knowledge15®
April 19–24, 2015 • Mandalay Bay • Las Vegas, NV

Lab Guide

Discovery 201:

Custom Probes and Sensors

Aleck Lin & Ryan Zulli

Default Login / Password:

admin / Knowledge15

itil / Knowledge15

employee / Knowledge15

This

Page

Intentionally

Left

Blank

Lab Prerequisites

Skills needed for this lab are a core understanding of the ServiceNow Discovery technology, comprehension of TCP/IP protocols, IP networking and base understanding of the ServiceNow core platform. Some basic JavaScript knowledge is helpful.

Lab Agenda

- Discover Windows Machine
  - Custom Windows Probe and Sensor
- Discover SNMP Devices
  - Discover a new SNMP Device
  - Classify non-OOB SNMP Devices
  - Custom SNMP Probe and Sensor
- Q & A

®2015 ServiceNow, Inc. All rights reserved.

Lab Goal

This lab explains how to use WMI to gather additional information from Windows machines.

Lab 1
Discover Windows Machine

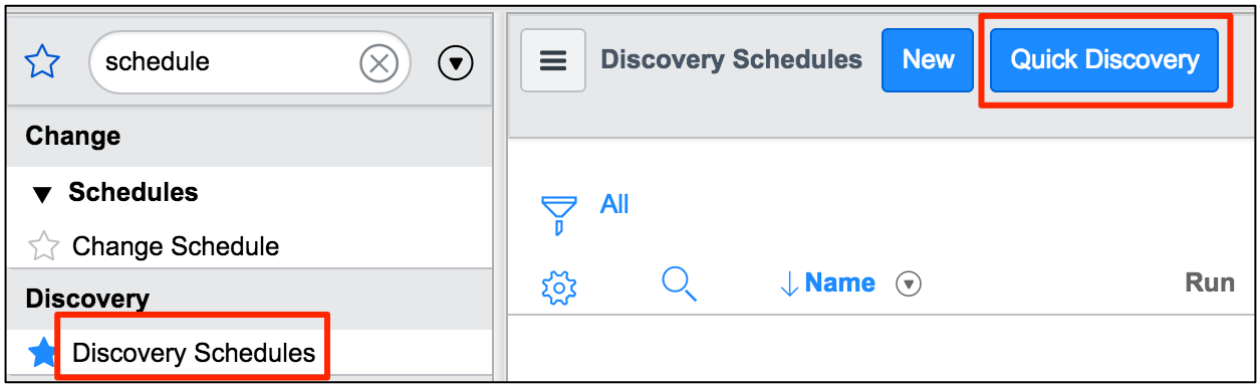
WMI Basics

WMI is an implementation of the Web-Based Enterprise Management (WBEM) standard. WMI provides a uniform access mechanism to a vast collection of Windows management data and methods. WMI offers access to this information via script, C++ programming interfaces, dot net classes (system. management), and a command line tool (WMIC). Other WMI capabilities also include eventing, remoting, query, views, user extensions to schema and instrumentation, and more.

Start a Discovery

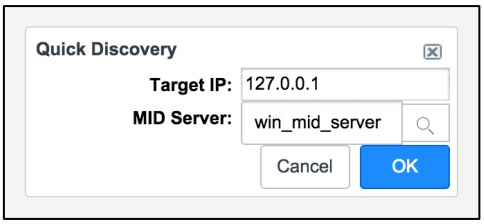
To start off the lab, a discovery run is obviously needed. Here we go!

1. Navigate to **Discovery > Discovery Schedule.** Click the **Quick Discovery** button.



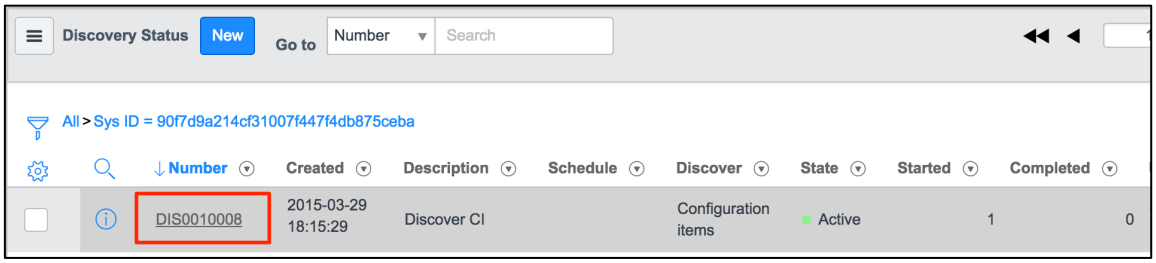
©2015 ServiceNow, Inc. All rights reserved.

2. In the center of the browser, a pop-up box appears. Enter the following:
   - Target IP: **127.0.0.1**
   - MID Server: **win_mid_server**



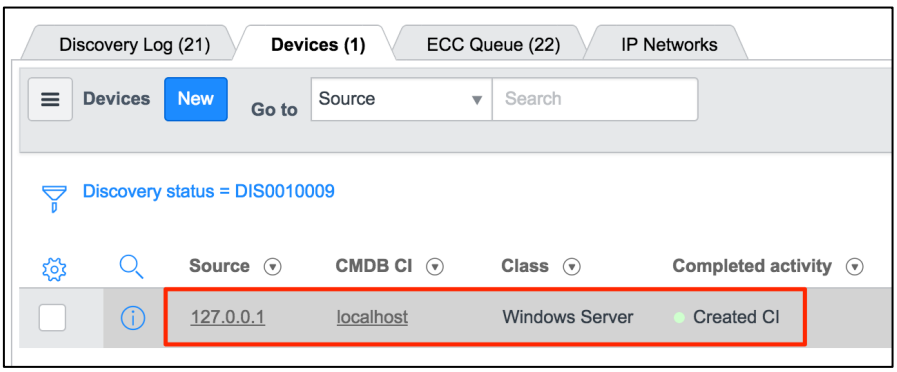
3. Click **OK** to start the discovery.

4. The window navigates directly to the Discovery status record. Click the **number** attribute to open the record.



What to Expect?

A windows server CI should be created with attributes and related data populated.



©2015 ServiceNow, Inc. All rights reserved.

Lab Goal

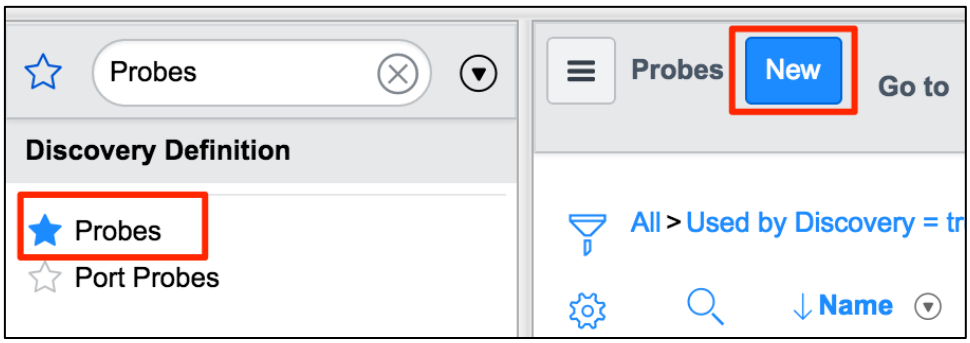
Lab 1.1 Custom Windows Probe and Sensor

This lab explains how to create a Windows probe and sensor to gather additional information from Windows. To see what information is available to gather, check out the Win32 classes (https://msdn.microsoft.com/en-us/library/aa394084(v=vs.85).aspx) on the MSDN.

This lab uses the **Win32_PerfFormattedData_PerfOS_System** class and the **SystemUpTime** attribute to find out when the Windows server was last restarted.

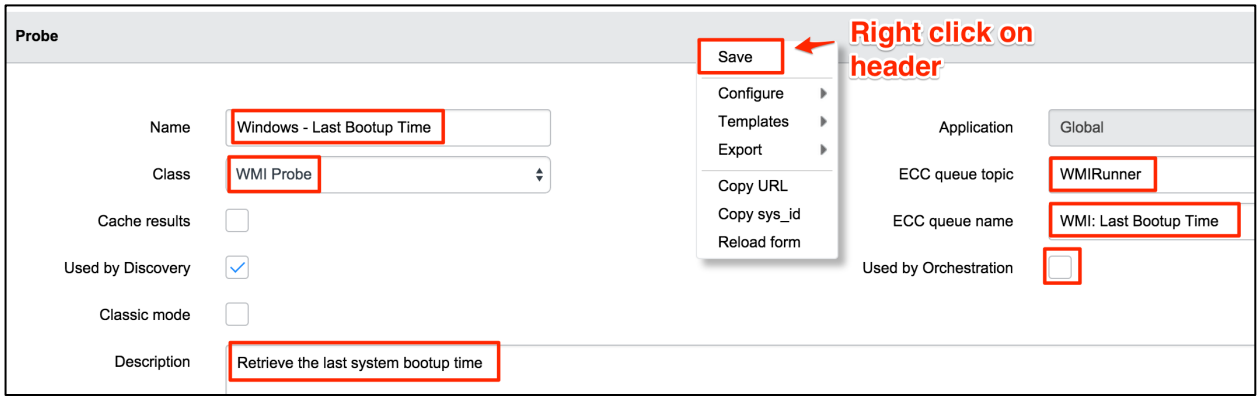
Build a Probe

1. Navigate to **Discovery Definition > Probes**.
2. Click **New**.



©2015 ServiceNow, Inc. All rights reserved.

3. Enter the following information in the **Probe** Form:
   - Name: **Windows – Last Bootup Time**
   - Class: **WMI Probe**
   - ECC queue topic: **WMIRunner**
   - ECC queue name: **WMI: Last Bootup Time**
   - Used by Orchestration: **Deselect**
   - Description: **Retrieve the last system bootup time**

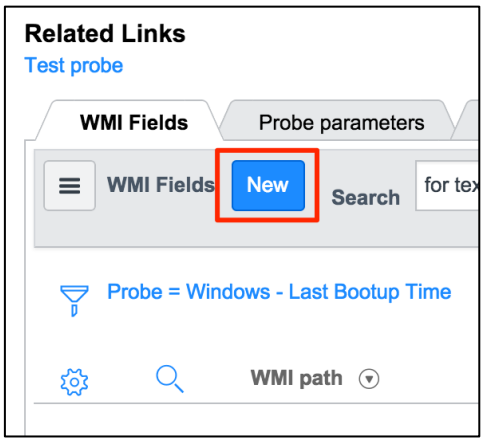


4. Right click the header and click **Save**.

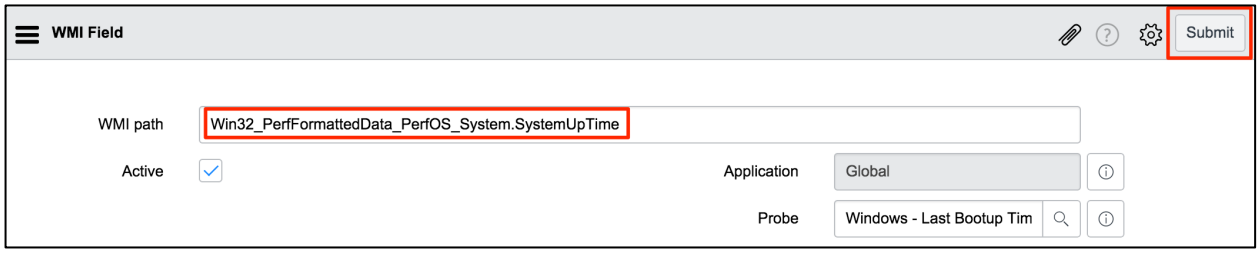
®2015 ServiceNow, Inc. All rights reserved.

Add WMI Fields to the Probe

1. Scroll to the bottom of the page and click **New**.



2. Enter the following information in the **WMI Field** table:
   - WMI path: **Win32_PerfFormattedData_PerfOS_System.SystemUpTime**

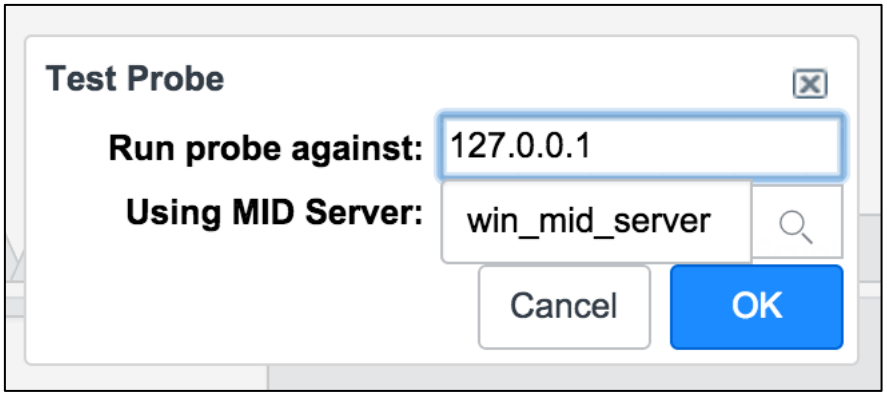


3. Click **Submit**.

©2015 ServiceNow, Inc. All rights reserved.

