



Demystifying Graph API and Service Now

Using a Service account, CrowdStrike and Ansible to
glue it all together

Hailaeos.Troy@DenverGov.org

Red Hat
Summit



Hailaeos.Troy@denvergov.org

A AnsibleFest



Sanitized Code
For All
Dudes and Dudettes

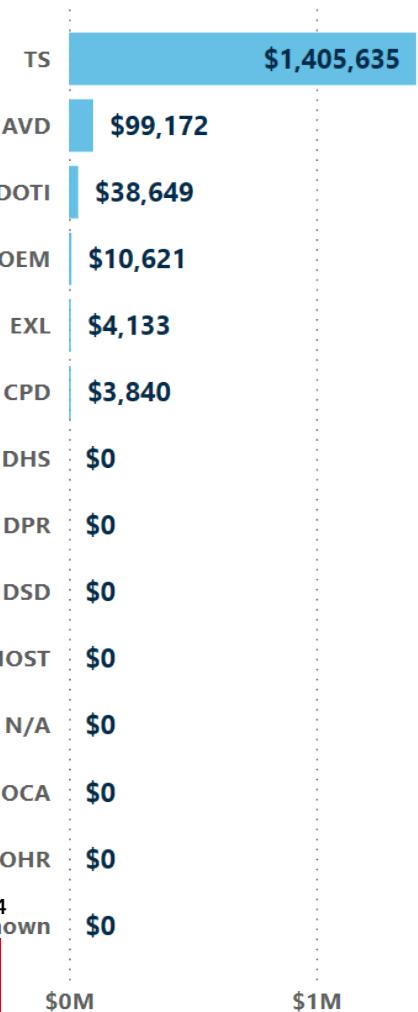
 Red Hat





Last Refresh: 5/8/2024 3:30:10 PM

Total Dollar Savings by Agency



Total Dollar Savings*

*Data from 2023 to present

\$1,562,051

\$1,025,923

TS Soft Savings

\$310,800

One-Time Savings

\$171,433

Non-TS Soft Savings

\$53,895

Hard Savings

Total Refocused Hours

24,804

20,518

TS Staff Hours Saved

4,286

Non-TS Staff Hours Saved

Averages

Rolling Average - Past 30 Days

\$4,513

Dollars Saved per Day

81.8

Hours Saved per Day

Automated Processes

133

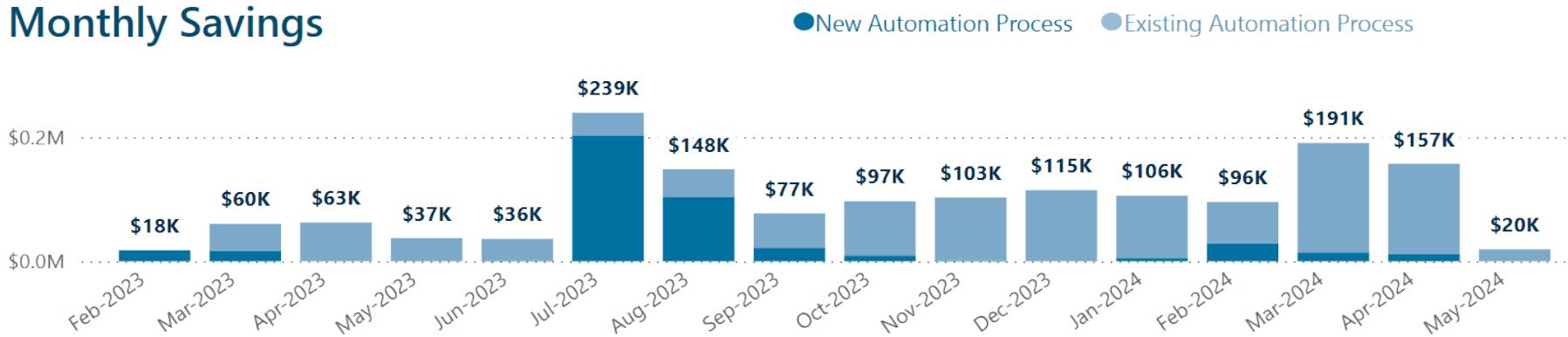
Year

All

Tool

Ansible

Monthly Savings



Accrued Savings



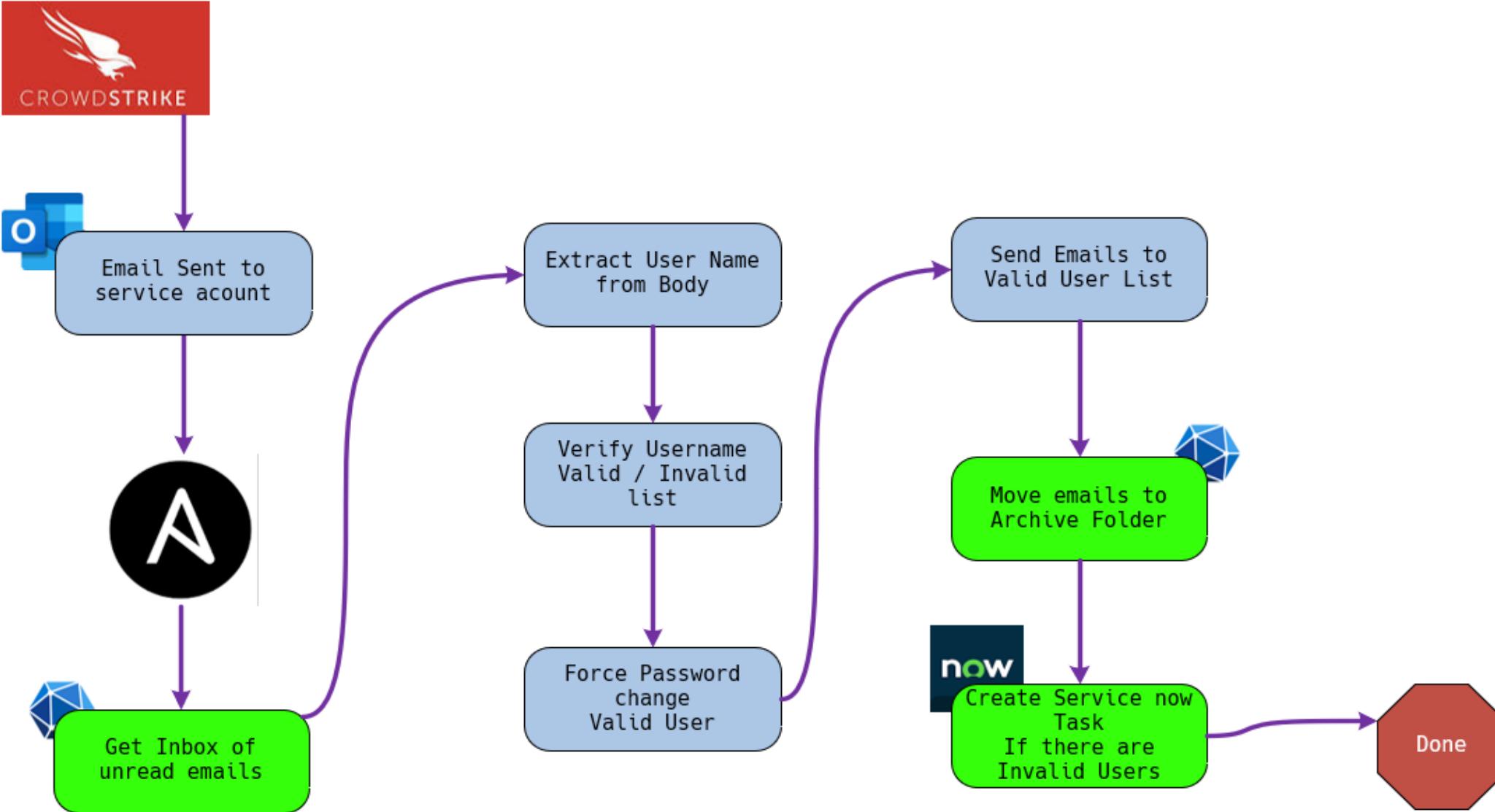
50,000 foot view

The Problem

- **CrowdStrike sends an email to a service account, each email is a user that is using a password that is on a known compromise list. Like “password123”**
- **Ansible once an hour will do the following:**
- **Grab any new mail and process them (Graph API)**
- **Ansible then will match the account and send a notification and force a password change (A D)**
- **Move all the messages that were processed to the Archive folder (Graph API)**
- **Unmatched accounts will get a ServiceNow task assigned to Security (Service Now)**

Step 1

The Problem



25,000 foot view

Pieces to get the job done

1. **Get with the Azure Admin and create an Enterprise application and get the Delegated and Application permissions you need.** (in my case I have the needed permissions)
2. **Put your app secrets in your Ansible vault or your favorite secure location like Secret Server**
3. **Get with the ServiceNow folks get access to your Dev/Test/Sandbox environment and permission to access the Rest API Explorer its your friend, like me.**
4. **Get a ServiceNow service account setup with the correct permissions to create TASK**
Bonus points for getting impersonate rights in Dev/Test/Sandbox or full Admin.
Trust me it helps

Down in the weeds

Graph API task pieces

This is where you need your Azure Admin

The screenshot shows the Microsoft Azure portal interface for managing enterprise applications. A specific application named 'ansible_app' is selected.

