knowledge14®

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

Discovery 101

Doug Schulze
Expert Services Team Lead for Automaton
ServiceNow

Aleck Lin
Lead Automation Developer
ServiceNow

servicenow®

© 2014 ServiceNow All Rights Reserved

Discovery 101

Populating Your CMDB with Agentless Discovery

© 2014 ServiceNow All Rights Reserved

Agenda

Setting up a Base Discovery on your lab instance

Understanding basic Discovery configuration

Executing Discovery

Understanding the Discovery process

Application Mapping

© 2014 ServiceNow All Rights Reserved

What is Discovery?

- ServiceNow discovery is an ***agentless*** method of populating your CMDB with relevant hardware and software assets within your enterprise enterprise environment

- Utilizing a specific step or *phased* process ServiceNow 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”…

- ServiceNow maps specific Application to Host *and* Application to Application dependencies

**We do not build physical, Layer 2, Hardware relationships*

© 2014 ServiceNow All Rights Reserved

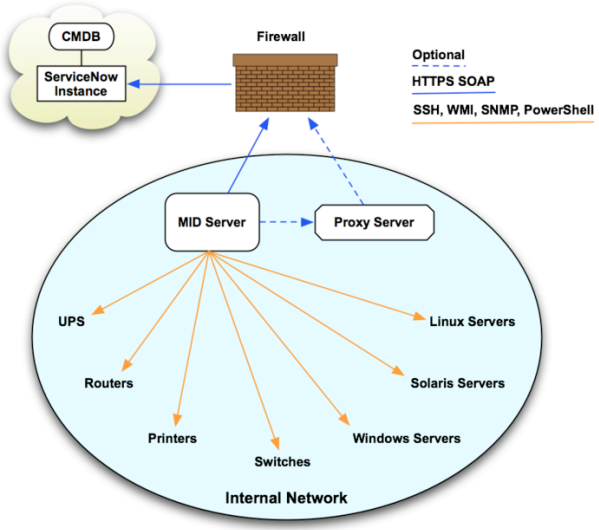
What is Discovery?

- 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 Discovery takes it to the next level by identifying the running applications, installed software, versions and patch levels
- Outage Impacts
  - ServiceNow provides 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 All Rights Reserved

Local Footprint from the Cloud

- The “MIDServer”
  - To gather your important data and providing for industry standard security requirements a MIDServer application will be deployed within your infrastructure for the agent less, behind the firewall “look” into your secure environment
  - Secure ***outbound only*** 128bit SSL communication to your specific ServiceNow applications, complying with strict Corporate and Regulatory standards



© 2014 ServiceNow All Rights Reserved

Time to Lab it up!

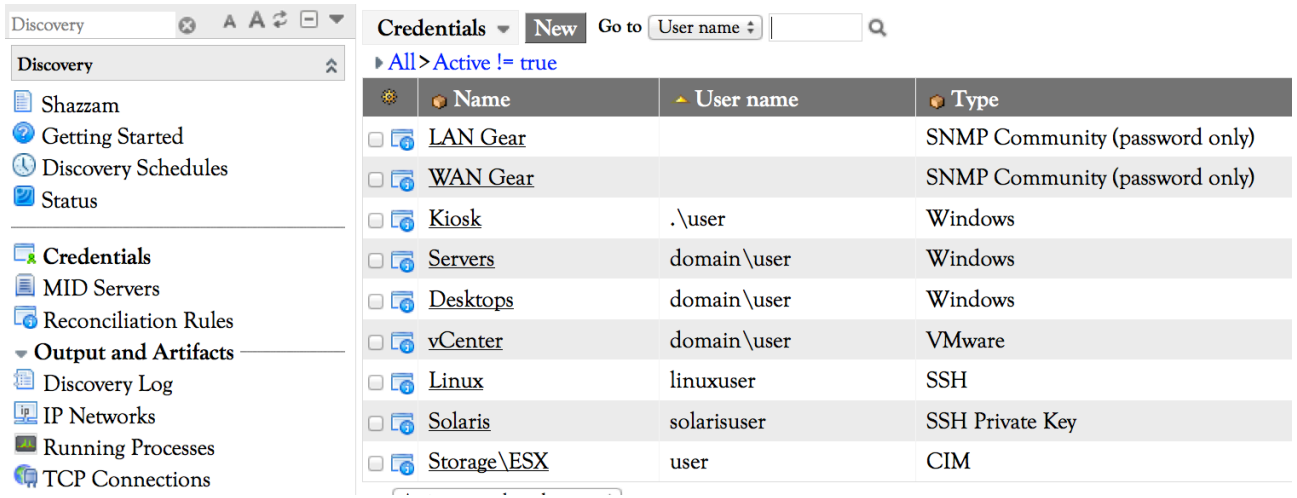


- From here you will be configuring your lab instance
- We will be creating schedules and running a discovery
- You will be using a pre-installed MIDServer on your instance

