ],
   "vendor_identifier": "McAfee",
   "dxl_topic": "/open/threat/v1/infoblox",
   "quoting": "ASIS",
   "instance_variables": [
      {
         "name": "DXL_MessageFormat",
         "type": "STRING"
      }
   ],
   "steps": [
      {
         "name": "Debug#0",
         "operation": "NOP",
         "body": "${XC:DEBUG:{H:}}${XC:DEBUG:{E:}}${XC:DEBUG:
{I:}}${XC:DEBUG:{L:}}${XC:DEBUG:{S:}}${XC:DEBUG:{P:}}${XC:DEBUG:
{UT:}}${XC:DEBUG:{R:}}"
      },
      {
         "name": "init_internal_data",
         "operation": "VARIABLEOP",
         "variable_ops": [
            {
               "operation": "ASSIGN",
               "type": "DICTIONARY",
               "destination": "L:internal",
               "keys": [
                  "analyzer_ipv4",
                  "analyzer_ipv6",
                  "source_ipv4",
                  "source_ipv6",
                  "target_ipv4",
                  "target_ipv6",
                  "severity"
               ],
```

```
                "values": [
                    "",
                    "",
                    "",
                    "",
                    "",
                    "",
                    "7"
                ]
            }
        ]
    },
    {
        "name": "Debug#1",
        "operation": "NOP",
        "body": "${XC:DEBUG:{H:}}${XC:DEBUG:{E:}}${XC:DEBUG:
{I:}}${XC:DEBUG:{L:}}${XC:DEBUG:{S:}}${XC:DEBUG:{P:}}${XC:DEBUG:
{UT:}}${XC:DEBUG:{R:}}"
    },
    {
        "name": "is_analyzer_ipv4",
        "operation": "CONDITION",
        "condition": {
            "statements": [
                {
                    "left": "${E::member_ip}",
                    "op": "!~",
                    "right": ":"
                }
            ],
            "condition_type": "AND",
            "eval": "${XC:COPY:{L:internal{analyzer_ipv4}}:
{E:member_ip}}",
            "else_eval": "${XC:COPY:{L:internal{analyzer_ipv6}}:
{E:member_ip}}"
        }
    },
    {
        "name": "Debug#2",
        "operation": "NOP",
        "body": "${XC:DEBUG:{H:}}${XC:DEBUG:{E:}}${XC:DEBUG:
{I:}}${XC:DEBUG:{L:}}${XC:DEBUG:{S:}}${XC:DEBUG:{P:}}${XC:DEBUG:
```

```
{UT:}}${XC:DEBUG:{R:}}"
        },
        {
            "name": "is_source_ipv4",
            "operation": "CONDITION",
            "condition": {
                "statements": [
                    {
                        "left": "${E::source_ip}",
                        "op": "!~",
                        "right": ":"
                    }
                ],
                "condition_type": "AND",
                "eval": "${XC:COPY:{L:internal{source_ipv4}}:
{E:source_ip}}${XC:ASSIGN:{L:IPv}:{I:4}}",
                "else_eval": "${XC:COPY:{L:internal{source_ipv6}}:
{E:source_ip}}${XC:ASSIGN:{L:IPv}:{I:6}}"
            }
        },
        {
            "name": "Debug#3",
            "operation": "NOP",
            "body": "${XC:DEBUG:{H:}}${XC:DEBUG:{E:}}${XC:DEBUG:
{I:}}${XC:DEBUG:{L:}}${XC:DEBUG:{S:}}${XC:DEBUG:{P:}}${XC:DEBUG:
{UT:}}${XC:DEBUG:{R:}}"
        },
        {
            "name": "check rpz or tunnel to assign destination_ip",
            "operation": "CONDITION",
            "condition": {
                "statements": [
                    {
                        "left": "${E::event_type}",
                        "op": "==",
                        "right": "TUNNEL"
                    }
                ],
                "condition_type": "AND",
                "next": "is_target_ipv4 for TUNNEL"
            }
        },
```

```
        {
            "name": "Debug#a",
            "operation": "NOP",
            "body": "${XC:DEBUG:{H:}}${XC:DEBUG:{E:}}${XC:DEBUG:
{I:}}${XC:DEBUG:{L:}}${XC:DEBUG:{S:}}${XC:DEBUG:{P:}}${XC:DEBUG:
{UT:}}${XC:DEBUG:{R:}}"
        },
        {
            "name": "is_target_ipv4 for RPZ",
            "operation": "CONDITION",
            "condition": {
                "statements": [
                    {
                        "left": "${E::destination_ip}",
                        "op": "!~",
                        "right": ":"
                    }
                ],
                "condition_type": "AND",
                "eval": "${XC:COPY:{L:internal{target_ipv4}}:{E:destination_ip}}",
                "else_eval": "${XC:COPY:{L:internal{target_ipv6}}:
{E:destination_ip}}",
                "next": "check if rpz or tunnel event for severity",
                "else_next": "check if rpz or tunnel event for severity"
            }
        },
        {
            "name": "Debug#b",
            "operation": "NOP",
            "body": "${XC:DEBUG:{H:}}${XC:DEBUG:{E:}}${XC:DEBUG:
{I:}}${XC:DEBUG:{L:}}${XC:DEBUG:{S:}}${XC:DEBUG:{P:}}${XC:DEBUG:
{UT:}}${XC:DEBUG:{R:}}"
        },
        {
            "name": "is_target_ipv4 for TUNNEL",
            "operation": "CONDITION",
            "condition": {
                "statements": [
                    {
                        "left": "${E::source_ip}",
                        "op": "!~",
                        "right": ":"
```

