knowledge14

April 27–May 1, 2014 • Moscone Center • San Francisco, CA

Lab Guide

Discovery 101

Doug Schulze & Aleck Lin

Lab instance: https://<<name>>.lab.service-now.com

Login / Passwords:

admin / Knowledge14

itil / Knowledge14

employee / Knowledge14

Lab Goal

- Define ServiceNow Discovery
- Identify Value Return
- 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.

Note: We do not build physical, Layer 2, Hardware relationships.

®2014 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.

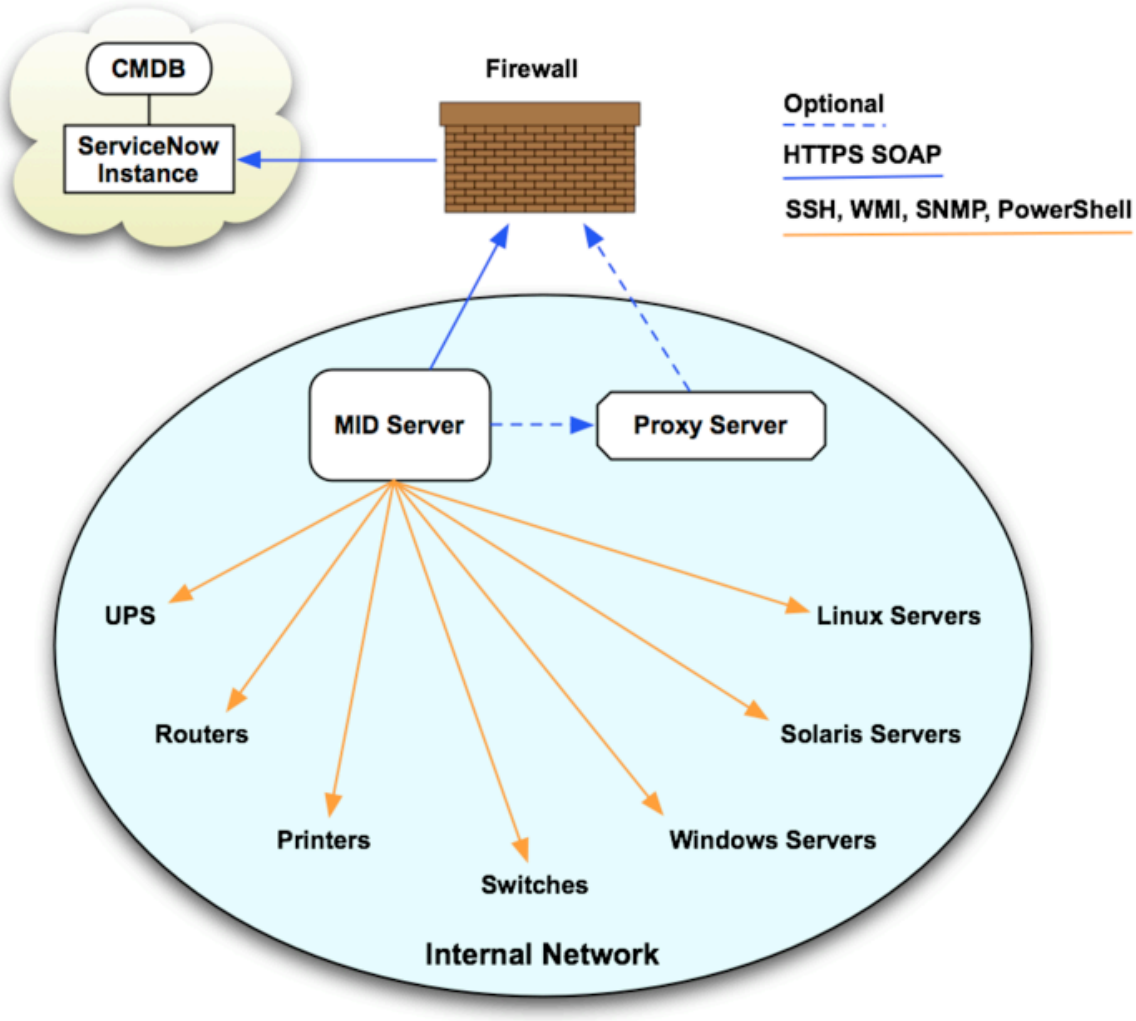
©2014 ServiceNow, Inc. All rights reserved.

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.



®2014 ServiceNow, Inc. All rights reserved.

Lab Goal

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

Lab 2 Deploy MID Server

Deploying a MID Server

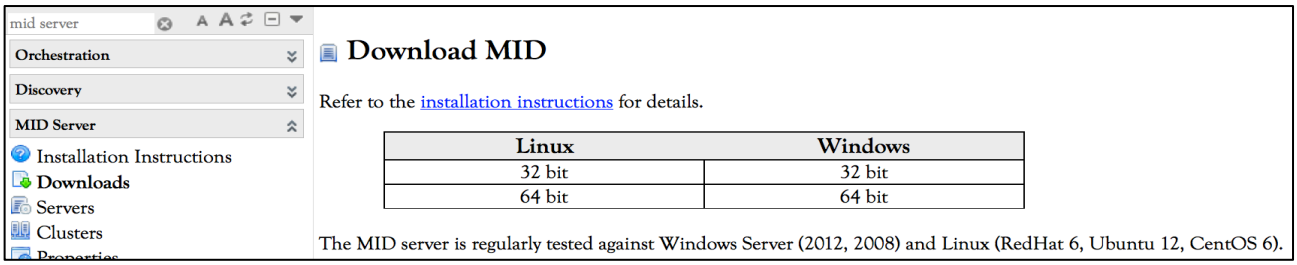
- Due to lab limitations this is an instructor-demonstrated piece. MID Servers have been pre-deployed to allow for our environment
- For those with access and ability you can deploy your own MID Server on your laptops so please follow along if you can
- Fun Fact: the MID in MID Server is an acronym that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

©2014 ServiceNow, Inc. All rights reserved.

Steps from your ServiceNow instance (Accessed via your MID Server HOST)

Download a MID Server

1. In the **Type filter text** field type **mid server**.

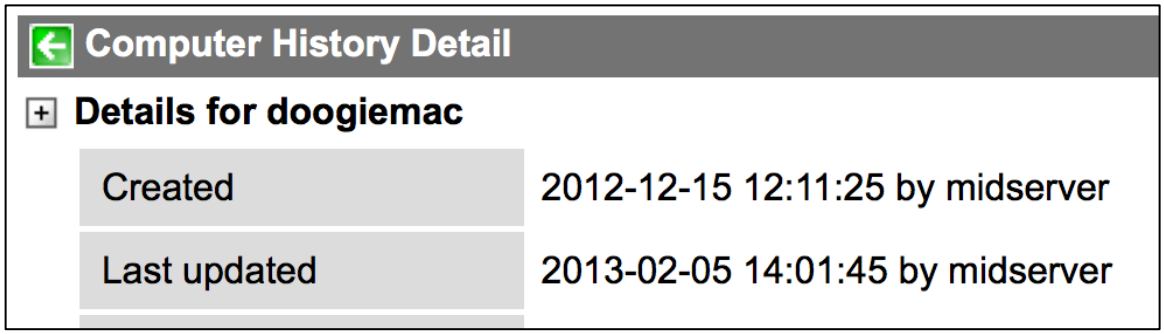


2. Click the **Downloads** link.

3. Select your Operating System saving the link to your desktop.

Configure a user for the MID Server to authenticate to the instance

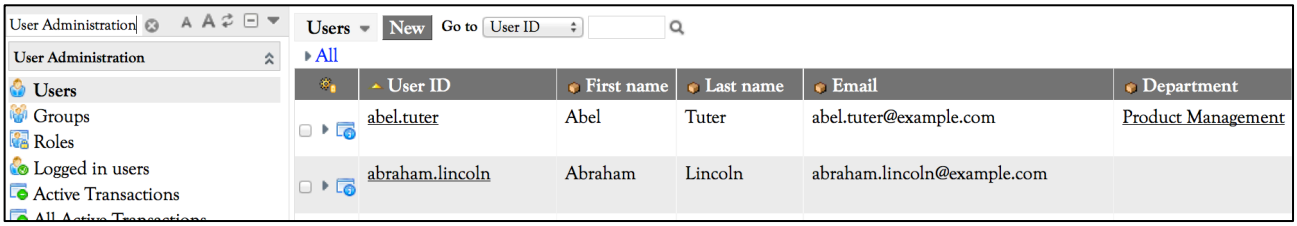
- The MID Server authenticates to the instance near like any other **user** when talking to ServiceNow, however with its own specific role …the **mid_server role**
- MID Servers can share logins
- The user will be the identity that creates and/or updates records



©2014 ServiceNow, Inc. All rights reserved.