Key elements highlighted with yellow circles and green boxes:

- 1**: The URL bar showing the address of the application registration page.
- 2**: The application name 'ansible_app' in the breadcrumb navigation.
- 3**: A callout box around the 'app_teamsid' and 'tenantId' fields in the 'Essentials' section of the application overview.
- 4**: The 'Certificates & secrets' tab in the left-hand navigation menu.
- 5**: The 'Client secrets (1)' tab under the 'Certificates & secrets' section.
- 6**: The 'New client secret' button.
- 7**: The 'Value' field containing the secret string 'app_teamssecret'.
- 8**: The 'Secret ID' field containing the identifier 'f63'.

Annotations with arrows point from the numbered circles to the corresponding UI elements:

- Annotation 3 points from circle 3 to the 'app_teamsid' and 'tenantId' fields.
- Annotation 4 points from circle 4 to the 'Certificates & secrets' tab.
- Annotation 5 points from circle 5 to the 'Client secrets (1)' tab.
- Annotation 6 points from circle 6 to the 'New client secret' button.
- Annotation 7 points from circle 7 to the 'Value' field.
- Annotation 8 points from circle 8 to the 'Secret ID' field.

Other visible details include the application's display name 'svc ansible msteams', its object ID, and the supported account types ('My organization only'). A note at the bottom indicates that starting June 30th, 2020, no new features will be added to Azure Active Directory.

Down in the weeds

Graph API task pieces

This is where you need your Azure Admin

The screenshot shows the Microsoft Azure portal interface. On the left, the navigation menu is visible with several items highlighted in yellow circles:

- Microsoft Azure (top left)
- 1: Home > App registrations > ansible > API permissions
- 2: API permissions
- 3: Add a permission (button)
- 4: Microsoft Graph (section)

The main content area displays the 'Request API permissions' dialog. At the top, it says 'Select an API' with tabs for Microsoft APIs, APIs my organization uses, and My APIs. The Microsoft APIs tab is selected, showing the 'Commonly used Microsoft APIs' section. The 'Microsoft Graph' section is highlighted with a green arrow and a callout box containing the text: 'get with your O365 admin to get permissions'. Below this, there's a warning about granting tenant-wide consent. The 'Configured permissions' section lists various permissions granted to the application, including several for Microsoft Graph.