Test the Probe

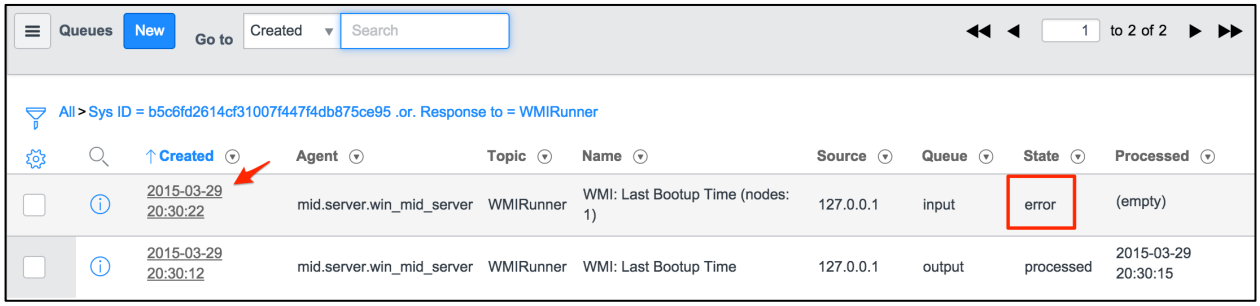
1. Click the UI action **Test probe** to see the result that returns.
2. Scroll to the bottom of the page and click **New**.
3. Entering the following information in the test probe **box**.
   - Run probe against: **127.0.0.1**
   - Using MID Server: **win_mid_server**



4. Click **Ok** to get it started.

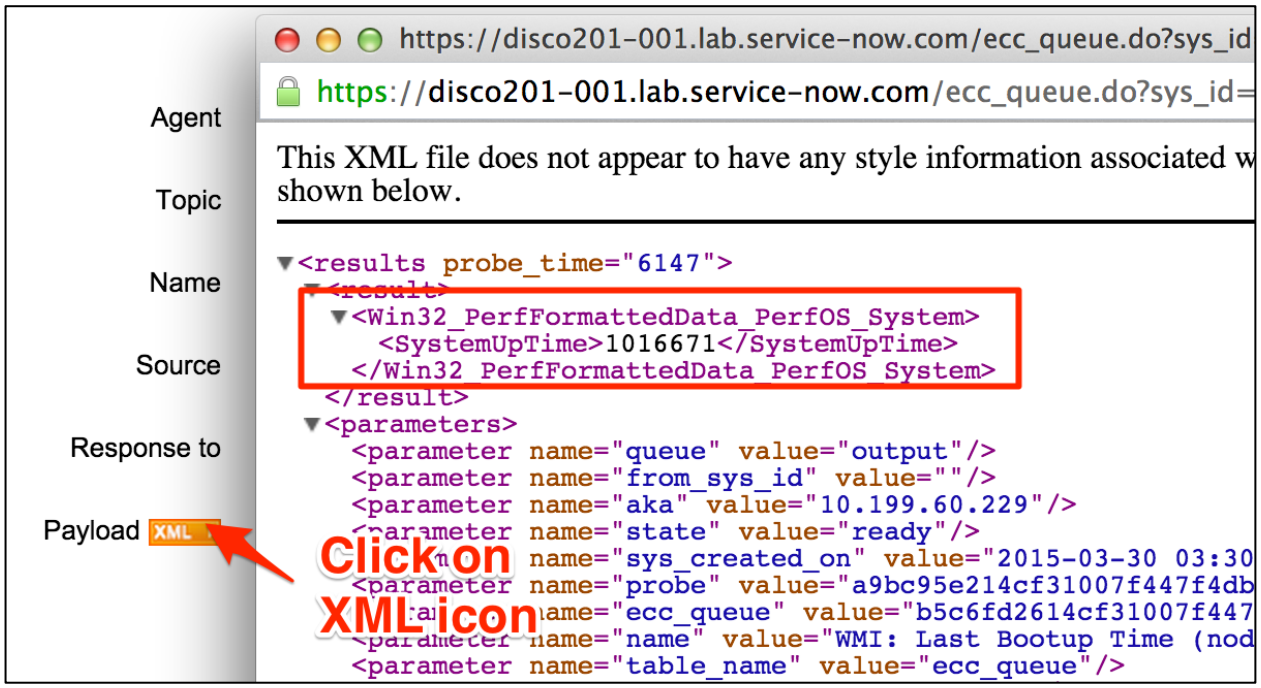
   After the test probe is done, it redirects the page to the ECC queue entries that represent the probe (output) and the result of the probe (input).

   The state of the probe result (input) is error because there is no sensor for the probe yet.



®2015 ServiceNow, Inc. All rights reserved.

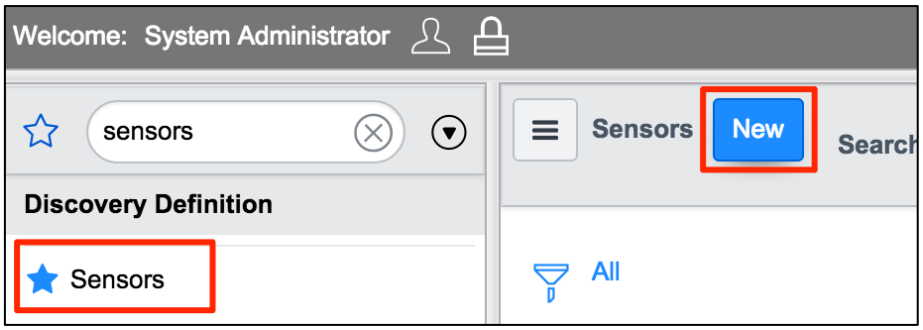
5. Click the **ECC input entry** and note the **SystemUpTime** value.



Build the Sensor

1. Navigate to **Discovery Definition > Sensors**.

2. Click **New**.



©2015 ServiceNow, Inc. All rights reserved.

3. Enter the following information:

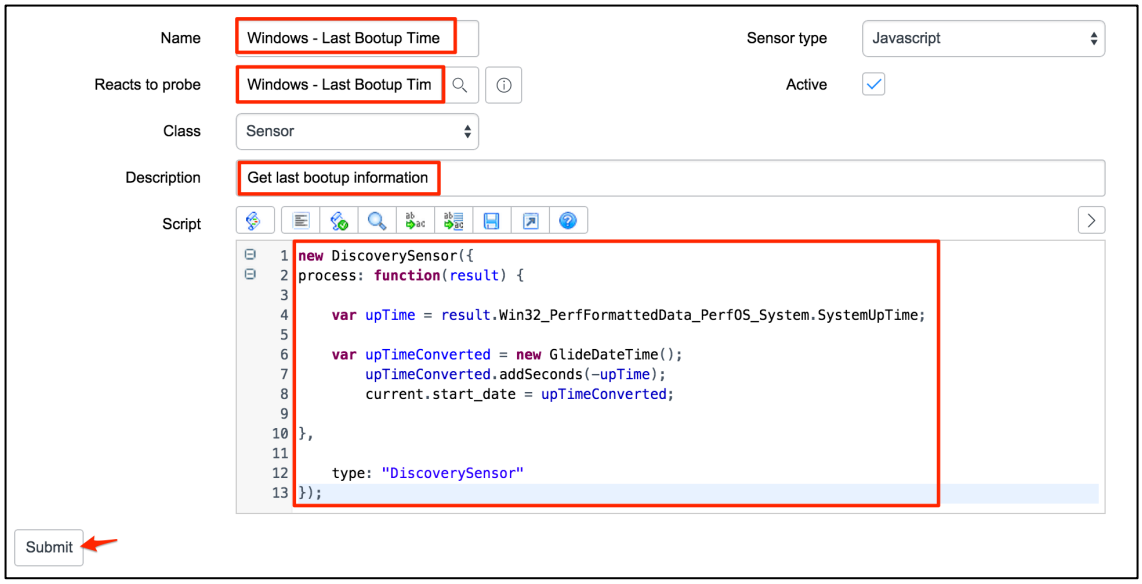
   - Name: **Windows – Last Bootup Time**
   - Reacts to probe: **Windows – Last Bootup Time**
   - Description: **Get last bootup information**
   - Script:

```
new DiscoverySensor({
process: function(result) {

    var upTime = result.Win32_PerfFormattedData_PerfOS_System.SystemUpTime;

    var upTimeConverted = new GlideDateTime();
        upTimeConverted.addSeconds(-upTime);
        current.start_date = upTimeConverted;
},

    type: "DiscoverySensor"
});
```

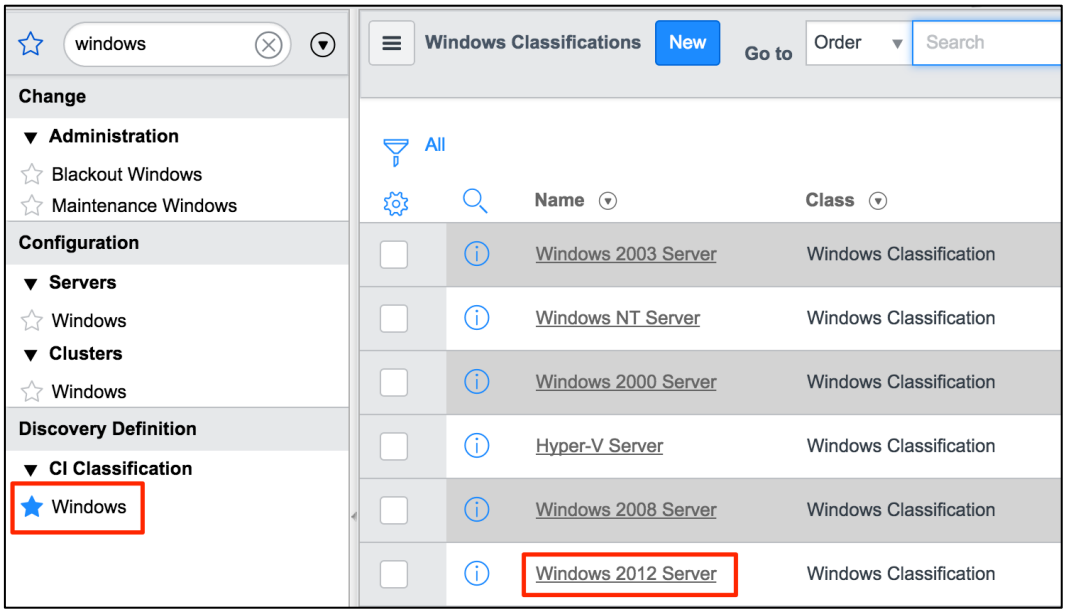


4. Click **Submit**.

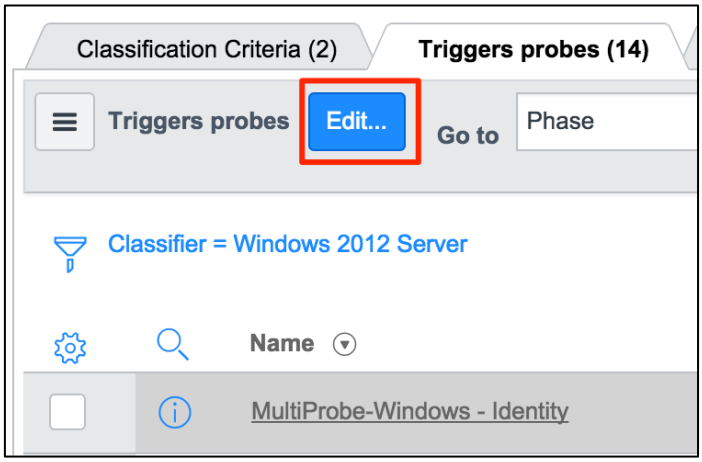
©2015 ServiceNow, Inc. All rights reserved.

Add the Probe to the Windows Classifier as an Exploration Probe

1. Navigate to **Discovery Definition > Windows**.
2. Click the **Windows 2012 Server** record.

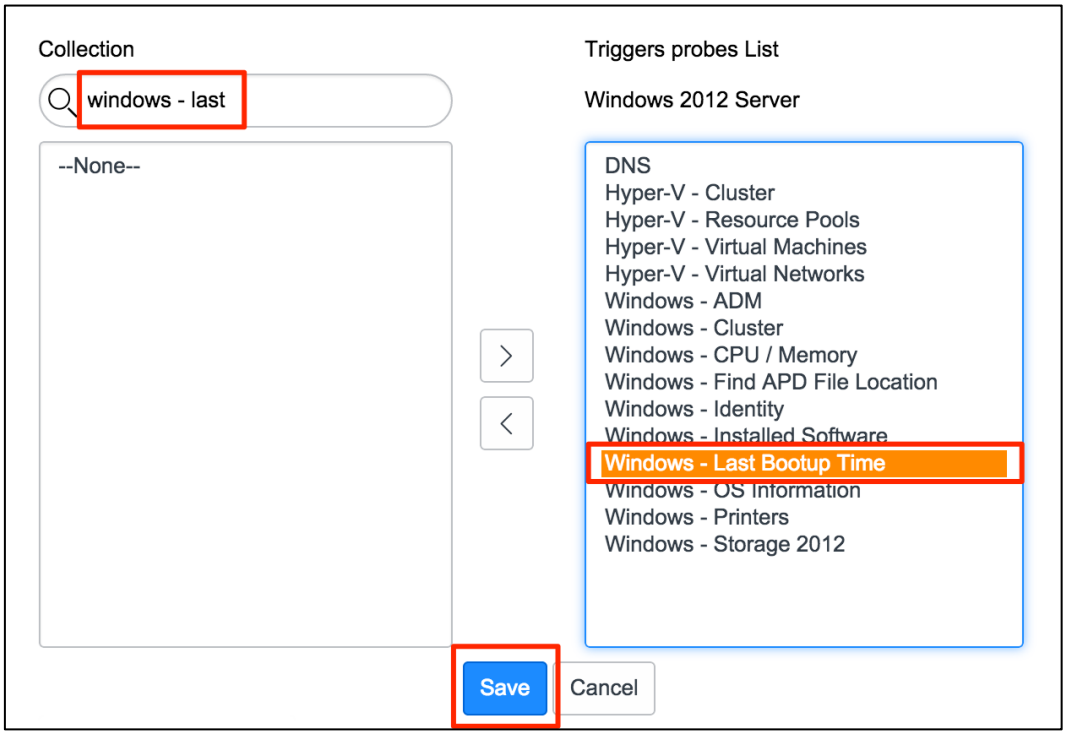


3. Click **Edit** under the **Triggers probes** tab.



©2015 ServiceNow, Inc. All rights reserved.

