

Ansible Tower: Project

Confidential

1

Managing Your Playbooks with Git

- You can manage playbooks and playbook directories by either placing them manually under the Project Base Path on your Tower server, or by placing your playbooks into a source code management (SCM) system supported by Tower, including Git, Subversion, Mercurial, and Red Hat Insights.
- We will be using a Git repository for this session

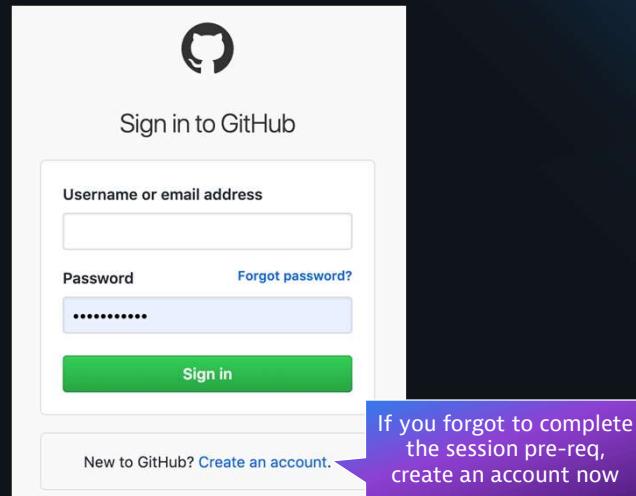


Confidential

2

Sign in to GitHub

- <https://github.com/login>



The image shows the GitHub sign-in page. It features a white header with the GitHub logo and the text "Sign in to GitHub". Below this is a form with two input fields: "Username or email address" and "Password". To the right of the password field is a link "Forgot password?". A green "Sign in" button is at the bottom of the form. At the very bottom, there is a link "New to GitHub? Create an account." A purple callout box with the text "If you forgot to complete the session pre-req, create an account now" points to this link.

Confidential

3

Create A New Repository

Create a new repo using the New button

popecruzdt

Repositories

New

Find a repository...

Configure the new repo

Create a new repository

A repository contains all project files, including the revision history. Already have a project repository elsewhere? [Import a repository](#).

Owner: popecruzdt / Repository name *: perform-dt-ansible

Description (optional): My Dynatrace Playbooks

Public: Anyone can see this repository. You choose who can commit.

Private: You choose who can see and commit to this repository.

Skip this step if you're importing an existing repository.

Initialize this repository with a README

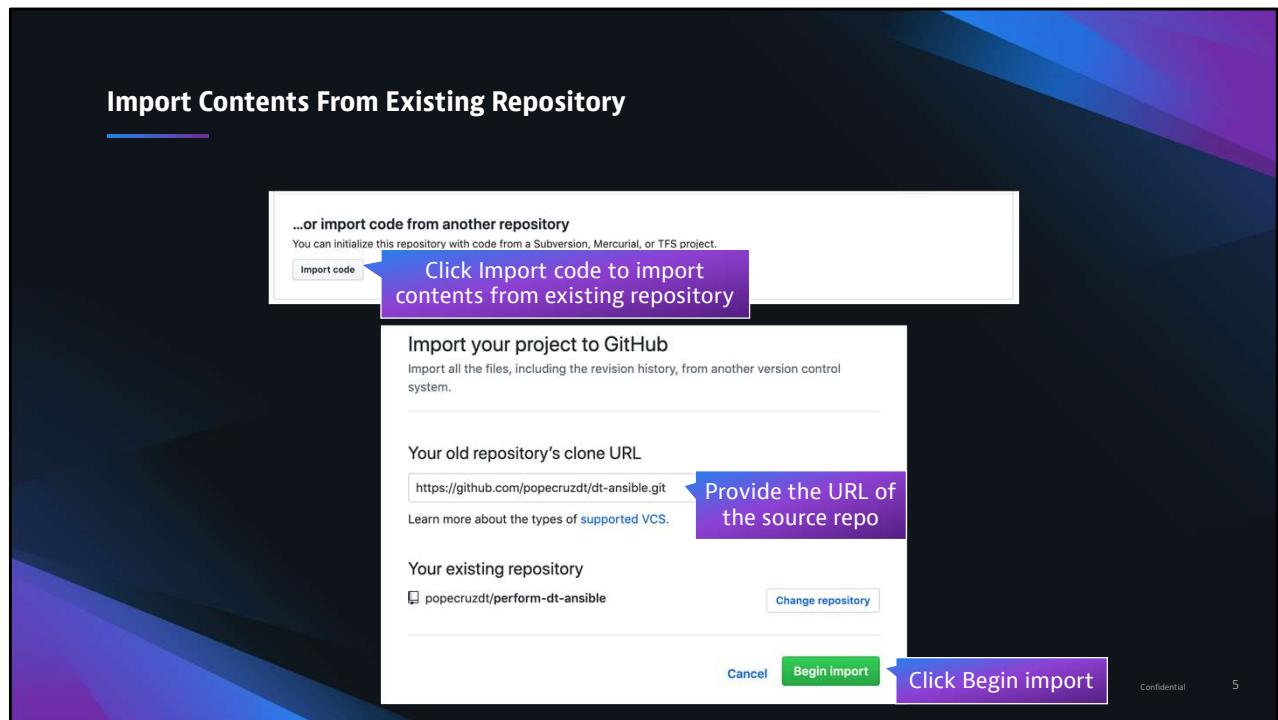
This will let you immediately clone the repository to your computer.