API / Permissions name	Type	Description
Application.Read.All	Delegated	Read applications
Application.Read.All	Application	Read all applications
Application.ReadWrite.All	Delegated	Read and write all applications
Application.ReadWrite.All	Application	Read and write all applications
Calendars.Read	Delegated	Read user calendars
Calendars.Read	Application	Read calendars in all mailboxes
Calendars.Read.Shared	Delegated	Read user and shared calendar
Calendars.ReadWrite	Delegated	Have full access to user calendar

Get a Token

To `curl://` or to `ansible.builtin.uri`

```
- name: Get Application Token for microsoft graph api
  ansible.builtin.shell: |
    curl -s -k -X POST -d "grant_type=client_credentials\
    &client_id={{ app_teamsid }}&client_secret={{ app_teamssecret }}&scope=https://graph.microsoft.com/.default" \
    https://login.microsoftonline.com/{{ tenantId }}/oauth2/v2.0/token \
    | jq -r ".access_token"
  register: shell_token
  changed_when: false

- name: Get Graph API Application Token
  ansible.builtin.uri:
    url: "https://login.microsoftonline.com/{{ tenantId }}/oauth2/v2.0/token"
    method: POST
    headers:
      Content-Type: "application/x-www-form-urlencoded"
    body_format: form-urlencoded
    body:
      grant_type: "client_credentials"
      client_id: "{{ app_teamsid }}"
      client_secret: "{{ app_teamssecret }}"
      scope: "https://graph.microsoft.com/.default"
    register: tokena
```

Microsoft Graph API

A screenshot of a search results page from a web browser. The search bar at the top contains the query "graph api mailfolders". Below the search bar is a navigation bar with tabs: ALL (which is selected), VIDEOS, IMAGES, NEWS, MAPS, SHOPPING, BOOKS, and SEARCH TOOLS. The main content area shows a single search result titled "List mailFolders - Microsoft Graph v1.0". The URL of the result is "learn.microsoft.com/en-us/graph/api/user-list-mailfolders?view=graph-rest-1.0&tabs=http". Below the title, there is a snippet of text: "Oct 27, 2023 · To return all mail folders in a mailbox, each child folder must be traversed separately. This API is available in the following national cloud ...". A green arrow points from the search bar down to the URL.

Permissions

Choose the permission or permissions marked as least privileged for this API. Use a higher privileged permission or permissions [only if your app requires it](#). For details about delegated and application permissions, see [Permission types](#). To learn more about these permissions, see the [permissions reference](#).

[Expand table](#)

Permission type	Least privileged permissions	Higher privileged permissions
Delegated (work or school account)	Mail.ReadBasic	Mail.ReadWrite, Mail.Read
Delegated (personal Microsoft account)	Mail.ReadBasic	Mail.ReadWrite, Mail.Read
Application	Mail.ReadBasic.All	Mail.ReadWrite, Mail.Read

HTTP request

To get all the mail folders in the root folder in the specified user's mailbox, excluding those that are hidden:

HTTP

```
GET /me/mailFolders  
GET /users/{id | userPrincipalName}/mailFolders
```

To include *hidden* mail folders in the response:

HTTP

```
GET /me/mailFolders/?includeHiddenFolders=true  
GET /users/{id | userPrincipalName}/mailFolders/?includeHiddenFolders=true
```

Optional query parameters

To return a list of all mailFolders including those that are hidden (their `isHidden` property is true), in the request URL, specify the `includeHiddenFolders` query parameter as `true`, as shown in the [HTTP request](#) section.

This method supports [OData query parameters](#) to help customize the response.

```
- name: "Get root folder of email "
  ansible.builtin.uri:
    url: "https://graph.microsoft.com/v1.0/users/{{ mailaccount }}/mailFolders"
    method: GET
    headers:
      Authorization: 'Bearer {{ token }}'
      Content-Type: application/json
    status_code:
      - 200
      - 201
      - 404
  register: root_folders
```

```
- name: show results of root folders
ansible.builtin.debug:
  msg:
    - "{{ root_folders }}"
  verbosity: "{{ verbosity_level }}"

- name: show results
ansible.builtin.debug:
  msg:
    - "{{ root_folders | json_query(query) }}"
  verbosity: "{{ verbosity_level }}"
vars:
  query: "json.value[?displayName=='Inbox'].id"
```