4. Search for **Windows – Last Bootup Time** probe and add it to the slush bucket. Click **Save**.



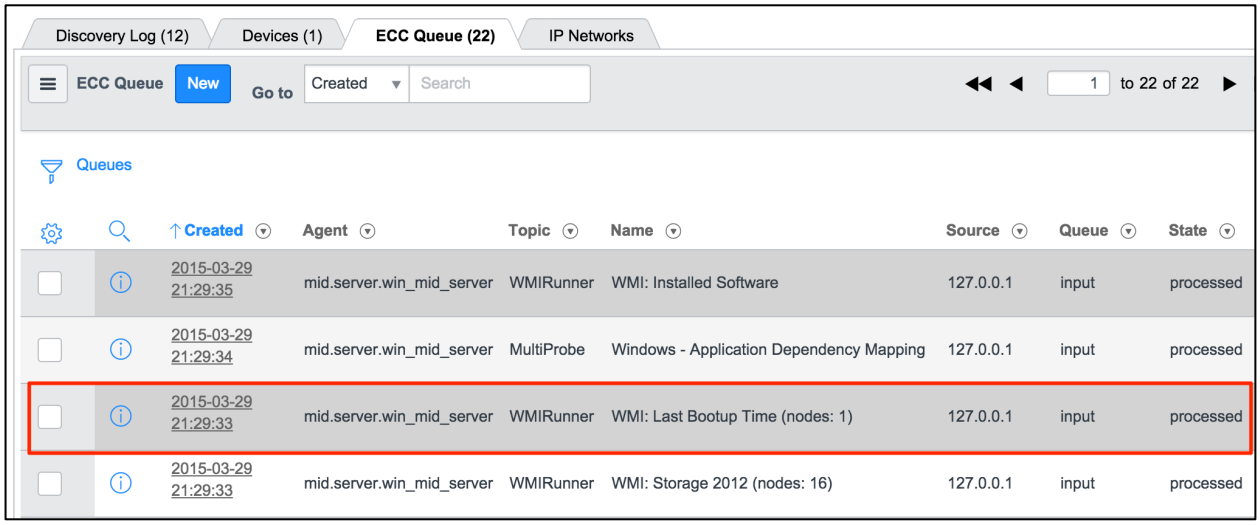
Start a New Discovery

Use **Quick Discovery** to start a Discovery against the host.

©2015 ServiceNow, Inc. All rights reserved.

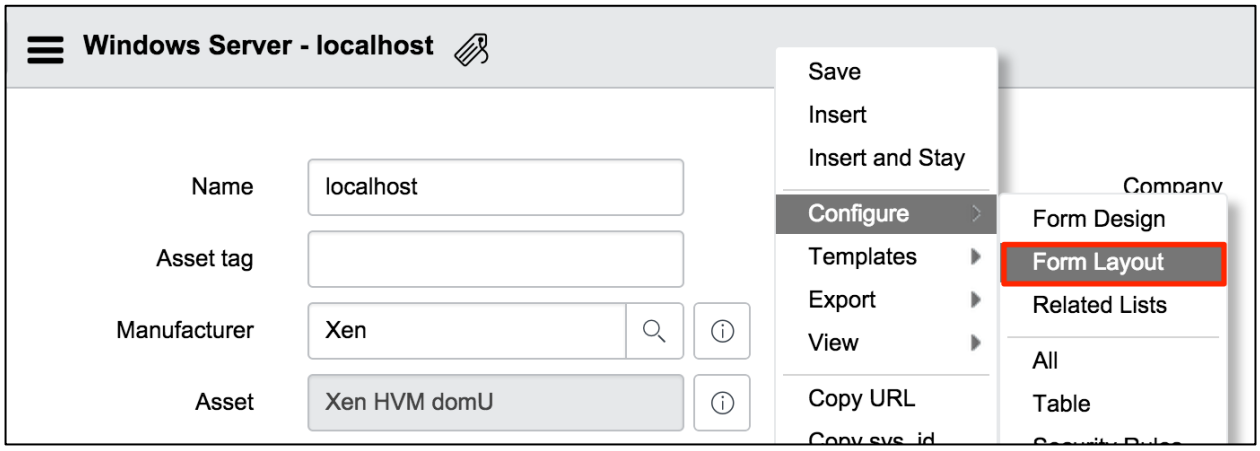
Lab Success Verification

1. Observe that the Discovery run has launched the new probe.



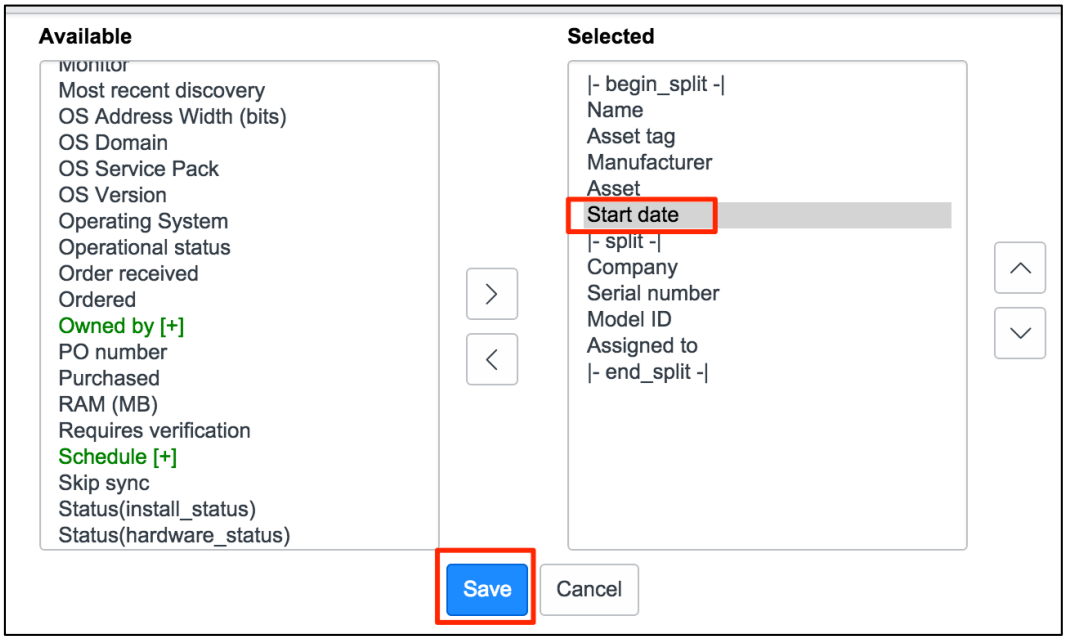
2. Go to the **Devices** related list and drill into the Windows CI record.

3. Right click the header and configure the **Form Layout**.

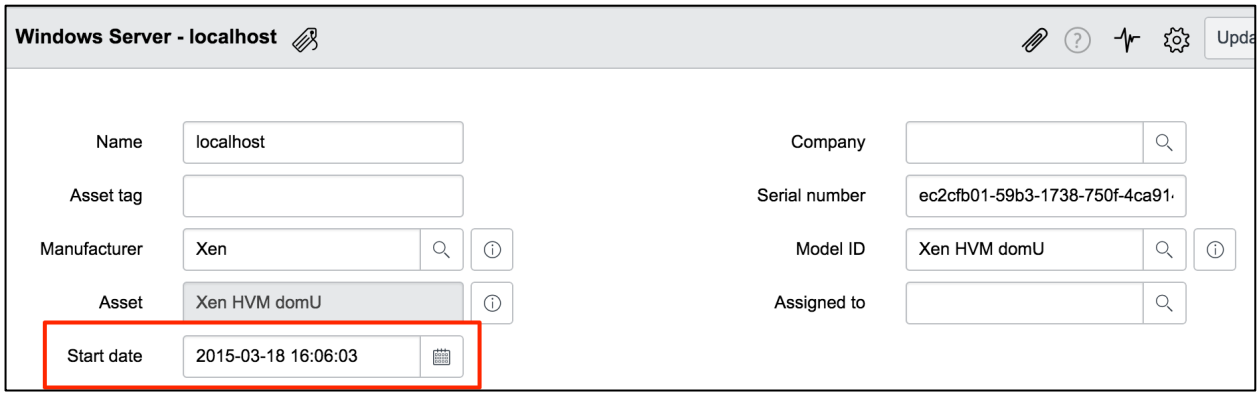


©2015 ServiceNow, Inc. All rights reserved.

4. Add the **Start date** field to the form and click **Save**.



5. Observe that the **Start date** field has been populated!



©2015 ServiceNow, Inc. All rights reserved.

Lab Goal

This lab explains how to use the SNMP protocol, which is common for discovering network devices. Before beginning, here is a quick overview of how SNMP works.

Lab 2
Discover SNMP Devices

SNMP Basics

SNMP stands for Simple Network Management Protocol. It is typically used to for network devices, such as routers, switches, printers, UPS, servers.

SNMP devices expose management data as variables (identified by OIDs), which are organized in hierarchies. These hierarchies and other metadata (such as type and description of the variable) are described by MIBs (Management Information Bases).

MIB (Management Information Base) typically consists of many managed objects (aka variables). There are two types of managed objects.

- Scalar object, which defines single object instance
- Tabular object, which defines multiple related object instances that are grouped in MIB tables.

OIDs, or Object Identifiers are what uniquely identify managed objects in a MIB hierarchy.

www.oid-info.com is a great site to look up OID information.

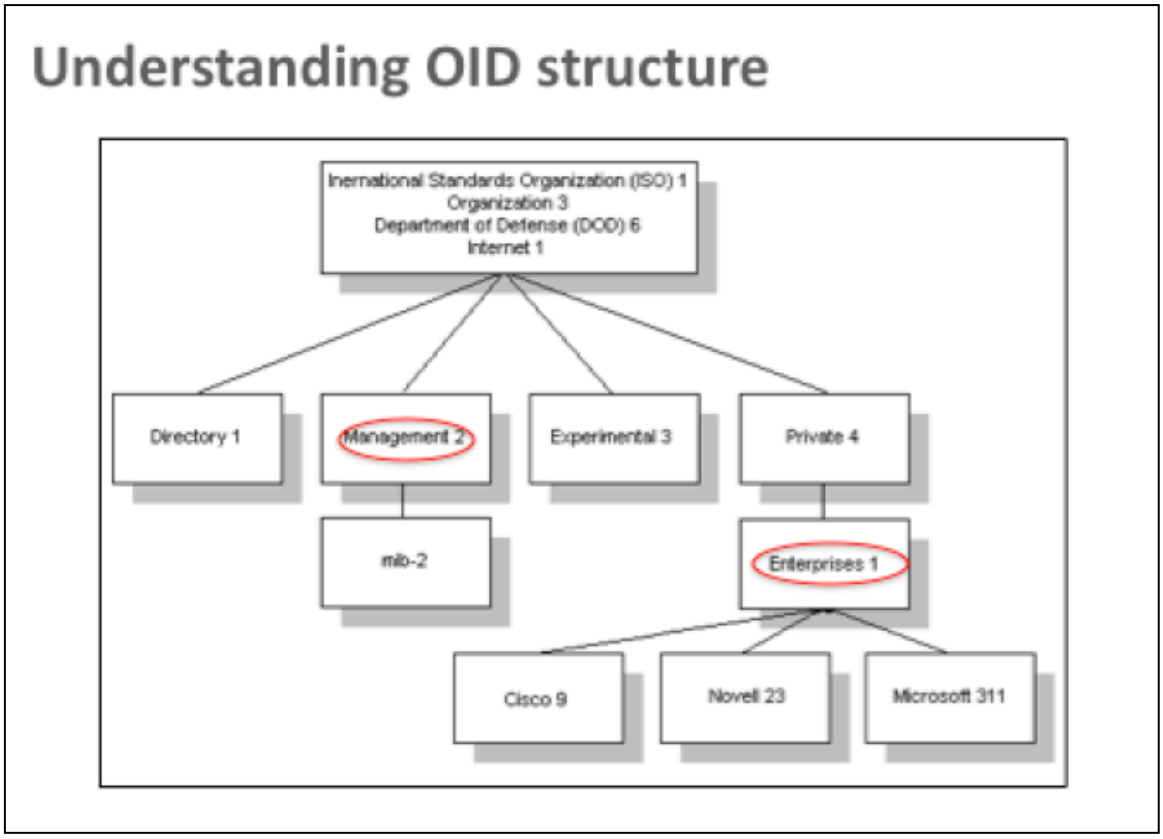
Understand OID Structure

Typically assume the path of ISO(1).Identified-organization(3).dod(6).internet(1).

And most MIBs that you care about are in the level below marked in red.

- Directory (1)
- Mgmt(2)
- Experimental(3)
- Private(4)
- Security(5)
- snmpV2(6)
- Mail(7)
- Features(8)

©2015 ServiceNow, Inc. All rights reserved.



What Kind of Device Is It?

"SNMP MIB-2" MIB (RFC 1213) is what you use…

ISO(1).Identified-organization(3).dod(6).internet(1).Mgmt(2).mib-2(1).system(1)

- sysDescr(1) -- Scalar object
- sysObjectID(2)
- sysUpTime(3)
- sysContact(4)
- sysName(5)
- sysLocationu(6)
- sysServices(7)
- sysORLastChange(8)
- sysORTable(9) -- Tabular object

©2015 ServiceNow, Inc. All rights reserved.

To access an object, for example, the sysDescr object with the OID "1.3.6.1.2.1.1.1", typically one uses command line tools to retrieve the object value through clients such as snmpwalk or snmpget.

For example, the following command:

```
snmpwalk -v 2c -c public xxx.xxx.xxx.xxx 1.3.6.1.2.1.1.1
```

returns a result such as:

```
SNMPv2-MIB::sysDescr.0 = STRING: Cisco Systems, Inc./VPN 3000 Concentrator Ver
```

Example of a Cisco VPN 3000 Concentrator

```
monster-MacBook:~ aleck.lin$ snmpwalk -v 2c -c public 54.151.51.29
SNMPv2-MIB::sysDescr.0 = STRING: Cisco Systems, Inc./VPN 3000 Concentrator Ver
SNMPv2-MIB::sysObjectID.0 = OID: SNMPv2-SMI::enterprises.3076.1.2.1.1.2.1
DISMAN-EVENT-MIB::sysUpTimeInstance = Timeticks: (129600000) 15 days, 0:00:00.00
SNMPv2-MIB::sysContact.0 = STRING: Jalasoft
SNMPv2-MIB::sysName.0 = STRING: JalaCiscoVPN3000 - 10.251.141.101 - V2*
SNMPv2-MIB::sysLocation.0 = STRING: 8th floor labs
SNMPv2-MIB::sysServices.0 = INTEGER: 76
```

®2015 ServiceNow, Inc. All rights reserved.

Lab Goal

This lab explains how to discover an SNMP device with its IP address provided for you.