Create a User for our MID Server application

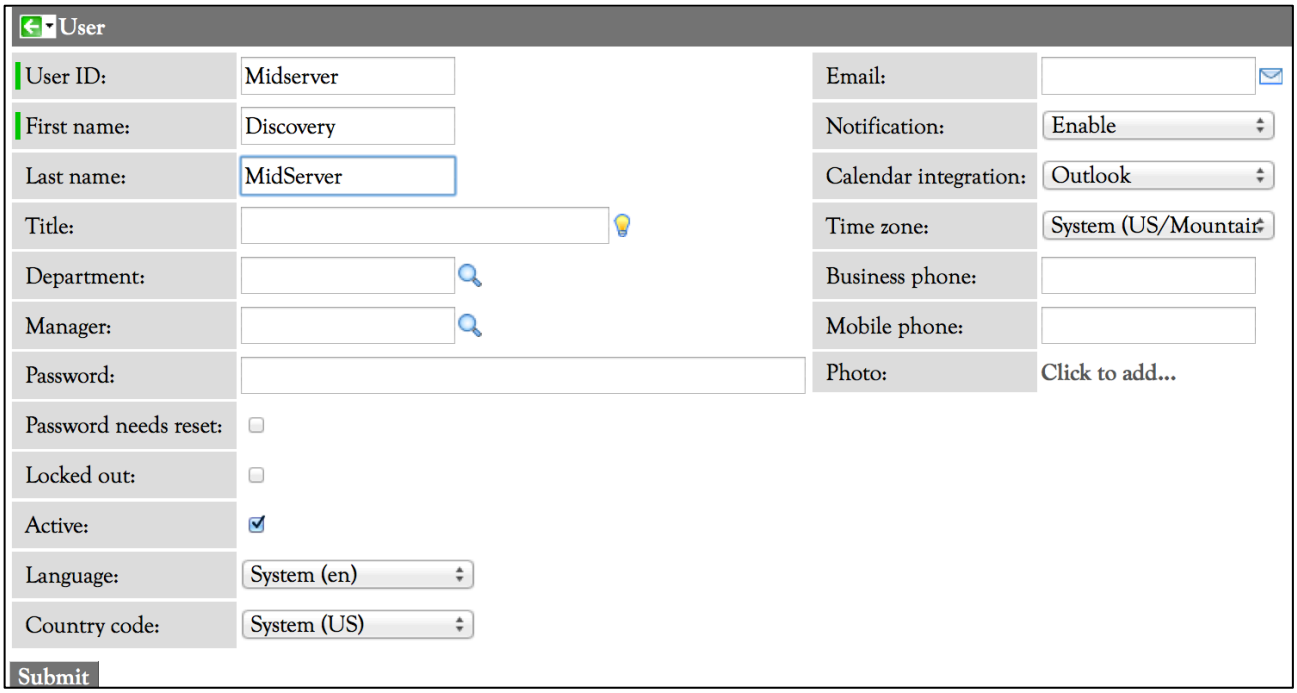
1. In the **Type filter text** field type **User Administration.**



2. Click **Users**

3. Select **New**

   User ID: **Midserver**
   First name: **Discovery**
   Last name: **MidServer**
   Provide a password that meets your internal security requirements. More complex is better!



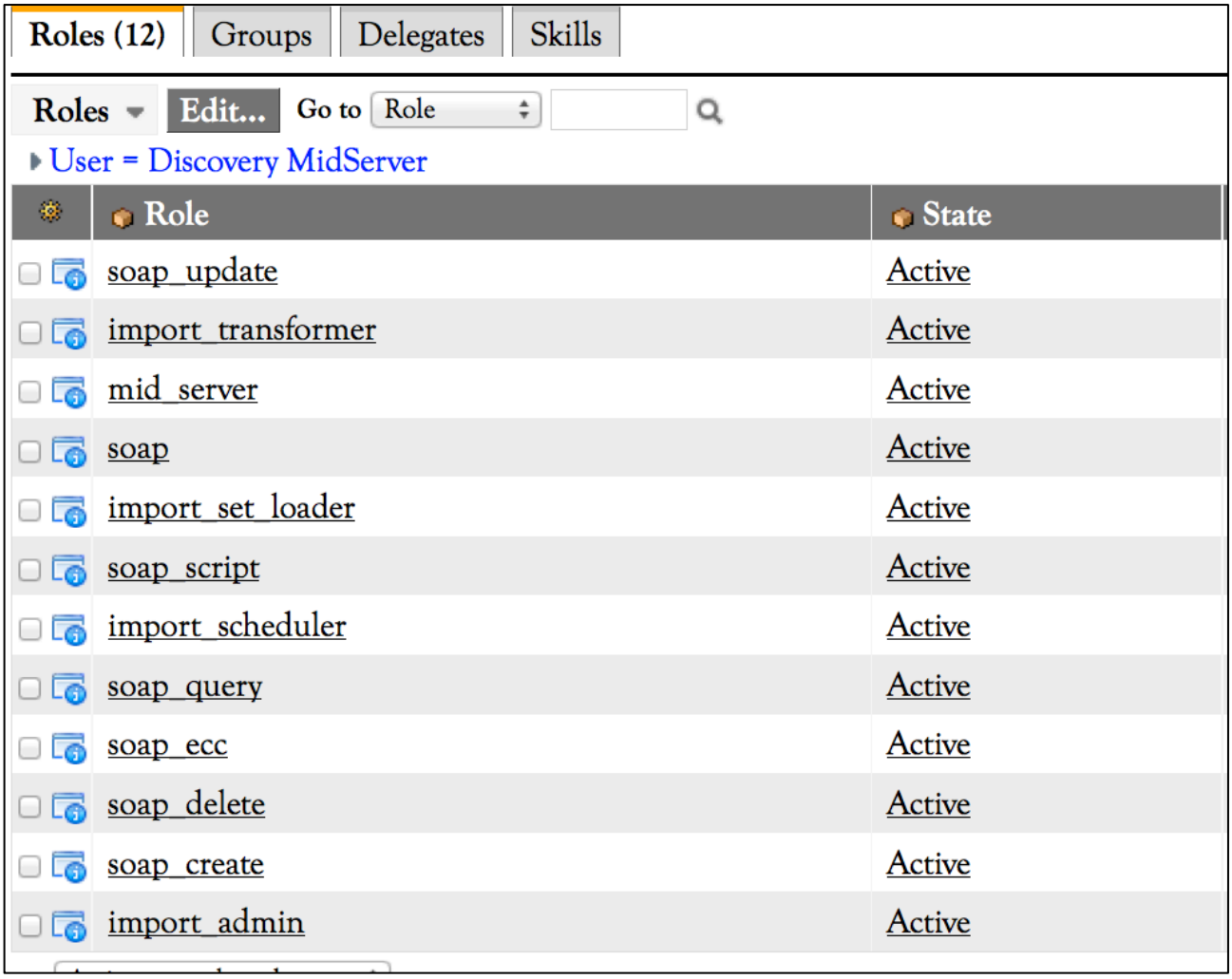
4. Right click and **Save** the user record.

©2014 ServiceNow, Inc. All rights reserved.

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

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

   You will see by adding one role, the user inherits other necessary roles to properly function.



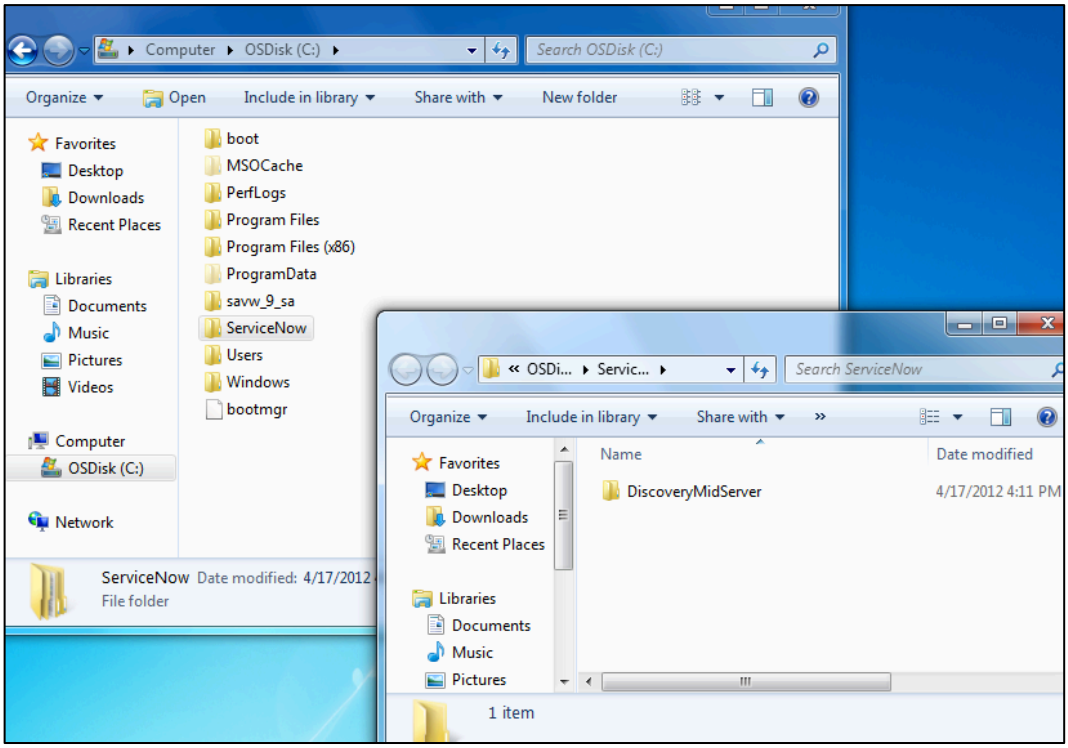
©2014 ServiceNow, Inc. All rights reserved.