```
                }
            ],
            "condition_type": "AND",
            "eval": "${XC:COPY:{L:internal{target_ipv4}}:{E:source_ip}}",
            "else_eval": "${XC:COPY:{L:internal{target_ipv6}}:
{E:source_ip}}"
        }
    },
    {
        "name": "Debug#4",
        "operation": "NOP",
        "body": "${XC:DEBUG:{H:}}${XC:DEBUG:{E:}}${XC:DEBUG:
{I:}}${XC:DEBUG:{L:}}${XC:DEBUG:{S:}}${XC:DEBUG:{P:}}${XC:DEBUG:
{UT:}}${XC:DEBUG:{R:}}"
    },
    {
        "name": "check if rpz or tunnel event for severity",
        "operation": "CONDITION",
        "condition": {
            "statements": [
                {
                    "left": "${E::event_type}",
                    "op": "!=",
                    "right": "TUNNEL"
                }
            ],
            "condition_type": "AND",
            "eval": "${XC:COPY:{L:rpz_severity}:{E:rpz_severity}}",
            "next": "is_severity_7"
        }
    },
    {
        "name": "Debug#4.1",
        "operation": "NOP",
        "body": "${XC:DEBUG:{H:}}${XC:DEBUG:{E:}}${XC:DEBUG:
{I:}}${XC:DEBUG:{L:}}${XC:DEBUG:{S:}}${XC:DEBUG:{P:}}${XC:DEBUG:
{UT:}}${XC:DEBUG:{R:}}"
    },
    {
        "name": "Get RPZ tunnel event",
        "operation": "GET",
        "transport": {
```

```
            "path": "record:rpz:cname?name~=/${E:A:domain_name}
&_return_fields=rp_zone"
         },
         "wapi": "v2.7"
      },
      {
         "name": "Debug#4.2",
         "operation": "NOP",
         "body": "${XC:DEBUG:{H:}}${XC:DEBUG:{E:}}${XC:DEBUG:
{I:}}${XC:DEBUG:{L:}}${XC:DEBUG:{S:}}${XC:DEBUG:{P:}}${XC:DEBUG:
{UT:}}${XC:DEBUG:{R:}}"
      },
      {
         "name": "Get RPZ tunnel event severity",
         "operation": "GET",
         "transport": {
            "path": "zone_rp?fqdn=${P:A:PARSE[0]{rp_zone}}
&_return_fields=rpz_severity"
         },
         "wapi": "v2.7"
      },
      {
         "name": "Debug#4.3",
         "operation": "NOP",
         "body": "${XC:DEBUG:{H:}}${XC:DEBUG:{E:}}${XC:DEBUG:
{I:}}${XC:DEBUG:{L:}}${XC:DEBUG:{S:}}${XC:DEBUG:{P:}}${XC:DEBUG:
{UT:}}${XC:DEBUG:{R:}}"
      },
      {
         "name": "assign tunneling severity level",
         "operation": "CONDITION",
         "condition": {
            "statements": [
               {
                  "left": "${E::event_type}",
                  "op": "==",
                  "right": "TUNNEL"
               }
            ],
            "condition_type": "AND",
            "eval": "${XC:COPY:{L:rpz_severity}:{P:PARSE[0]
{rpz_severity}}}",
            "next": "is_severity_7"
```

```
            }
        },
        {
            "name": "Debug#c",
            "operation": "NOP",
            "body": "${XC:DEBUG:{H:}}${XC:DEBUG:{E:}}${XC:DEBUG:
{I:}}${XC:DEBUG:{L:}}${XC:DEBUG:{S:}}${XC:DEBUG:{P:}}${XC:DEBUG:
{UT:}}${XC:DEBUG:{R:}}"
        },
        {
            "name": "is_severity_7",
            "operation": "CONDITION",
            "condition": {
                "statements": [
                    {
                        "left": "${L::rpz_severity}",
                        "op": "==",
                        "right": "INFORMATIONAL"
                    }
                ],
                "condition_type": "AND",
                "eval": "${XC:ASSIGN:{L:internal{severity}}:{I:7}}",
                "next": "severity_found"
            }
        },
        {
            "name": "Debug#5",
            "operation": "NOP",
            "body": "${XC:DEBUG:{H:}}${XC:DEBUG:{E:}}${XC:DEBUG:
{I:}}${XC:DEBUG:{L:}}${XC:DEBUG:{S:}}${XC:DEBUG:{P:}}${XC:DEBUG:
{UT:}}${XC:DEBUG:{R:}}"
        },
        {
            "name": "is_severity_4",
            "operation": "CONDITION",
            "condition": {
                "statements": [
                    {
                        "left": "${L::rpz_severity}",
                        "op": "==",
                        "right": "WARNING"
                    }
```

```
            ],
            "condition_type": "AND",
            "eval": "${XC:ASSIGN:{L:internal{severity}}:{I:4}}",
            "next": "severity_found"
        }
    },
    {
        "name": "Debug#6",
        "operation": "NOP",
        "body": "${XC:DEBUG:{H:}}${XC:DEBUG:{E:}}${XC:DEBUG:
{I:}}${XC:DEBUG:{L:}}${XC:DEBUG:{S:}}${XC:DEBUG:{P:}}${XC:DEBUG:
{UT:}}${XC:DEBUG:{R:}}"
    },
    {
        "name": "is_severity_2",
        "operation": "CONDITION",
        "condition": {
            "statements": [
                {
                    "left": "${L::rpz_severity}",
                    "op": "==",
                    "right": "MAJOR"
                }
            ],
            "condition_type": "AND",
            "eval": "${XC:ASSIGN:{L:internal{severity}}:{I:2}}",
            "next": "severity_found"
        }
    },
    {
        "name": "Debug#7",
        "operation": "NOP",
        "body": "${XC:DEBUG:{H:}}${XC:DEBUG:{E:}}${XC:DEBUG:
{I:}}${XC:DEBUG:{L:}}${XC:DEBUG:{S:}}${XC:DEBUG:{P:}}${XC:DEBUG:
{UT:}}${XC:DEBUG:{R:}}"
    },
    {
        "name": "is_severity_1",
        "operation": "CONDITION",
        "condition": {
            "statements": [
                {
```