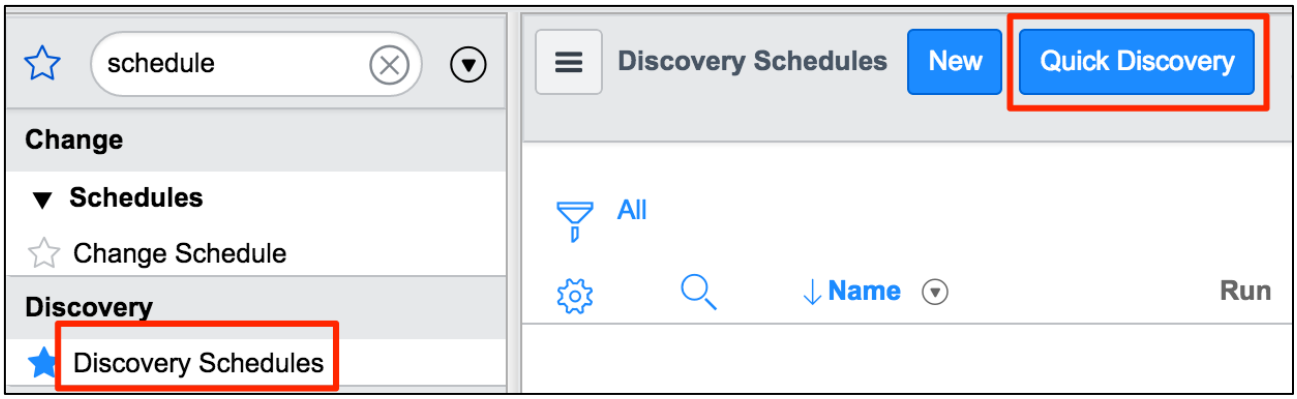
A VPN concentrator device is available for the purpose of this lab.

Lab 2.1 Discover a New SNMP Device

Start a Discovery

To start off the lab, a discovery run is needed. Follow these steps.

1. Navigate to **Discovery > Discovery Schedules**.
2. Click **Quick Discovery**.



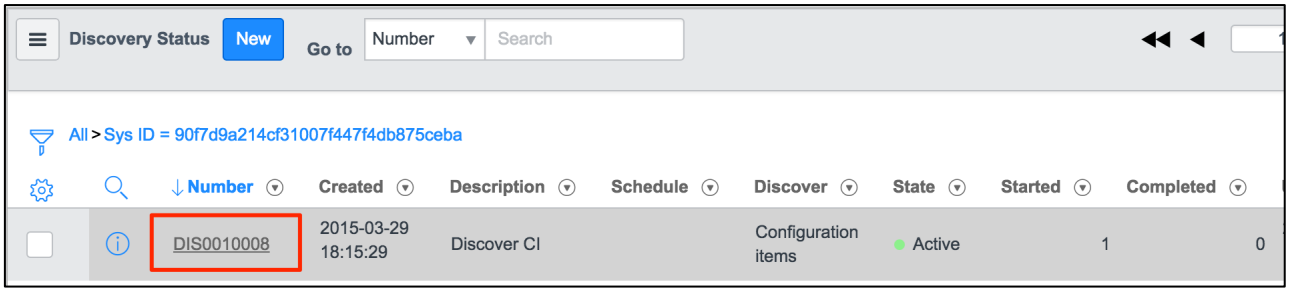
©2015 ServiceNow, Inc. All rights reserved.

3. In the center of the browser, a pop-up appears. Enter the following:
   - Target IP: **127.0.0.1**
   - MID Server: **win_mid_server**



4. Click **OK** to start the discovery.

5. After clicking OK, the navigation takes you directly to the Discovery status record the represent the Discovery.

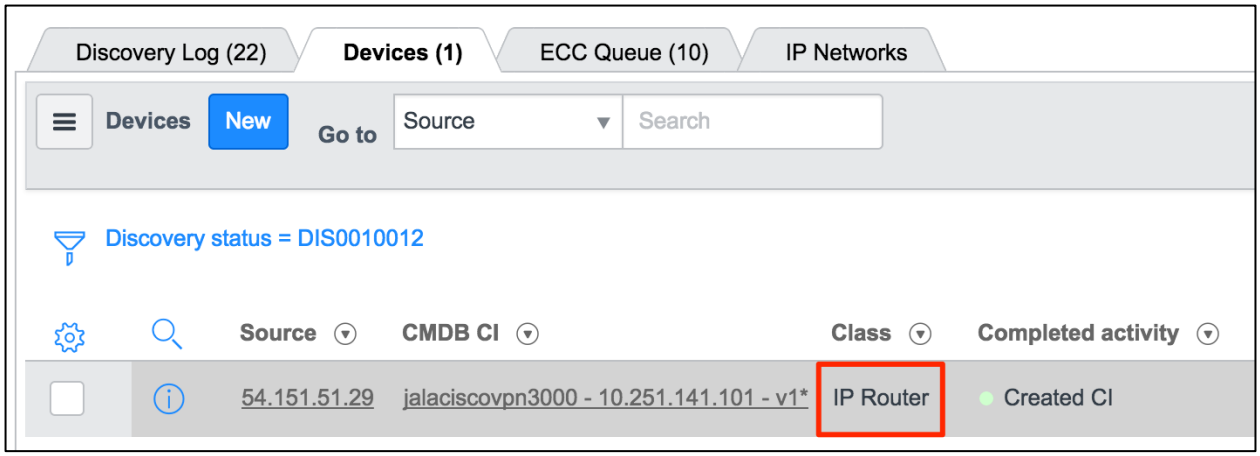


®2015 ServiceNow, Inc. All rights reserved.

What Is Happening?

Discovery found the Cisco VPN concentrator, but has classified it as an IP router. Take a look by clicking on the Discovery status record.

1. Click the related **Devices**.

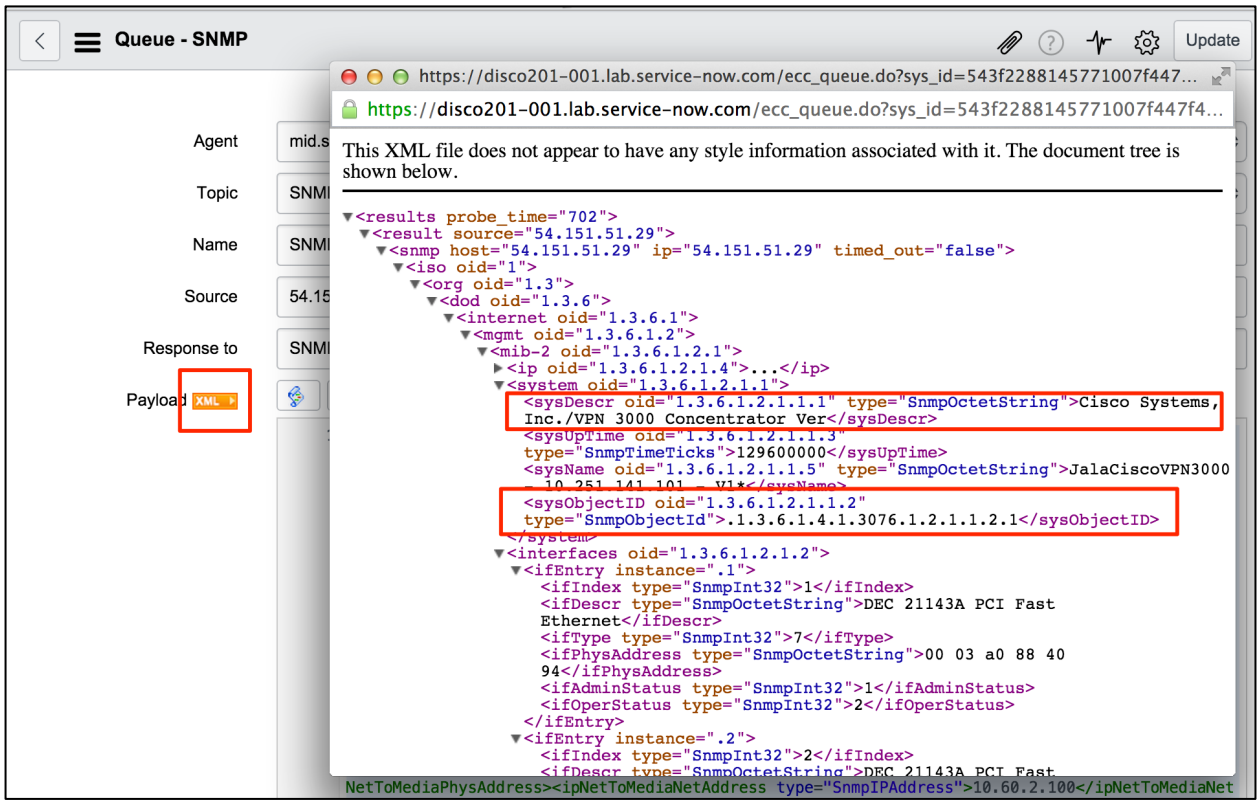


2. Navigate to the **ECC Queue** related list, and click the **SNMP – Classified: xxx OIDs** Input record.

Created	Agent	Topic	Name	Source	Queue	State
2015-04-03 16:28:04	mid.server.win_mid_server	SNMP	SNMP - Routing: 51 OIDs	54.151.51.29	input	processed
2015-04-03 16:27:50	mid.server.win_mid_server	SNMP	SNMP - Routing	54.151.51.29	output	processed
2015-04-03 16:27:49	mid.server.win_mid_server	MultiProbe	SNMP - Identity	54.151.51.29	input	processed
2015-04-03 16:27:40	mid.server.win_mid_server	MultiProbe	SNMP - Identity	54.151.51.29	output	processed
2015-04-03 16:27:34	mid.server.win_mid_server	SNMP	SNMP - Classify: 181 OIDs	54.151.51.29	input	processed
2015-04-03 16:27:31	mid.server.win_mid_server	SNMP	SNMP - Classify	54.151.51.29	output	processed
2015-04-03 16:27:21	mid.server.win_mid_server	Shazzam	http,slp,wins,dns,ssh,wbem,wmi,vmapp,snmp	See Payload	input	processed
2015-04-03 16:27:12	mid.server.win_mid_server	Shazzam	http,slp,wins,dns,ssh,wbem,wmi,vmapp,snmp	See Payload	output	processed

©2015 ServiceNow, Inc. All rights reserved.

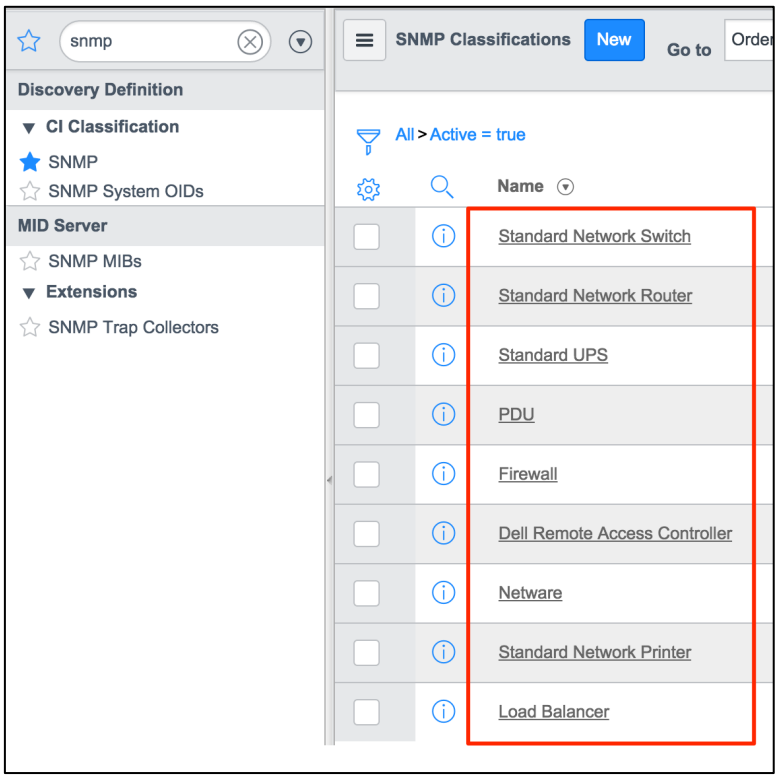
3. Click the **XML** icon and from the data, note the **sysDescr** OID that shows **Cisco Systems, Inc./VPN 3000 Concentrator Ver.**



©2015 ServiceNow, Inc. All rights reserved.

4. Navigate to **Discovery Definition > SNMP**.

5. Notice that **VPN Concentrator** is not a device classified out of the box, so you need an **SNMP classifier** for it!



®2015 ServiceNow, Inc. All rights reserved.

Lab Goal

This lab explains how to classify a SNMP device that Discovery does not find out of the box.

Lab 2.2
Classify an non-OOB SNMP Devices

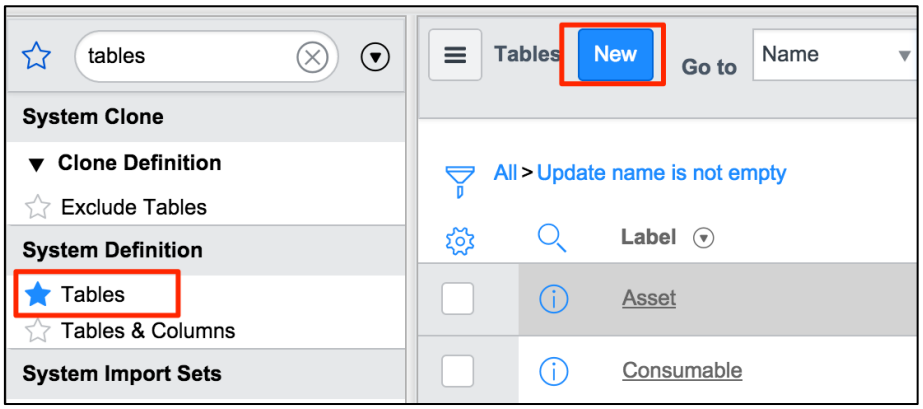
Create a Table for the VPN Concentrator

Before creating a new SNMP classification for the VPN Concentrator, we'll create a VPN concentrator table to properly store the CI record.

In this lab, we'll create a **u_cmdb_ci_vpn_concentrator** table that extends the **cmdb_ci_netgear** table. Notice the "**u_"** is automatically added so that your table never clashes with the ones that ServiceNow creates (or will create).