© 2014 ServiceNow All Rights Reserved

Defining your Credentials

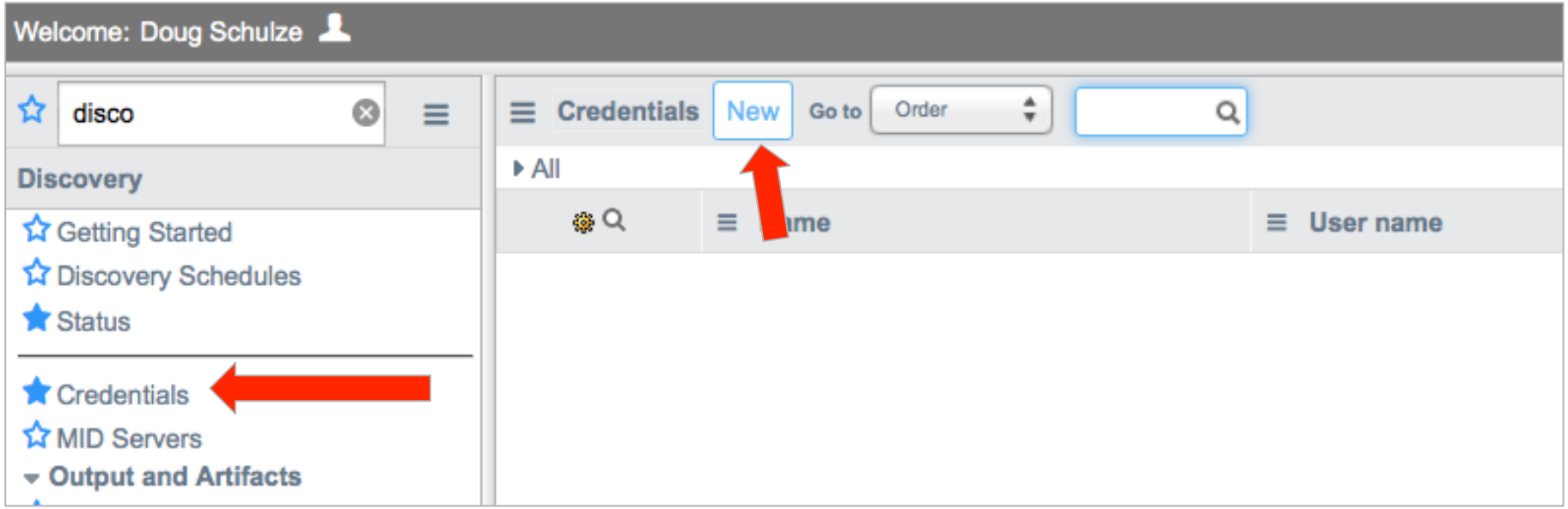
- Select the credentials module in the Discovery Application
- Enter Credentials for the entire environment (Windows does need PowerShell discovery enabled)*See wiki
- Unix credentials need limited SUDO permissions*See wiki
- Let's Enter yours!



© 2014 ServiceNow All Rights Reserved

Create a New Unix Credential

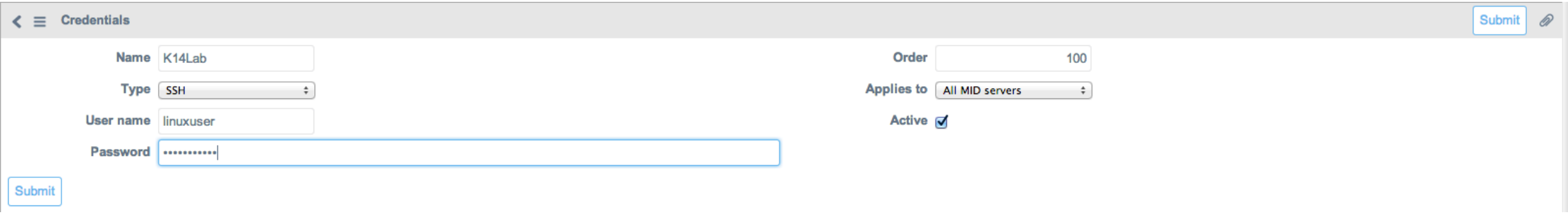
- Select the credentials module in the Discovery Application
- Select ‘new’



© 2014 ServiceNow All Rights Reserved

Configure Credentials

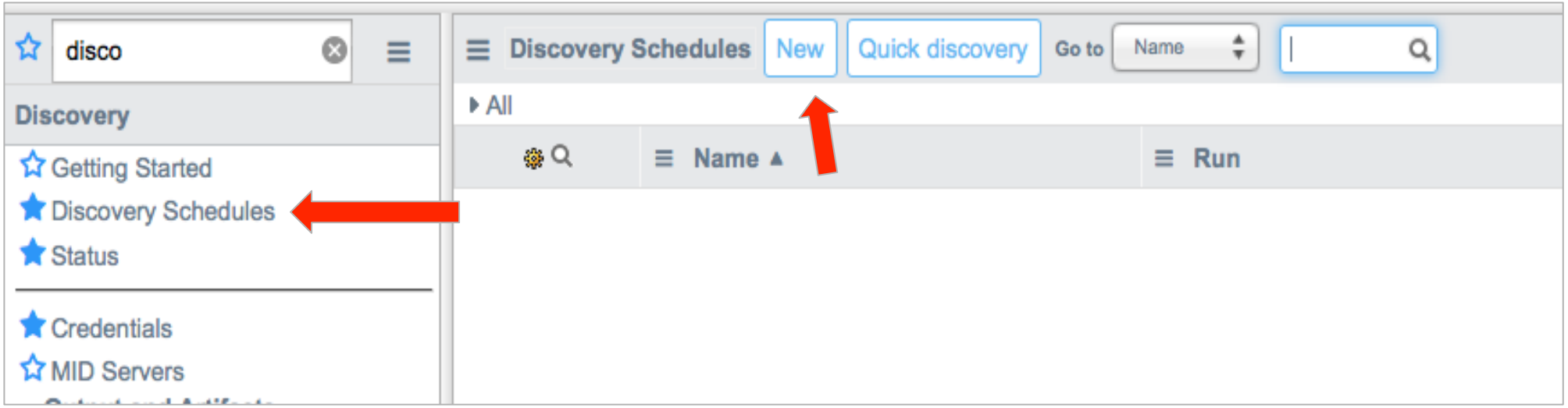
- Name it : K14 Lab
- Select Type : SSH
- Username : linuxuser
- Password : p@ssword



© 2014 ServiceNow All Rights Reserved

Create a Discovery Schedule

- Select Discovery Schedule module in the Discovery application
- Select ‘New’