Add .gitignore: None | Add a license: None

Create repository

Click Create repository

Confidential 4



<https://github.com/popecruzdt/dt-ansible>

Import Contents From Existing Repository

Preparing your new repository

There is no need to keep this window open, we'll email you when the import is done.

 [popecruzdt/perform-dt-ansible](#)

✓ Importing complete! Your new repository [popecruzdt/perform-dt-ansible](#) is ready.

Confidential

6

Copy Your Git URL and Branch

The screenshot shows a GitHub repository page for the branch 'popecruzdt'. The page includes a list of files and their last modified dates. A callout box highlights the 'Clone with HTTPS' button, which is used to copy the repository's URL.

File	Last Modified
popecruzdt	11-23-2019 15:12
dt-ansible-email-notification.yml	11-19-2019 22:23
dt-api-alerting-profile.yml	11-17-2019 18:24
dt-api-application-config.yml	11-17-2019 18:24
dt-api-dashboard-clone.yml	11-23-2019 15:12

Clone with HTTPS ⓘ Use SSH
Use Git or checkout with SVN using the web URL.
<https://github.com/popecruzdt/perform>

URL Open in Desktop Download ZIP

Confidential 7

Create Your Project

PROJECTS / CREATE PROJECT

Name your Project based on your participant identifier

NEW PROJECT

DETAILS PERM

* NAME hot-proj-XX

* SCM TYPE Git

SOURCE DETAILS

* SCM URL URL

Branch

SCM BRANCH/TAG/COMMIT

DESCRIPTION

* ORGANIZATION hot-org-instructor

Assign your Inventory to your Organization

SCM REFSPEC