We'll create the table first and then come back to create the new classification for the VPN concentrator.

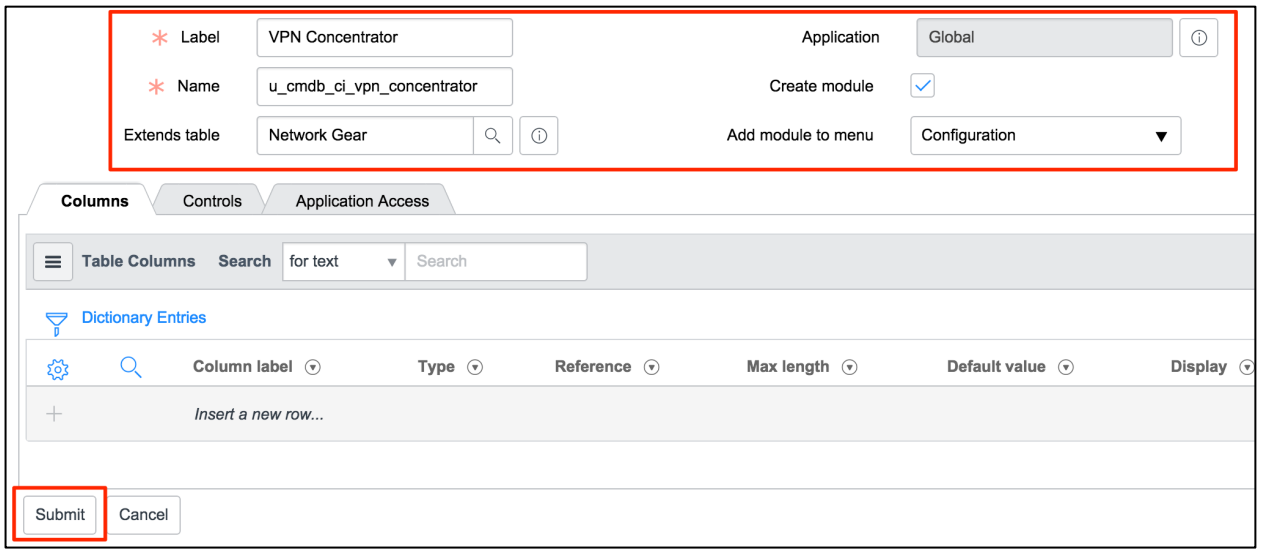
1. Navigation to **System Definition > Table**.
2. Click **New**.



©2015 ServiceNow, Inc. All rights reserved.

3. Enter the following information in the Table.

   - Label: **VPN Concentrator**
   - Name: **u_cmdb_ci_vpn_concentrator**
   - Extends table: **Network Gear**
   - Create module: **checked**
   - Add module to menu: **Configuration**



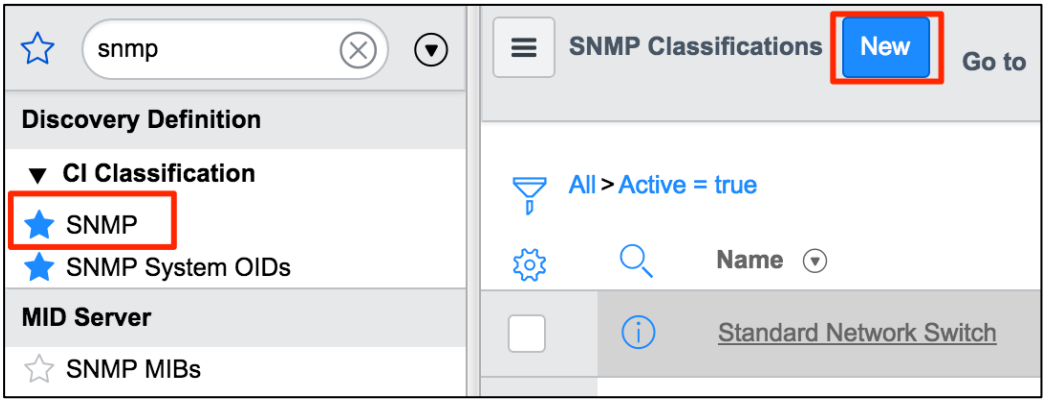
4. Click **Submit**.

5. For more details regarding table creation, see wiki page: http://wiki.servicenow.com/index.php?title=Creating_a_Custom_Table

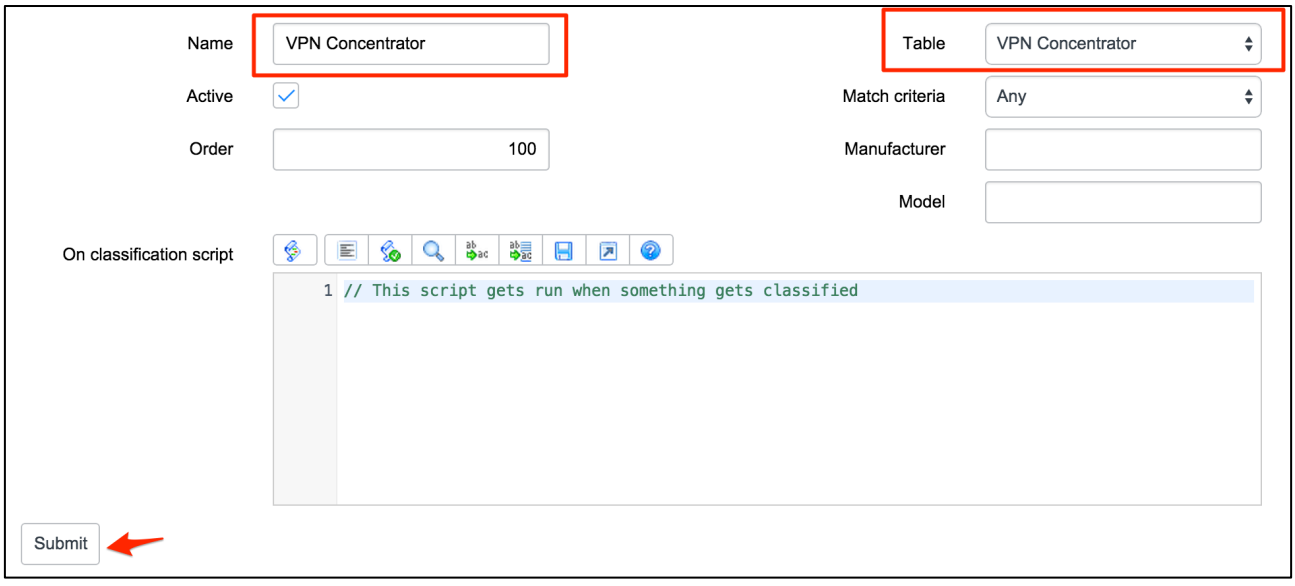
©2015 ServiceNow, Inc. All rights reserved.

Create SNMP Classifier

1. Navigate to **Discovery Definition > SNMP**.
2. Click **New**.



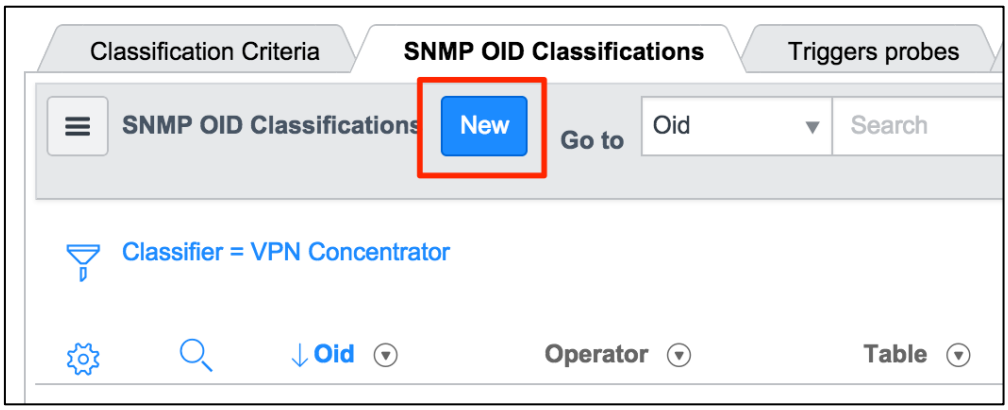
3. Enter the following information in the classifier record
   - Name: **VPN Concentrator**
   - Table: **VPN Concentrator**
4. Click **Submit**.



5. Drill back into the record.

©2015 ServiceNow, Inc. All rights reserved.

6. Click **New** under the **Classification Criteria** tab.



7. Enter the following information in the criteria record.

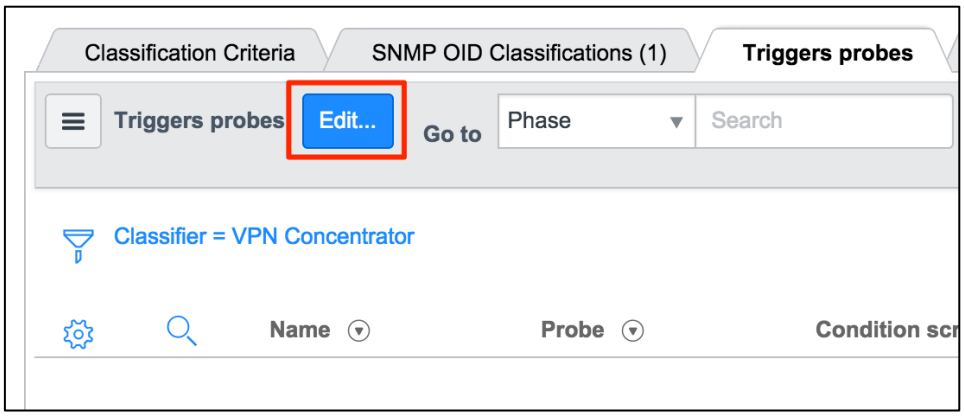
- Oid: **1.3.6.1.4.1.3076.1.2.1.1.2.1**
- Operator: **Is**
- Manufacturer: **Cisco**
- Model: **VPN 3000 Series Concentrator**
- Active: **Checked**
- Table: **VPN Concentrator**
- Classifier: **VPN Concentrator**



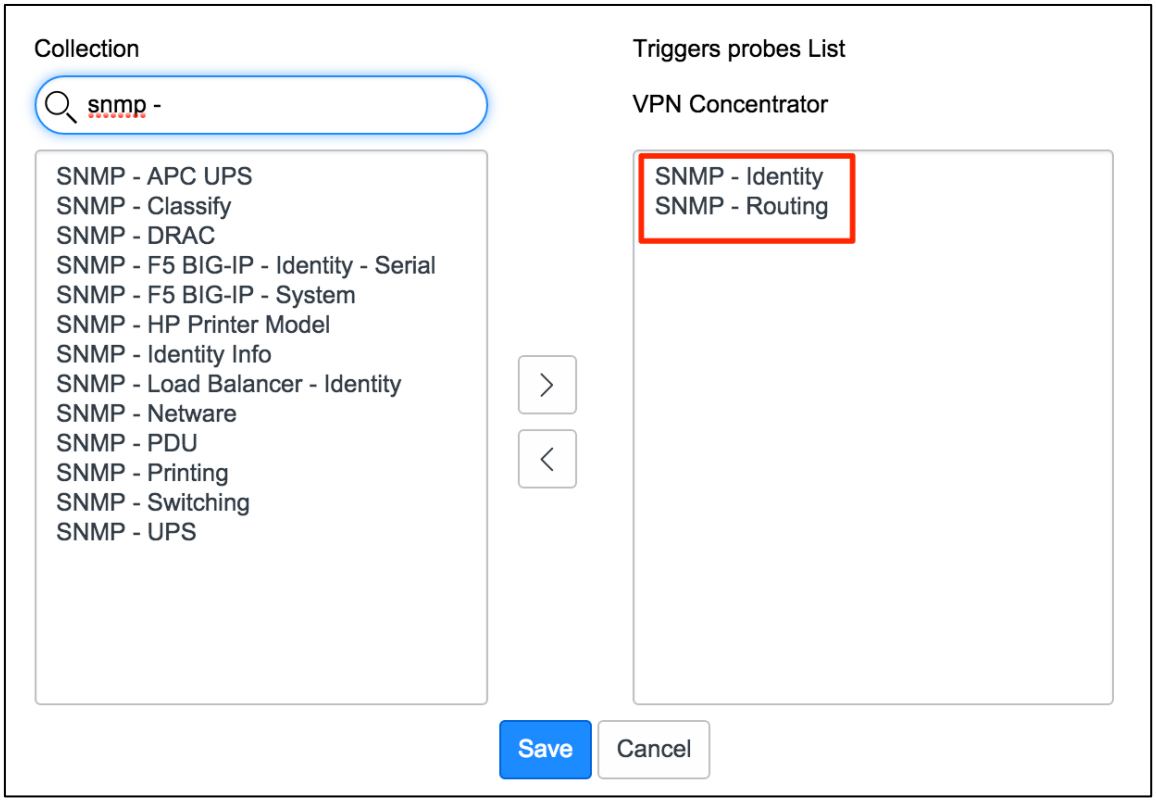
8. Click **Submit**.

©2015 ServiceNow, Inc. All rights reserved.