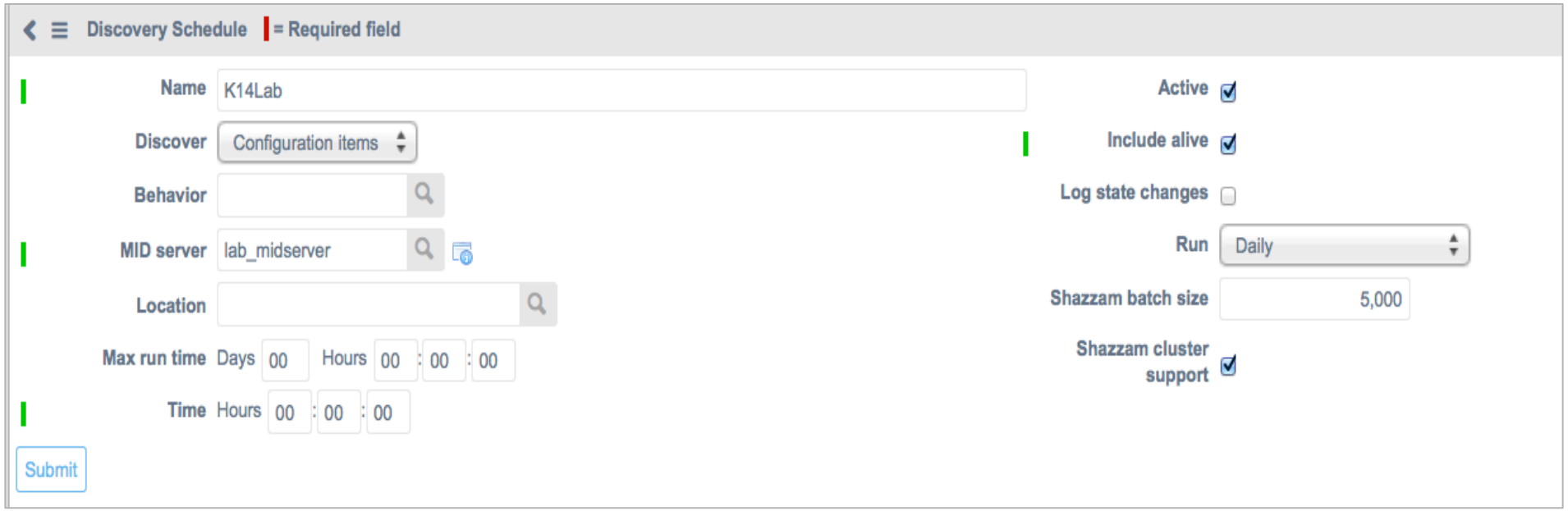
© 2014 ServiceNow All Rights Reserved

Create a Discovery Schedule

- Enter the name of your schedule, in this case K14Lab
- Set the MIDServer to ‘lab MIDServer’
- Check Active and Alive
  - 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 – Provides additional information of the transition of a record through the discovery process