```
                    "left": "${L::rpz_severity}",
                    "op": "==",
                    "right": "CRITICAL"
                }
            ],
            "condition_type": "AND",
            "eval": "${XC:ASSIGN:{L:internal{severity}}:{I:1}}"
        }
    },
    {
        "name": "Debug#8",
        "operation": "NOP",
        "body": "${XC:DEBUG:{H:}}${XC:DEBUG:{E:}}${XC:DEBUG:
{I:}}${XC:DEBUG:{L:}}${XC:DEBUG:{S:}}${XC:DEBUG:{P:}}${XC:DEBUG:
{UT:}}${XC:DEBUG:{R:}}"
    },
    {
        "name": "severity_found",
        "operation": "NOP",
        "body": ""
    },
    {
        "name": "Debug#9",
        "operation": "NOP",
        "body": "${XC:DEBUG:{H:}}${XC:DEBUG:{E:}}${XC:DEBUG:
{I:}}${XC:DEBUG:{L:}}${XC:DEBUG:{S:}}${XC:DEBUG:{P:}}${XC:DEBUG:
{UT:}}${XC:DEBUG:{R:}}"
    },
    {
        "name": "check rpz or tunnel for source_port",
        "operation": "CONDITION",
        "condition": {
            "statements": [
                {
                    "left": "${E::event_type}",
                    "op": "==",
                    "right": "RPZ"
                }
            ],
            "condition_type": "AND",
            "eval": "${XC:COPY:{L:source_port}:{E:source_port}}",
            "else_eval": "${XC:ASSIGN:{L:source_port}:{I:00000}}"
```

```
            }
        },
        {
            "name": "Debug#d",
            "operation": "NOP",
            "body": "${XC:DEBUG:{H:}}${XC:DEBUG:{E:}}${XC:DEBUG:
{I:}}${XC:DEBUG:{L:}}${XC:DEBUG:{S:}}${XC:DEBUG:{P:}}${XC:DEBUG:
{UT:}}${XC:DEBUG:{R:}}"
        },
        {
            "name": "check rpz or tunnel for threat type",
            "operation": "CONDITION",
            "condition": {
                "statements": [
                    {
                        "left": "${E::event_type}",
                        "op": "==",
                        "right": "RPZ"
                    }
                ],
                "condition_type": "AND",
                "eval": "${XC:COPY:{L:rpz_type}:{E:rpz_type}}",
                "else_eval": "${XC:COPY:{L:rpz_type}:{E:event_type}}"
            }
        },
        {
            "name": "Debug#e",
            "operation": "NOP",
            "body": "${XC:DEBUG:{H:}}${XC:DEBUG:{E:}}${XC:DEBUG:
{I:}}${XC:DEBUG:{L:}}${XC:DEBUG:{S:}}${XC:DEBUG:{P:}}${XC:DEBUG:
{UT:}}${XC:DEBUG:{R:}}"
        },
        {
            "name": "set threatName ruleName DetectedUTC",
            "operation": "CONDITION",
            "condition": {
                "statements": [
                    {
                        "left": "${E::event_type}",
                        "op": "==",
                        "right": "RPZ"
                    }
```

```
                ],
                "condition_type": "AND",
                "eval": "${XC:COPY:{L:ruleName}:
{E:rule_name}}${XC:FORMAT:TRUNCATE:{L:ruleName}:
{-128f}}${XC:COPY:{L:threatName}:
{E:query_name}}${XC:FORMAT:TRUNCATE:{L:threatName}:
{-128f}}${XC:COPY:{L:DetectedUTC}:{E:timestamp}}${XC:ASSIGN:
{L:Obj_ref}:{S:}}${XC:ASSIGN:{L:network_view}:{S:default}}",
                "else_eval": "${XC:COPY:{L:ruleName}:
{E:domain_name}}${XC:FORMAT:TRUNCATE:{L:ruleName}:
{-128f}}${XC:COPY:{L:threatName}:
{E:domain_name}}${XC:FORMAT:TRUNCATE:{L:threatName}:
{-128f}}${XC:COPY:{L:DetectedUTC}:{E:timestamp}}${XC:ASSIGN:
{L:Obj_ref}:{S:}}${XC:ASSIGN:{L:network_view}:{S:default}}"
            }
        },
        {
            "name": "Debug#10",
            "operation": "NOP",
            "body": "${XC:DEBUG:{H:}}${XC:DEBUG:{E:}}${XC:DEBUG:
{I:}}${XC:DEBUG:{L:}}${XC:DEBUG:{S:}}${XC:DEBUG:{P:}}${XC:DEBUG:
{UT:}}${XC:DEBUG:{R:}}"
        },
        {
            "name": "set threatActionTaken threatHandled",
            "operation": "CONDITION",
            "condition": {
                "statements": [
                    {
                        "left": "${E::rpz_policy}",
                        "op": "==",
                        "right": "PASSTHRU"
                    }
                ],
                "condition_type": "AND",
                "eval": "${XC:ASSIGN:{L:threatActionTaken}:{S:}}${XC:ASSIGN:
{L:threatHandled}:{I:0}}",
                "else_eval": "${XC:ASSIGN:{L:threatActionTaken}:
{S:block}}${XC:ASSIGN:{L:threatHandled}:{I:1}}"
            }
        },
        {
```