SCM UPDATE OPTIONS

- CLEAN
- DELETE ON UPDATE
- UPDATE REVISION ON LAUNCH
- ALLOW BRANCH OVERRIDE

CACHE TIMEOUT (SECONDS) 60

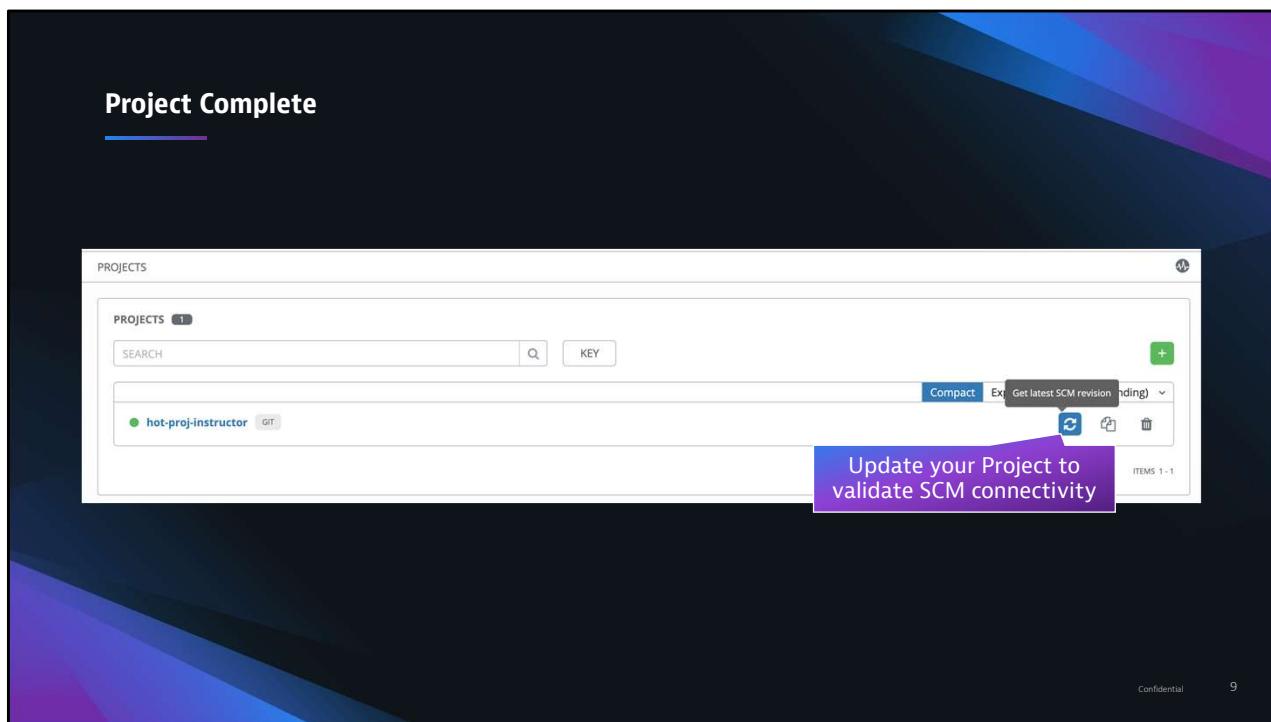
Apply these SCM update options

CANCEL SAVE

Click SAVE

8

Project Complete



Confidential

9

Ansible Tower: Inventory

Create Your Inventory

INVENTORIES / CREATE INVENTORY

NEW INVENTORY

DETAILS PERMISSIONS GROUPS SOURCES COMPLETED JOBS

* NAME: hot-inv-##

DESCRIPTION:

* ORGANIZATION: hot-org-instructor

INSIGHTS CREDENTIAL:

INSTANCE GROUPS:

VARIABLES: [YAML](#) [JSON](#)

1 ---

CANCEL SAVE

Name your Inventory based on your participant identifier

Assign your Inventory to your Organization

Click SAVE

Confidential 11

Create Your Target Group: Linux

The screenshot shows the Ansible web interface for managing inventories. The URL in the address bar is `INVENTORIES / hot-inv-instructor / ALL GROUPS`. The main content area displays the `hot-inv-instructor` group with tabs for `DETAILS`, `PERMISSIONS`, `HOSTS`, `SOURCES`, and `COMPLETED JOBS`. The `HOSTS` tab is currently selected. At the top right, there is a button labeled `Create a new group`. Below the tabs, there are three buttons: `ALL GROUPS`, `ROOT GROUPS`, and `RUN COMMANDS`, followed by a green `+` button. A purple callout box points to the `HOSTS` tab with the text "Switch to the HOSTS tab". Another purple callout box points to the green `+` button with the text "Click the + to create a Group".