© 2014 ServiceNow All Rights Reserved

Configure your Discovery Schedule

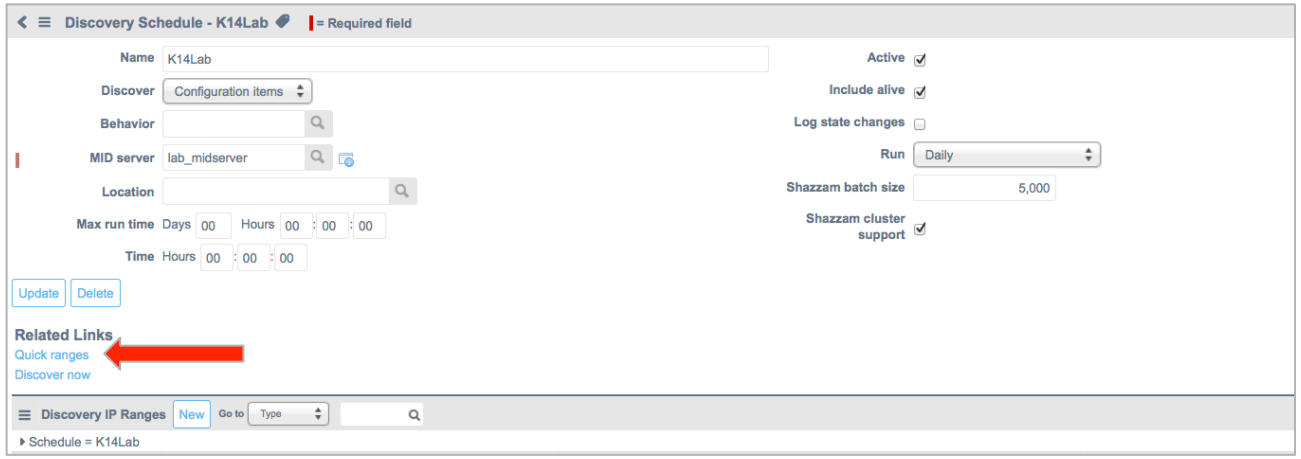


© 2014 ServiceNow All Rights Reserved

Configure your Discovery Schedule

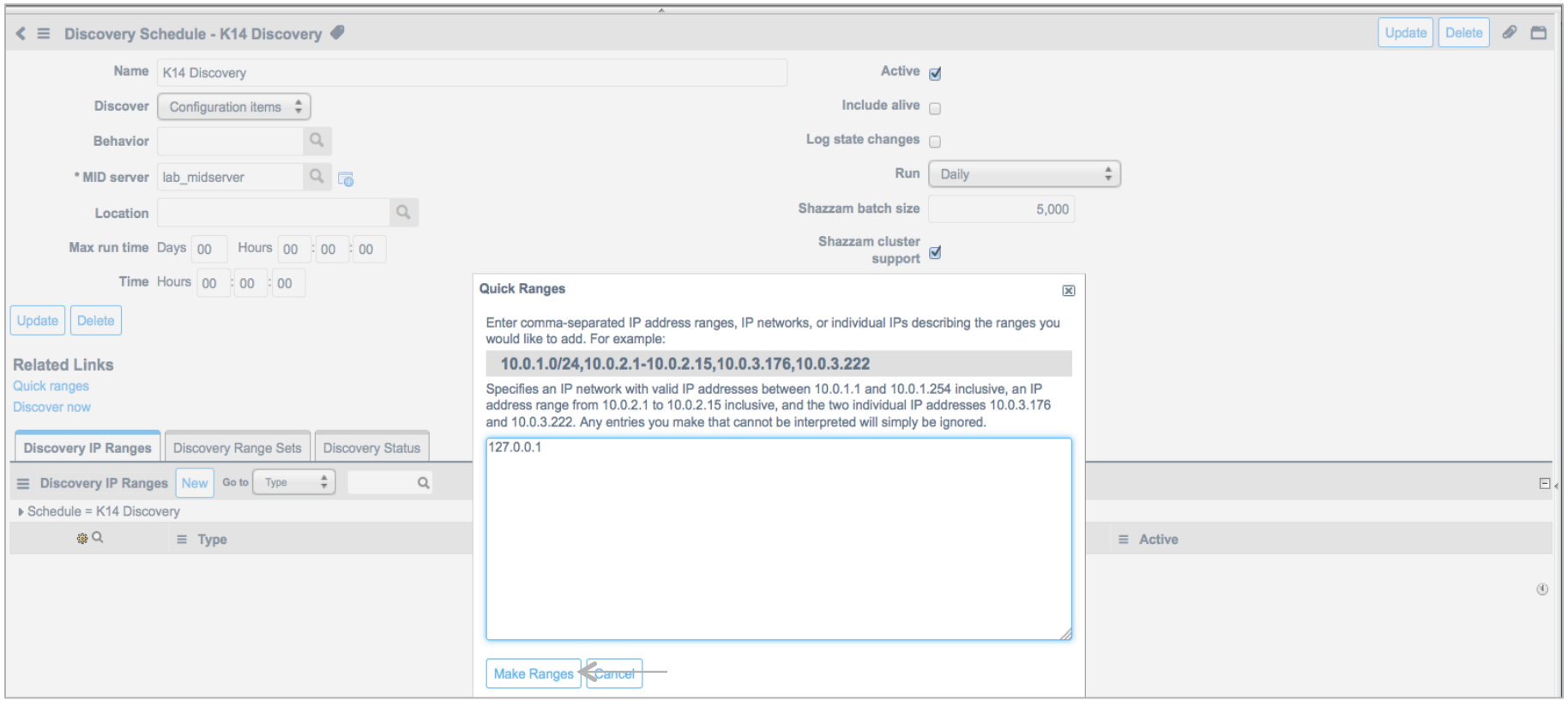
Adding IP Ranges

- 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
- Today click 'Quick Ranges' on the form and enter the Lab loopback IP address : 127.0.0.1
- Click 'Make Ranges'



© 2014 ServiceNow All Rights Reserved

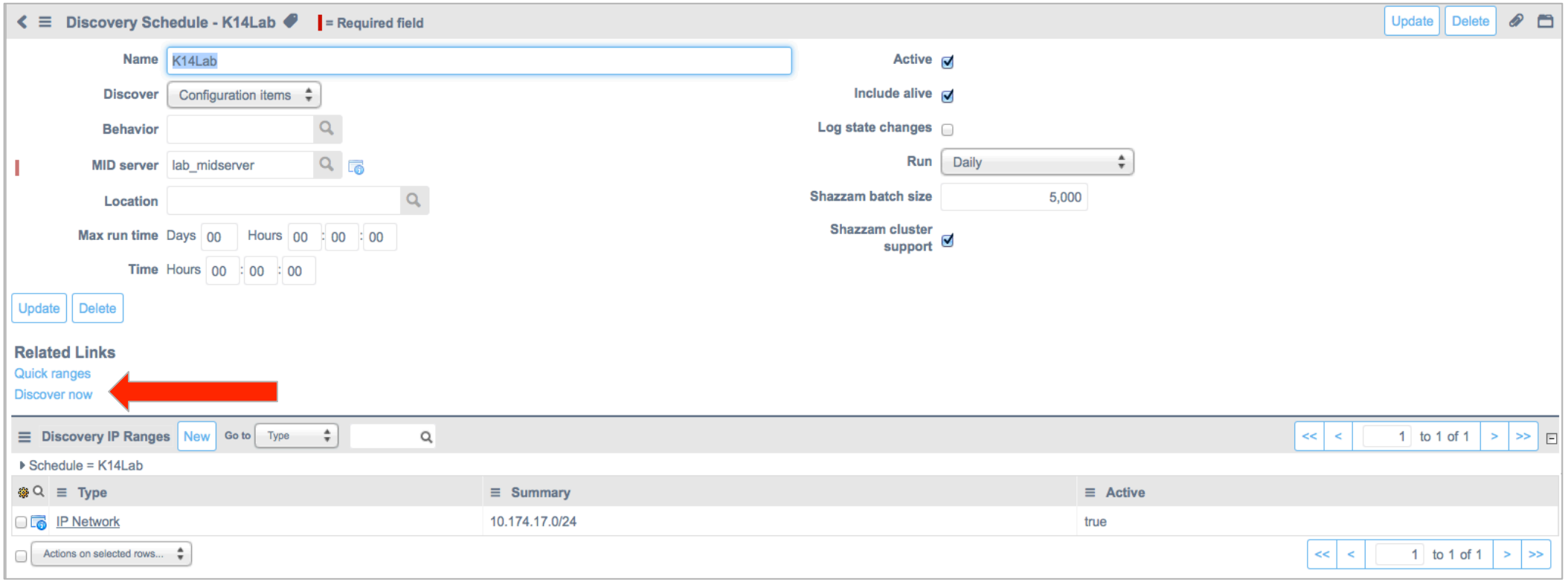
Configure your Discovery Schedule



© 2014 ServiceNow All Rights Reserved

Configure your Discovery Schedule

- Time to make it run.. Click ‘Discovery Now’ !