Steps on the MID Server HOST

Create the folder structure

1. Create a folder under the preferred local drive root called **ServiceNow**.

2. Create a subfolder under **ServiceNow** called **DiscoveryMidServer.**



3. Extract the MID Server from the file downloaded earlier.

   You will now see an **agent** folder.

©2014 ServiceNow, Inc. All rights reserved.

4. Click into the **agent** folder and open the **config.xml** file with **wordpad**.

   To do so, right click the file chose **open with > wordpad**.

   Or you can choose your favorite advanced text editor such as **Text Wrangler** 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.  -->

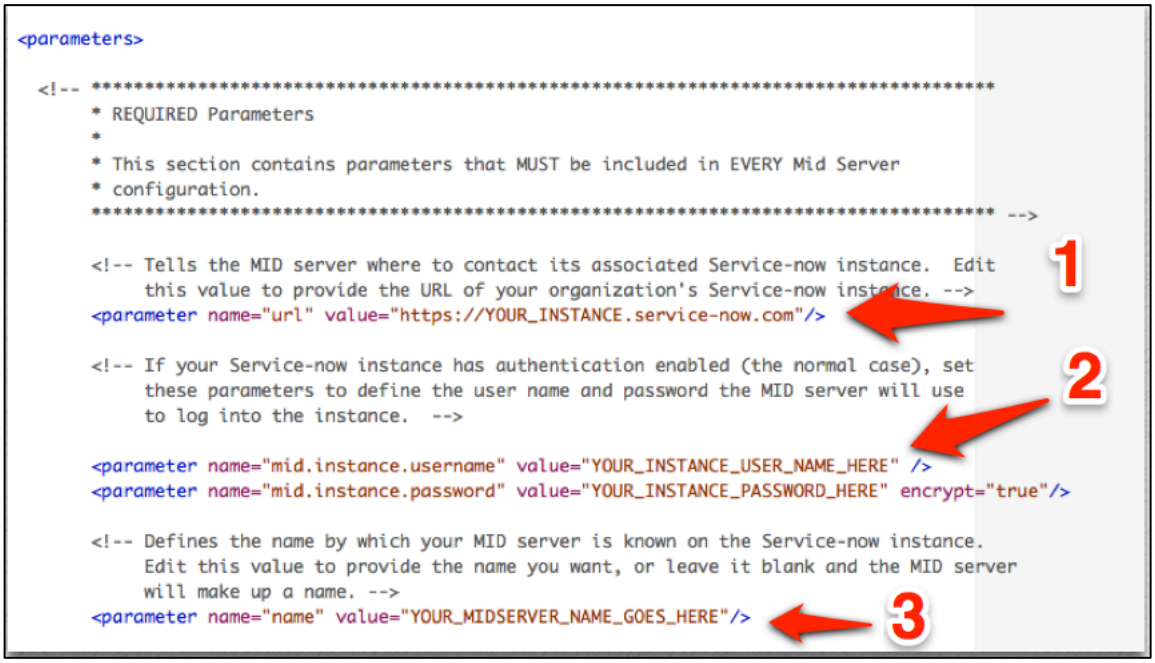
       <parameter name="mid.instance.username" value="YOUR_INSTANCE_USER_NAME_HERE" />
       <parameter name="mid.instance.password" value="YOUR_INSTANCE_PASSWORD_HERE" encrypt="true"/>

       <!-- 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"/>
```

®2014 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.
4. Save and close the record.