```
            "name": "Debug#11",
            "operation": "NOP",
            "body": "${XC:DEBUG:{H:}}${XC:DEBUG:{E:}}${XC:DEBUG:
{I:}}${XC:DEBUG:{L:}}${XC:DEBUG:{S:}}${XC:DEBUG:{P:}}${XC:DEBUG:
{UT:}}${XC:DEBUG:{R:}}"
        },
        {
            "name": "check GUID",
            "operation": "CONDITION",
            "condition": {
                "condition_type": "OR",
                "statements": [
                    {
                        "left": "${E:A:ip.extattrs{ePO_GUID}}",
                        "op": "==",
                        "right": ""
                    }
                ],
                "eval": "${XC:COPY:{L:GUID}:{UT:UUID}}${XC:ASSIGN:
{L:GUIDtype}:{S:generated}}",
                "else_eval": "${XC:COPY:{L:GUID}:
{E:ip.extattrs{ePO_GUID}}}${XC:ASSIGN:{L:GUIDtype}:{S:local}}"
            }
        },
        {
            "name": "Debug#12",
            "operation": "NOP",
            "body": "${XC:DEBUG:{H:}}${XC:DEBUG:{E:}}${XC:DEBUG:
{I:}}${XC:DEBUG:{L:}}${XC:DEBUG:{S:}}${XC:DEBUG:{P:}}${XC:DEBUG:
{UT:}}${XC:DEBUG:{R:}}"
        },
        {
            "name": "jump if have GUID or no WAPI credentials",
            "operation": "CONDITION",
            "condition": {
                "condition_type": "OR",
                "statements": [
                    {
                        "left": "${L:A:GUIDtype}",
                        "op": "==",
                        "right": "local"
                    },
```

```
                {
                    "left": "${UT:A:WAPIUSERNAME}",
                    "op": "==",
                    "right": ""
                }
            ],
            "next": "CheckEventTypeForEventId"
        }
    },
    {
        "name": "CheckEventTypeForEventId",
        "operation": "CONDITION",
        "condition": {
            "condition_type": "AND",
            "statements": [
                {
                    "left": "${E::event_type}",
                    "op": "==",
                    "right": "TUNNEL"
                }
            ],
            "eval": "${XC:ASSIGN:{L:eventID}:{S:204151}}",
            "else_eval": "${XC:ASSIGN:{L:eventID}:{S:204150}}"
        }
    },
    {
        "name": "Debug#13",
        "operation": "NOP",
        "body": "${XC:DEBUG:{H:}}${XC:DEBUG:{E:}}${XC:DEBUG:
{I:}}${XC:DEBUG:{L:}}${XC:DEBUG:{S:}}${XC:DEBUG:{P:}}${XC:DEBUG:
{UT:}}${XC:DEBUG:{R:}}"
    },
    {
        "name": "check IPv6",
        "operation": "CONDITION",
        "condition": {
            "condition_type": "OR",
            "statements": [
                {
                    "left": "${L:A:IPv}",
                    "op": "==",
                    "right": "6"
```

```
                }
            ],
            "next": "Get IPv6Fixed _ref"
        }
    },
    {
        "name": "Debug#14",
        "operation": "NOP",
        "body": "${XC:DEBUG:{H:}}${XC:DEBUG:{E:}}${XC:DEBUG:
{I:}}${XC:DEBUG:{L:}}${XC:DEBUG:{S:}}${XC:DEBUG:{P:}}${XC:DEBUG:
{UT:}}${XC:DEBUG:{R:}}"
    },
    {
        "name": "Get IPv4Fixed _ref",
        "operation": "GET",
        "transport": {
            "path": "fixedaddress?ipv4addr=${E:U:source_ip}
&network_view=${L:U:network_view}&_return_fields=extattrs"
        },
        "wapi": "v2.7"
    },
    {
        "name": "Debug#15",
        "operation": "NOP",
        "body": "${XC:DEBUG:{H:}}${XC:DEBUG:{E:}}${XC:DEBUG:
{I:}}${XC:DEBUG:{L:}}${XC:DEBUG:{S:}}${XC:DEBUG:{P:}}${XC:DEBUG:
{UT:}}${XC:DEBUG:{R:}}"
    },
    {
        "operation": "CONDITION",
        "name": "wapi_response_getIPv4Fix_ref",
        "condition": {
            "condition_type": "AND",
            "statements": [
                {
                    "left": "${P:A:PARSE[0]{_ref}}",
                    "op": "!=",
                    "right": ""
                }
            ],
            "next": "Get_Objref"
        }
```

```
        },
        {
            "name": "Debug#16",
            "operation": "NOP",
            "body": "${XC:DEBUG:{H:}}${XC:DEBUG:{E:}}${XC:DEBUG:
{I:}}${XC:DEBUG:{L:}}${XC:DEBUG:{S:}}${XC:DEBUG:{P:}}${XC:DEBUG:
{UT:}}${XC:DEBUG:{R:}}"
        },
        {
            "name": "Get HostIPv4 _ref",
            "operation": "GET",
            "transport": {
                "path": "record:host?ipv4addr=${E:U:source_ip}&network_view=
${L:U:network_view}&_return_fields=extattrs"
            },
            "wapi": "v2.7"
        },
        {
            "name": "Debug#17",
            "operation": "NOP",
            "body": "${XC:DEBUG:{H:}}${XC:DEBUG:{E:}}${XC:DEBUG:
{I:}}${XC:DEBUG:{L:}}${XC:DEBUG:{S:}}${XC:DEBUG:{P:}}${XC:DEBUG:
{UT:}}${XC:DEBUG:{R:}}"
        },
        {
            "operation": "CONDITION",
            "name": "wapi_response_getIPv4Host_ref",
            "condition": {
                "condition_type": "AND",
                "statements": [
                    {
                        "left": "${P:A:PARSE[0]{_ref}}",
                        "op": "!=",
                        "right": ""
                    }
                ],
                "next": "Get_Objref"
            }
        },
        {
            "name": "Debug#18",
            "operation": "NOP",
```