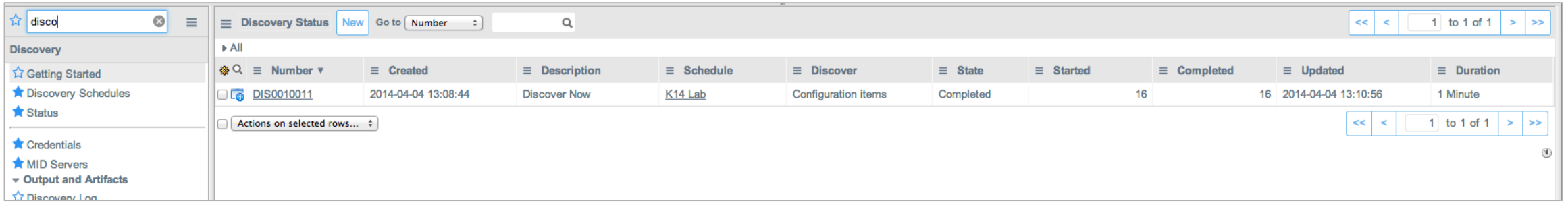
© 2014 ServiceNow All Rights Reserved

Discovery 101
Reviewing Results

© 2014 ServiceNow All Rights Reserved

Reviewing Results

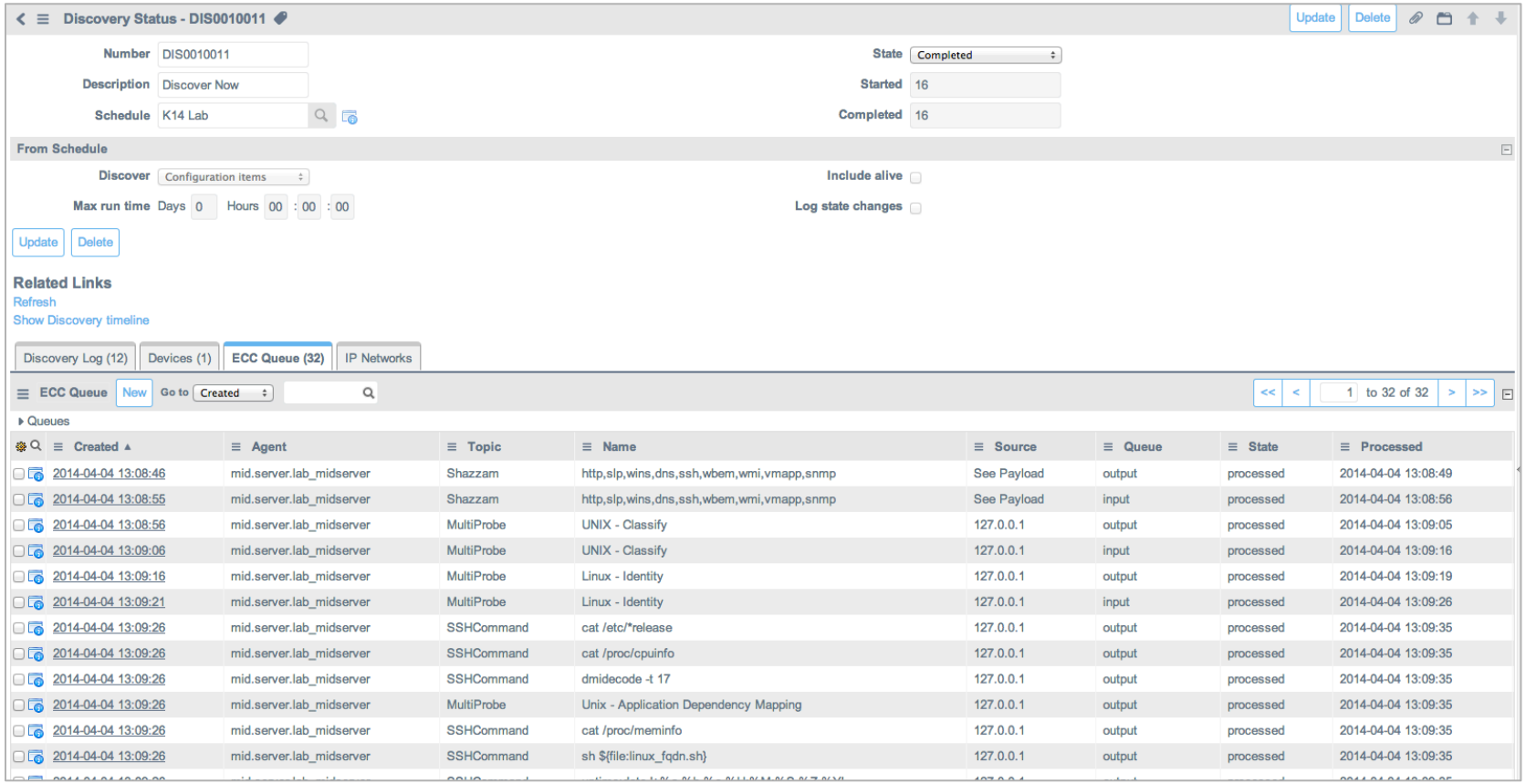
- Click on Status under the discovery application
- This list contains all discoveries run either on a scheduled basis on on demand



© 2014 ServiceNow All Rights Reserved

Reviewing Results

- Here in the status record we can see all the work taking place
- The different sections include the Discovery log, ECC Queue and the devices discovered