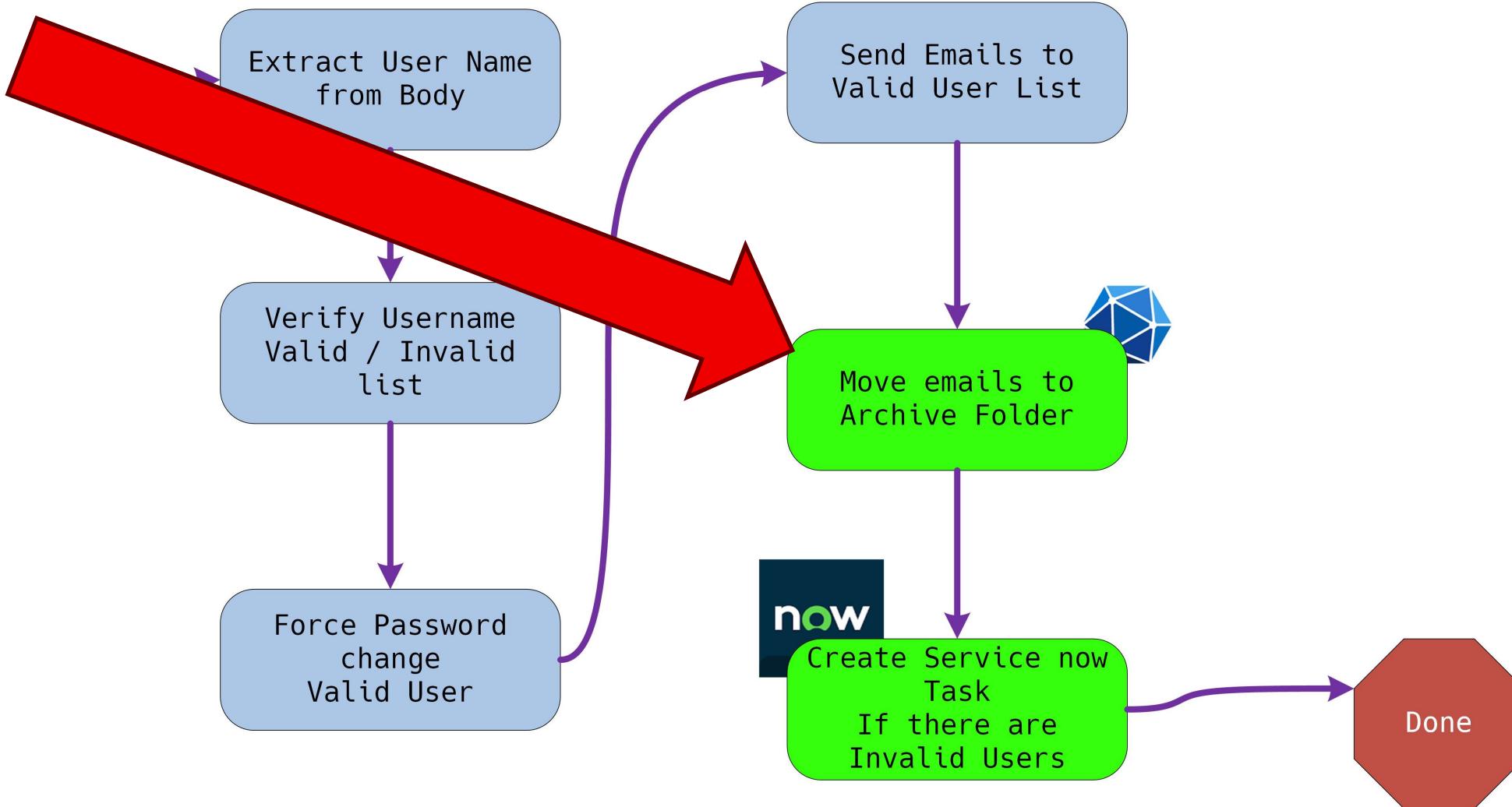
```
- name: set fact for root folder
ansible.builtin.set_fact:
  inbox: "{{ (root_folders | json_query(query))[0] }}"
vars:
  query: "json.value[?displayName=='Inbox'].id"
```

```
# subject_search: "CrowdStrike Identity Protection Policy Notification - Rule 'Compromised Password Detected'  
1  
- name: "Get Inbox email"  
  ansible.builtin.uri:  
    url: "{{ url_search }}"  
    method: GET  
    headers:  
      Authorization: 'Bearer {{ token }}'  
      Content-Type: application/json  
    status_code:  
      - 200  
      - 201  
      - 404  
      - 400  
  vars:  
    url_search: "https://graph.microsoft.com/v1.0/users/{{ mailaccount }}/mailFolders/{{ inbox }}/messages?  
    \\$filter=startswith(Subject,'{{ subject_search|urlencode }}')&$top=2000" 2  
  register: messages
```

The reason behind using \$top=2000 is because I am lazy, I didn't want to loop using the @odata.nextLink but if you do wind up having to do pagination Microsoft style this is now you do it

```
- set_fact:  
  nextpage: "graphapidataresult.json['@odata.nextLink']"
```

Mark the messages read and move them to the archive folder



Mark messages read and move to Archive folder

Set a fact to the email id's but do it as a batch of 100 messages to avoid a graph timeout

```
1 - name: set fact to emails id
  ansible.builtin.set_fact:
    | email_id: "{{ messages | json_query(queryid) }}"
  vars:
    queryid: "json.value[*].id"

2 - name: set fact to email list batch
  set_fact:
    | email_id_batch: "{{ email_id | batch(100) }}"

3 - name: include graph batch
  include_tasks:
    | tasks/graph_batch.yml
  loop: "{{ email_id_batch }}"

4 - name: Get Graph API Application Token
  ansible.builtin.uri:
    url: "https://login.microsoftonline.com/{{ tenantId }}/oauth2/v2.0/token"
    method: POST
    headers:
      Content-Type: "application/x-www-form-urlencoded"
    body_format: form-urlencoded
    body:
      grant_type: "client_credentials"
      client_id: "{{ app_teamsid }}"
      client_secret: "{{ app_teamssecret }}"
      scope: "https://graph.microsoft.com/.default"
    register: tokena
```

Mark messages read and move to Archive folder

Patch the mail record and mark it read

```
- name: "Mark messages read"
  ansible.builtin.uri:
    url: "{{ url_search }}"
    method: PATCH ①
    headers:
      Authorization: 'Bearer {{ token }}'
      Content-Type: application/json
    body_format: json
    body:
      isRead: true ⑤
    status_code:
      - 200
      - 201
      - 404
      - 400
  vars:
    url_search: "https://graph.microsoft.com/v1.0/users/{{ mailaccount }}/messages/{{ item_z }}"
    ignore_errors: true          #####
    until: message_patch is not failed # This is for unstable API's #
    retries: 20 ⑥                #
    delay: 60                     #####
    loop: "{{ item }}" ②
    loop_control:
      extended: true
      loop_var: item_z ③
    register: message_patch
```

1) Patch the mail id
2) loop our 100 messages
3) set a custom loop
4) item_z = our message id
5) mark the message read
6) if the message is failed
retry 20 times every minute