```
<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"/>

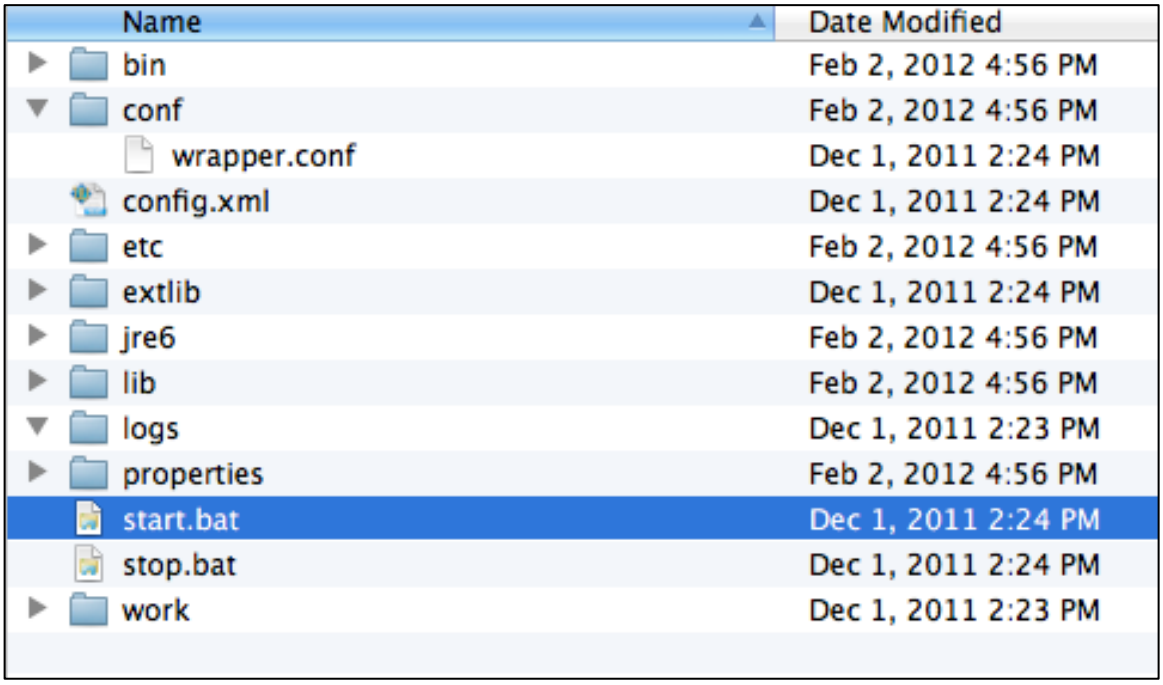
       <!-- Defines the name by which your MID server is known on the Service-now instance.
            Edit this value to provide the name you want, or leave it blank and the MID server
            will make up a name. -->
       <parameter name="name" value="YOUR_MIDSERVER_NAME_GOES_HERE"/>
```

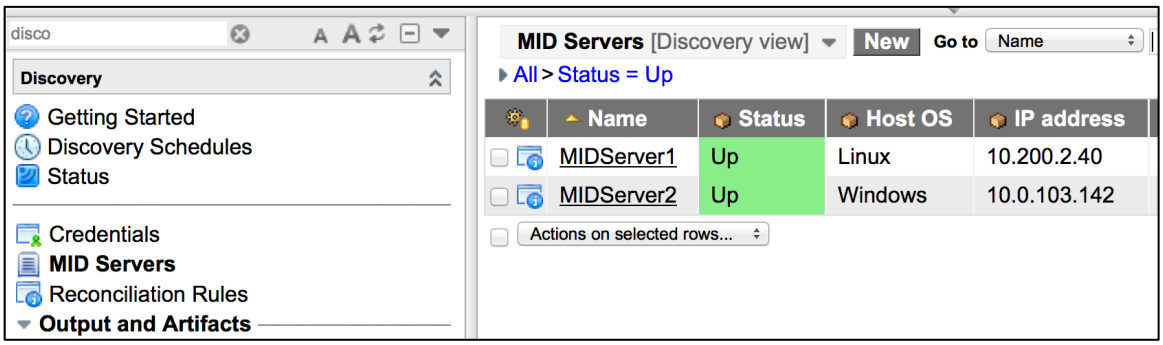
©2014 ServiceNow, Inc. All rights reserved.

Start it Up!

1. In the **/agent** folder, double-click **start.bat**!

   Check the wiki for unique start up instructions for OS types.





©2014 ServiceNow, Inc. All rights reserved.

Lab Goal

- Configure discovery
- Defining Credentials
- Defining Schedules

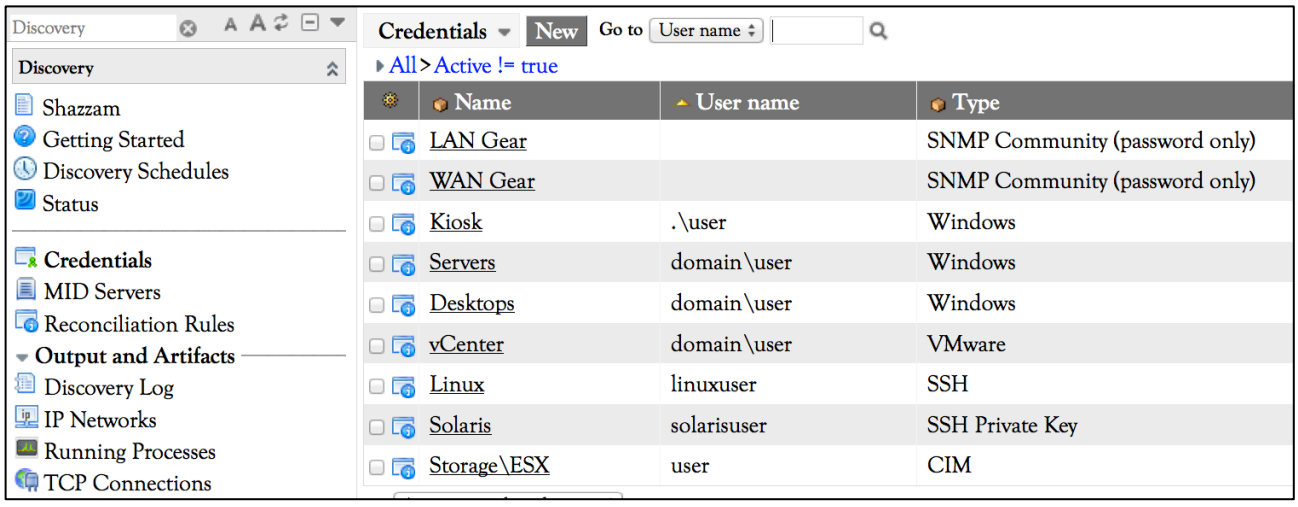
Lab 3
Discovery Configuration

ServiceNow Discovery

- You will be configuring the pre-installed MID Server on your instances
- We will be creating schedules and running a discovery

For reference

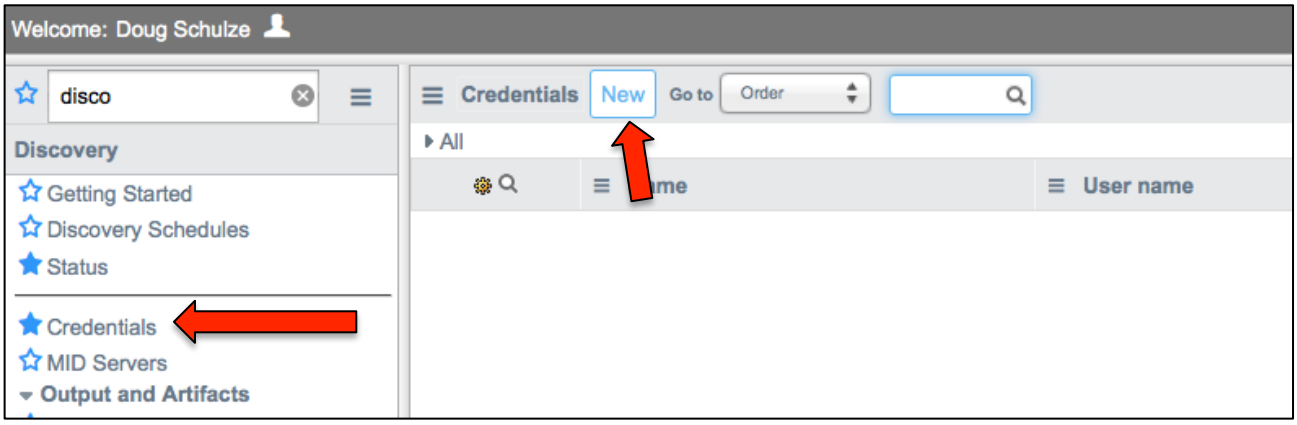
- The credentials module in the Discovery Application contains the user/passwords for your systems you wish to discovery
- Windows does need PowerShell discovery enabled. *See wiki
- Unix credentials need limited SUDO permissions. *See wiki



©2014 ServiceNow, Inc. All rights reserved.

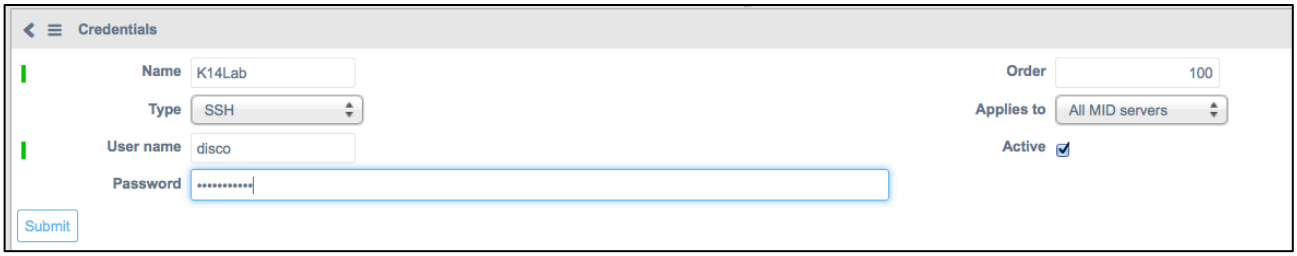
In your lab instance, lets set some credentials

