Navigate Service Mapping

Lab

⌛15m

Lab Objectives

Cloud Dimensions just purchased Service Mapping and wants to become familiar with the Service Mapping application and identify key modules and configuration areas.

In this lab, you will complete the following tasks:

- Navigate the Service Mapping and Discovery Applications
- View Discovery Patterns and Credentials
- View the MID Server module and Schedules

Request a Lab Instance

- In NowLearning, on the Service Mapping Fundamentals On Demand enrollment page, top left, click **Request a Lab Instance**. Your instance and MID Server may be available very soon or you may have to wait a short while.
- After they are running, you can access your instance from this same Course page, or you can wait for the email with the necessary links and credentials. You will need to access the Windows MID Server in future labs. Use Microsoft Remote Desktop with the link and credentials provided. You will be asked to use the public and private IP addresses in future labs. These are displayed on the MID Server desktop in the top right. Use the hostname provided in the email for initial remote access.
- **Hibernation:** After four hours of no activity (idle, overnight, etc.) on the instance or Windows MID Server, they will be placed in hibernation. When accessing a hibernating instance, a message will display, and they will be started again. When the Windows MID Server is started, it will keep the previous Private IP address, but the Public IP address will change. If the Public IP address has been configured somewhere (remote desktop, browser, etc.), you will need to update with the new one.

A. Service Mapping and Discovery Applications

1. Navigate to **Service Mapping > Administration > Discovery Dashboard.**

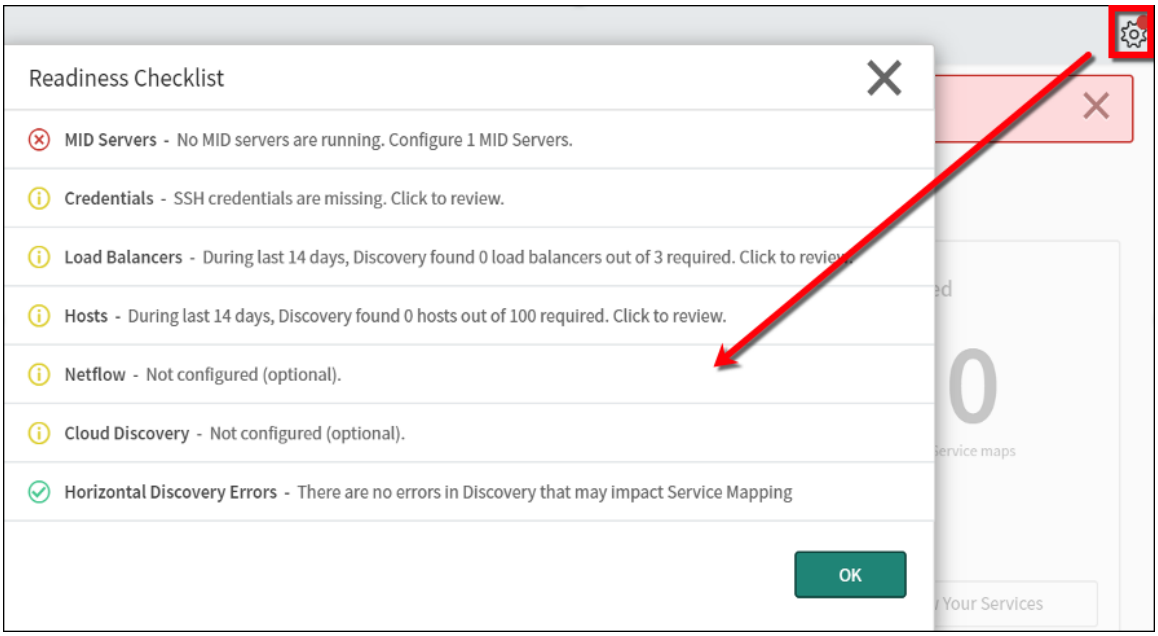
> ***Note:*** *There is no data yet but after the initial discovery, the Discovery Dashboard lights up with valuable data around discovered devices, applications, errors, schedules, and unused credentials.*

2. Navigate to **Service Mapping > Home**.

> ***Note:*** *A message appears that Service Mapping is not ready for discovery. The Home page is the starting point for all Service Mapping discoveries and allows a Service Mapping administrator to access Service Mapping workflow tasks. This page also displays important progress statistics. For example, the number of services discovered with errors, waiting to be approved, and completed.*

3. From the bottom of the **Home** page, click the **Additional Options** link to view the options available.

4. From the top right of the **Home** page, click the **Readiness Checklist** icon to view a list of tasks that need to be completed.