④

Mark messages read and move to Archive folder

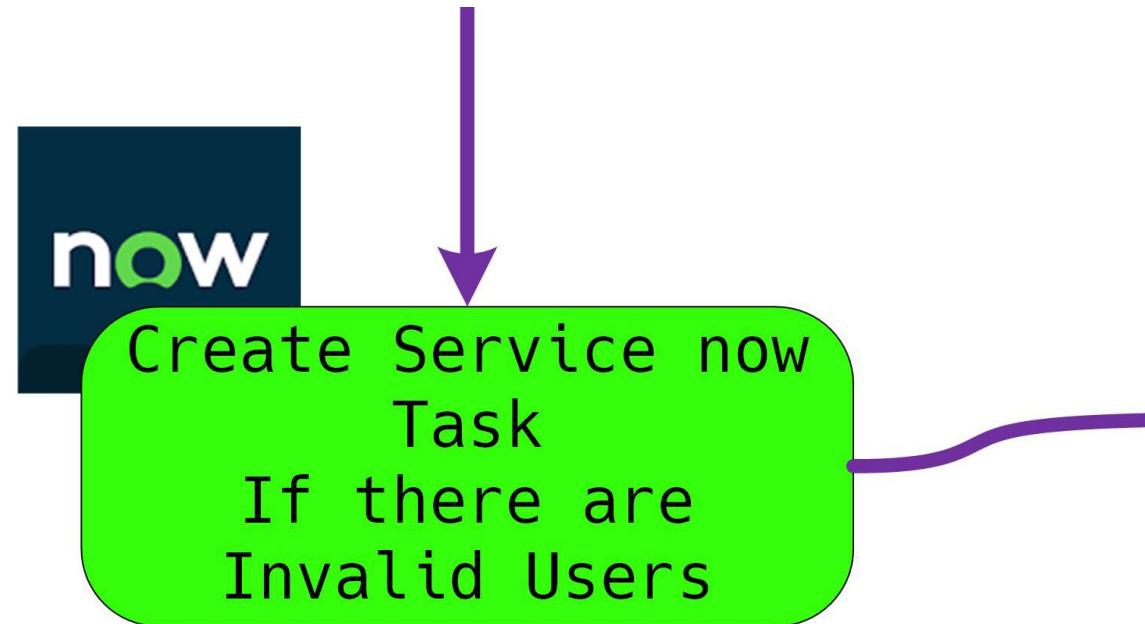
Move the message now

```
- name: "Move message to Archive "
  ansible.builtin.uri:
    url: "{{ url_move }}"
    method: POST
    headers:
      Authorization: 'Bearer {{ token }}'
      Content-Type: application/json
    body_format: json
    body:
      destinationId: "{{ (root_folders | json_query(destfolder))[0] }}"
    status_code:
      - 200
      - 201
      - 404
      - 400
  vars:
    url_move: "https://graph.microsoft.com/v1.0/users/{{ mailaccount }}/messages/{{ item_z }}/move"
    destfolder: "json.value[?displayName=='Archive'].id"
  register: message_move
  ignore_errors: true
  until: message_move is not failed
  retries: 20
  delay: 60
  loop: "{{ item }}"
  loop_control:
    loop_var: item_z
```