1. Select the **Credentials** module in the **Discovery** application.



2. Click **New**.

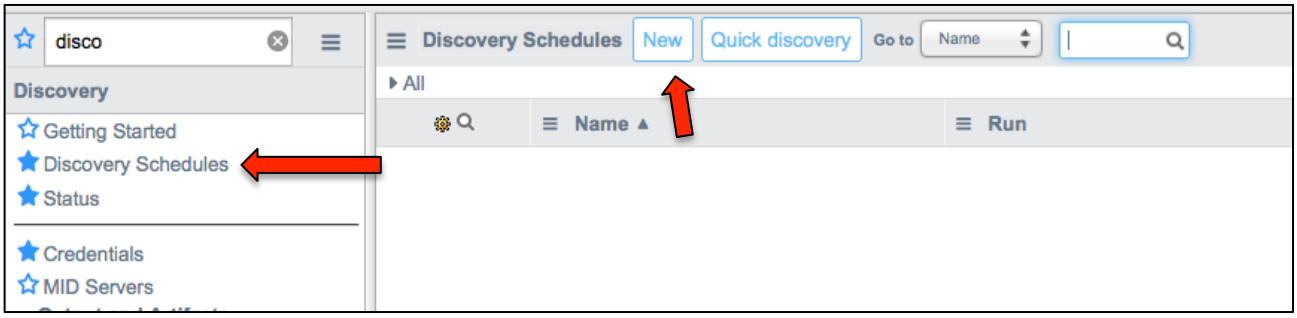
   Name: **K14 LAB**
   Select Type: **SSH**
   User name: **linuxuser**
   Password: **p@ssword**



©2014 ServiceNow, Inc. All rights reserved.

Create a Discovery Schedule

1. Select the **Discovery Schedules** module in the **Discovery** Application



2. Select **New**

   Name: **K14Lab**
   MID server: **lab_midserver**
   Active: **check**
   Include alive: **check**
   Log state change: **uncheck**



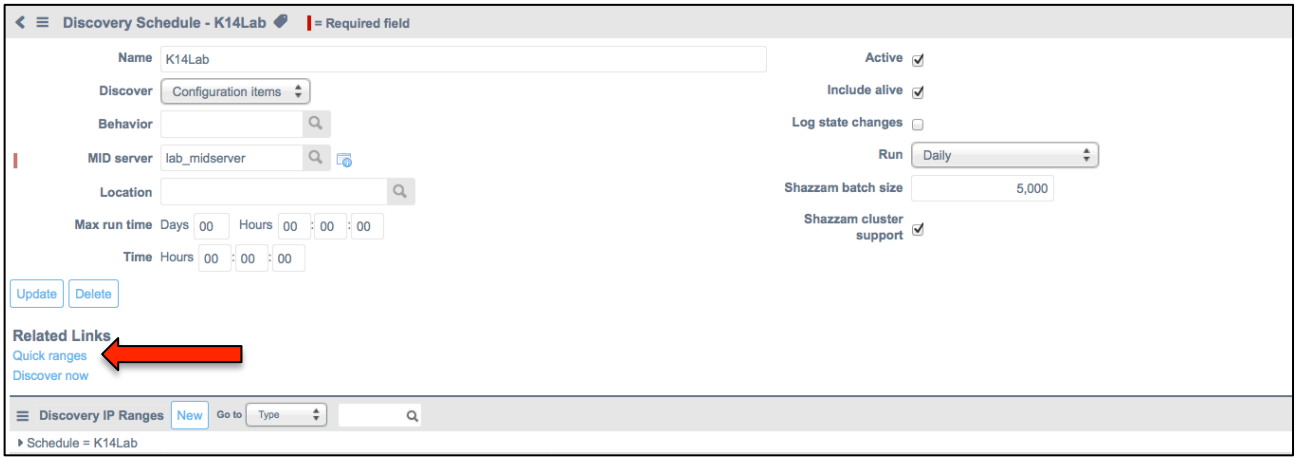
- **Active**: Run the schedule at the designated time
- **Alive**: Log the IP addresses that were responsive but not available to be discovered
- **Log state changes**: tell me about the complete transition of a record through its discovery process

©2014 ServiceNow, Inc. All rights reserved.

3. Right click the form header and **Save** the schedule.

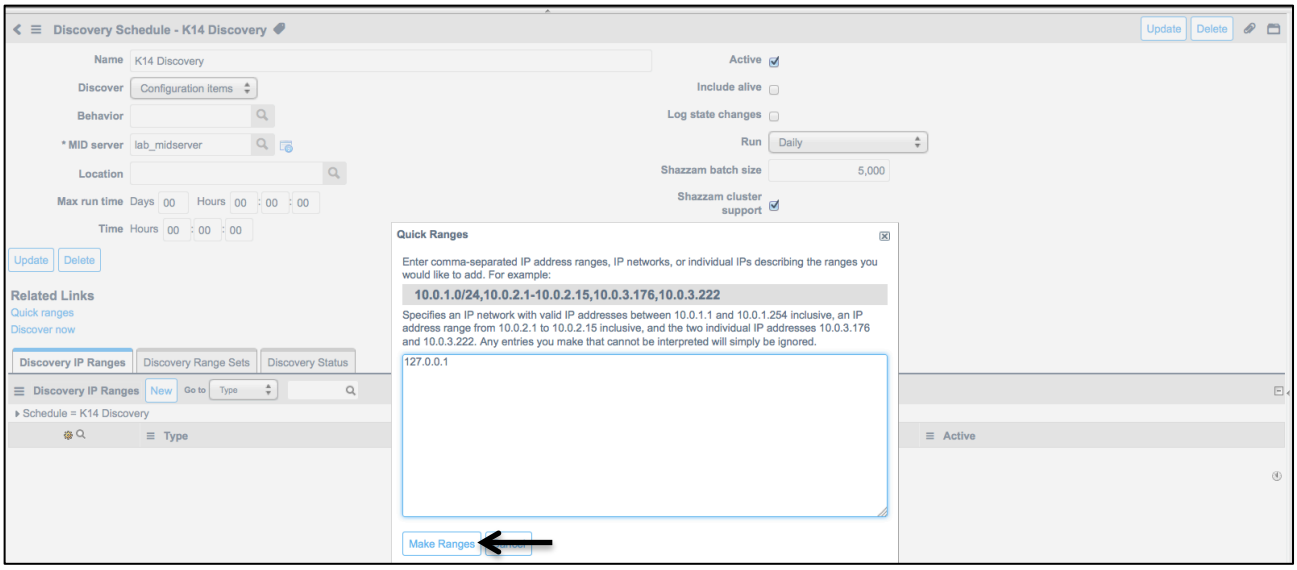
   Related Links and the Discovery IP Ranges related list become visible on the form.

   - This is where you will enter you IP Ranges
   - In real life you could have full networks, individual IP's or range groups to a limit of 100k per schedule



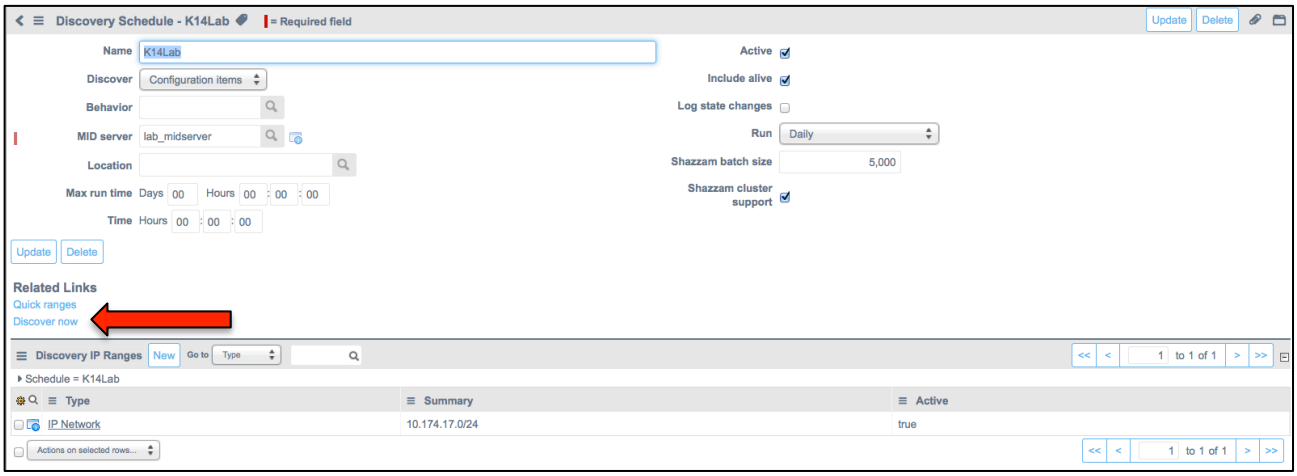
4. For this lab, click **Quick Ranges** on the form and enter the Lab loopback IP address: **127.0.0.1**