```
            "body": "${XC:DEBUG:{H:}}${XC:DEBUG:{E:}}${XC:DEBUG:
{I:}}${XC:DEBUG:{L:}}${XC:DEBUG:{S:}}${XC:DEBUG:{P:}}${XC:DEBUG:
{UT:}}${XC:DEBUG:{R:}}"
        },
        {
            "name": "IPv4 object was not found",
            "operation": "CONDITION",
            "condition": {
                "condition_type": "OR",
                "statements": [
                    {
                        "left": "1",
                        "op": "==",
                        "right": "1"
                    }
                ],
                "next": "GET Lease data"
            }
        },
        {
            "name": "Debug#19",
            "operation": "NOP",
            "body": "${XC:DEBUG:{H:}}${XC:DEBUG:{E:}}${XC:DEBUG:
{I:}}${XC:DEBUG:{L:}}${XC:DEBUG:{S:}}${XC:DEBUG:{P:}}${XC:DEBUG:
{UT:}}${XC:DEBUG:{R:}}"
        },
        {
            "name": "Get IPv6Fixed _ref",
            "operation": "GET",
            "transport": {
                "path": "ipv6fixedaddress?ipv6addr=${E:U:source_ip}
&network_view=${L:U:network_view}&_return_fields=extattrs"
            },
            "wapi": "v2.7"
        },
        {
            "name": "Debug#20",
            "operation": "NOP",
            "body": "${XC:DEBUG:{H:}}${XC:DEBUG:{E:}}${XC:DEBUG:
{I:}}${XC:DEBUG:{L:}}${XC:DEBUG:{S:}}${XC:DEBUG:{P:}}${XC:DEBUG:
{UT:}}${XC:DEBUG:{R:}}"
        },
```

```
        {
            "operation": "CONDITION",
            "name": "wapi_response_getIPv6Fix_ref",
            "condition": {
                "condition_type": "AND",
                "statements": [
                    {
                        "left": "${P:A:PARSE[0]{_ref}}",
                        "op": "!=",
                        "right": ""
                    }
                ],
                "next": "Get_Objref"
            }
        },
        {
            "name": "Debug#21",
            "operation": "NOP",
            "body": "${XC:DEBUG:{H:}}${XC:DEBUG:{E:}}${XC:DEBUG:
{I:}}${XC:DEBUG:{L:}}${XC:DEBUG:{S:}}${XC:DEBUG:{P:}}${XC:DEBUG:
{UT:}}${XC:DEBUG:{R:}}"
        },
        {
            "name": "Get HostIPv6 _ref",
            "operation": "GET",
            "transport": {
                "path": "record:host?ipv6addr=${E:U:source_ip}&network_view=
${L:U:network_view}&_return_fields=extattrs"
            },
            "wapi": "v2.7"
        },
        {
            "name": "Debug#22",
            "operation": "NOP",
            "body": "${XC:DEBUG:{H:}}${XC:DEBUG:{E:}}${XC:DEBUG:
{I:}}${XC:DEBUG:{L:}}${XC:DEBUG:{S:}}${XC:DEBUG:{P:}}${XC:DEBUG:
{UT:}}${XC:DEBUG:{R:}}"
        },
        {
            "operation": "CONDITION",
            "name": "wapi_response_getIPv6Host_ref",
            "condition": {
```

```
            "condition_type": "AND",
            "statements": [
               {
                  "left": "${P:A:PARSE[0]{_ref}}",
                  "op": "!=",
                  "right": ""
               }
            ],
            "next": "Get_Objref"
         }
      },
      {
         "name": "Debug#23",
         "operation": "NOP",
         "body": "${XC:DEBUG:{H:}}${XC:DEBUG:{E:}}${XC:DEBUG:
{I:}}${XC:DEBUG:{L:}}${XC:DEBUG:{S:}}${XC:DEBUG:{P:}}${XC:DEBUG:
{UT:}}${XC:DEBUG:{R:}}"
      },
      {
         "name": "Get_Objref",
         "operation": "CONDITION",
         "condition": {
            "condition_type": "AND",
            "statements": [
               {
                  "left": "${P:A:PARSE[0]{_ref}}",
                  "op": "!=",
                  "right": ""
               }
            ],
            "eval": "${XC:COPY:{L:Obj_ref}:{P:PARSE[0]{_ref}}}"
         }
      },
      {
         "name": "Debug#24",
         "operation": "NOP",
         "body": "${XC:DEBUG:{H:}}${XC:DEBUG:{E:}}${XC:DEBUG:
{I:}}${XC:DEBUG:{L:}}${XC:DEBUG:{S:}}${XC:DEBUG:{P:}}${XC:DEBUG:
{UT:}}${XC:DEBUG:{R:}}"
      },
      {
         "name": "jump if no Obj_ref",
```

