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

Lab Guide

Discovery 101:

Populate Your CMDB with Agentless Discovery

Ryan Zulli & Doug Schulze

Default Login / Password:

admin / Knowledge15

itil / Knowledge15

employee / Knowledge15

This

Page

Intentionally

Left

Blank

Lab Goal

- Define ServiceNow Discovery
- Identify Value Return
- Explain ServiceNow inside your network

Lab 1
Discovery
Overview

ServiceNow Discovery

- ServiceNow Discovery is an ***agentless*** method of populating your CMDB with relevant hardware and software assets within your enterprise environment.
- Utilizing a specific step or *phased* process, we remotely discover your Windows and Unix computers/servers, network devices, powering and printing equipment, and most any other IP enabled device that we can "talk to."
- With our platform, we map specific Application to Host *and* Application-to-Application dependencies.

®2015 ServiceNow, Inc. All rights reserved.

Discovery Value Return

Asset Management

Many enterprise environments have limited visibility to the hundreds or thousands of devices that make up their IT environment. It is critical to have the capability to account for and identify IP-connected computers, services, printers, and the multitudes of different IP-enabled assets within a global or local environment.

Application Management

Knowing just that an asset exists can be valuable in any environment. However, ServiceNow's discovery takes it to the next level by identifying the running applications, installed software, versions, and patch levels.

Outage Impacts

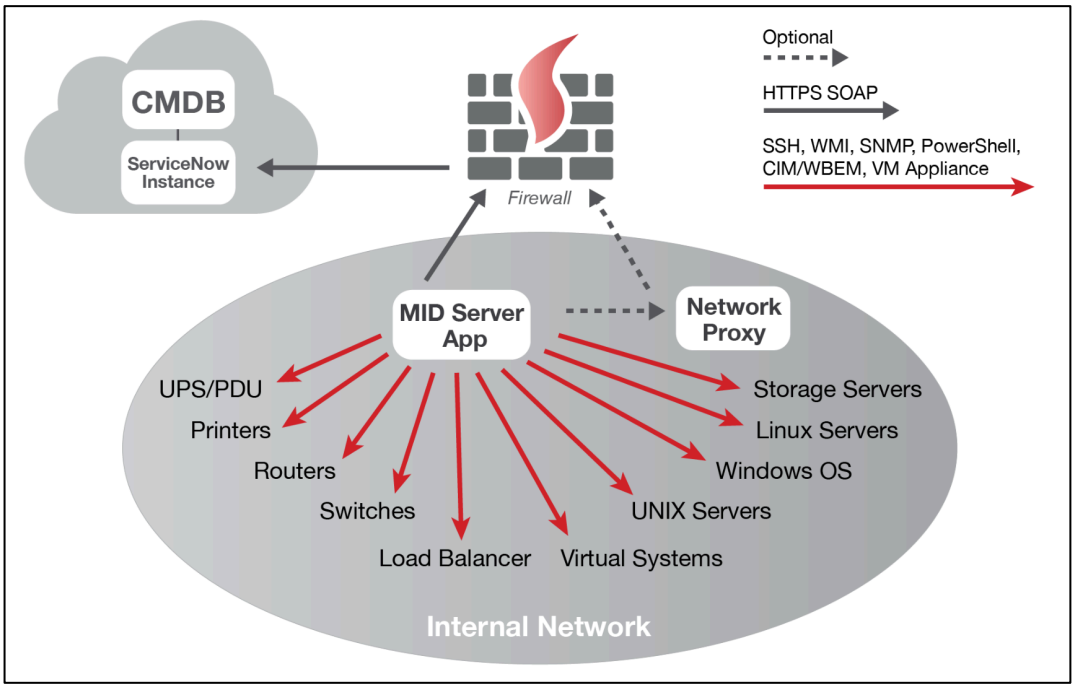
With our advanced mapping technology, not only are you provided the ability to understand what physical assets are under your control, but what applications they are running. We provide the insight of application dependencies so you can quickly identify the impact a server or related services have on your environment when they go down for maintenance or suffer an unexpected outage.

®2015 ServiceNow, Inc. All rights reserved.

ServiceNow Inside your Network – the "MID Server"

To gather your important data and providing for industry standard security requirements a MID Server *application* will be deployed within your infrastructure for the agent less, behind the firewall "look" into your secure environment.

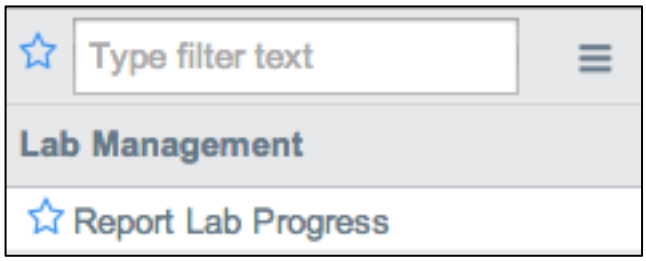
The MID Server provides for Secure, *outbound only* 128bit SSL communication to your specific ServiceNow applications, complying with strict Corporate and Regulatory standards.



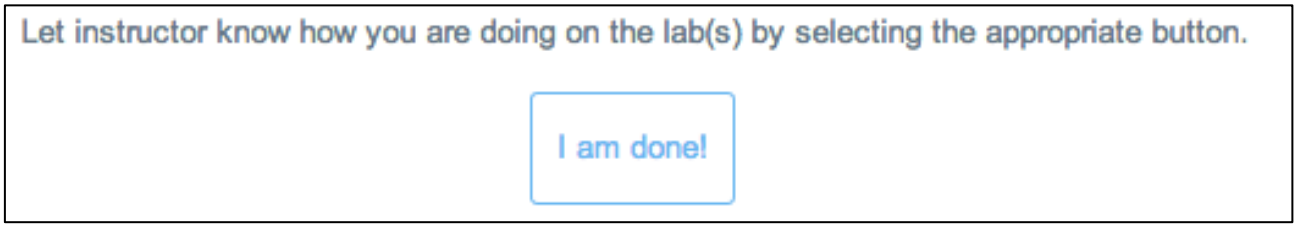
®2015 ServiceNow, Inc. All rights reserved.

Progress Report

1. Navigate to **Lab Management > Report Lab Progress**.



2. Click **I am Done!**



®2015 ServiceNow, Inc. All rights reserved.

Lab Goal

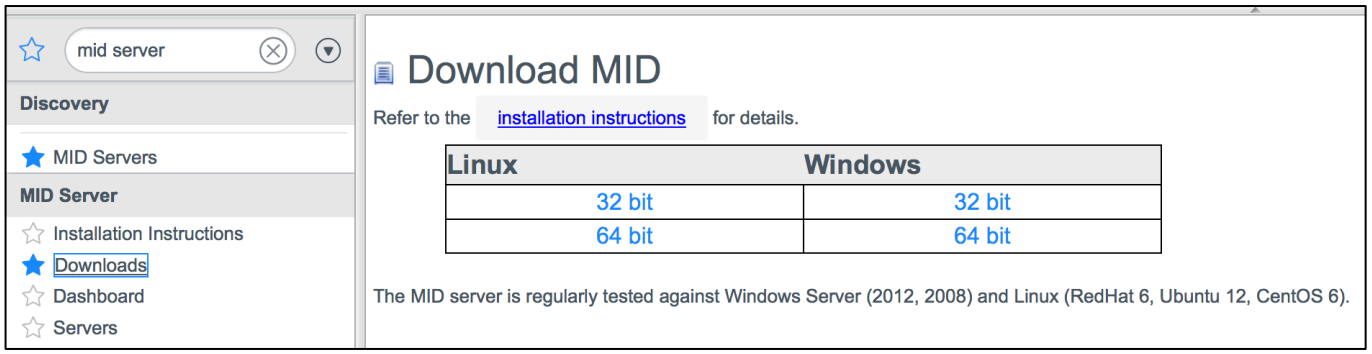
- Download MID Server for Discovery (on your provided HOST)
- Configure MID Server and instance
- Run Discovery for the first time

Lab 2
Deploy MID Server

Download a MID Server

- Due to lab limitations, this is an instructor-demonstrated piece. MID Servers have been pre-deployed.
- For those with access and ability, you can deploy your own MID Server on your laptops, so please follow along if you can.
- Fun Fact: The "MID" in "MID Server" stands for "Management, Integration, Discovery."

1. In your ServiceNow instance (accessed via your MID Server HOST), in the **application search bar**, type in **mid server**.



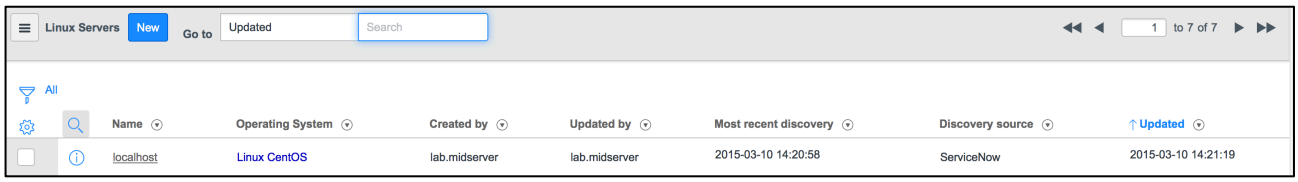
2. Click the **Downloads** link.

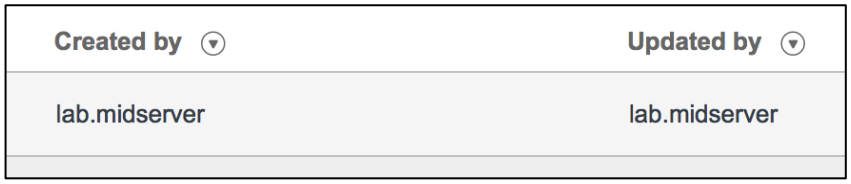
3. Select your Operating System to save the file to your desktop.