5. Click **Make Ranges**.



©2014 ServiceNow, Inc. All rights reserved.

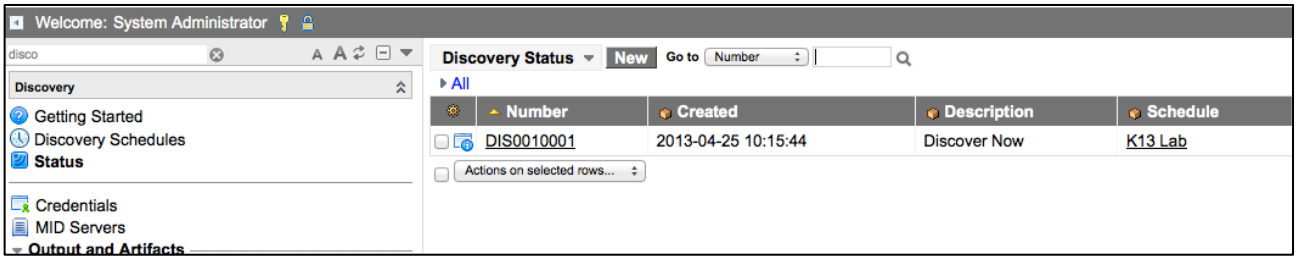
6. Click **Discover Now**!



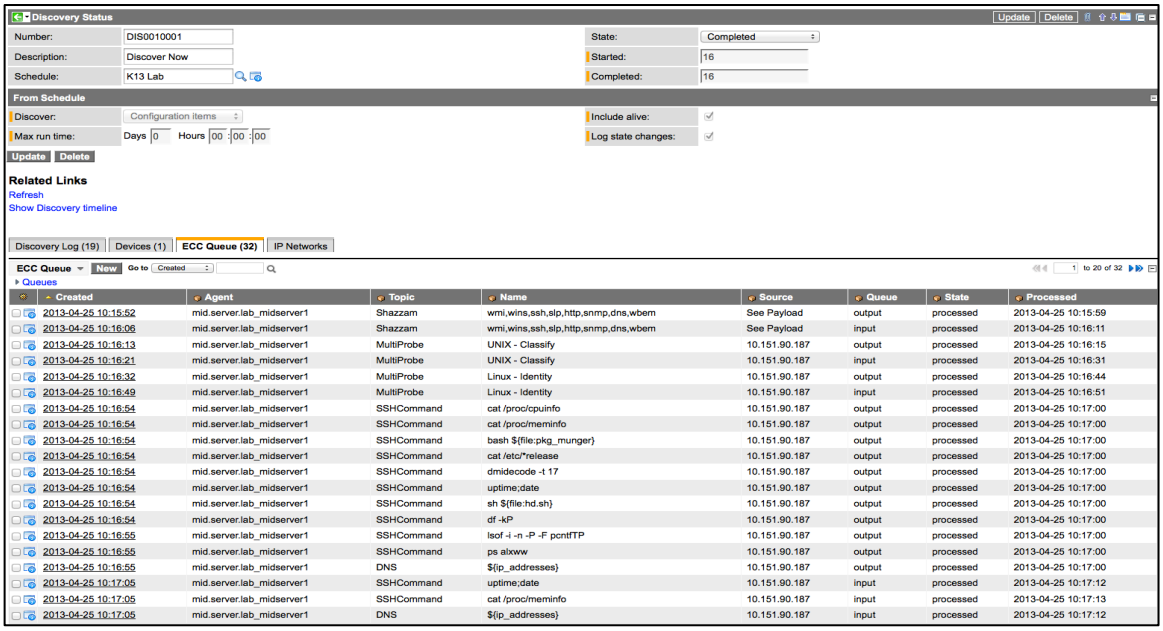
®2014 ServiceNow, Inc. All rights reserved.

Lab Success Verification

1. Click on **Status** under the **Discovery** application.



2. This list contains all discoveries run either on a scheduled basis or on demand



- Within in the status record, we can see all the work taking place.
- The Different sections include the log, ECC Queue Table and the devices we discovered

®2014 ServiceNow, Inc. All rights reserved.

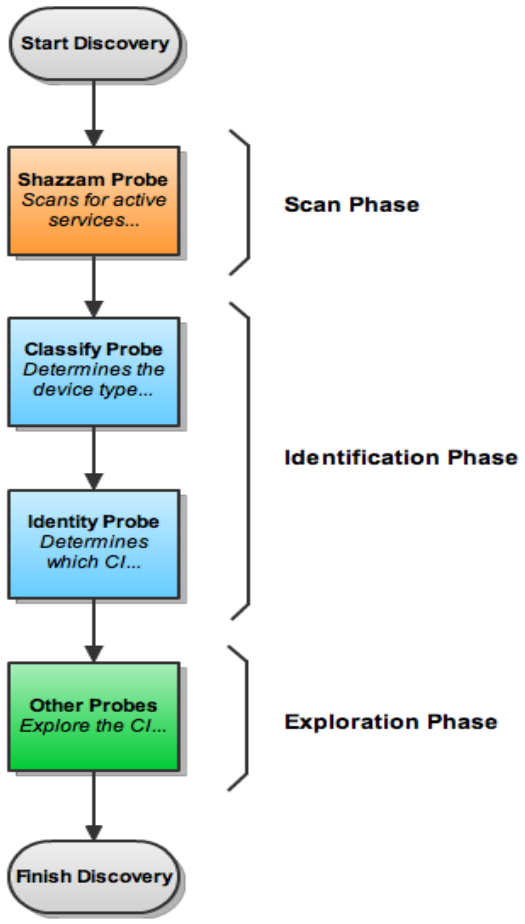
Lab Goal

- Follow along as we discuss the four phases of the discovery process

Lab 4 Discovery Process Flow

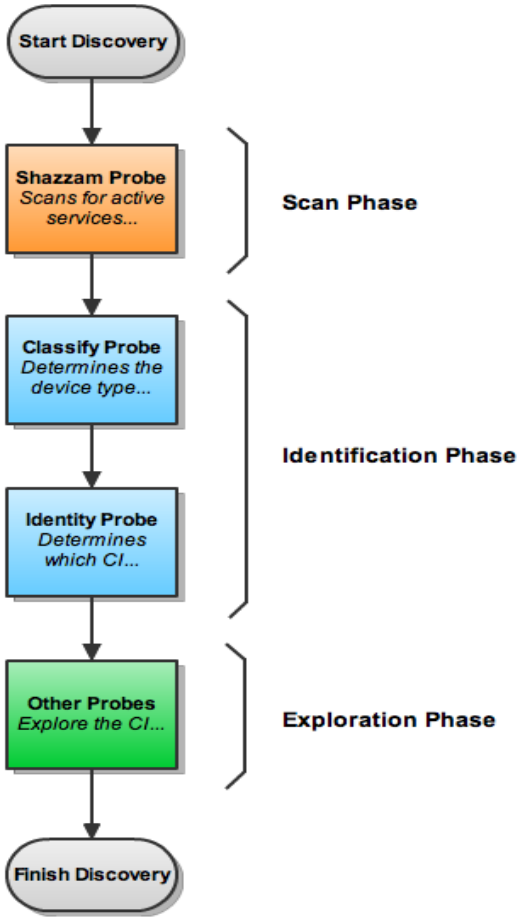
Discovery uses a repetitive step-by-step process to populate the CMDB to ensure we are bringing back only the most valued of information.

- **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)



©2014 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 | 1 to 6 of 6

All > Active != false

Name	Description	Active	Order ▲	Applies to
ESX UUID	Identify ESX servers based on VMWare UUID.	true	900	ESX Server [cmdb_ci_esx_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]

- **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"

©2014 ServiceNow, Inc. All rights reserved.

Lab Goal