```
            "operation": "CONDITION",
            "condition": {
               "condition_type": "OR",
               "statements": [
                  {
                     "left": "${L:A:Obj_ref}",
                     "op": "==",
                     "right": ""
                  }
               ],
               "next": "GET Lease data"
            }
         },
         {
            "name": "Debug#25",
            "operation": "NOP",
            "body": "${XC:DEBUG:{H:}}${XC:DEBUG:{E:}}${XC:DEBUG:
{I:}}${XC:DEBUG:{L:}}${XC:DEBUG:{S:}}${XC:DEBUG:{P:}}${XC:DEBUG:
{UT:}}${XC:DEBUG:{R:}}"
         },
         {
            "name": "Update GUID",
            "operation": "PUT",
            "transport": {
               "path": "${L:A:Obj_ref}"
            },
            "wapi": "v2.7",
            "wapi_quoting": "JSON",
            "body_list": [
               "{\"extattrs+\":{\"ePO_GUID\": { \"value\": \"${L:A:GUID}\"},
\"DXL_LastEventSentAt\": { \"value\": \"${E:A:timestamp}\"}}}"
            ]
         },
         {
            "name": "Debug#26",
            "operation": "NOP",
            "body": "${XC:DEBUG:{H:}}${XC:DEBUG:{E:}}${XC:DEBUG:
{I:}}${XC:DEBUG:{L:}}${XC:DEBUG:{S:}}${XC:DEBUG:{P:}}${XC:DEBUG:
{UT:}}${XC:DEBUG:{R:}}"
         },
         {
            "name": "GET Lease data",
```

```
            "operation": "GET",
            "transport": {
               "path": "lease?address=${E::source_ip}&_return_fields=address
,client_hostname,ipv6_duid,binding_state,cltt,ends,fingerprint,hardware,ip
v6_prefix_bits,is_invalid_mac,network,network_view,never_ends,never_st
arts,protocol,served_by,server_host_name,starts,tstp,variable"¢           ÒÊ
            "wapi": "v2.7"
         },
         {
            "name": "Check if lease exists",
            "operation": "CONDITION",
            "condition": {
               "condition_type": "AND",
               "statements": [
                  {
                     "left": "${P::PARSE[0]}",
                     "op": "==",
                     "right": ""
                  }
               ],
               "next": "set variables to nothing because there is no lease"
            }
         },
         {
            "name": "Debug#43",
            "operation": "NOP",
            "body": "${XC:DEBUG:{H:}}${XC:DEBUG:{E:}}${XC:DEBUG:
{I:}}${XC:DEBUG:{L:}}${XC:DEBUG:{S:}}${XC:DEBUG:{P:}}${XC:DEBUG:
{UT:}}${XC:DEBUG:{R:}}"
         },
         {
            "name": "set Lease vars",
            "operation": "NOP",
            "body_list": [
               "${XC:COPY:{L:address}:{P:PARSE[0]{address}}}",
               "${XC:COPY:{L:binding_state}:{P:PARSE[0]{binding_state}}}",
               "${XC:COPY:{L:cltt}:{P:PARSE[0]{cltt}}}",
               "${XC:COPY:{L:ends}:{P:PARSE[0]{ends}}}",
               "${XC:COPY:{L:fingerprint}:{P:PARSE[0]{fingerprint}}}",
               "${XC:COPY:{L:hardware}:{P:PARSE[0]{hardware}}}",
               "${XC:COPY:{L:ipv6_prefix_bits}:{P:PARSE[0]
{ipv6_prefix_bits}}}",
               "${XC:COPY:{L:is_invalid_mac}:{P:PARSE[0]
```

```
{is_invalid_mac}}}",
            "${XC:COPY:{L:network}:{P:PARSE[0]{network}}}",
            "${XC:COPY:{L:network_view}:{P:PARSE[0]{network_view}}}",
            "${XC:COPY:{L:never_ends}:{P:PARSE[0]{never_ends}}}",
            "${XC:COPY:{L:never_starts}:{P:PARSE[0]{never_starts}}}",
            "${XC:COPY:{L:protocol}:{P:PARSE[0]{protocol}}}",
            "${XC:COPY:{L:served_by}:{P:PARSE[0]{served_by}}}",
            "${XC:COPY:{L:server_host_name}:{P:PARSE[0]
{server_host_name}}}",
            "${XC:COPY:{L:starts}:{P:PARSE[0]{starts}}}",
            "${XC:COPY:{L:variable}:{P:PARSE[0]{variable}}}"
        ]
    },
    {
        "name": "Check client_hostname",
        "operation": "CONDITION",
        "condition": {
            "condition_type": "AND",
            "statements": [
                {
                    "left": "${P::PARSE[0]{client_hostname}}",
                    "op": "!=",
                    "right": ""
                }
            ],
            "eval": "${XC:COPY:{L:client_hostname}:{P:PARSE[0]
{client_hostname}}}",
            "else_eval": "${XC:ASSIGN:{L:client_hostname}:{S:}}"
        }
    },
    {
        "name": "Check ipv6_duid",
        "operation": "CONDITION",
        "condition": {
            "condition_type": "AND",
            "statements": [
                {
                    "left": "${P::PARSE[0]{ipv6_duid}}",
                    "op": "!=",
                    "right": ""
                }
            ],
```