©2015 ServiceNow, Inc. All rights reserved.

MID Server User Account Overview

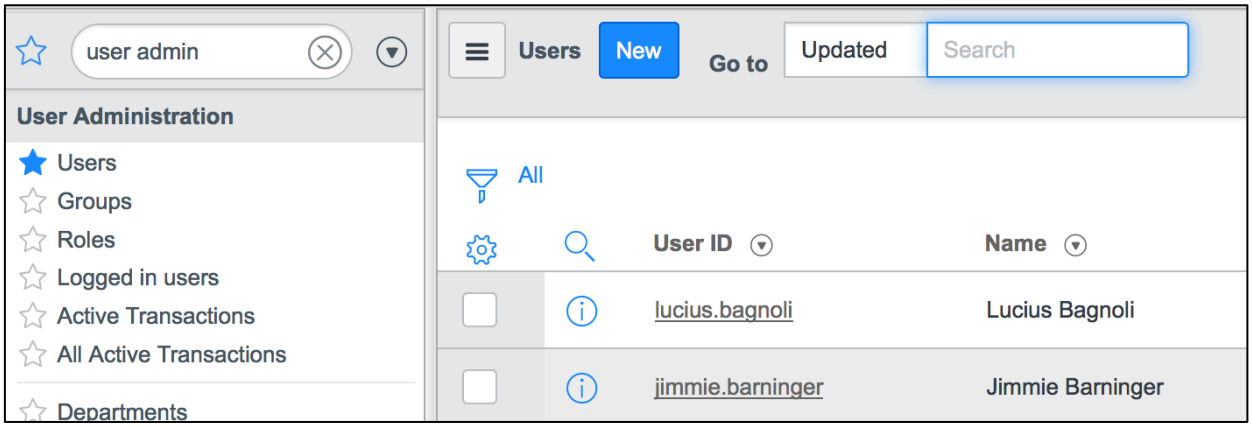
- The MID Server authenticates to the instance just like any other user when talking to ServiceNow, however with its own specific role - the **mid_server role**.
- MID Servers can share logins.
- The MID Server user will be the identity that creates and/or updates records.





Create a User for the MID Server application

1. In the application search bar, search for **User Administration**.

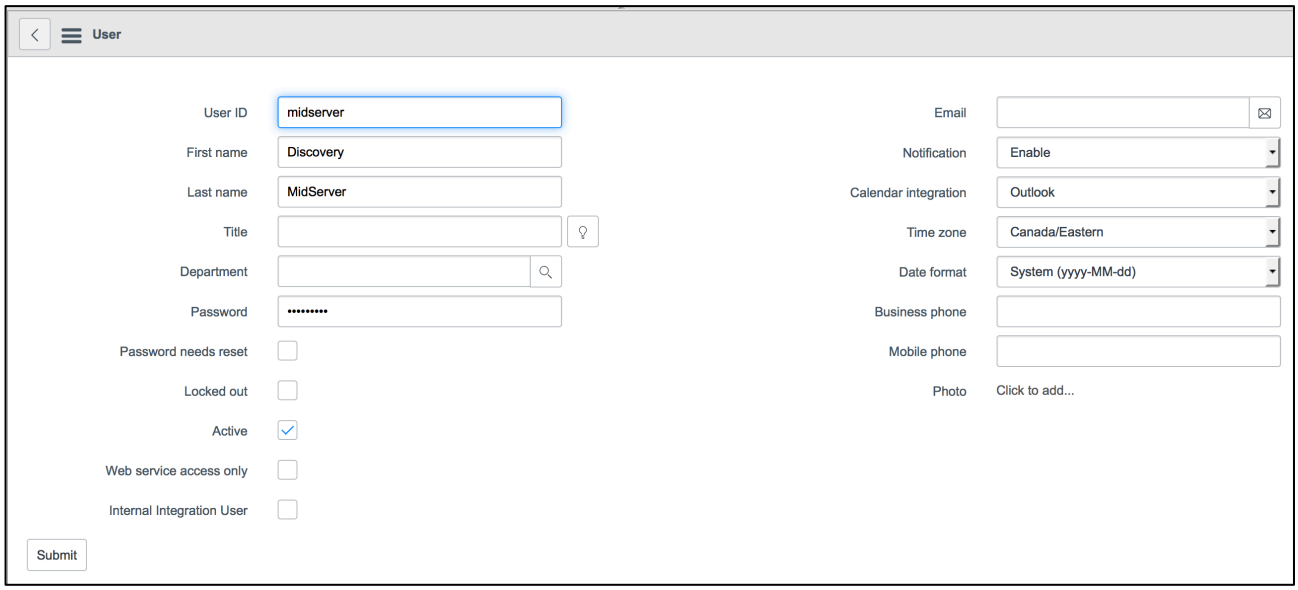


2. Click **Users**.

©2015 ServiceNow, Inc. All rights reserved.

3. Click **New**.

   UserID: **midserver** or any unique name.
   First name: **Discovery**
   Last name: **MidServer**
   Provide a **complex password** that meets your internal security requirements.



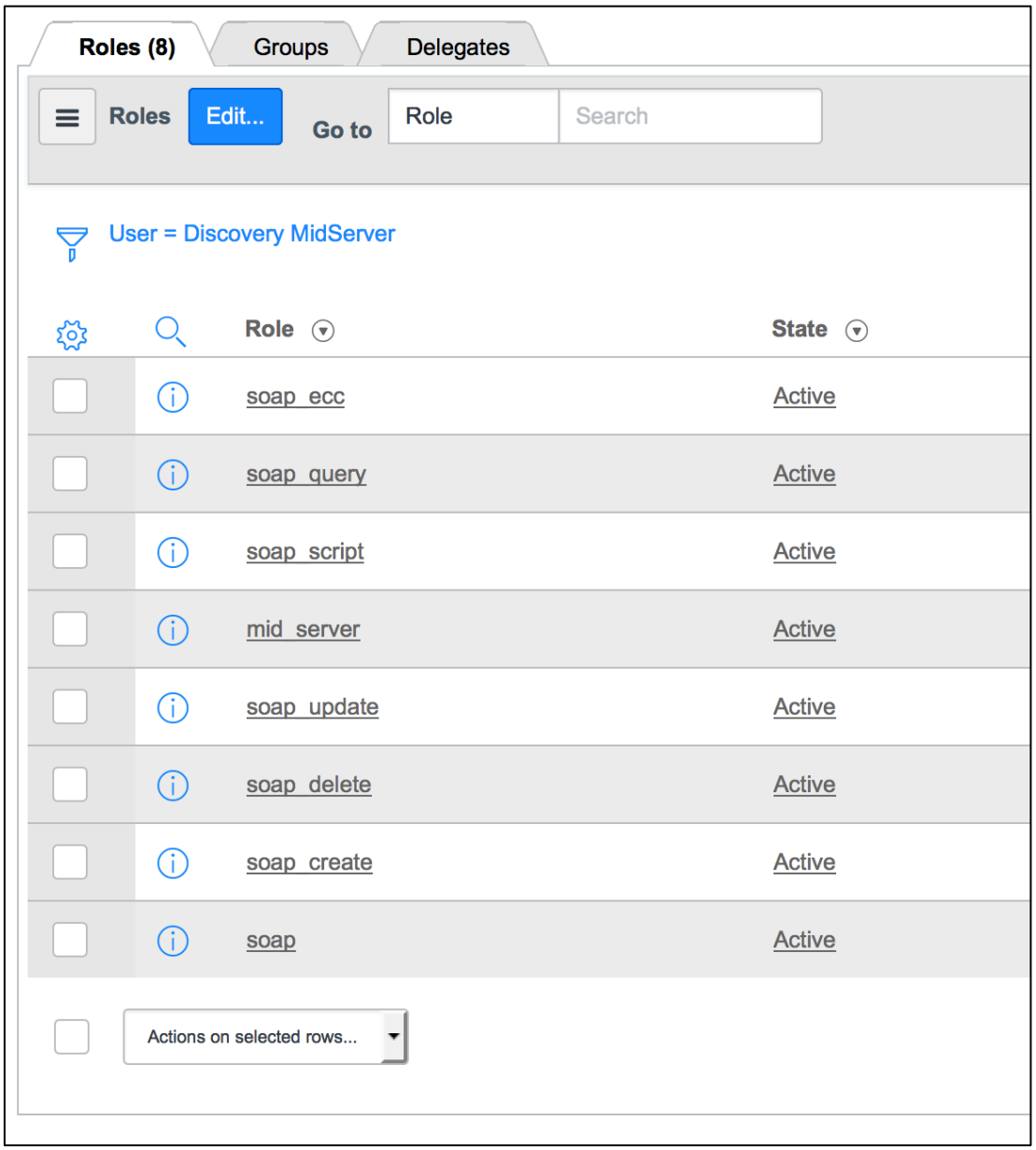
4. Right-click and **Save** the record.

5. You will see a new related list **Roles**, click **Edit**.

6. Provide this user with the **mid_server** role, then **Save**.

®2015 ServiceNow, Inc. All rights reserved.