Diagram the issue

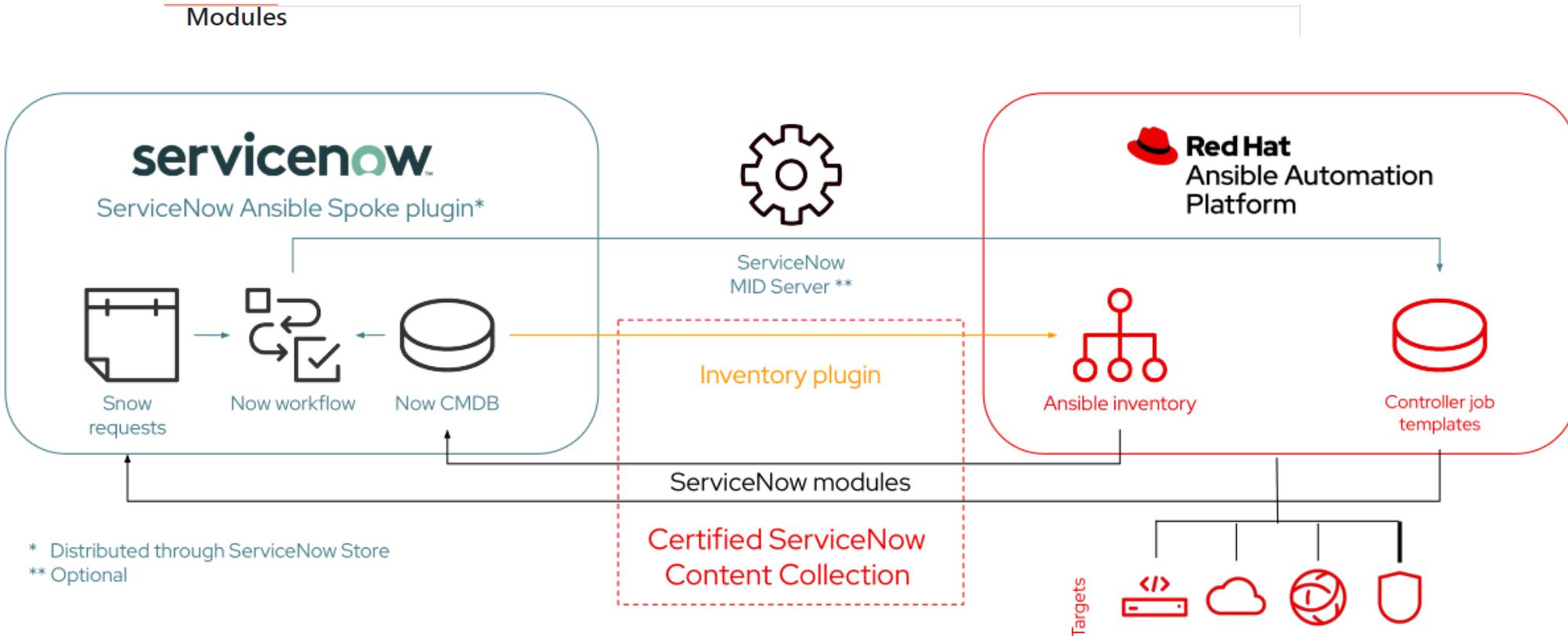
1,000 foot view

Lay it out, use your favorite diagram program I use Visio



ServiceNow, SNOW

`servicenow.itsm` vs. `ansible.builtin.uri`



<u>servicenow.itsm.problem</u>	Manage ServiceNow problems
<u>servicenow.itsm.problem_info</u>	List ServiceNow problems
<u>servicenow.itsm.problem_task</u>	Manage ServiceNow problem tasks
<u>servicenow.itsm.problem_task_info</u>	List ServiceNow problem tasks

Manage ServiceNow problems
List ServiceNow problems
Manage ServiceNow problem tasks
List ServiceNow problem tasks

ServiceNow – Its in front of you just Look

The screenshot shows a ServiceNow Catalog Task record for TASK0518733. The 'Caller' field is highlighted with a green box and a red circle containing the number '1'. A callout bubble points to it with the text 'Thats the user'. To the right, a green box and a red circle containing the number '2' points to the 'Open Record' button, with a callout bubble pointing to it and the text 'open the record'.

Catalog Task
TASK0518733

Number: TASK0518733
Caller: Tyler Zimmerer

User

Opened: 02-06-2024 17:54:22
Opened by:

... Discuss Update Add to Azure DevOps Close Task

Open Record

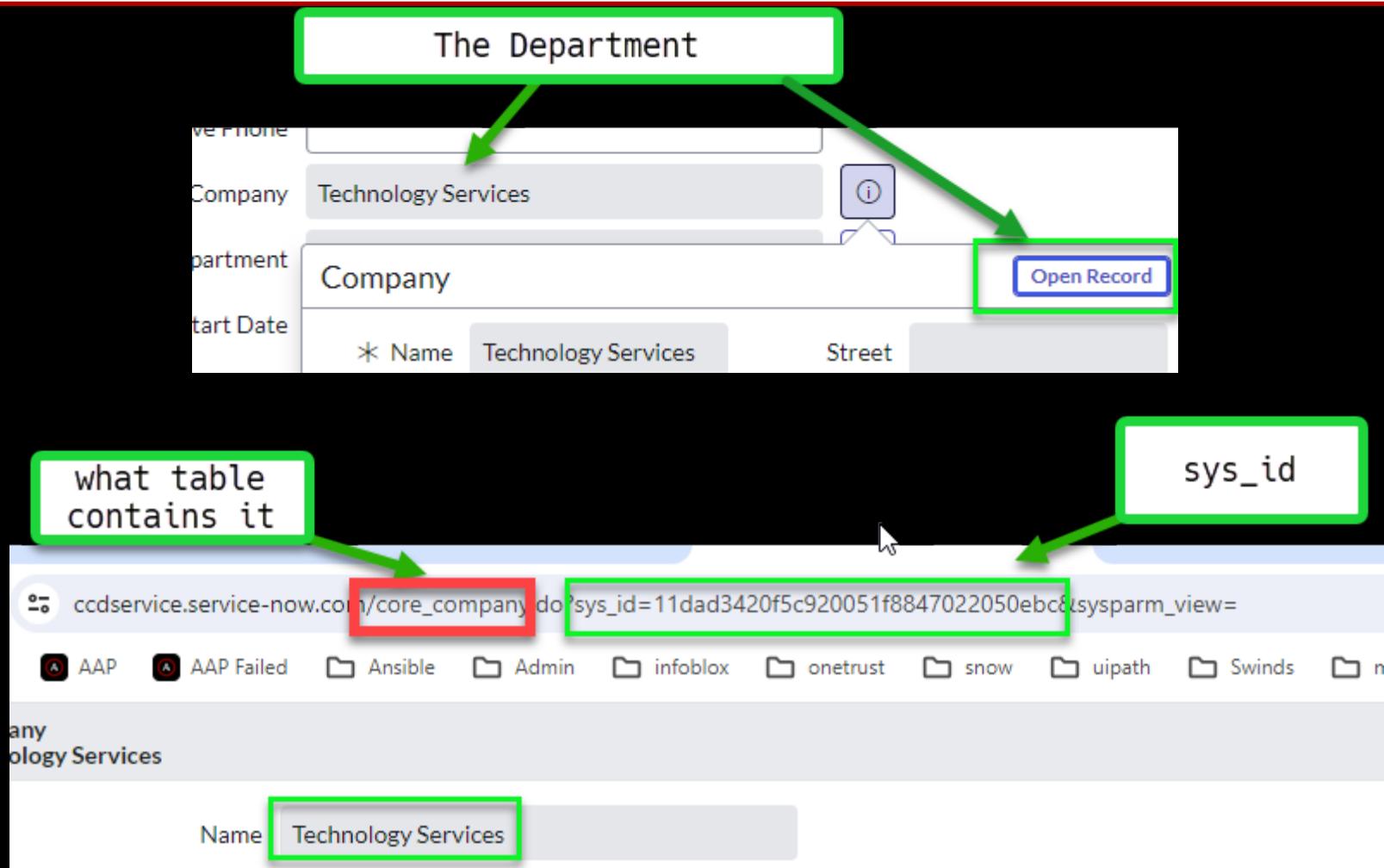
The screenshot shows a browser window with the title '733 | Catalog Task | Se X'. Below it, the address bar displays the URL 'ccdservice.service-now.com/sys_user.do?sys_id=dd7647fedba67e00391c7c1ebf96193b&sysparm_view=' followed by a red box with a red circle containing the number '3'. Below the address bar, the URL is partially visible with a red box and a red circle containing the number '4'.