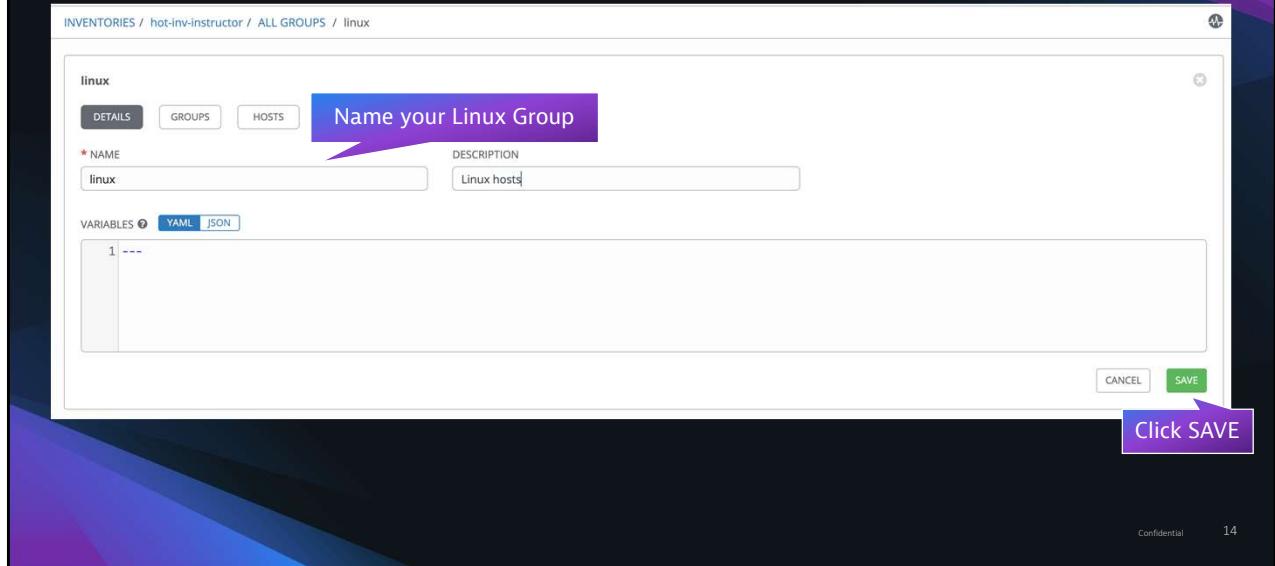
Confidential

12

Managing Linux Hosts

- By default, Ansible Tower uses SSH to connect and manage Linux hosts
- By default, Ansible Tower assumes you are using SSH keys to connect to remote machines. SSH keys are encouraged, but you can use password authentication if needed
 - We will be using password authentication for this session
- Control Nodes will need remote network access to managed Linux hosts on TCP port 22
- Authentication Options
 - Username and password of target host for password authentication
 - Ansible RSA key added to target host for key based authentication
 - RSA key of target host for key based authentication

Create Your Target Group: Linux



Confidential

14

Add Your Target Hosts: Linux

The screenshot shows the Ansible Inventory Manager interface. The URL in the address bar is `INVENTORIES / hot-inv-instructor / ALL GROUPS / linux / ASSOCIATED HOSTS`. The main navigation tabs are `DETAILS`, `GROUPS`, and `HOSTS`, with `HOSTS` being the active tab. A purple callout box points to the `HOSTS` tab with the text "Switch to the HOSTS tab". Below the tabs is a search bar and a sorting dropdown set to `HOSTS`. To the right of the search bar are `SEARCH`, `KEY`, and a magnifying glass icon. On the far right, there's a toolbar with `RUN COMMANDS` and a green plus button. A dropdown menu is open next to the plus button, showing options `Existing Host` and `New Host`. A purple callout box points to the green plus button with the text "Click the + to add a host". The bottom right corner of the interface shows the text "Confidential 15".

Add Your Target Hosts: Linux

INVENTORIES / hot-inv-instructor / ALL GROUPS / linux / ASSOCIATED HOSTS / CREATE HOST

CREATE HOST

DETAILS FACTS GROUPS

Enter the DNS host name or IP address of your first Linux host

* HOST NAME

DESCRIPTION

VARIABLES YAML JSON

1 ---

CANCEL SAVE

Click SAVE

Confidential 16

Add Your Target Hosts: Linux

INVENTORIES / hot-inv-instructor / ALL GROUPS / linux / ASSOCIATED HOSTS

linux

HOSTS

SEARCH KEY

HOSTS DESCRIPTION

Add a host

RUN COMMANDS

Existing Host New Host

Repeat this process and add the remaining Linux hosts you have been provided

Confidential 17

Create Your Target Group: Windows

The screenshot shows the Ansible Inventory interface for the 'hot-inv-instructor' inventory. The 'GROUPS' tab is highlighted. A purple callout box points to the 'GROUPS' tab with the text: 'Navigate back to your Inventory and switch to the GROUPS tab'. Another purple callout box points to a green '+' button in the top right corner of the main content area with the text: 'Click the + to create a Group'.