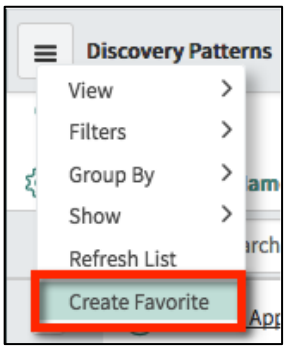
5. From the **Readiness Checklist**, click **Ok**.

B. Discovery Patterns

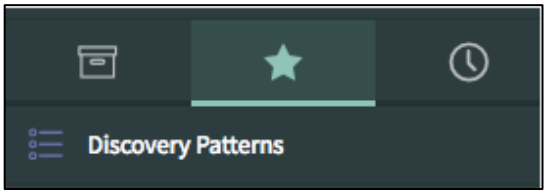
Discovery Patterns attempt to identify applications and their outbound connections supporting the Service. Application CI data and their attributes captured from the patterns are associated to the CI in the CMDB.

1. Navigate to **Pattern Designer > Discovery Patterns**.

2. From the **List controls** menu, click **Create Favorite** to save this menu as a favorite in order to simply navigate to this module in future labs.

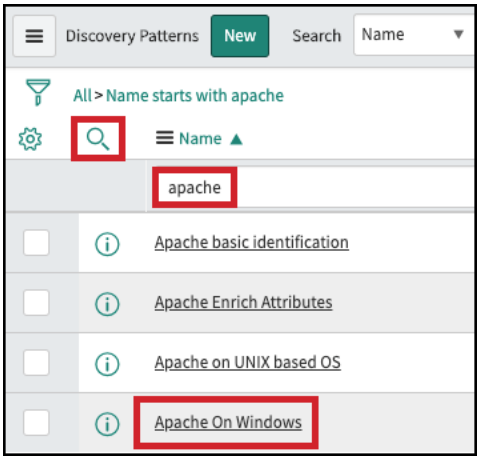


3. From the **Create Favorite** form, click **Done**.



> ***Note:*** *Favorites are easily accessible from the left navigator under the* ***Favorites*** *icon.*

4. From the **Discovery Patterns** list, search for and open the **Apache on Windows** record



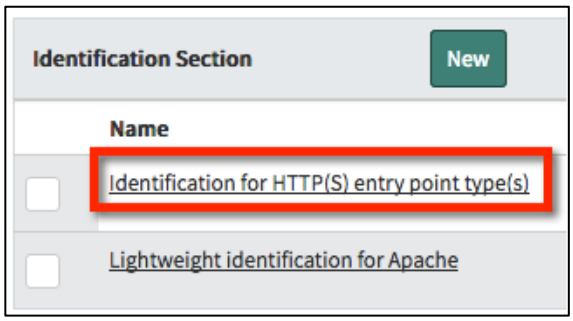
> ***Note:*** *A new tab opens and displays the pattern. A pattern is responsible for identifying a specific CI Type/class. This CI Type corresponds to a table extended from the Application Configuration Item [cmdb_ci_appl] table in the CMDB.*

The Pattern opens in a new browser tab and contains three sections in the Basic tab of the Pattern:

- **Identification Section**: used to identify applications by performing a series of identification steps by reading configuration details exposed by the CI.
- **Extension Section**: used to modify the discovery logic in identification sections without changing the identification sections themselves.
- **Connection Section***:* based on the results of the identification section, the connection section steps are attempted to identify any outgoing connections from the identified application.

> *In future modules in this class, you work more in depth with modifying and building your own Pattern, Identification, and Connection Sections.*

5. Click and open the first record under the **Identification Section**.



> ***Note:*** *The Pattern Designer opens and displays all the steps that comprise the Identification Section. You will work with Identification Sections more in detail later in the class.*

6. Click the browser back button to return to the **Apache On Windows** pattern.

C. Discovery Credentials

Credentials must be defined before a device can be successfully discovered. Without proper credentials, the discovery process cannot complete.