Tyler Zimmerer | User | ServiceN X +

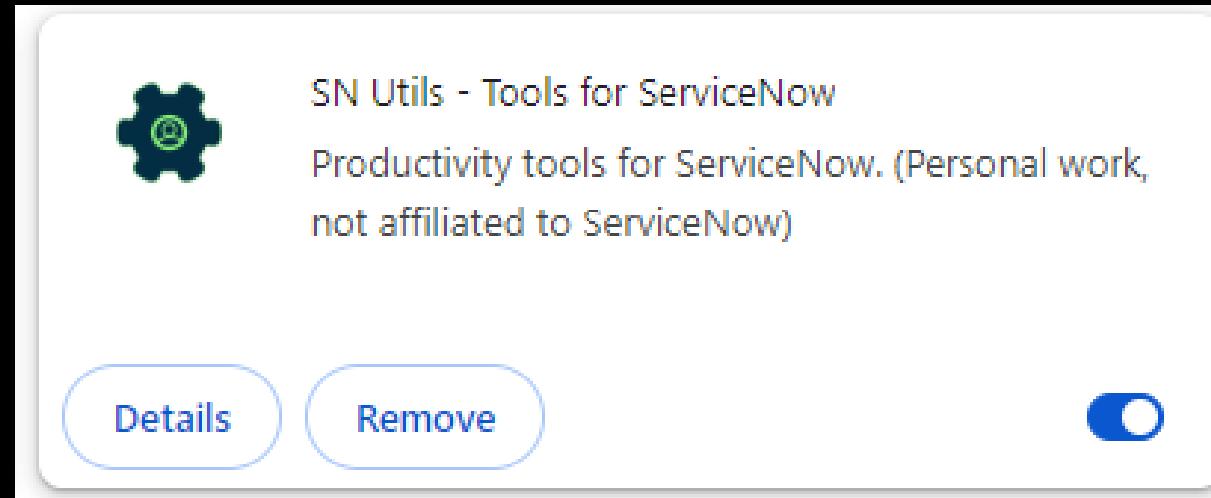
ccdservice.service-now.com/sys_user.do?sys_id=dd7647fedba67e00391c7c1ebf96193b&sysparm_view=

AAP AAP Failed Ansible Admin infoblox onetrust snow uipath Swi

ServiceNow – Its in front of you just Look



ServiceNow – There is a tool



ServiceNow – There is a tool

Catalog Task
TASK0532527 | sc_task [scratchpad][table fields][toggle label]

Discuss Update Add to Azure DevOps Close Task Start Microsoft Teams Chat

* Business Application | SR_Application ⓘ
GIS

* Sequence Number (000-999) | SR_Sequence ⓘ
023

* Operating System | SR_OperatingSystem ⓘ
Windows 2022 | Windows 2022

IP Address | SR_ip_address

* Patch Track | patch_track ⓘ
Patch Track 1 | Patch Track 1

PROD: TRACKS 1&2 Run concurrently during the 3rd week of the month (This is known as Track "A")
TRACKS 3&4 Run concurrently during the 3rd week of the month (This is known as Track "B")
TRACK OTHER Runs concurrently during the 3rd week and REQUIRES MANUAL REBOOT BY APPLICATION OWNER | prod_label

* Reboot times | reboot_times ⓘ
3:00 AM Reboot | 300

* Server Function | SR_ServerFunction ⓘ
Web server | WEB

* Server Environment | SR_ServerEnvironment ⓘ
QA | Q

Server Name | SR_ServerName
GISWEB023Q

Mic Drop

NON PROD: TRACK 1 occurs Thursday of 2nd week TRACK 2 occurs Friday of 2nd week TRACK 3 occurs Saturday of 2nd week TRACK 4 occurs Sunday of 2nd week TRACK OTHER Occurs Sunday of 2nd week and REQUIRES MANUAL REBOOT BY APPLICATION OWNER | nonprod_label

ServiceNow – Rest API Explorer – get a user

Table API

Allows you to perform create, read, update and delete (CRUD) operations on existing tables



Retrieve records from a table

```
GET https://ccdsandbox.service-now.com/api/now/table/{tableName}
```

Prepare request

Path parameters

Name	Value
* tableName	-- Select a table --

Query parameters

Name	Value	Description
sysparm_query	<input type="text"/>	An encoded query string used to filter the results
sysparm_display_value	<input type="text"/>	Return field display values (true), actual values (false), or both (all) (default: false)
sysparm_exclude_reference_link	<input type="text"/>	True to exclude Table API links for reference fields (default: false)
sysparm_suppress_pagination_header	<input type="text"/>	True to suppress pagination header (default: false)

ServiceNow – Rest API Explorer

REST API Explorer

Namespace: now

API Name: Table API

API Version: latest

Table API
Allows you to perform create, read, update and delete (CRUD) operations on existing tables

Retrieve records from a table
GET https://ccdsandbox.service-now.com/api/now/table/{tableName}

Prepare request

Create a record (POST) **(highlighted)**

Retrieve a record (GET)

Modify a record (PUT)

Delete a record (DELETE)

Update a record (PATCH)

Export OpenAPI Specification (YAML)

Export OpenAPI Specification (JSON)

Path parameters

Name: * tableName Value: Catalog Task (sc_task)

Query parameters

Name Value Description

sysparm_query

Return field display string used to filter the results

sysparm_display_value

Return field display values (true), actual values (false), or both (all) (default: false)