9. Click **Edit** under the **Triggers probes** tab.



10. Type **snmp** in the **search** box of the slush bucket.



11. Move the **SNMP – Identity** and **SNMP – Routing** probes to the right side of the slush bucket.

12. Click **Save**

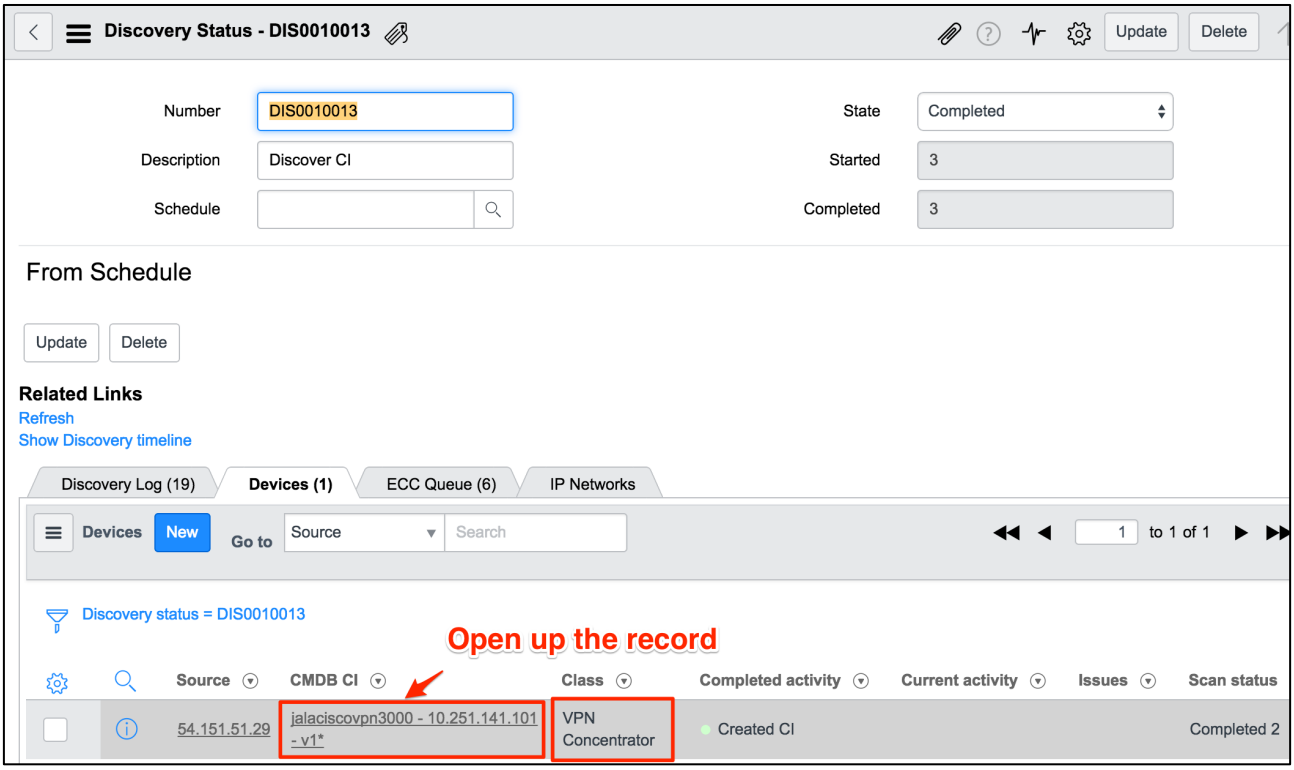
©2015 ServiceNow, Inc. All rights reserved.

Start a New Discovery

Use **Quick Discovery** to start a Discovery against host.

Lab Success Verification

You successfully discovered the Cisco VPN Concentrator. Drill into the CI record to see what was found.



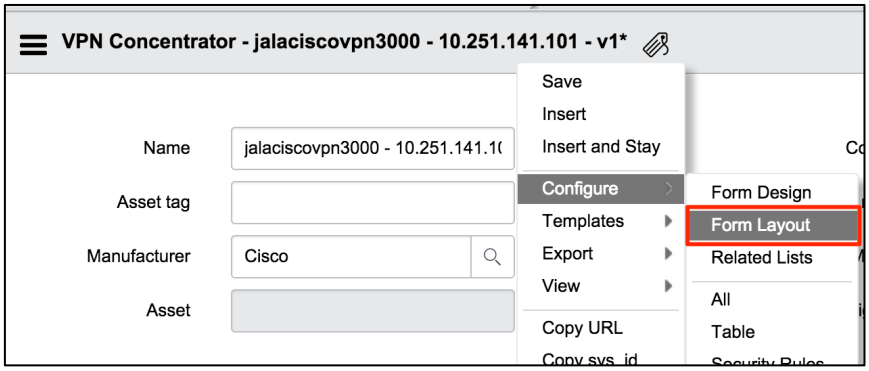
®2015 ServiceNow, Inc. All rights reserved.

Customize the Form Layout and Related lists

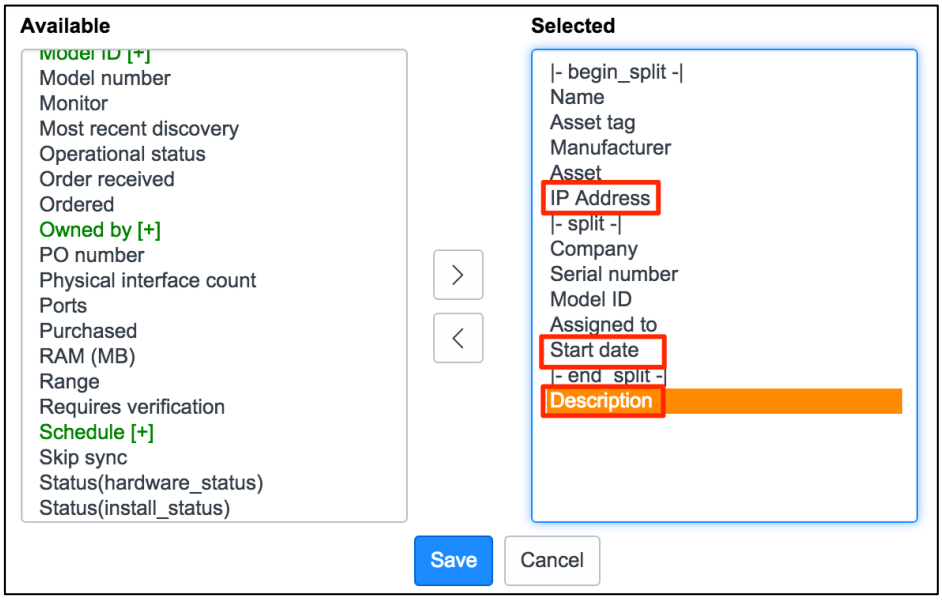
The out-of-the-box form layout is not very exciting. Customize it by adding the **IP address, Start date** and **description** fields to the form. This also helps in the later exercises.

1. Right-click the header and hover over **Configure**.

2. Click **Form Layout**.

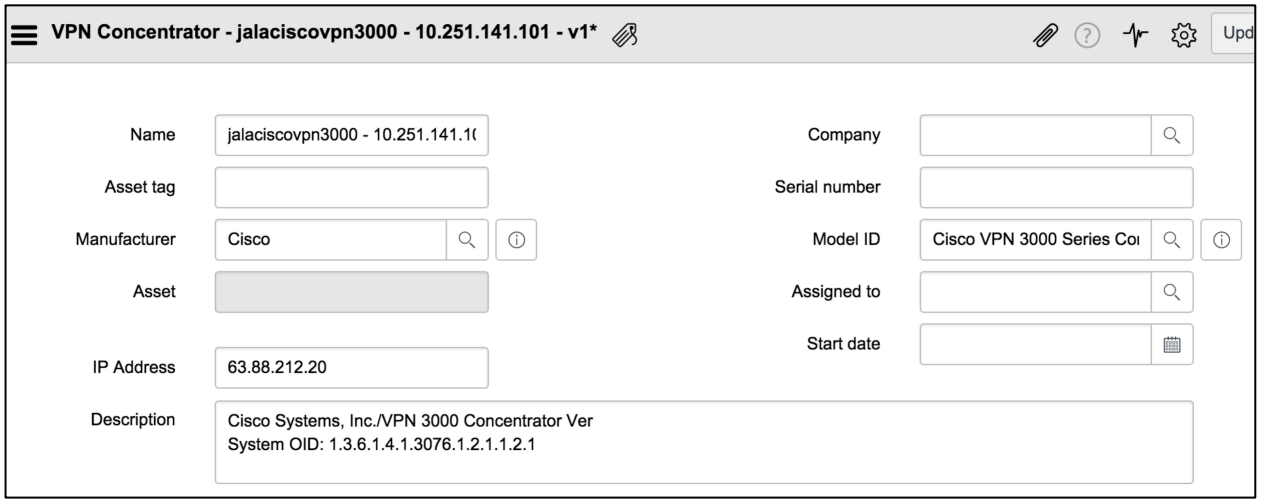


3. Move **IP address**, **Start Date**, **Description** fields to the right of the slush bucket.



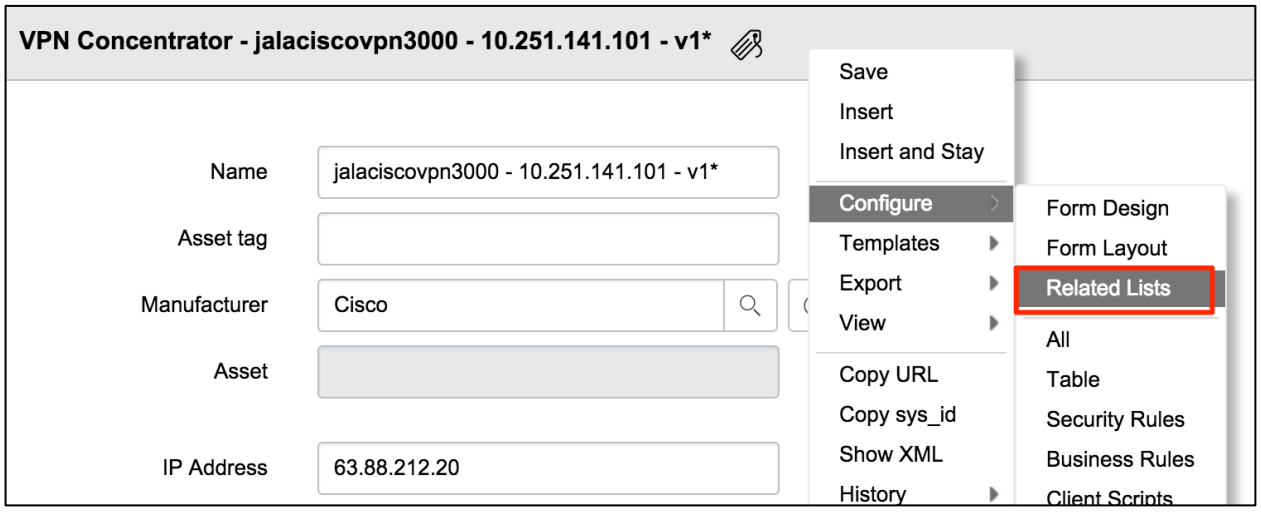
©2015 ServiceNow, Inc. All rights reserved.

4. Click **Save.** The form should look like the example.



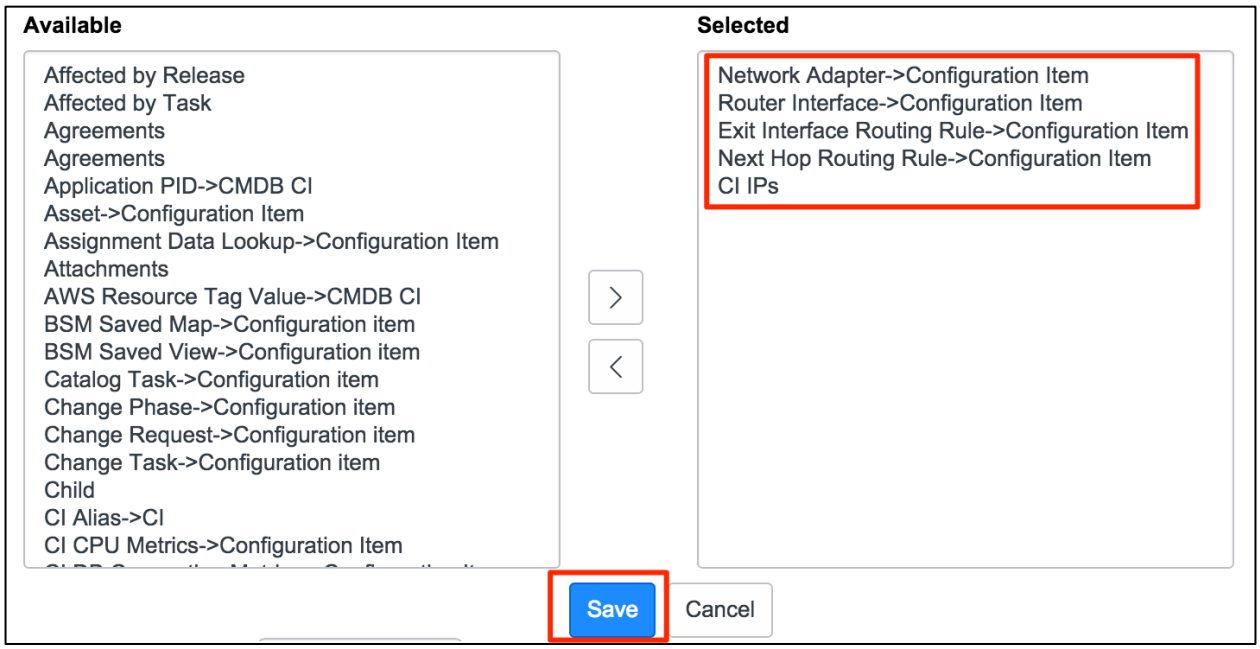
5. Right-click the header and hover over **Configure**.

6. Click on **Related Lists**.



©2015 ServiceNow, Inc. All rights reserved.

7. Move the following related lists into the right side.
   - **Network Adapter->Configuration Item**
   - **Router interface-> Configuration Item**
   - **Exit Interface Routing Rule-> Configuration Item**
   - **Next Hop Routing Rule-> Configuration Item**
   - **CI IPs**



8. Click **Save**.

9. Observe that the related data has already been populated.

®2015 ServiceNow, Inc. All rights reserved.

Lab Goal

This lab explains how to create custom SNMP probes and sensors.