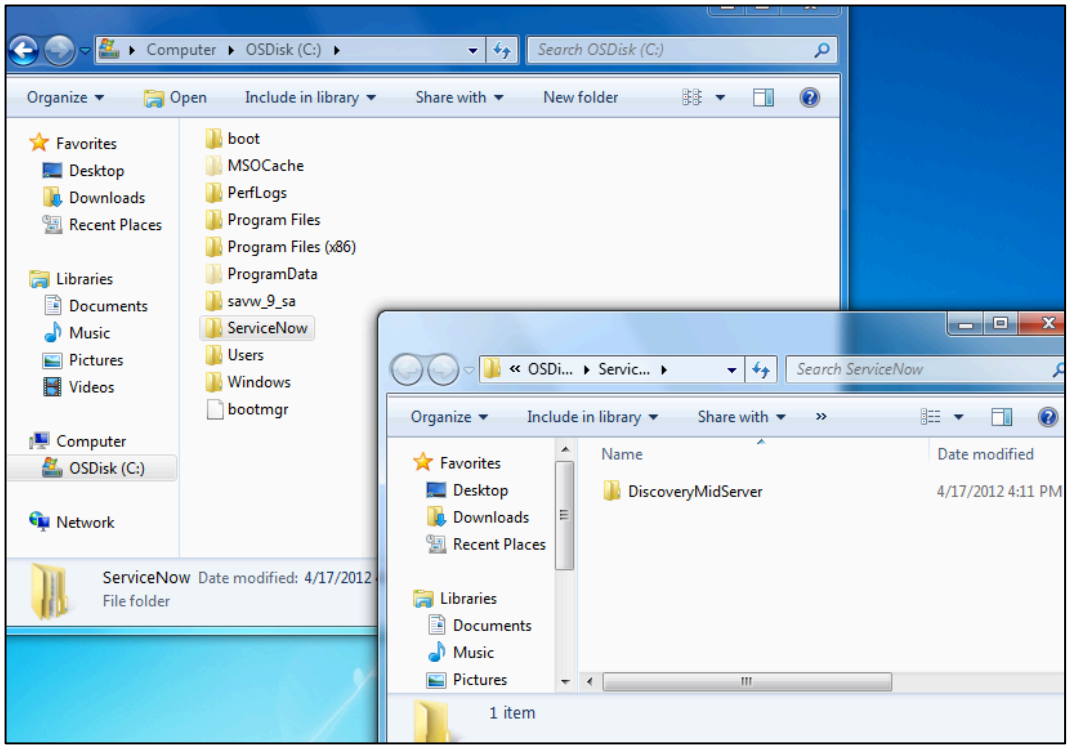
7. By adding one role, the user inherits other necessary roles to properly function.



©2015 ServiceNow, Inc. All rights reserved.

Deploy the MID Sever on the "Host"

1. In your preferred local drive, create a folder called **ServiceNow**.
2. Create a subfolder under ServiceNow called **DiscoveryMIDServer**.



3. Extract the downloaded MID Server file into **DiscoveryMIDServer**.

®2015 ServiceNow, Inc. All rights reserved.

Extract the MID Server

1. You now have an **Agent** subfolder.
2. Click into that folder and open the **config.xml** file with Wordpad. Right-click the file and choose **Open with > Wordpad**.
3. Or you can choose your favorite *advanced* text editor such as TextWranger or Notepad++.

```
<parameters>

  <!-- ************************************************************************************
       * REQUIRED Parameters
       *
       * This section contains parameters that MUST be included in EVERY Mid Server
       * configuration.
       ************************************************************************************ -->

       <!-- Tells the MID server where to contact its associated Service-now instance.  Edit
            this value to provide the URL of your organization's Service-now instance. -->
       <parameter name="url" value="https://YOUR_INSTANCE.service-now.com"/>

       <!-- If your Service-now instance has authentication enabled (the normal case), set
            these parameters to define the user name and password the MID server will use
            to log into the instance.  -->

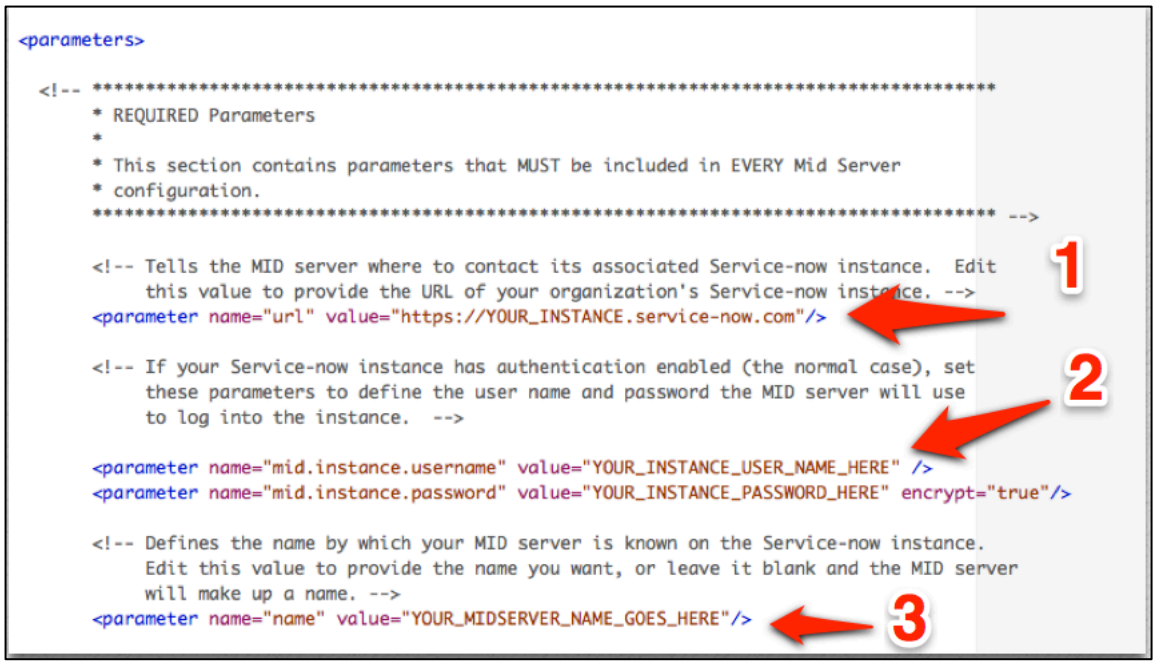
       <parameter name="mid.instance.username" value="YOUR_INSTANCE_USER_NAME_HERE" />
       <parameter name="mid.instance.password" value="YOUR_INSTANCE_PASSWORD_HERE" encrypt="true"/>

       <!-- Defines the name by which your MID server is known on the Service-now instance.
            Edit this value to provide the name you want, or leave it blank and the MID server
            will make up a name. -->
       <parameter name="name" value="YOUR_MIDSERVER_NAME_GOES_HERE"/>
```

©2015 ServiceNow, Inc. All rights reserved.

Configure the MID Server

1. Add the URL to your ServiceNow instance.
2. Enter the username and password you initially created for the MID Server.
3. Give the MID Server a unique name.




```
<parameters>

  <!-- ************************************************************************************
       * REQUIRED Parameters
       *
       * This section contains parameters that MUST be included in EVERY Mid Server
       * configuration.
       ************************************************************************************ -->

       <!-- Tells the MID server where to contact its associated Service-now instance.  Edit
            this value to provide the URL of your organization's Service-now instance. -->
       <parameter name="url" value="https://YOUR_INSTANCE.service-now.com"/>

       <!-- If your Service-now instance has authentication enabled (the normal case), set
            these parameters to define the user name and password the MID server will use
            to log into the instance.  -->

       <parameter name="mid.instance.username" value="YOUR_INSTANCE_USER_NAME_HERE" />
       <parameter name="mid.instance.password" value="YOUR_INSTANCE_PASSWORD_HERE" encrypt="true"/>

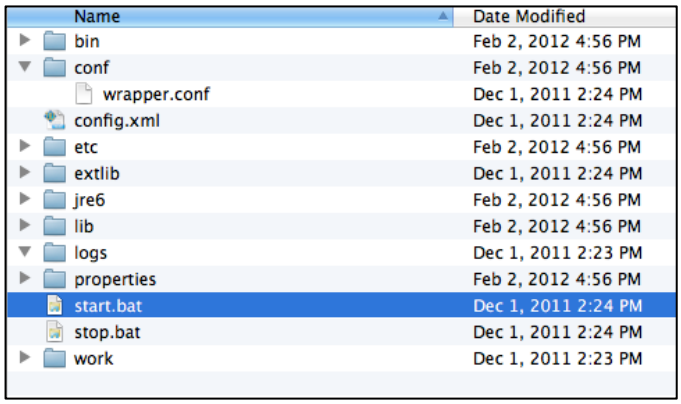
       <!-- Defines the name by which your MID server is known on the Service-now instance.
            Edit this value to provide the name you want, or leave it blank and the MID server
            will make up a name. -->
       <parameter name="name" value="YOUR_MIDSERVER_NAME_GOES_HERE"/>
```

4. Save and close the record.

©2015 ServiceNow, Inc. All rights reserved.

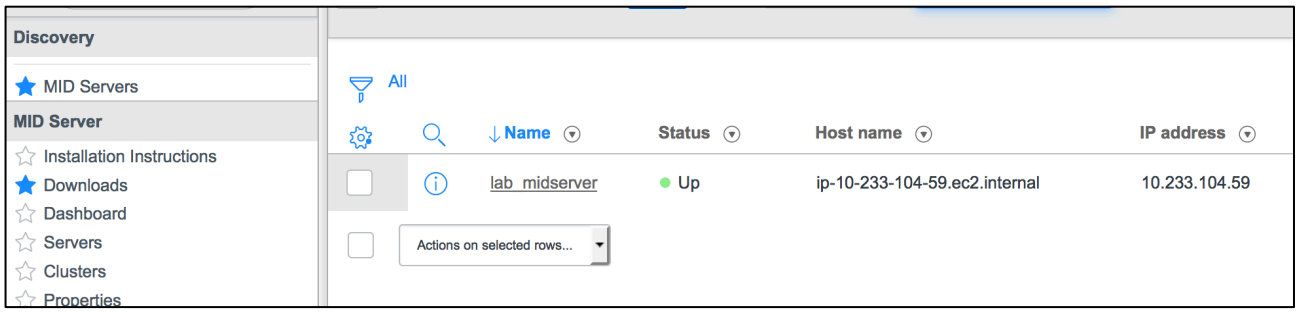
Start the MID Server

1. In the **Agent** folder, double-click **start.bat**.



Note: Check the wiki for unique start up instructions by OS.
http://wiki.servicenow.com/index.php?title=MID_Server_Installation

2. Verify the MID Server Status is **Up**.



Progress Report

1. Navigate to **Lab Management > Report Lab Progress**.

2. Click **I am Done!**

©2015 ServiceNow, Inc. All rights reserved.