1. Close the **Apache On Windows** pattern browser tab, and navigate to **Service Mapping > Administration > Credentials**.

> ***Note:*** *Discovery and Service Mapping use credentials that are stored in the same table and can be shared between both applications. Credentials are used to access target devices in order to query them for specific attributes.*

2. Click **New** and view the different credential types.

> ***Note:*** *Later in class you create several credentials to discover numerous CIs in the training environment that support various services.*

D. MID Servers and Discovery Schedules

1. Navigate to **Service Mapping > Administration > MID Servers**.

> ***Note:*** *No MID Servers are currently configured. MID Servers subscribe to messages published by an Asynchronous Message Bus (AMB) on the ServiceNow instance, which notifies the MID Server that it has pending tasks in the ECC queue. The tasks are in the form of a Probe or Pattern. MID Servers use the credentials defined in the Credentials table to access devices to perform their work. In the next lab, you will set up a MID Server.*

2. Navigate to **Discovery > Discovery Schedules**.

> ***Note:*** *Discovery Schedules under the Discovery menu define how often infrastructure configuration items such as servers, routers, and switches are discovered.*

3. Select **Quick Discovery**.

> ***Note:*** *Quick Discovery is used to discover a single target IP address. This discovery method is useful for testing discovery against a specific CI without having to build a schedule. It is important to note that the underlying discovery process is the same between Quick Discovery and a complete discovery schedule. The main difference is Quick Discovery is a faster method to configure discovery of a single device, while creating a discovery schedule can be useful for rediscovery on a scheduled basis.*

4. From the **Quick Discovery** dialog window, click **Cancel**.

5. Navigate to **Service Mapping > Administration > Discovery Schedules**.

> ***Note:*** *Discovery Schedules under the Service Mapping menu define when and how often Service Mapping discovery (also known as top-down discovery) will execute on a scheduled basis. Service Mapping schedules define how often an application or set of applications are discovered that pertain to a service.*

6. Select and open the **All Applications** Discovery Schedule.

> ***Note:*** *This baseline schedule defines the CI Type discovered by the schedule, the frequency of the schedule, and the MID Server to use. The Discover field is read only and does not allow the user to modify the type of discovery to perform. All other types of Discovery have to be performed under the Discovery > Discovery Schedules menu.*

REVIEW QUESTIONS:

Based on the navigation skills learned, answer the following questions. Refer to the end of the lab to check your answers.

1. How many identification sections are configured for the Microsoft SharePoint pattern?

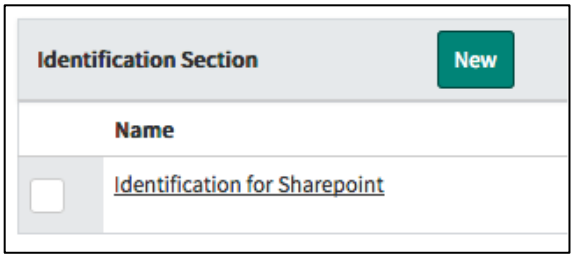
2. In the **IIS** discovery pattern, what IIS versions are listed in the identification section?

3. What field is used to define the frequency in a discovery schedule?

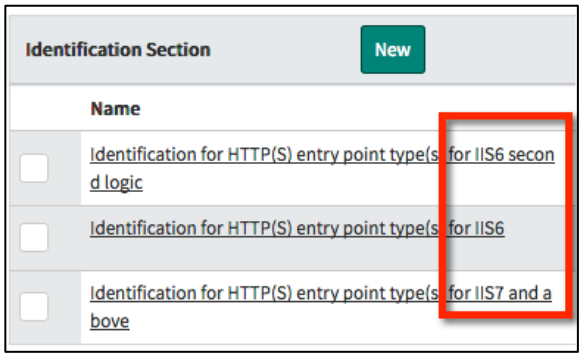
4. How many different credential types exist in a baseline instance?

REVIEW ANSWERS:

1. **One**



2. **IIS6** and **IIS7**



3. The **Run** field

4. 18