```
        "eval": "${XC:COPY:{L:ipv6_duid}:{P:PARSE[0]{ipv6_duid}}}",
        "else_eval": "${XC:ASSIGN:{L:ipv6_duid}:{S:}}"
    }
},
{
    "name": "skip to checking message type",
    "operation": "CONDITION",
    "condition": {
        "condition_type": "AND",
        "statements": [
            {
                "left": "1",
                "op": "==",
                "right": "1"
            }
        ],
        "next": "check DXL_MessageFormat"
    }
},
{
    "name": "set variables to nothing because there is no lease",
    "operation": "NOP",
    "body_list": [
        "${XC:ASSIGN:{L:address}:{S:}}",
        "${XC:ASSIGN:{L:binding_state}:{S:}}",
        "${XC:ASSIGN:{L:cltt}:{S:}}",
        "${XC:ASSIGN:{L:ends}:{S:}}",
        "${XC:ASSIGN:{L:fingerprint}:{S:}}",
        "${XC:ASSIGN:{L:hardware}:{S:}}",
        "${XC:ASSIGN:{L:ipv6_prefix_bits}:{S:}}",
        "${XC:ASSIGN:{L:is_invalid_mac}:{S:}}",
        "${XC:ASSIGN:{L:network}:{S:}}",
        "${XC:ASSIGN:{L:network_view}:{S:}}",
        "${XC:ASSIGN:{L:never_ends}:{S:}}",
        "${XC:ASSIGN:{L:never_starts}:{S:}}",
        "${XC:ASSIGN:{L:protocol}:{S:}}",
        "${XC:ASSIGN:{L:served_by}:{S:}}",
        "${XC:ASSIGN:{L:server_host_name}:{S:}}",
        "${XC:ASSIGN:{L:starts}:{S:}}",
        "${XC:ASSIGN:{L:variable}:{S:}}",
        "${XC:ASSIGN:{L:client_hostname}:{S:}}",
        "${XC:ASSIGN:{L:ipv6_duid}:{S:}}"
```

```
        ]
      },
      {
        "name": "check DXL_MessageFormat",
        "operation": "CONDITION",
        "condition": {
          "condition_type": "AND",
          "statements": [
            {
              "left": "${I::DXL_MessageFormat}",
              "op": "==",
              "right": "CEF"
            }
          ],
          "next": "send_CEF"
        }
      },
      {
        "name": "Debug#27",
        "operation": "NOP",
        "body": "${XC:DEBUG:{H:}}${XC:DEBUG:{E:}}${XC:DEBUG:
{I:}}${XC:DEBUG:{L:}}${XC:DEBUG:{S:}}${XC:DEBUG:{P:}}${XC:DEBUG:
{UT:}}${XC:DEBUG:{R:}}"
      },
      {
        "name": "send_OpenDXL",
        "operation": "DXL_SEND_EVENT",
        "body_list": [
          "{",
          "  \"eventMsgType\": \"Infoblox Security Event\",",
          "  \"eventMsgVersion\": \"1.0\",",
          "  \"event\":",
          "  {",
          "    \"category\": \"RPZ\",",
          "    \"eventDesc\": \"DNS RPZ event\",",
          "    \"eventId\": \"${L::eventID}\",",
          "    \"threatActionTaken\": \"${L::threatActionTaken}\",",
          "    \"threatHandled\": ${L::threatHandled},",
          "    \"threatName\": \"bad domain: ${L::threatName}\",",
          "    \"threatSeverity\": ${L::internal{severity}},",
          "    \"threatType\": \"${L::rpz_type}\",",
          "    \"analyzer\":",
```

```
"    {",
"      \"id\": \"S_INFBLX0802\",",
"      \"version\": \"8.2.1\",",
"      \"name\": \"NIOS\",",
"      \"detectionMethod\": \"RPZ\",",
"      \"hostName\": \"${E::member_name}\",",
"      \"detectedUTC\": \"${E::timestamp}\",",
"      \"ipv4\": \"${L::internal{analyzer_ipv4}}\",",
"      \"ipv6\": \"${L::internal{analyzer_ipv6}}\"",
"    },",
"    \"entity\":",
"    {",
"      \"ruleName\": \"${L::ruleName}\",",
"      \"id\": \"${L::GUID}\",",
"      \"groupName\": \"\",",
"      \"osPlatform\": \"\",",
"      \"osType\": \"\",",
"      \"type\": \"\",",
"      \"address\": \"${L::address}\",",
"      \"binding_state\": \"${L::binding_state}\",",
"      \"cltt\": \"${L::cltt}\",",
"      \"ends\": \"${L::ends}\",",
"      \"fingerprint\": \"${L::fingerprint}\",",
"      \"hardware\": \"${L::hardware}\",",
"      \"ipv6_prefix_bits\": \"${L::ipv6_prefix_bits}\",",
"      \"is_invalid_mac\": \"${L::is_invalid_mac}\",",
"      \"network\": \"${L::network}\",",
"      \"network_view\": \"${L::network_view}\",",
"      \"never_ends\": \"${L::never_ends}\",",
"      \"never_starts\": \"${L::never_starts}\",",
"      \"protocol\": \"${L::protocol}\",",
"      \"served_by\": \"${L::served_by}\",",
"      \"server_host_name\": \"${L::server_host_name}\",",
"      \"starts\": \"${L::starts}\",",
"      \"variable\": \"${L::variable}\",",
"      \"client_hostname\": \"${L::client_hostname}\",",
"      \"ipv6_duid\": \"${L::ipv6_duid}\",",
"      \"sessionID\": \"\"",
"    },",
"    \"source\":",
"    {",
"      \"ipv4\": \"${L::internal{source_ipv4}}\",",
```