Lab Goal

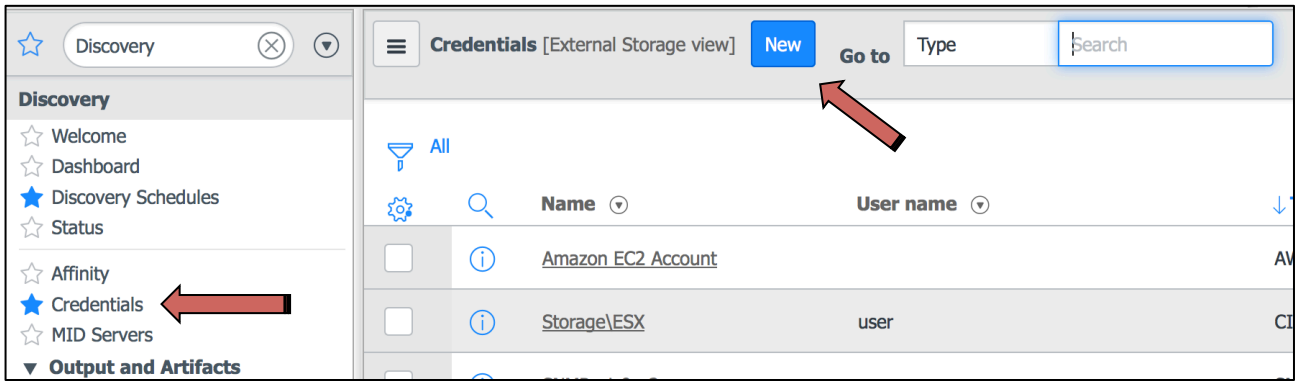
- Enter Credentials
- Define Schedules

In this lab, you configure your lab instance. You create schedules and run a discovery. You use the pre-installed MID Server on your instances.

Lab 3
Discovery Credentials & Schedule

Enter Credentials for Target Systems

1. In the **Discovery** application, select the **Credentials** module.



2. Select **New**.

3. Fill in the fields:

   Name: **K15Lab**
   Select Type: **SSH**
   User name: **linuxuser**
   Password: **p@ssword**

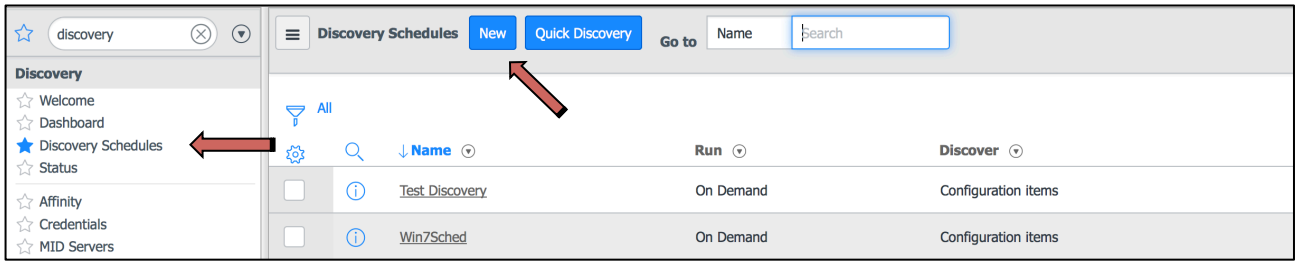


®2015 ServiceNow, Inc. All rights reserved.

Create a Discovery Schedule

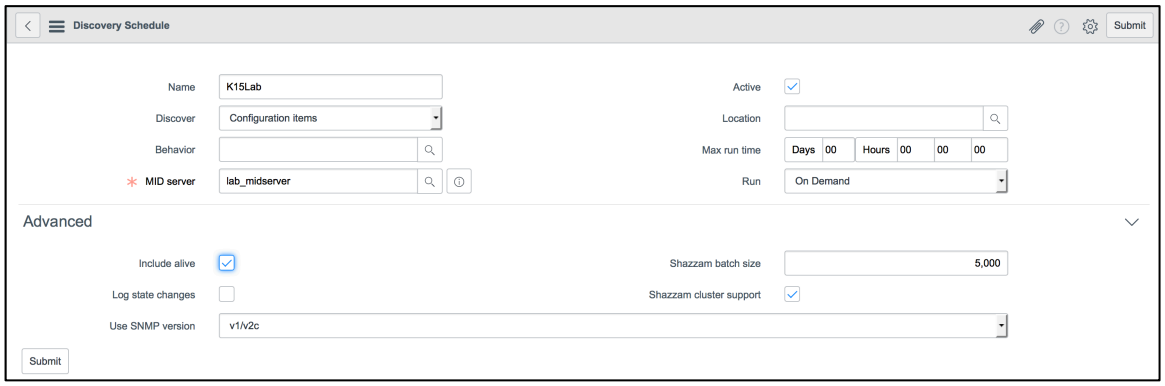
1. In the **Discovery** application, select the **Discovery Schedules** module.

2. Select **New**.



3. Fill in the fields:

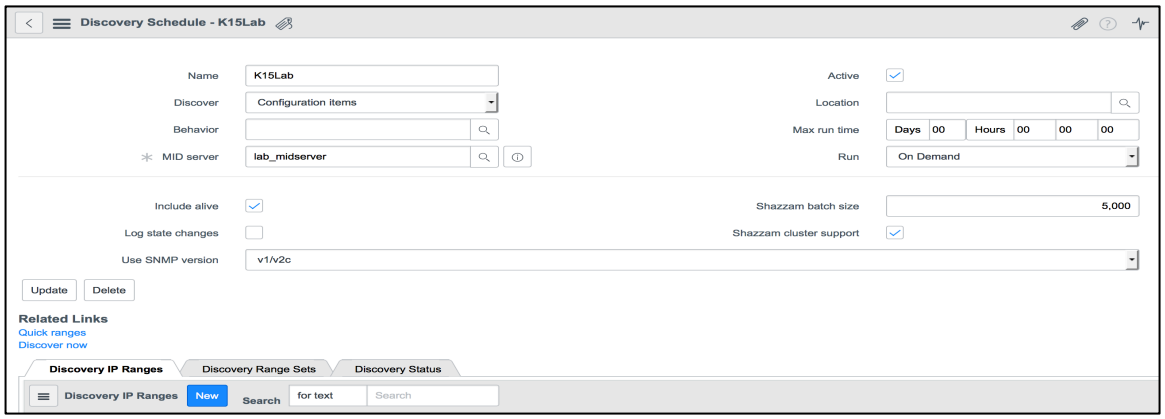
   Name: **K15Lab**
   MID Server: **lab_midserver**
   Active: **check**
   Runs schedule at designated time.
   Include alive: **checked**.
   This logs the IP addresses that were responsive but not available to be discovered.
   Log state changes: **unchecked**.
   This logs the complete transition of a record through its discovery process.



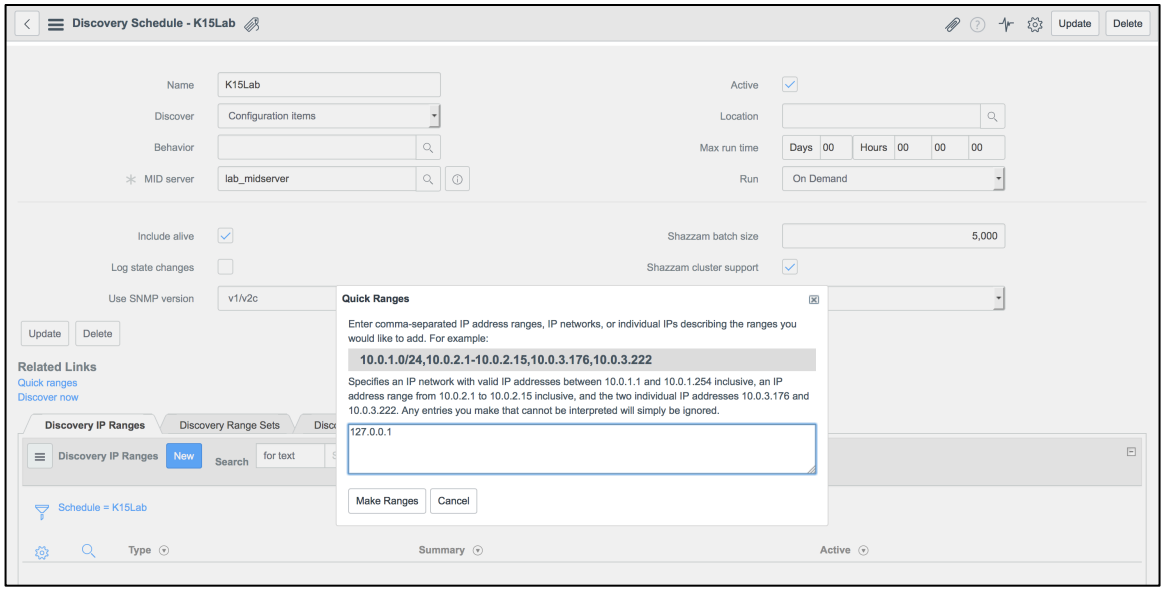
4. Right-click on header and select **Save**.