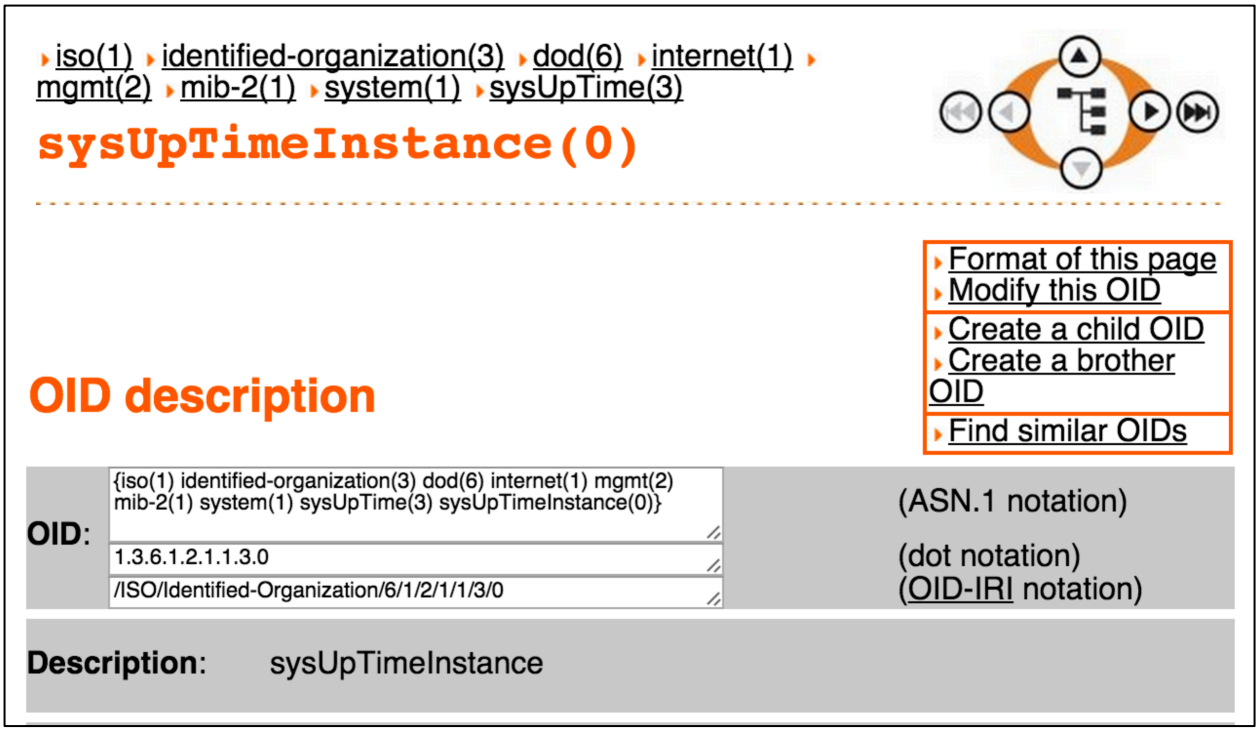
The goal is to help you figure out how you can leverage the Discovery tool to gather data that is meaningful to your organization.

Lab 2.3 Custom SNMP Probe and Sensor

Gather Scalar OID Objects

In this exercise, you walk through how to build a probe to retrieve a scalar OID and a sensor to process the information and store it in the SNMP device.

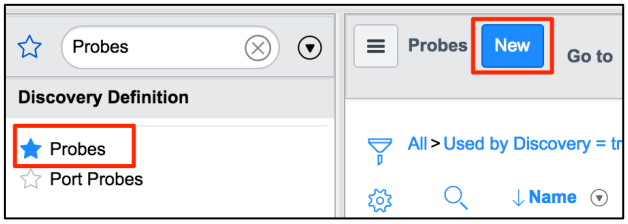
The probe uses the following OID**, sysUpTimeInstance (www.oid-info.com).**



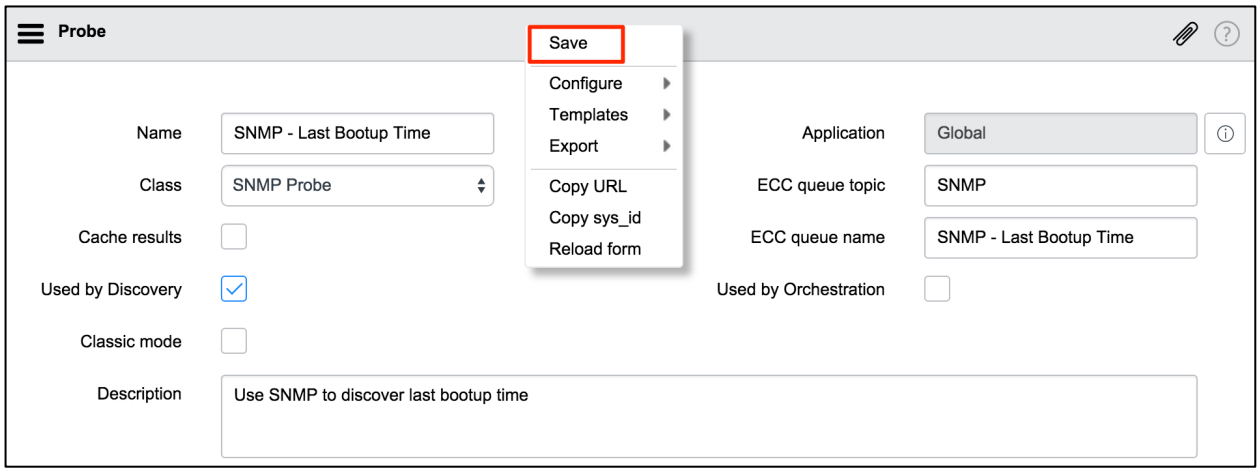
®2015 ServiceNow, Inc. All rights reserved.

Build a Probe

1. Navigate to **Discovery Definition > Probes**.
2. Click **New**.



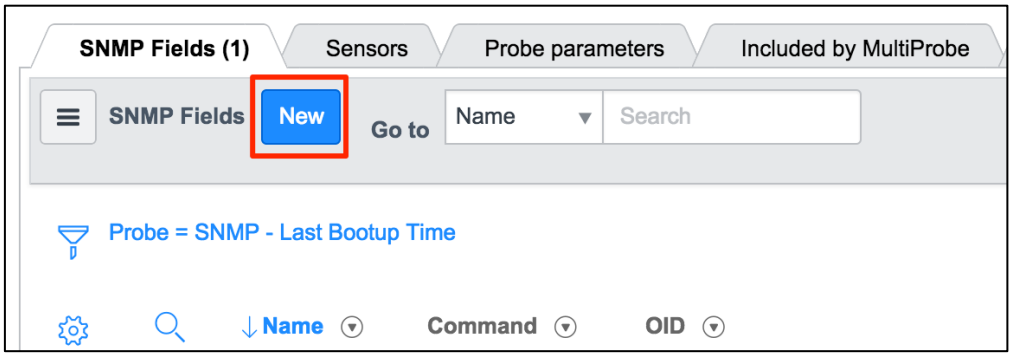
3. Enter the following information in the Probe table.
   - Name: **SNMP – Last Bootup Time**
   - Class: **SNMP Probe**
   - Cached results: **Unchecked**
   - Used by Discovery: **Checked**
   - Classic mode: **Unchecked**
   - Description: **Use SNMP to discover last bootup time**
   - ECC Queue topic: **SNMP**
   - ECC queue name: **SNMP – Last Bootup Time**
   - Used by Orchestration: **Unchecked**



4. Right click the header and click **Save**.

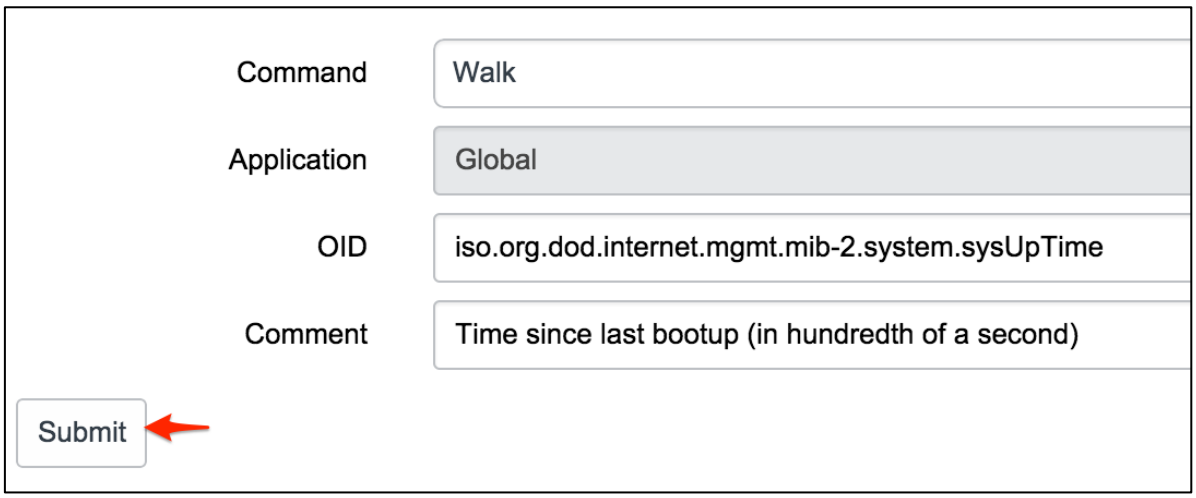
©2015 ServiceNow, Inc. All rights reserved.

5. Click **New** under the **SNMP Fields** related list.



6. Enter the following information in the **SNMP Fields** table:

   - OID: **iso.org.dod.internet.mgmt.mib-2.system.sysUpTime**
   - Comment: **Time since last bootup (in hundredth of a second)**

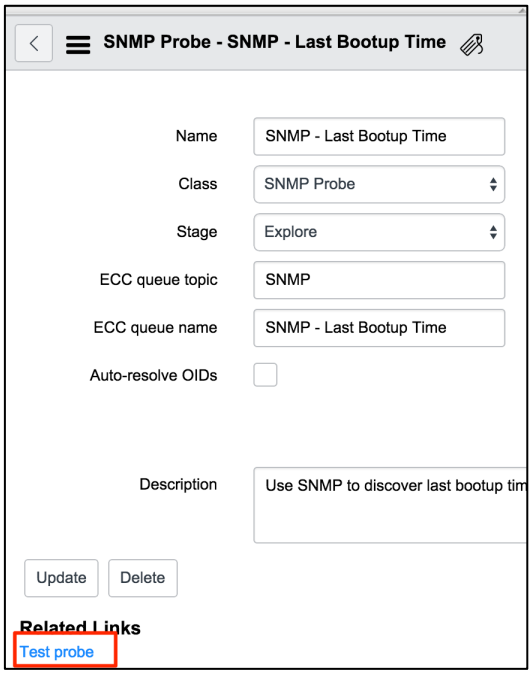


7. Click **Submit**.

©2015 ServiceNow, Inc. All rights reserved.

Test the Probe

1. Click the UI action **Test Probe** to trigger a test probe.



2. Enter the following information:

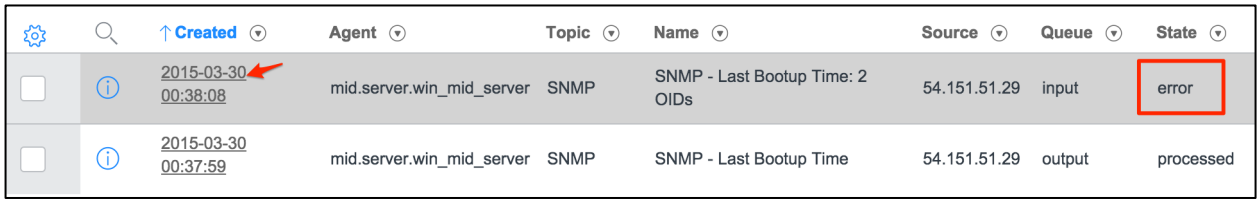
   - Run probe against: **target IP**.
   - Using MID server: **win_mid_server**.



3. Click **OK** to start it.

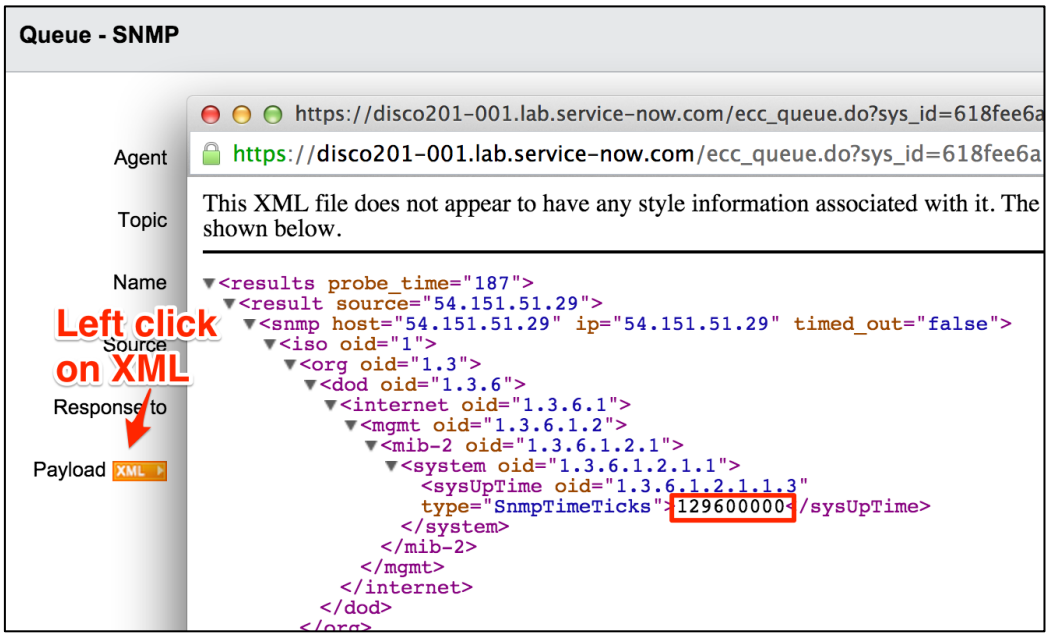
©2015 ServiceNow, Inc. All rights reserved.

4. After the test probe is done, it redirects the page to the ECC queue entries that represent the probe (output) and the result of the probe (input). The state of the probe result (input) is error because there is no sensor for the probe yet.