```
            "      \"ipv6\": \"${L::internal{source_ipv6}}\",",
            "      \"port\": ${L::source_port}",
            "    },",
            "    \"target\":",
            "    {",
            "      \"ipv4\": \"${L::internal{target_ipv4}}\",",
            "      \"ipv6\": \"${L::internal{target_ipv6}}\",",
            "      \"port\": 53",
            "    }",
            "  }",
            "}"
         ],
         "dxl_topic": "/open/threat/v1/${E::event_type}/infoblox"
      },
      {
         "name": "Debug#28",
         "operation": "NOP",
         "body": "${XC:DEBUG:{H:}}${XC:DEBUG:{E:}}${XC:DEBUG:
{I:}}${XC:DEBUG:{L:}}${XC:DEBUG:{S:}}${XC:DEBUG:{P:}}${XC:DEBUG:
{UT:}}${XC:DEBUG:{R:}}"
      },
      {
         "name": "goFin",
         "operation": "CONDITION",
         "condition": {
            "condition_type": "OR",
            "statements": [
               {
                  "left": "1",
                  "op": "==",
                  "right": "1"
               }
            ],
            "next": "Fin"
         }
      },
      {
         "name": "Debug#29",
         "operation": "NOP",
         "body": "${XC:DEBUG:{H:}}${XC:DEBUG:{E:}}${XC:DEBUG:
{I:}}${XC:DEBUG:{L:}}${XC:DEBUG:{S:}}${XC:DEBUG:{P:}}${XC:DEBUG:
{UT:}}${XC:DEBUG:{R:}}"
```

```
        },
        {
            "name": "send_CEF",
            "operation": "DXL_SEND_EVENT",
            "body_list": [
                "{\"DXLCommonEvent\":{",
                "\"AgentGUID\": \"${L::GUID}\",",
                "\"Analyzer\":
\"${L::internal{analyzer_ipv4}}${L::internal{analyzer_ipv6}}\",",
                "\"AnalyzerDATVersion\": \"\",",
                "\"AnalyzerDetectionMethod\": \"RPZ\",",
                "\"AnalyzerHostName\": \"${E::member_name}\",",
                "\"AnalyzerIPV4\": \"${L::internal{analyzer_ipv4}}\",",
                "\"AnalyzerIPV6\": \"${L::internal{analyzer_ipv6}}\",",
                "\"AnalyzerMAC\": \"\",",
                "\"AnalyzerName\": \"NIOS\",",
                "\"AnalyzerVersion\": \"8.2.1\",",
                "\"DetectedUTC\": \"${L::DetectedUTC}\",",
                "\"ServerID\":
\"${L::internal{analyzer_ipv4}}${L::internal{analyzer_ipv6}}\",",
                "\"SourceIPV4\": \"${L::internal{source_ipv4}}\",",
                "\"SourceIPV6\": \"${L::internal{source_ipv6}}\",",
                "\"SourceMAC\": \"\",",
                "\"SourcePort\": \"${L::source_port}\",",
                "\"SourceProcessName\": \"\",",
                "\"SourceURL\": \"\",",
                "\"SourceUserName\": \"\",",
                "\"TargetFileName\": \"\",",
                "\"TargetHostName\": \"${E::member_name}\",",
                "\"TargetIPV4\": \"${L::internal{analyzer_ipv4}}\",",
                "\"TargetIPV6\": \"${L::internal{analyzer_ipv6}}\",",
                "\"TargetPort\": \"53\",",
                "\"TargetProcessName\": \"\",",
                "\"TargetProtocol\": \"dns\",",
                "\"TargetUserName\": \"\",",
                "\"ThreatActionTaken\": \"${L::threatActionTaken}\",",
                "\"ThreatCategory\": \"RPZ\",",
                "\"ThreatEventID\": \"${L::eventID}\",",
                "\"ThreatHandled\": \"${L::threatHandled}\",",
                "\"ThreatName\": \"bad domain: ${L::threatName}\",",
                "\"ThreatSeverity\": \"${L::internal{severity}}\",",
                "\"ThreatType\": \"${L::rpz_type}\",",
```

```
            "\"address\": \"${L::address}\",",
            "\"binding_state\": \"${L::binding_state}\",",
            "\"cltt\": \"${L::cltt}\",",
            "\"ends\": \"${L::ends}\",",
            "\"fingerprint\": \"${L::fingerprint}\",",
            "\"hardware\": \"${L::hardware}\",",
            "\"ipv6_prefix_bits\": \"${L::ipv6_prefix_bits}\",",
            "\"is_invalid_mac\": \"${L::is_invalid_mac}\",",
            "\"network\": \"${L::network}\",",
            "\"network_view\": \"${L::network_view}\",",
            "\"never_ends\": \"${L::never_ends}\",",
            "\"never_starts\": \"${L::never_starts}\",",
            "\"protocol\": \"${L::protocol}\",",
            "\"served_by\": \"${L::served_by}\",",
            "\"server_host_name\": \"${L::server_host_name}\",",
            "\"starts\": \"${L::starts}\",",
            "\"variable\": \"${L::variable}\",",
            "\"client_hostname\": \"${L::client_hostname}\",",
            "\"ipv6_duid\": \"${L::ipv6_duid}\"",
            "}}"
         ],
         "dxl_topic": "/infoblox/outbound/${E::event_type}"
      },
      {
         "name": "Debug#30",
         "operation": "NOP",
         "body": "${XC:DEBUG:{H:}}${XC:DEBUG:{E:}}${XC:DEBUG:
{I:}}${XC:DEBUG:{L:}}${XC:DEBUG:{S:}}${XC:DEBUG:{P:}}${XC:DEBUG:
{UT:}}${XC:DEBUG:{R:}}"
      },
      {
         "name": "Fin",
         "operation": "NOP",
         "body": ""
      },
      {
         "name": "Debug#31",
         "operation": "NOP",
         "body": "${XC:DEBUG:{H:}}${XC:DEBUG:{E:}}${XC:DEBUG:
{I:}}${XC:DEBUG:{L:}}${XC:DEBUG:{S:}}${XC:DEBUG:{P:}}${XC:DEBUG:
{UT:}}${XC:DEBUG:{R:}}"
      }
```

```
    ]
}
```