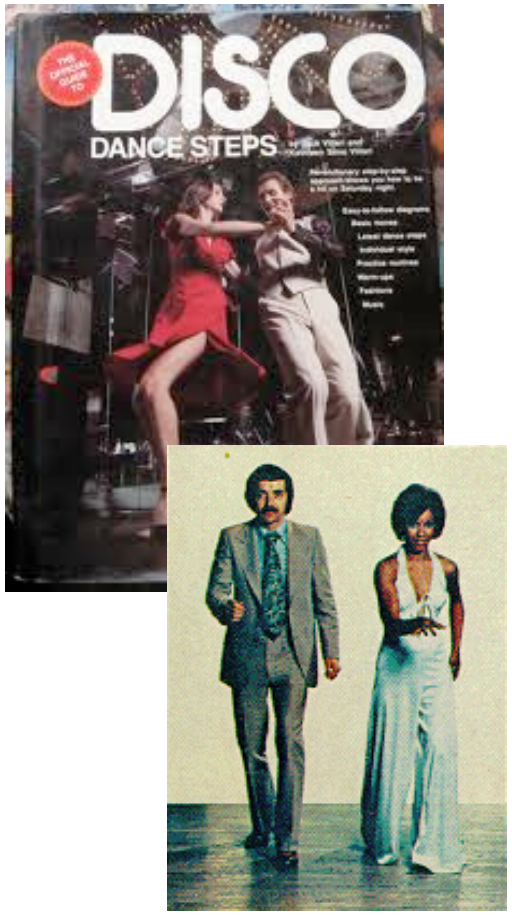
© 2014 ServiceNow All Rights Reserved

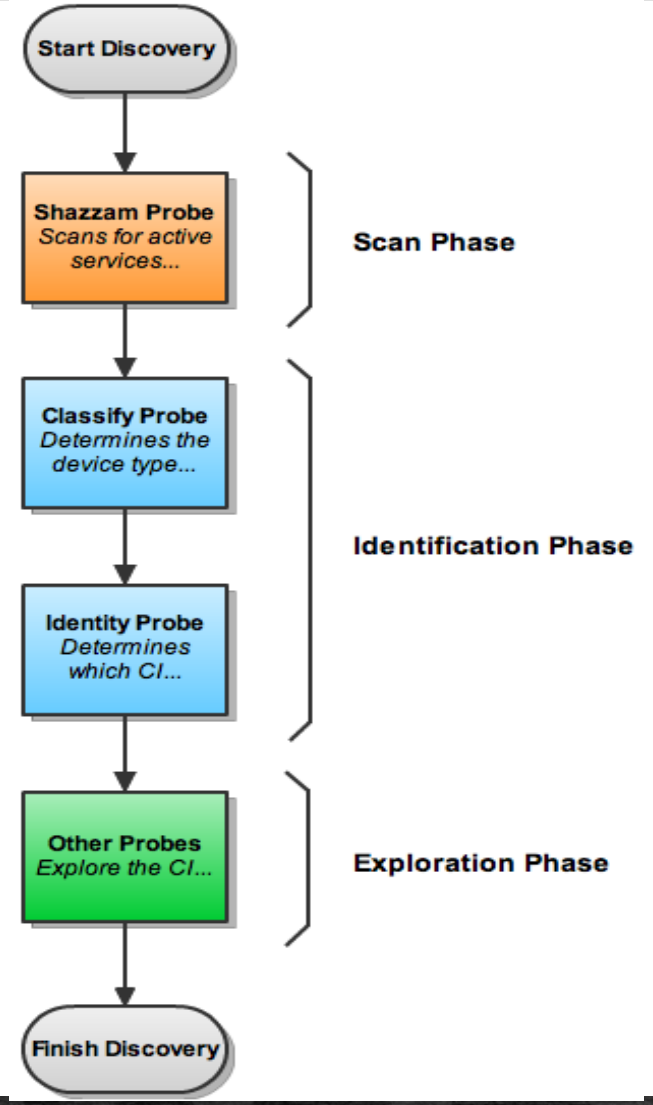
Discovery 101
Discovery Flow

© 2014 ServiceNow All Rights Reserved

Understanding the Discovery Process

- Discovery uses a repetitive step by step process to populate the CMDB to ensure we are bringing back only the most valued of information
- Port Scan (Shazzam)
- Classification
- Identification
- Exploration
  - Process Classification



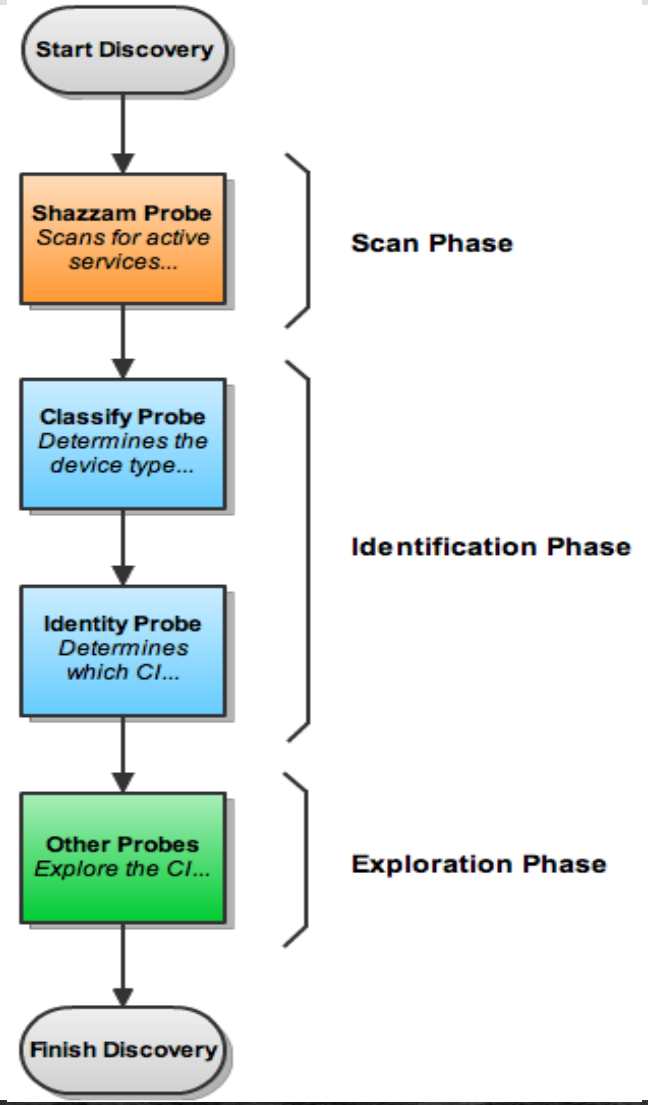


© 2014 ServiceNow All Rights Reserved

Port Scan – Shazzam!