Request Body

Builder Raw

Active: true

Assignment Group: reference , Eg .. 9605e0c3c611227c017f67

you can see fields that are needed ***mostly**

Send

```
{"active":"true","assignment_group":""}
```

ServiceNow – Rest API Explorer

The screenshot shows the ServiceNow Rest API Explorer interface. At the top left, there's a 'CURL Code Sample' section with a yellow circle containing the number '2'. Below it is a code block containing a cURL command to create a task in the 'sc_task' table. To the right of the code block are three buttons: 'Select Snippet', 'X', and a large 'Add header' button. A 'Send' button is located at the bottom left of the main panel. At the bottom, there's a 'Code Samples' section with a yellow circle containing the number '1' and a note about using provided samples to send requests from various languages. A horizontal navigation bar at the very bottom includes links for ServiceNow Script, cURL, Python, Ruby, JavaScript, Perl, and Powershell.

CURL Code Sample

2

```
curl "https://ccdsandbox.service-now.com/api/now/table/sc_task" \
--request POST \
--header "Accept:application/json" \
--header "Content-Type:application/json" \
--data "{\"active\":\"true\",\"assignment_group\":\"\"}" \
--user 'admin':'admin'
```

Select Snippet X

Add header

Send

Code Samples

1

Use the provided code samples to send this request from commonly used languages.

[ServiceNow Script] [cURL] [Python] [Ruby] [JavaScript] [Perl] [Powershell]

ServiceNow – uri get user

```
- name: Search for user
  ansible.builtin.uri:
    url: "https://{{ snow_instance }}.service-now.com/api/now/table/sys_user?name={{ task_assignment_user|urlencode }}"
    method: GET
    user: "{{ Uname }}"
    password: "{{ Upass }}"
    headers:
      Accept: application/json
      Content-Type: application/json
    body_format: json
    status_code:
      - 200
      - 201
    register: snow_user_results
```

```
- name: set key facts based searches
  ansible.builtin.set_fact:
    assignedto: "{{ snow_user_results.json.result[0].sys_id }}"
    cmdbci: "{{ snow_cmdb_ci_results.json.result[0].sys_id }}"
    assignedgroup: "{{ snow_group_results.json.result[0].sys_id }}"
```

ServiceNow – uri create task

```
- name: Create Task
  ansible.builtin.uri:
    url: "https://{{ snow_instance }}.service-now.com/api/now/table/sc_task"
    method: POST
    body_format: json
    headers:
      Accept: "application/json"
      Content-Type: "application/json"
    body:
      1 active: "true"
      assigned_to: "{{ assignedto }}"
      u_ci_class: "{{ task_ci_class }}"
      assignment_group: "{{ assignedgroup }}"
      cmdb_ci: "{{ cmdbci }}"
      description: "{{ task_description }}"
      short_description: "{{ task_short_name }}"
      priority: "{{ task_priority }}"
      work_notes: "{{ task_work_notes }}"
      Approval: "approved"
      url_password: "{{ Upass }}"
      url_username: "{{ Uname }}"
      status_code: 201
      validate_certs: false
  register: create_task
```

ServiceNow – Make is a role in your collection

```
- name: Create Task for Security for accounts not found in AD
when: '(email_addresses_notfound |length | int ) > 0'
include_role:
  name: ccd.master_roles.snow_create_task          # if using automation hub
  public: true
vars:
  snow_instance: "{{ servicenow }}" ①             # snow instance to use
  task_short_name: "CS compromised accounts not found" ② # short description
  ③task_description: "Crowdstrike compromised accounts users not found: [code]{{ email_addresses_notfound |regex_replace(sqq,'<br>')|regex_replace(sq,'')|regex_replace('\\\\[','<br>') |regex_replace('\\\\]','<br>') }}[/code]" # long description
  ④task_assignment_group: "TS Information Security"      # assignment group if empty then gotten from user below
  task_cmdb_ci: "Crowdstrike" ⑤                      # ci aka SERVER
  task_ci_class: "Business Application" ⑥            # can be Server just take a look at snow drop down
  ⑦task_work_notes: "[code]{{ email_addresses_notfound |regex_replace(sqq,'<br>')|regex_replace(sq,'')|regex_replace('\\\\[','<br>') |regex_replace('\\\\]','<br>') }}[/code]"
  ⑧task_priority: "4" #1 = high 3 moderate 4 low
```

Hailaeos.Troy@DenverGov.org

Red Hat
Summit



Hailaeos.Troy@denvergov.org

A AnsibleFest

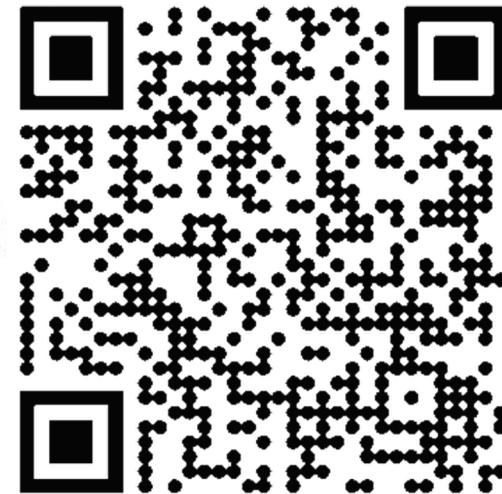


Sanitized Code
For All
Dudes and Dudettes





Thank you



Hailaeos.Troy@denvergov.org



Sanitized Code
For All
Dudes and Dudettes



[linkedin.com/company/red-hat](https://www.linkedin.com/company/red-hat)



[facebook.com/redhatinc](https://www.facebook.com/redhatinc)



[youtube.com/user/RedHatVideos](https://www.youtube.com/user/RedHatVideos)



twitter.com/RedHat