Created	Agent	Topic	Name	Source	Queue	State
2015-03-30 00:38:08	mid.server.win_mid_server	SNMP	SNMP - Last Bootup Time: 2 OIDs	54.151.51.29	input	error
2015-03-30 00:37:59	mid.server.win_mid_server	SNMP	SNMP - Last Bootup Time	54.151.51.29	output	processed

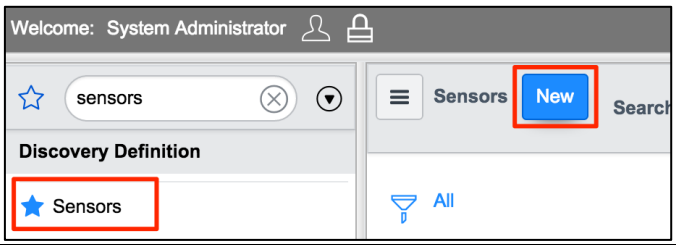
5. Click the **ECC input** entry and observe that the payload is **129600000** for the **sysUpTime** OID.



Build a Sensor

1. Navigation to **Discovery Definition > Sensor**.

2. Click **New**.



©2015 ServiceNow, Inc. All rights reserved.

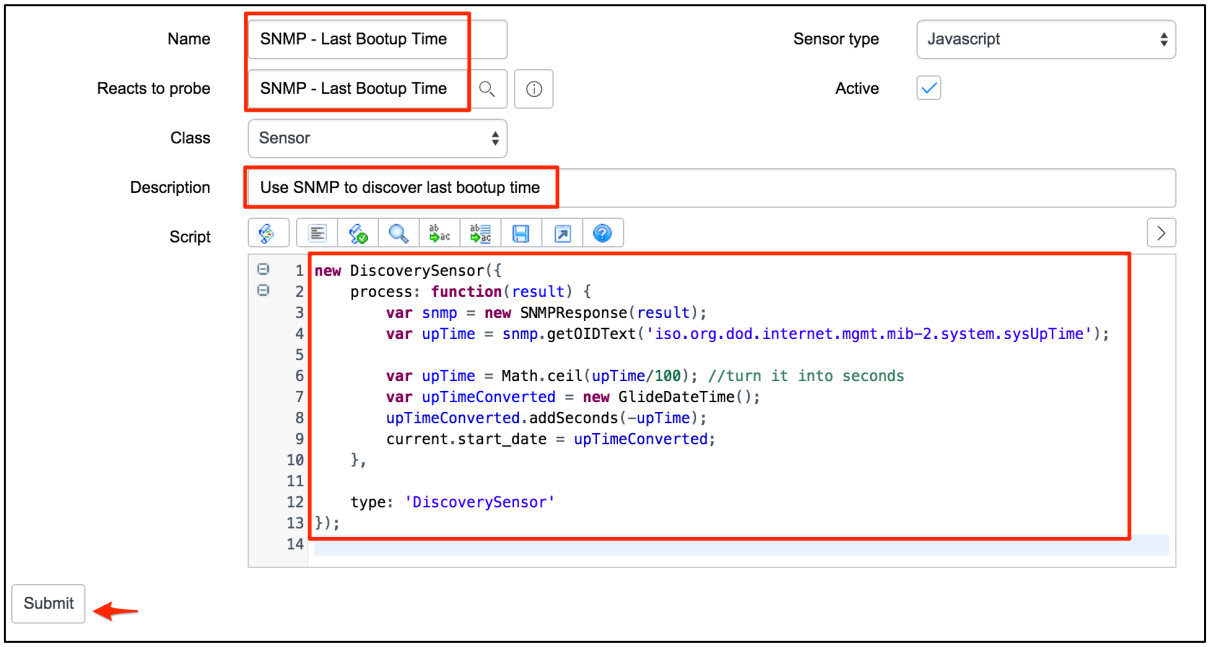
3. Enter the following information in the sensor table

   - Name: **SNMP – Last Bootup Time**
   - Reacts to probe: **SNMP – Last Bootup Time**
   - Description: **Use SNMP to discover last bootup time**
   - Script:

```
new DiscoverySensor({
    process: function(result) {
        var snmp = new SNMPResponse(result);
        var upTime = snmp.getOIDText('iso.org.dod.internet.mgmt.mib-2.system.sysUpTime');

        var upTime = Math.ceil(upTime/100); //turn it into seconds
        var upTimeConverted = new GlideDateTime();
        upTimeConverted.addSeconds(-upTime);
        current.start_date = upTimeConverted;
    },

    type: 'DiscoverySensor'
});
```

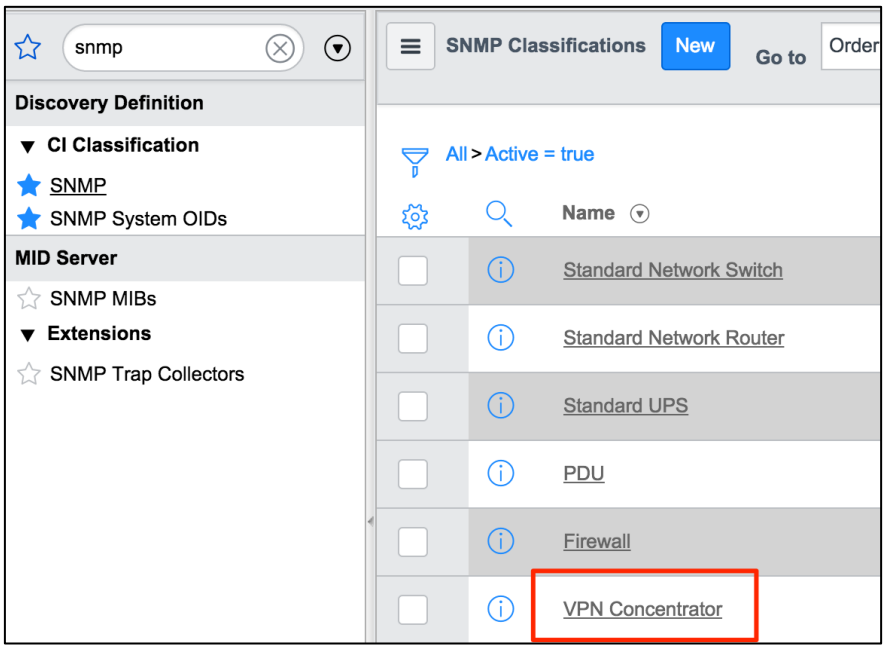


4. Click **Submit** to save the record.

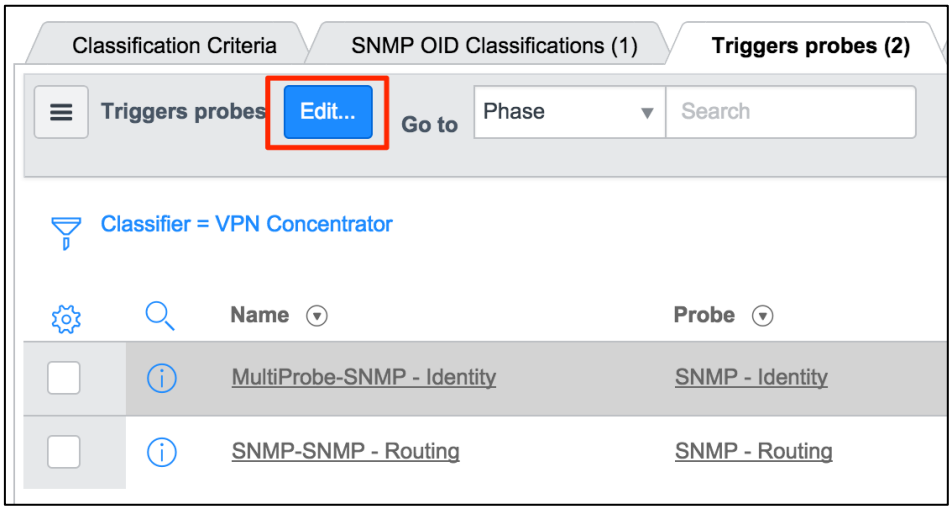
©2015 ServiceNow, Inc. All rights reserved.

Add Probe to the SNMP VPN Concentrator Classifier as an Exploration Probe

1. Navigate to **Discovery Definition > SNMP**.
2. Click the **VPN Concentrator** record.



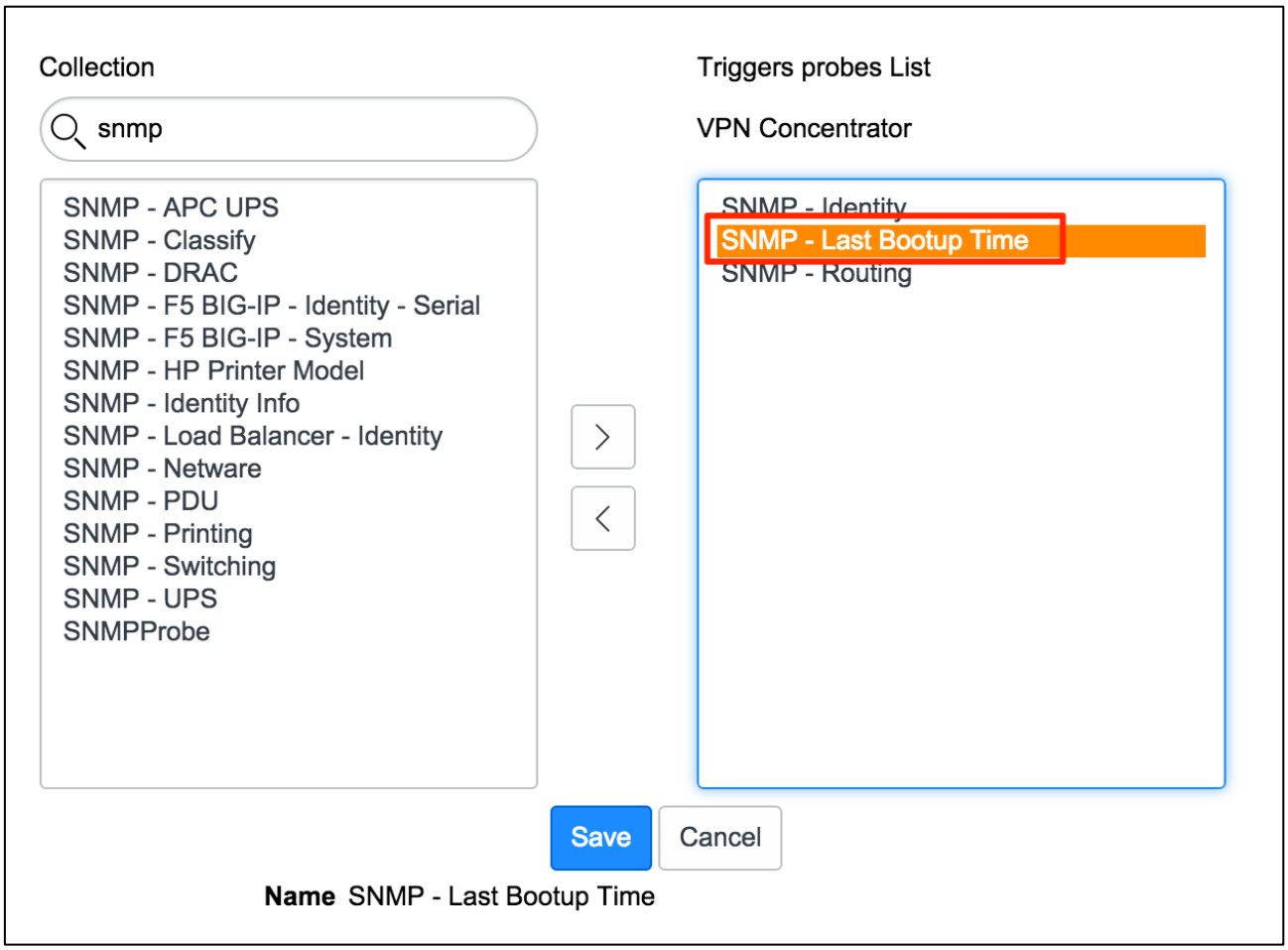
3. Click **Edit** under the **Triggers probes** tab.



4. Type **snmp** in the **Search** box of the slush box.

©2015 ServiceNow, Inc. All rights reserved.

5. Move the **SNMP – Last Bootup Time** record to the right side of the slush bucket.



6. Click **Save**.

©2015 ServiceNow, Inc. All rights reserved.

Start a New Discovery

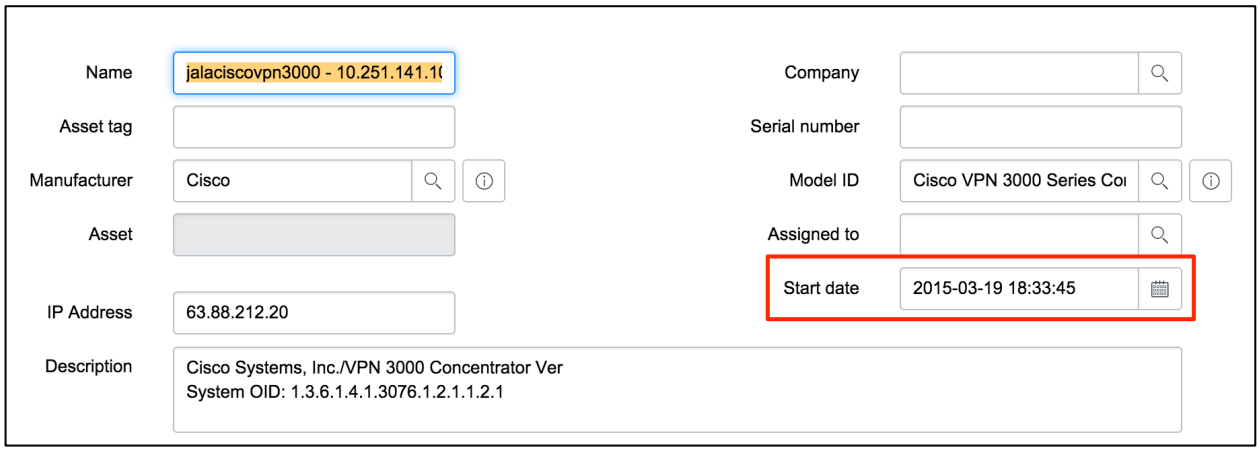
Use **Quick Discovery** to Discover the host.

Lab Success Verification

1. Observe that the Discovery run has launched the new probe.



2. Go to the **Devices** related list and drill into the CI and observe that the value of the OID has indeed been added to the **Start Date** field.



®2015 ServiceNow, Inc. All rights reserved.