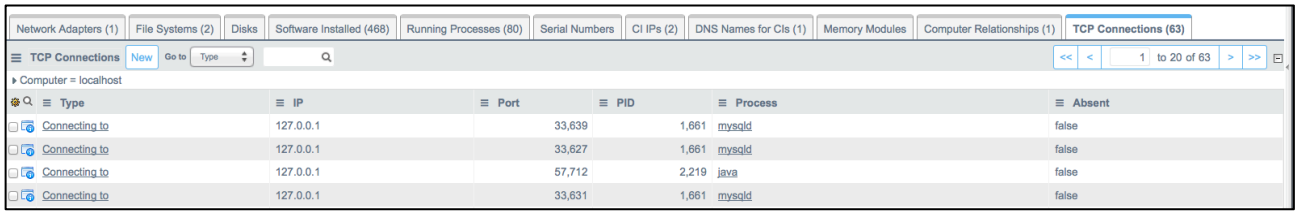
- Create Custom Process Classifier
- Identify Automatic relationship Building

Lab 5
Creating Process Classifiers

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

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

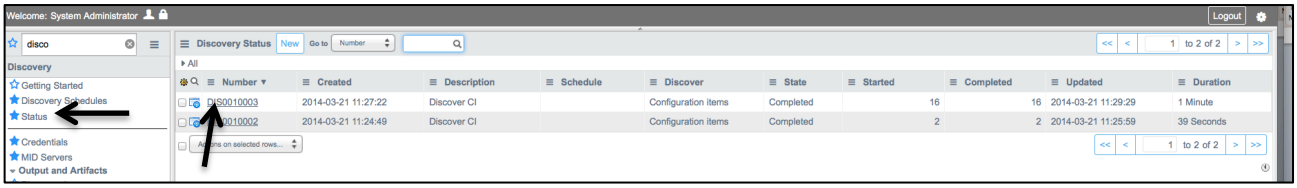
- Application to host – **Runs on::Runs**
  - Based on the running process
- Application to application – **Depends on::Used by**
  - Based on the running processes TCP connections



Review a returned device record

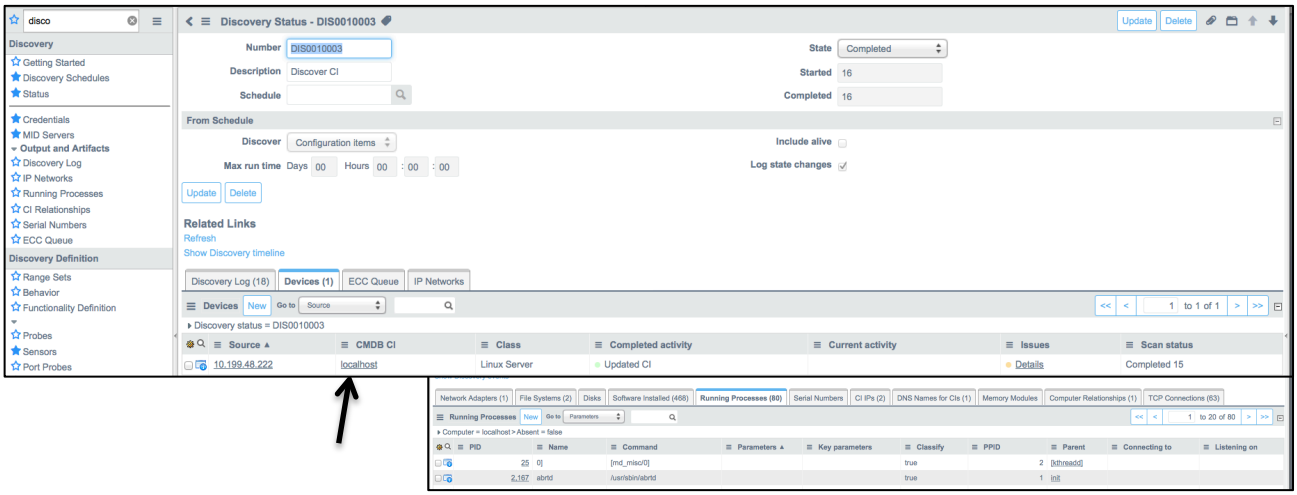
1. Navigate to **Discovery > Status**

2. Click the most recent **Discovery Status** record.

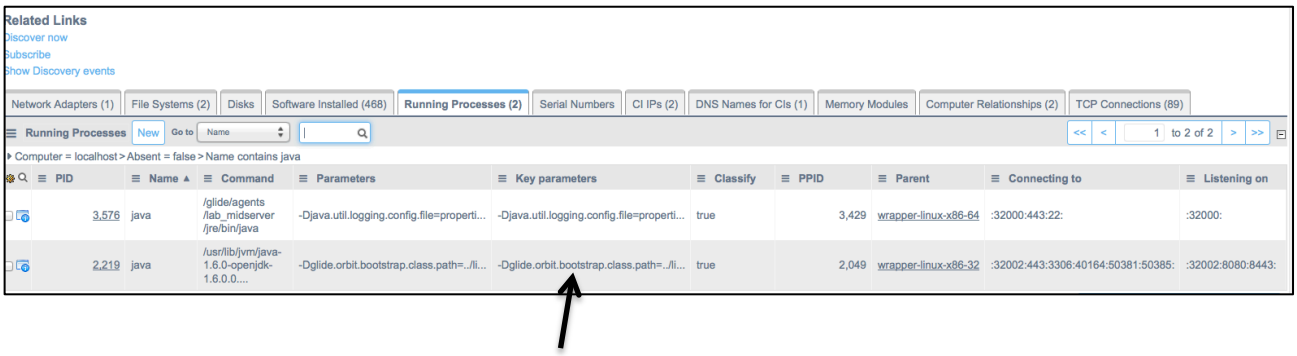


©2014 ServiceNow, Inc. All rights reserved.

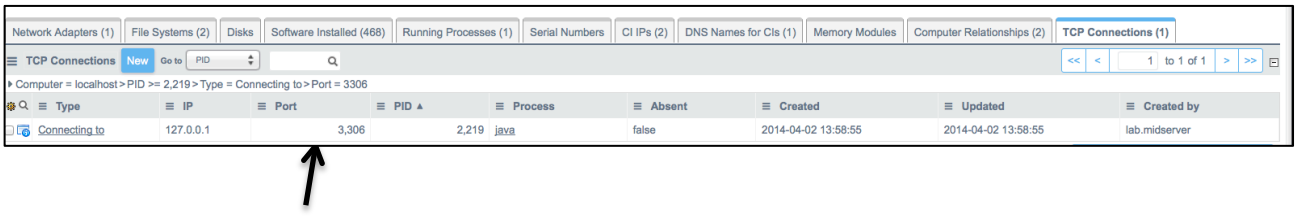
3. Click the **localhost** link under the **Device** tab in the **CMDB CI** column.



We want to focus on the running process. In today's lab we will be creating a relationship of a Tomcat instance running on this host. Look for a 'Java' process that has parameters that contain **bootstrap**.



And let's be sure that same process makes the expected connections to other applications. We do this by checking the TCP connections and see if that same PID is communicating with anything else.



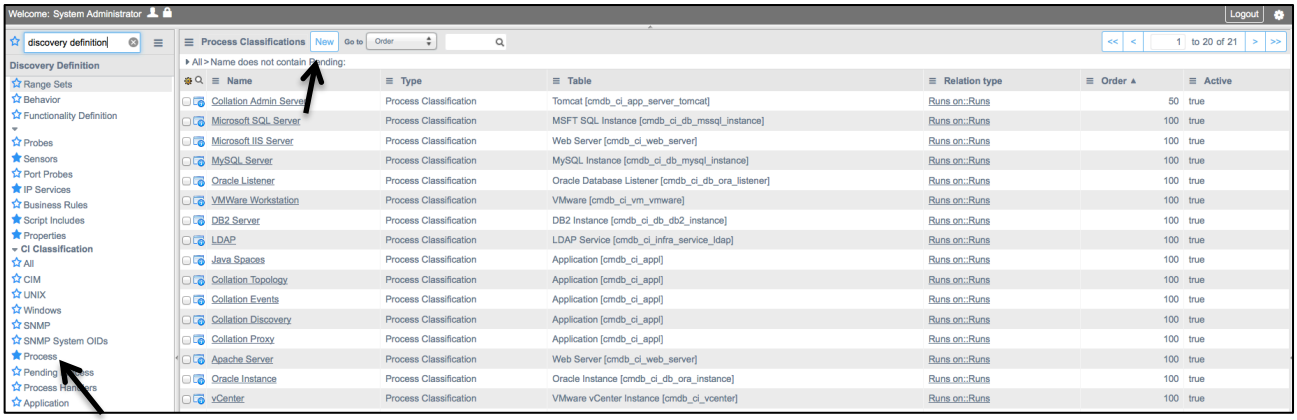
Indeed it is talking to the MSSQL (3306) instance running on the same host.