(1) **SHAZZAM**

- Scan for “active” devices – Shazzam probe
- Ports determined by Port Probes and/or specific behavior
- Each Port Probe is determined by IP Services
- You can have multiple ports per Port Probe
  - ex: multiple ssh ports

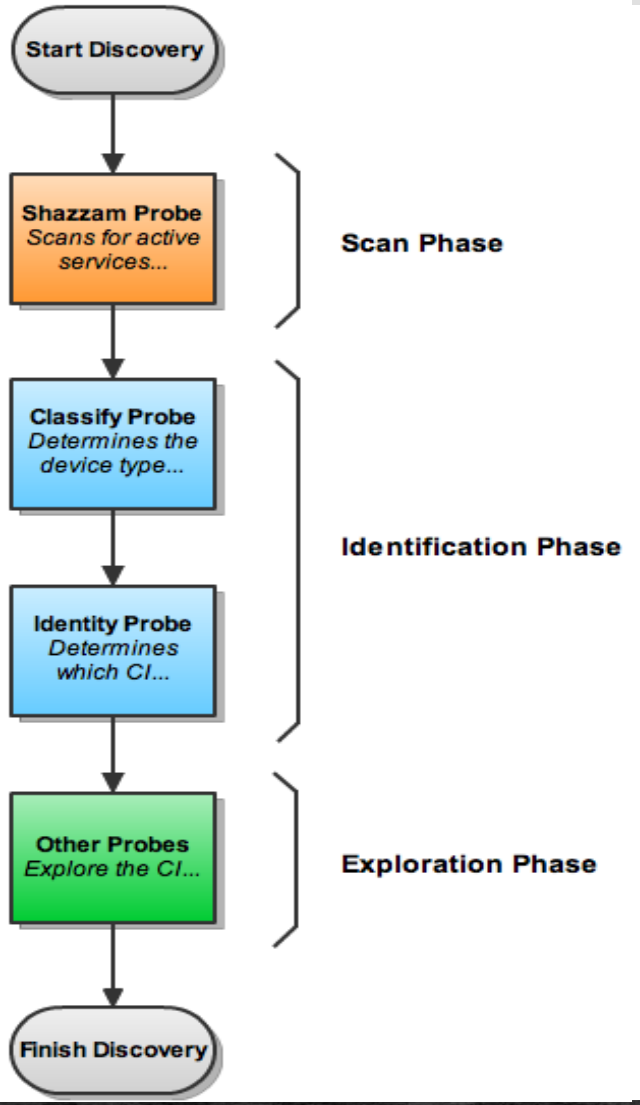


© 2014 ServiceNow All Rights Reserved

Classification

(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)

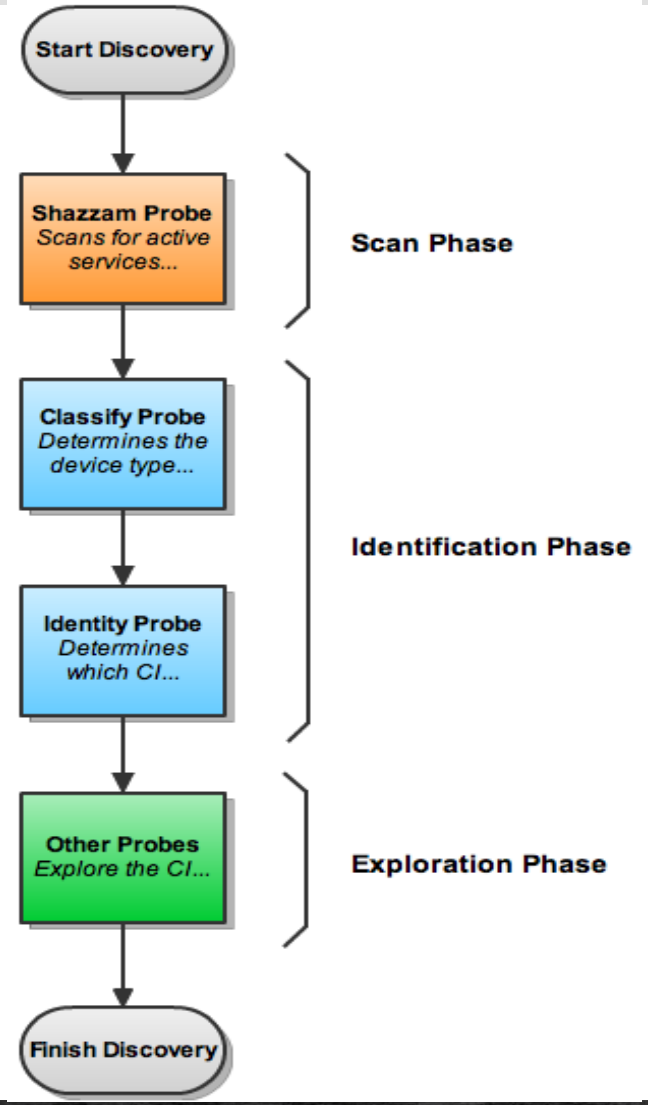


© 2014 ServiceNow All Rights Reserved

Identification

(3) IDENTIFICATION

- *Identify* the particular device following a specific set of rules
- The “identity probe” launched is dictated within the CIs classification
- After the identity probe finishes the sensor evaluates against the “CI Identifiers” looking for a match within the CMDB



© 2014 ServiceNow All Rights Reserved

Identification Rules

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]