©2015 ServiceNow, Inc. All rights reserved.

5. Under **Related** Links, click **Quick Ranges**. This is where you enter your IP Ranges. In real life you could have full networks, individual IPs, or range groups to a limit of 100k per schedule.



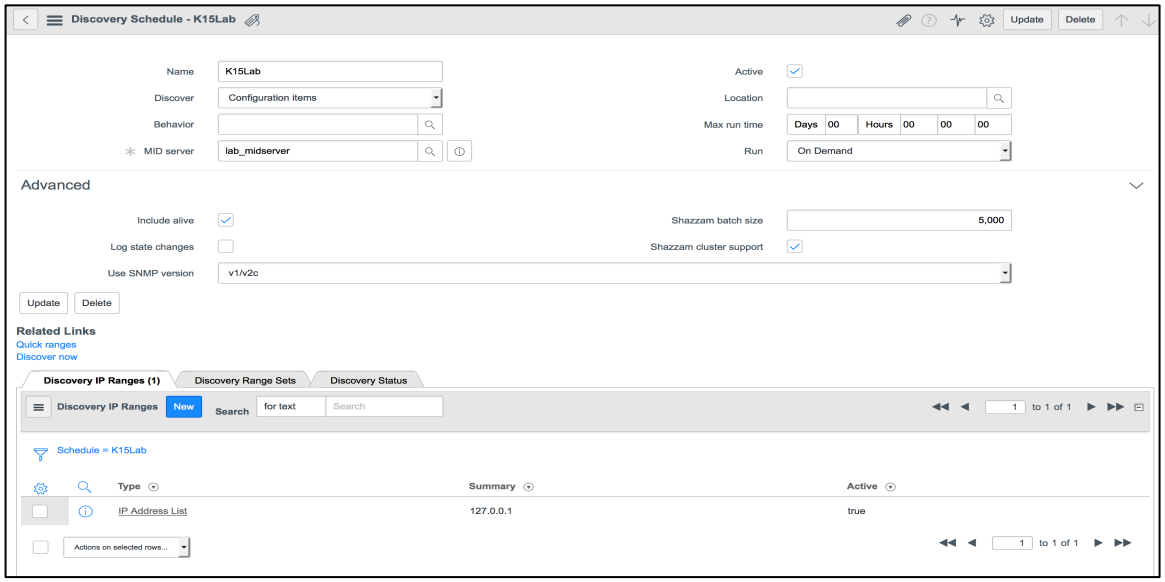
6. Enter the Lab loopback IP address: **127.0.0.1**



7. Click **Make Ranges**.

®2015 ServiceNow, Inc. All rights reserved.

8. Under **Related Links**, click **Discover now**.



Progress Report

1. Navigate to **Lab Management > Report Lab Progress**.

2. Click **I am Done!**

®2015 ServiceNow, Inc. All rights reserved.

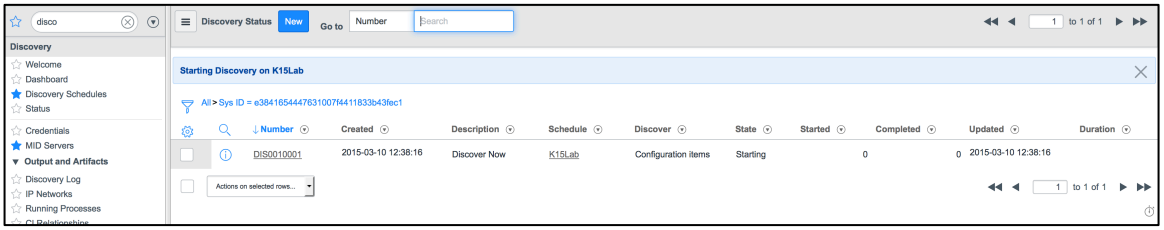
Lab Goal

- Identify where to find Discovery results
- Understand the Discovery process

Lab 4 Review Results

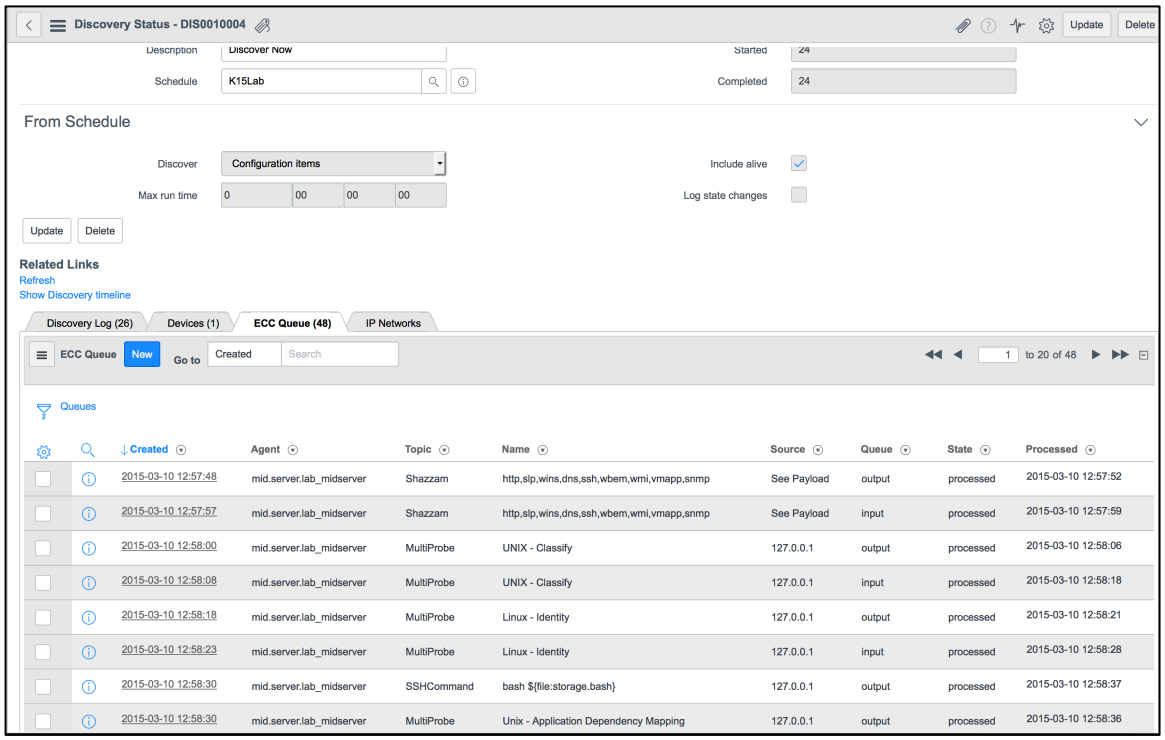
Discovery Results

1. In the **Discovery** application, click on **Status**.
2. This list contains all discoveries run either on a scheduled basis or on demand.



©2015 ServiceNow, Inc. All rights reserved.

3. In the **Discovery Status** record, we see all the work take place. The different sections include the **Discovery Log**, **ECC Queue** table, and **Devices** we discovered



Progress Report

1. Navigate to **Lab Management > Report Lab Progress**.

2. Click **I am Done!**

®2015 ServiceNow, Inc. All rights reserved.

Lab Goal

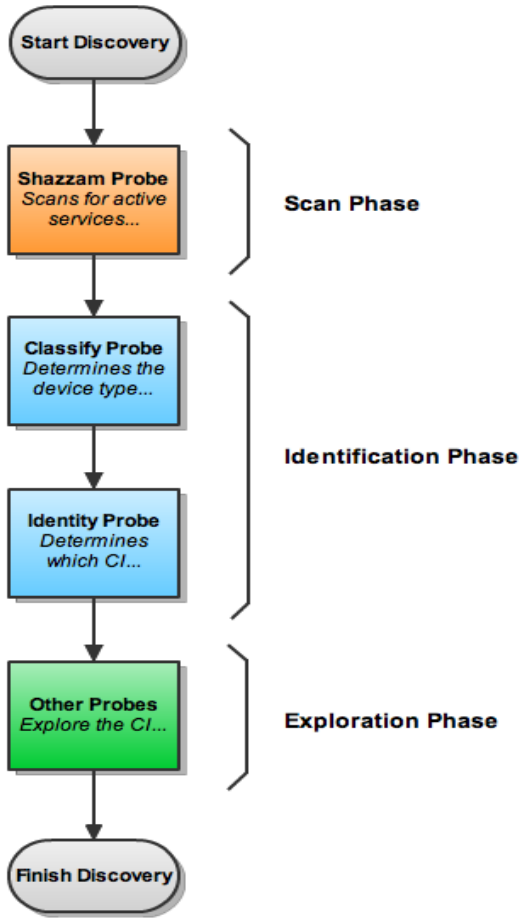
ServiceNow Discovery uses a repetitive step-by-step process to populate the CMDB to ensure only the most valuable information is returned using four phases:

1. Scan
2. Classification
3. Identification
4. Exploration

Lab 5
Discovery Phases

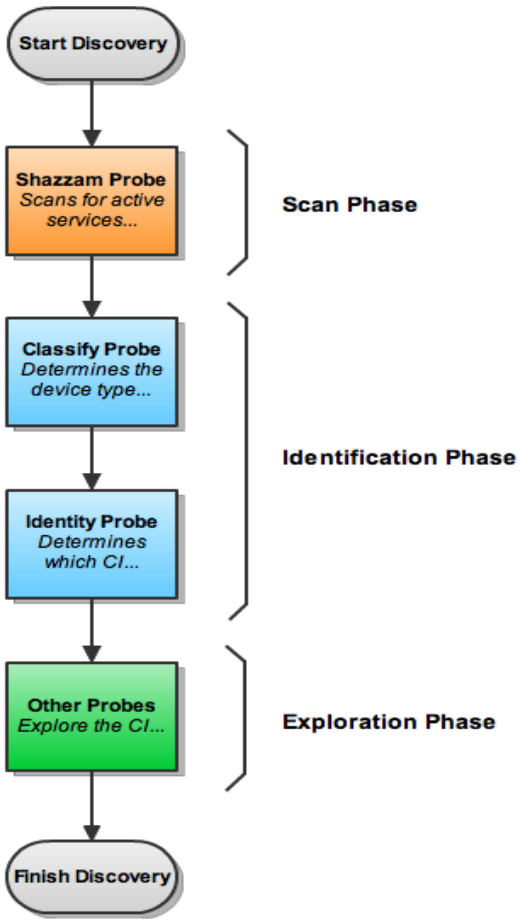
- **Phase 1: Port Scan (Shazzam)**
  - Scan for "active" devices – Shazzam probe
  - Ports determined by Port Probes and/or specific behavior
  - Each Port Probe is determined by IP Services

- **Phase 2: Classification**
  - Classify **type** of device
    - Unix
    - Windows
    - Network Device
  - Computers are classified by operating system
  - Network Devices are classified primarily by functionality (power, print, switch, route)



©2015 ServiceNow, Inc. All rights reserved.

- **Phase 3: Identification**
  - **Identify** the particular device following a specific set of rules
  - The "identity probe" launched is dictated by the CI classification
  - After the identity probe finishes, the sensor runs through the "CI Identifiers" looking for a match in the CMDB. Three things can happen based on a ***complete*** match…
    - Find no complete match – **create**
    - Find single complete match - **update**
      - Stop evaluation we found the match
    - Find multiple matches – **stop**
      - But first check all the rules to make sure there isn't a complete match



CI Identifiers | New | Go to | Order | Search | 1 to 8 of 8

All > Active != false

Name	Description	Active	Order	Applies to
WBEM Service	Identifies a WBEM Service	true	100	WBEM Service [cmdb_ci_wbem_service]
ESX UUID	Identify ESX servers based on VMWare UUID.	true	900	ESX Server [cmdb_ci_esx_server]
Storage Server	Identifies Storage Server CIs in the CMDB using name, serial numbers, and/or CIM object path.	true	910	Storage Server [cmdb_ci_storage_server]
Serial Number Table & Class Name	Identify CIs in the CMDB based on serial number(s) in the serial number table and sys_class_name.	true	1,000	Hardware [cmdb_ci_hardware]
Serial Number & Class Name	Identify CIs in the CMDB based on the serial_number field and matching sys_class_name.	true	1,050	Hardware [cmdb_ci_hardware]
Name & Class Name	Identify CIs in the CMDB based on name field and matching sys_class_name.	true	1,100	Hardware [cmdb_ci_hardware]
Network	Identify CIs in the CMDB based on IPs and MAC Address(es) in the network adapter table.	true	1,200	Hardware [cmdb_ci_hardware]
Serial Number Table & Name	Identify CIs in the CMDB based on serial number(s) in the serial number table and name. This is the fallback identifier in the case that discovery via SNMP receives a fraction of the requested data.	true	1,500	Network Gear [cmdb_ci_netgear]

Actions on selected rows... | 1 to 8 of 8

- **Phase 4: Exploration**
  - **Explore** the device – Time to find the good stuff!
- Probes launched are dictated by the CI classification **trigger_probes** list with phase equal to **Exploration**

©2015 ServiceNow, Inc. All rights reserved.

Lab Goal

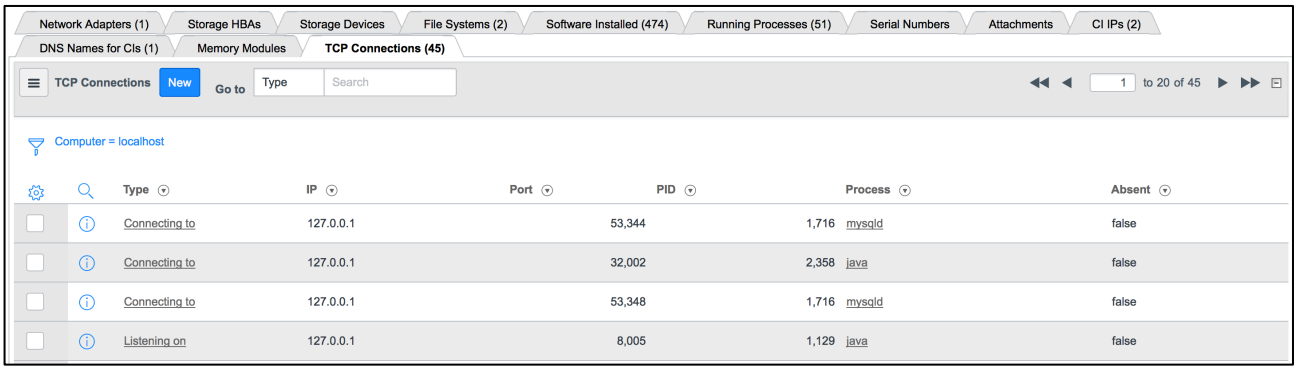
- Create a custom Process Classification
- Identify automatic relationship building

Lab 6
Custom Process Classifications

The exploration phase gathered all the processes that were running at the time of discovery.

Discovery uses these to build two primary types of application relationships:

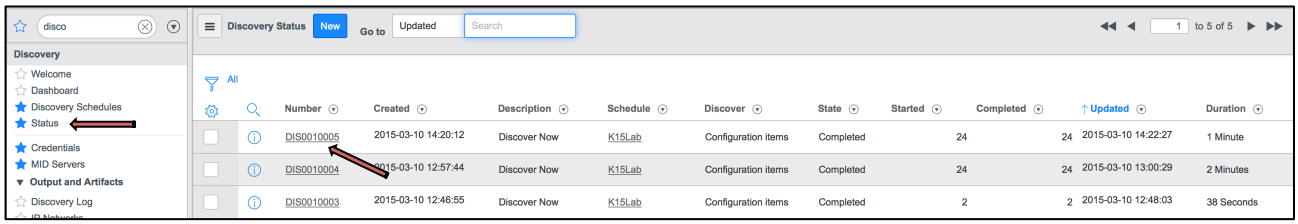
- Application to Host – **Runs on::Runs**
  - Based on the running process
- Application to Application – **Depends on::Used by**
  - Based on the running processes TCP connections



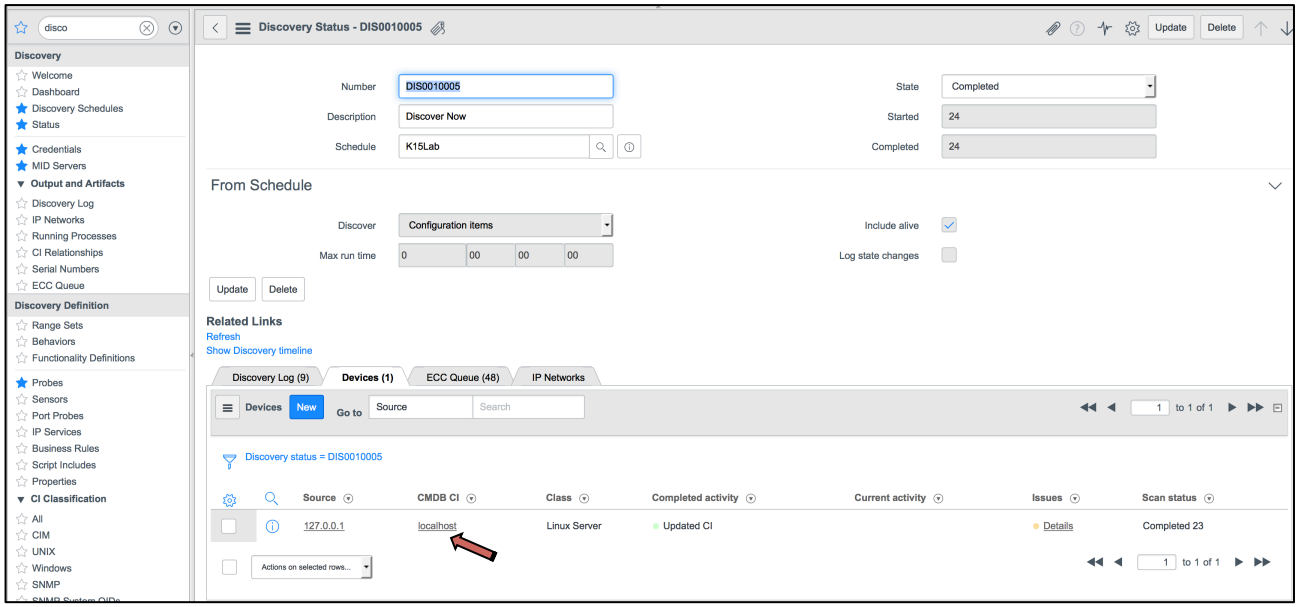
®2015 ServiceNow, Inc. All rights reserved.