®2014 ServiceNow, Inc. All rights reserved.

Create the process classifier

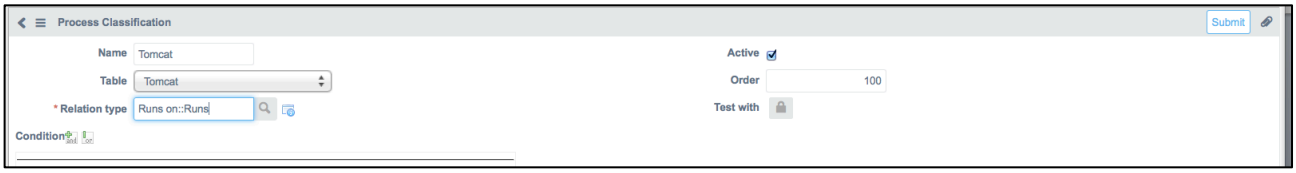
1. Navigate to **Discovery Definition > CI Classification Group > Process**

2. Click **New**.



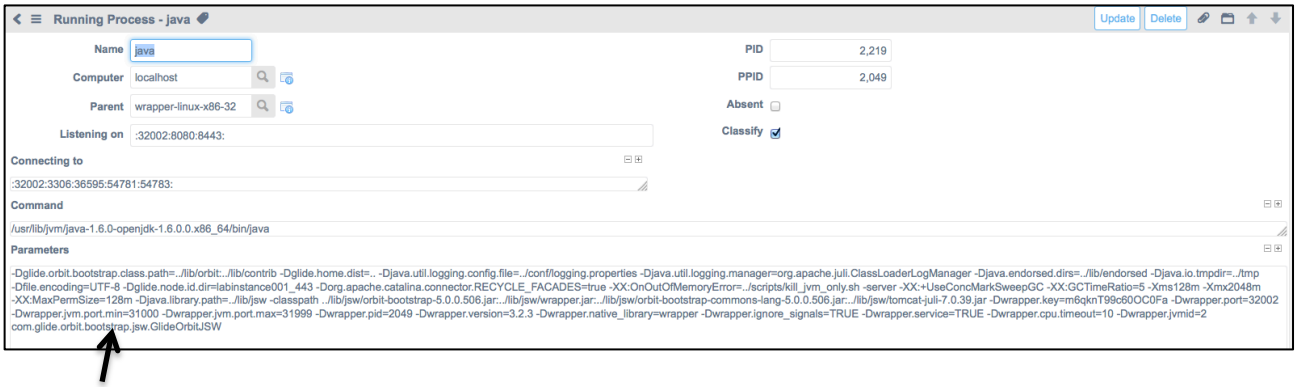
3. Enter the following information:

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

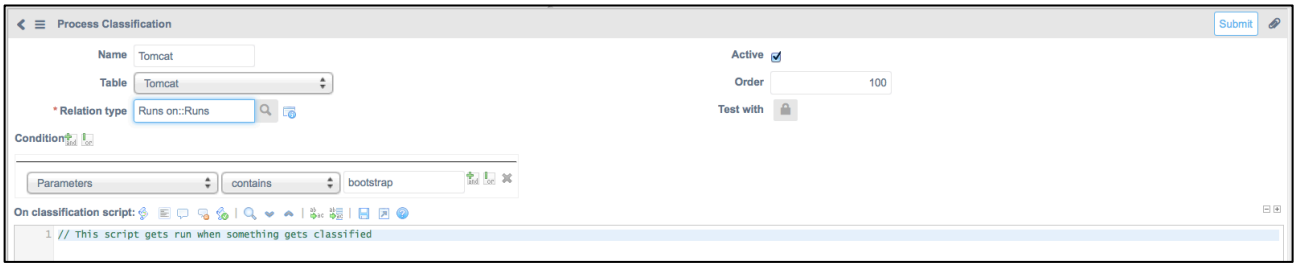


©2014 ServiceNow, Inc. All rights reserved.

4. Now you want to set the condition or better yet the signature of the running process that we want to build our relationship for. Recall from the parameters value we are looking for **bootstrap**.

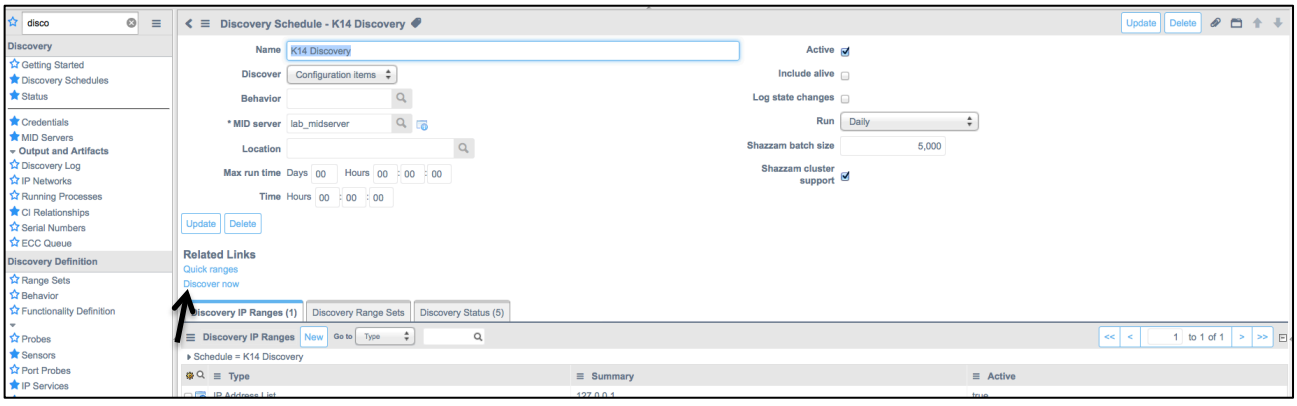


Add **Parameters contains bootstrap** as a condition to your process classifier and click **Submit**.



Excellent! Now we will go run another discovery against our devices.

5. Navigate to **Discovery > Discovery Schedules**, select **K14 Discovery** and click **Discover now**.

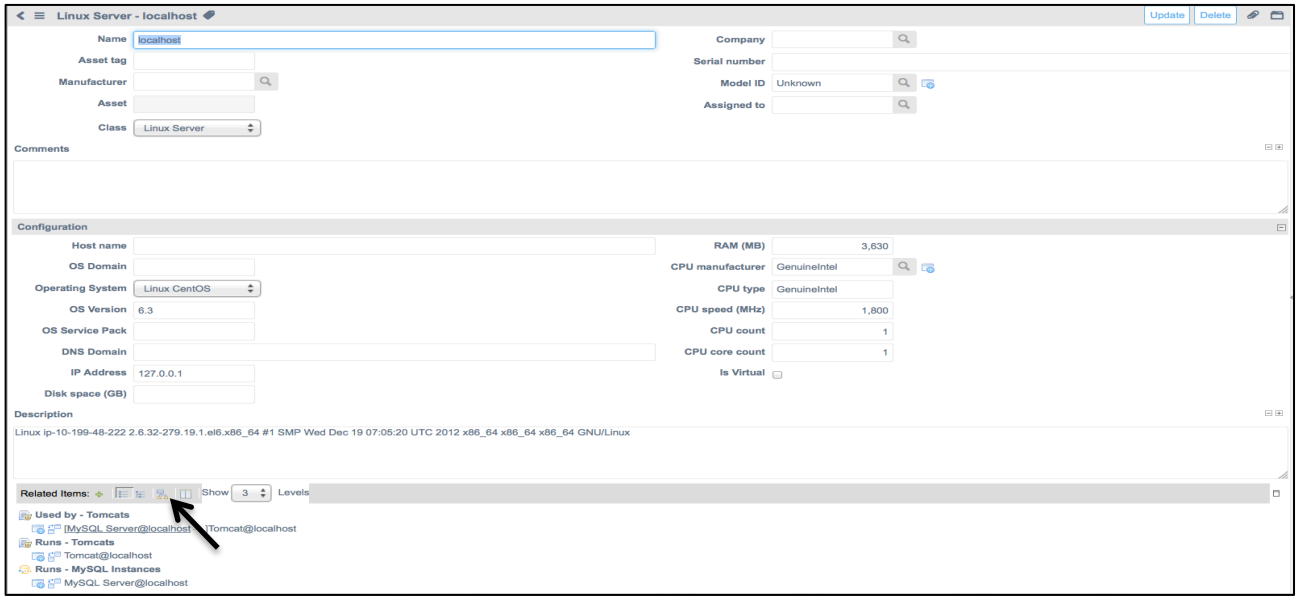


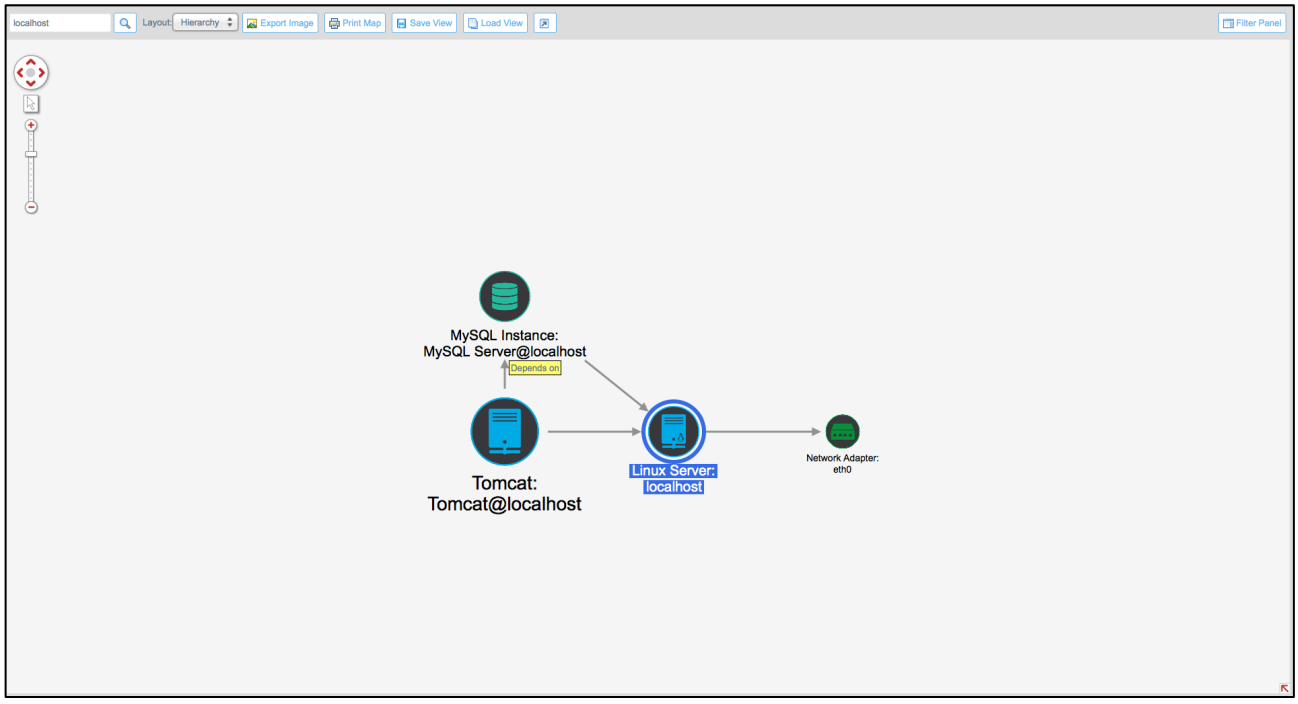
Note: Remember you can always add additional probes to your classifier to gather additional information from the application when found.

®2014 ServiceNow, Inc. All rights reserved.

Lab Success Verification

Review your results from the scan and enjoy your newly created relationships. For an added bonus, click on the BSM Icon.





®2014 ServiceNow, Inc. All rights reserved.