- In identification 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

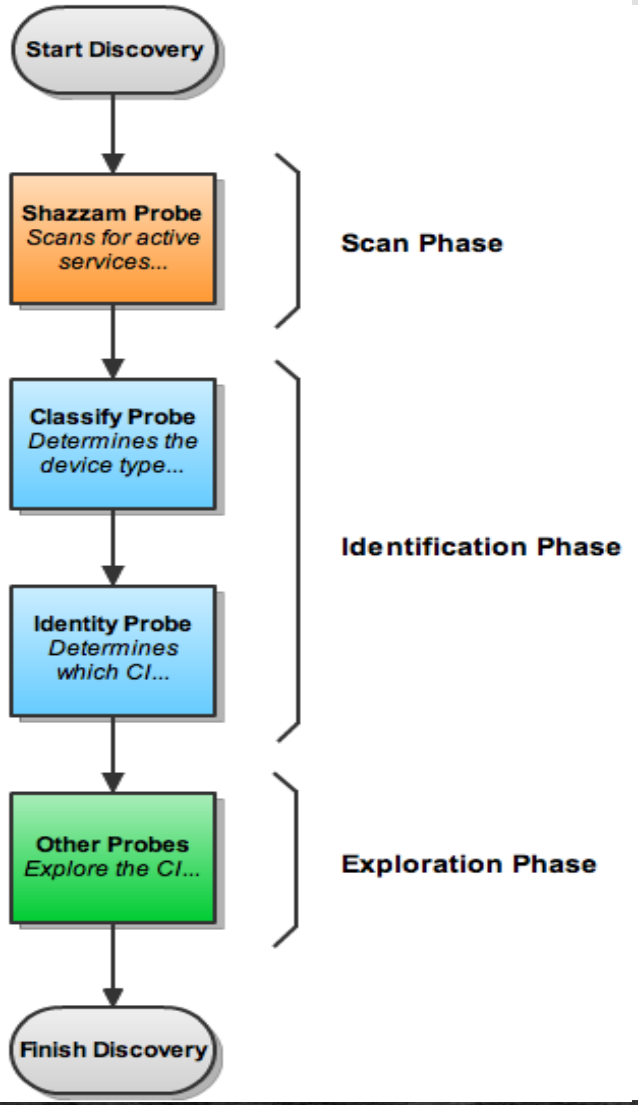
© 2014 ServiceNow All Rights Reserved

Exploration

(3) IDENTIFICATION

- *Explore* the device
  - Tome to find the good stuff

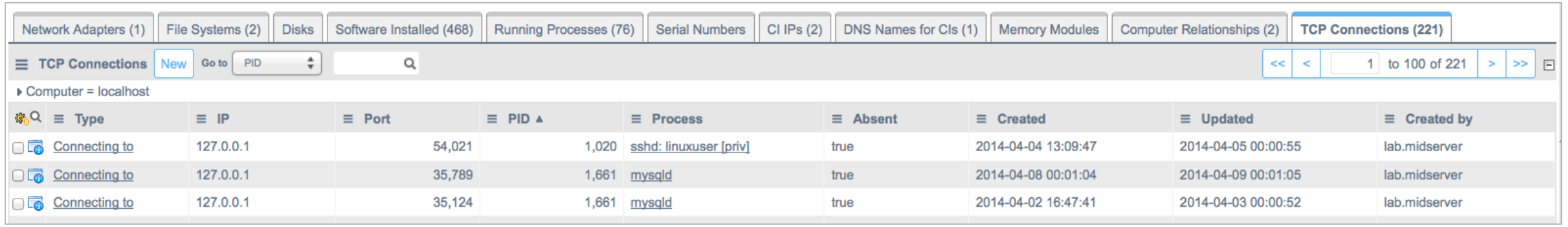
- Probes launched are dictated by the CI classification "trigger probe" with the phase equal to "Exploration"



© 2014 ServiceNow All Rights Reserved

Process Classification

- Within the exploration phase we gather all the process that we running at the time of discovery.
- Discovery will 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 process' TCP connections



Type	IP	Port	PID ▲	Process	Absent	Created	Updated	Created by
Connecting to	127.0.0.1	54,021	1,020	sshd: linuxuser [priv]	true	2014-04-04 13:09:47	2014-04-05 00:00:55	lab.midserver
Connecting to	127.0.0.1	35,789	1,661	mysqld	true	2014-04-08 00:01:04	2014-04-09 00:01:05	lab.midserver
Connecting to	127.0.0.1	35,124	1,661	mysqld	true	2014-04-02 16:47:41	2014-04-03 00:00:52	lab.midserver

© 2014 ServiceNow All Rights Reserved

Discovery 101
Building Application Dependencies

© 2014 ServiceNow All Rights Reserved

Top Takeaways

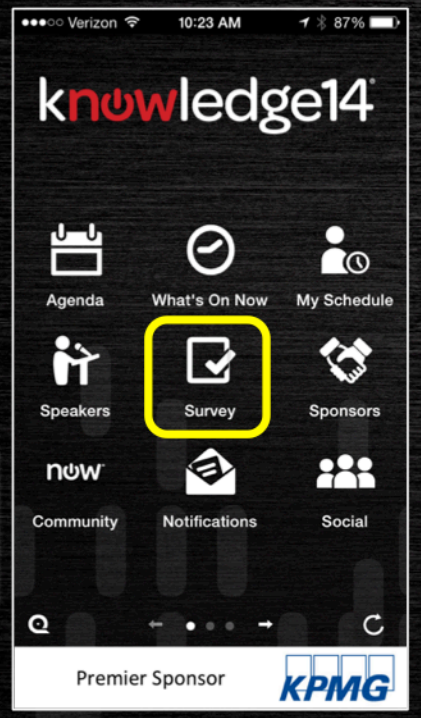
1 Discovery is agentless

2 Easily configurable

3 Extensible

© 2014 ServiceNow All Rights Reserved

Tell us what you think!



Click on the survey link in your Knowledge14 mobile app. Help us make Knowledge 15 even more valuable!

Thank You

Doug Schulze

Expert Services
Team Lead for Automation

ServiceNow

Doug.Schulze@servicenow.com

Aleck Lin

Lead Discovery Developer

ServiceNow

Aleck.Lin@servicenow.com

Want a copy of this deck?

Sign into the BuzzHub to unlock all the slides and lab guides from Knowledge14 sessions