Review a Discovered Device Record

1. Navigate to **Discovery > Status**.
2. Click the most recent **Discovery Number**.



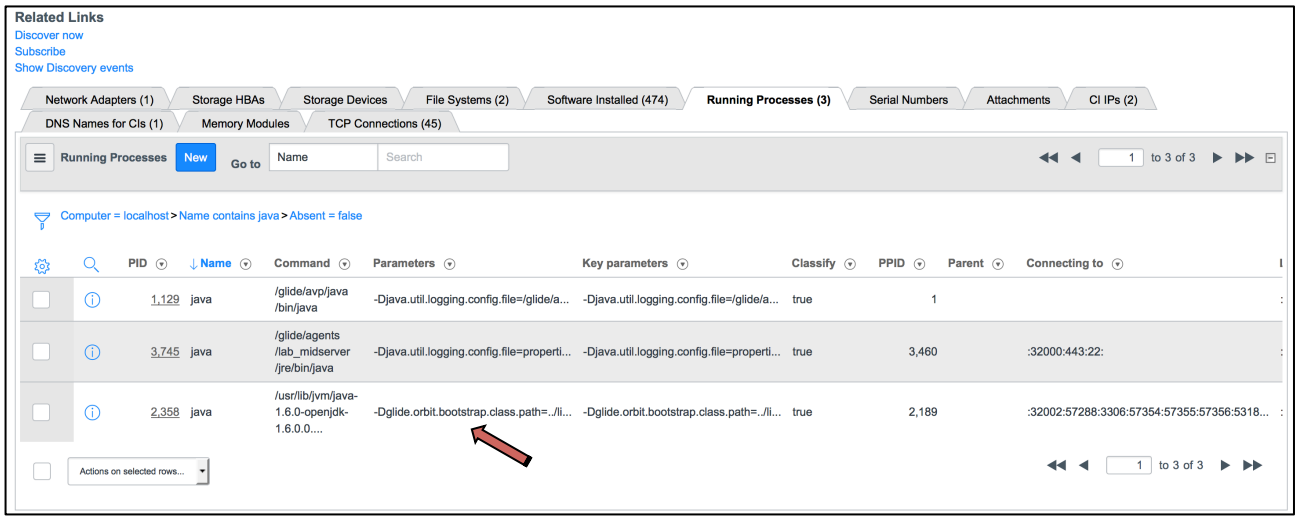
3. Click on the CMDB CI record **localhost**.



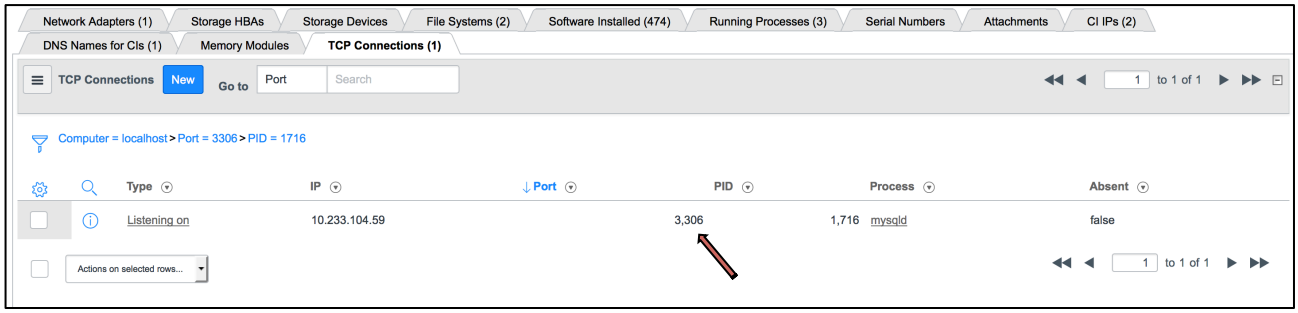
®2015 ServiceNow, Inc. All rights reserved.

Create a Relationship of a Tomcat Instance Running on this Host

1. Look for a **Java** process that has parameters that contain **bootstrap**.



2. Be sure that the same process makes the expected connections to other applications. Check the TCP connections and see if that same PID is communicating with anything else.

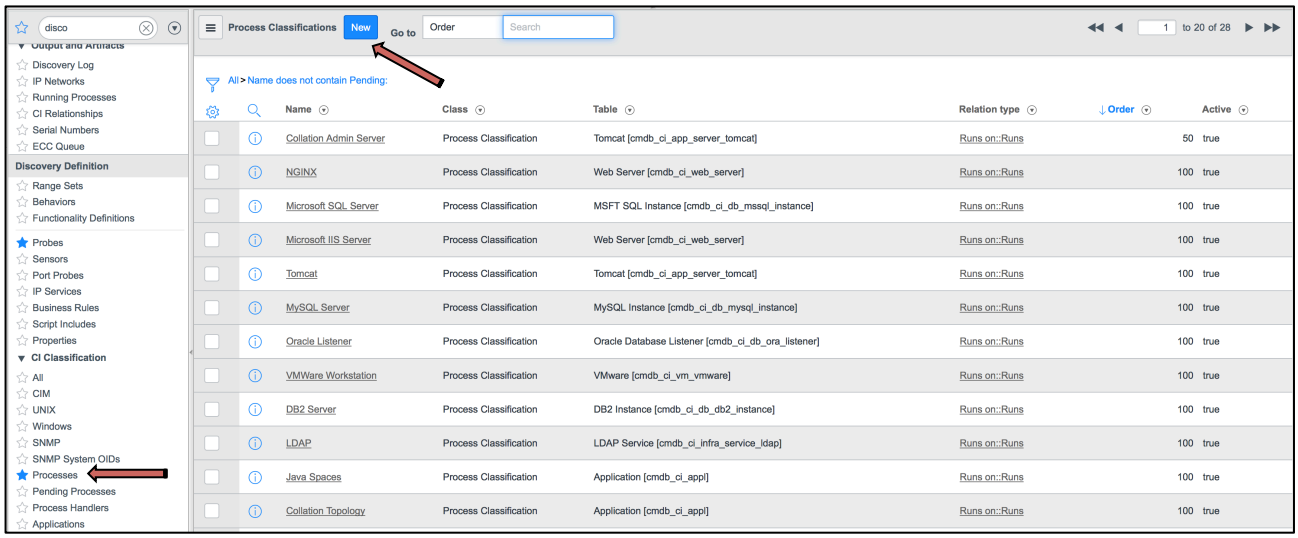


Yes, it is talking to the MSSQL (3306) instance running on the same host.

®2015 ServiceNow, Inc. All rights reserved.

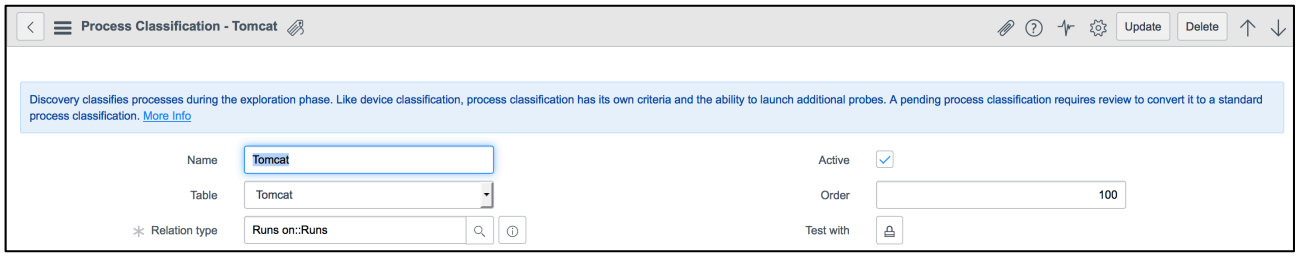
Create a Process Classification

1. Under **Discovery Definition > CI Classification Group > Process**, select **New**.



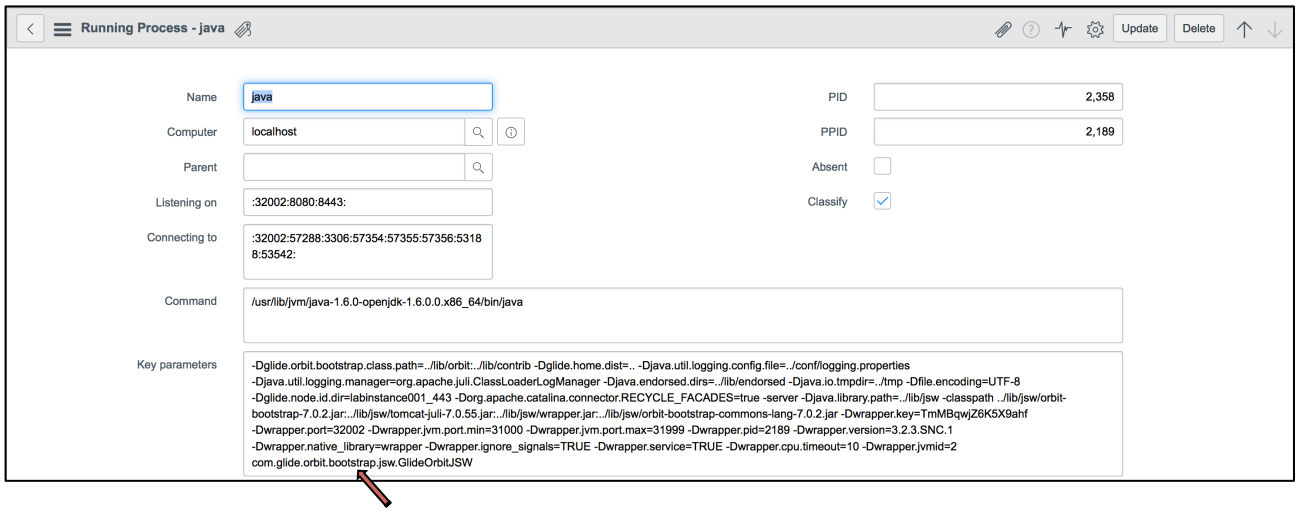
2. Fill in the fields:

   Name: **Tomcat**
   Table: **Tomcat** (This is an out-of-box table)
   Relationship type: **Runs on::Runs** (This is the most common type)

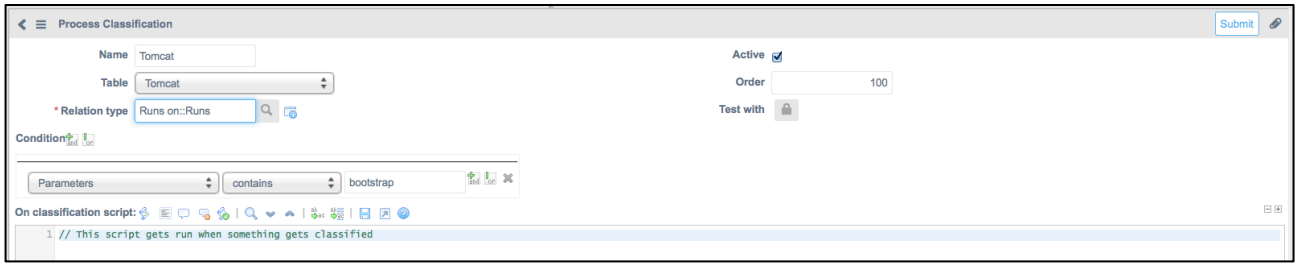


©2015 ServiceNow, Inc. All rights reserved.

3. Set the Process Classification condition to the signature of the running process that we want to build our relationship for. Look in the **Key parameters** value for **bootstrap**.



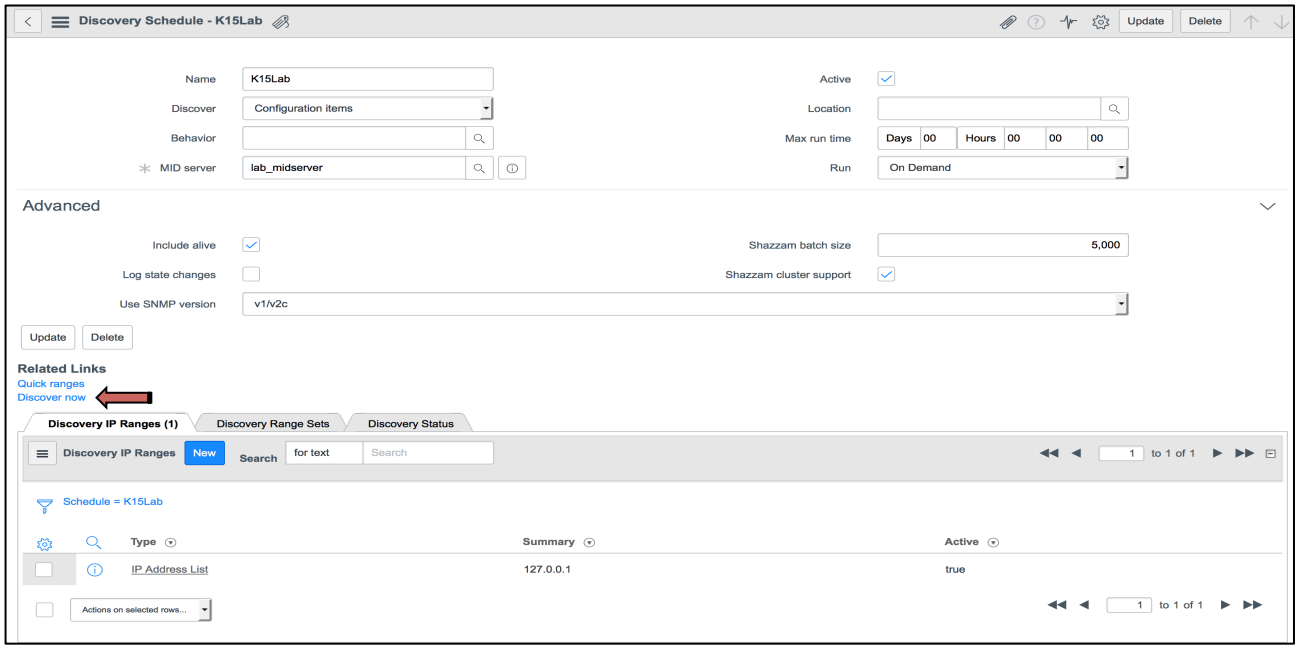
Add condition **Parameters contains bootstrap** to your **Process Classification** and click **Submit**.



®2015 ServiceNow, Inc. All rights reserved.

Run another Discovery

1. Navigate to **Discovery > Discovery schedules**, select **Lab schedule**, and click **Discover now** under **Related Links**.

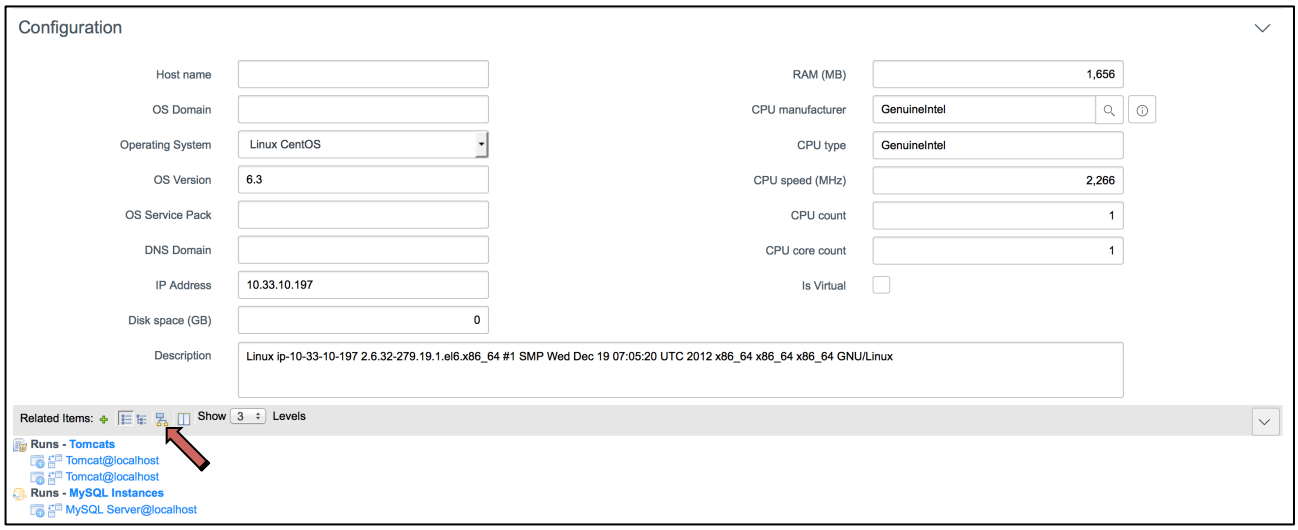


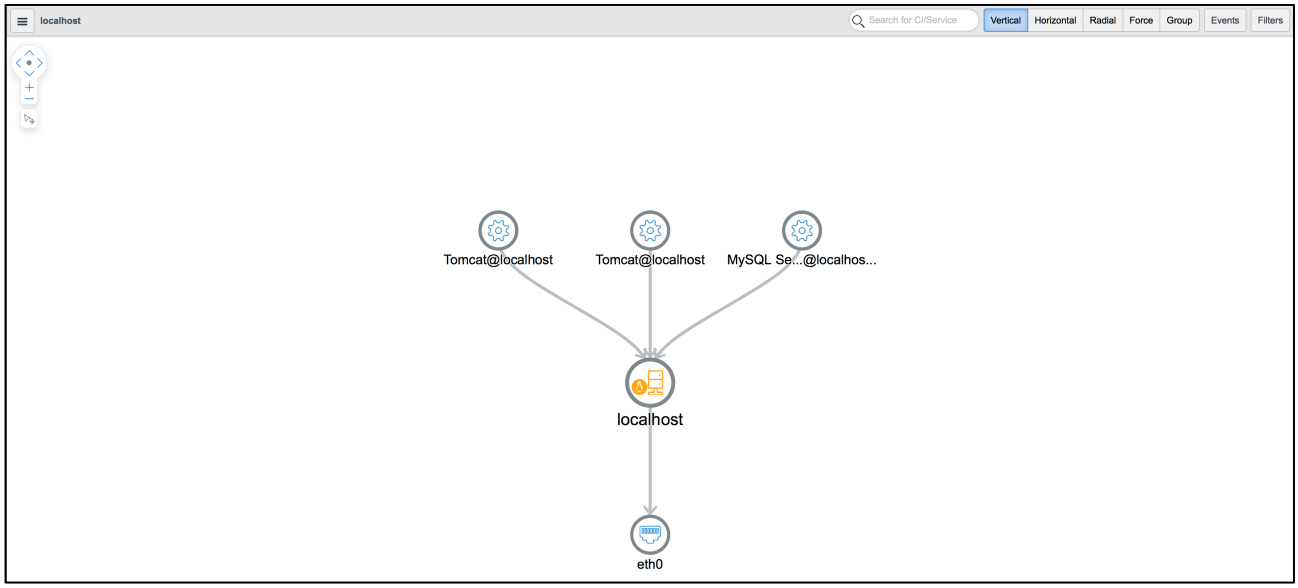
Note: You can always add additional probes to your classifier to gather additional information from the application when found.

®2015 ServiceNow, Inc. All rights reserved.

View Discovery Results

1. Click on the **Business Service Management Map** icon.





Progress Report

1. Navigate to **Lab Management > Report Lab Progress**.
2. Click **I am Done!**

®2015 ServiceNow, Inc. All rights reserved.