INVENTORIES / hot-inv-instructor / ALL GROUPS

hot-inv-instructor

DETAILS PERMISSIONS GROUPS HOSTS SOURCES COMPLETED JOBS

SEARCH

GROUPS

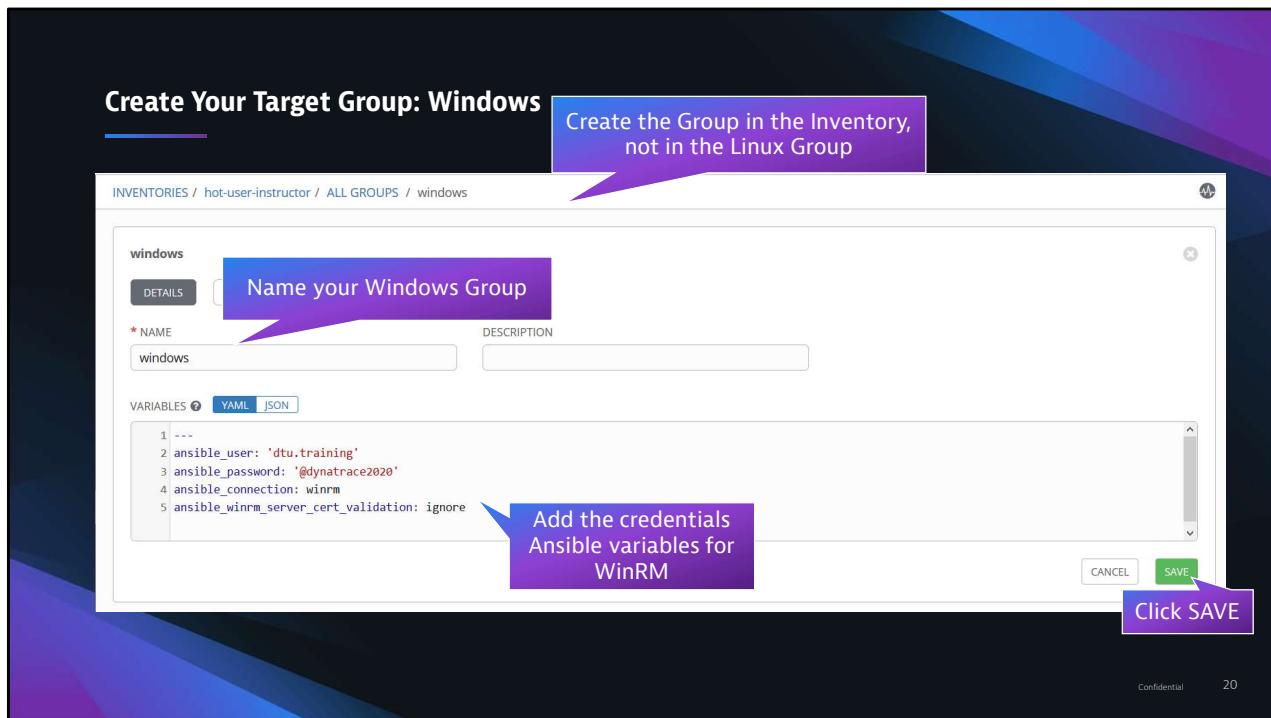
linux

ALL GROUPS ROOT GROUPS RUN COMMANDS +

Confidential 18

Managing Windows Hosts

- Ansible Tower can manage Windows hosts using WinRM
- Windows Remote Management (WinRM) is the Microsoft implementation of WS-Management Protocol, a standard Simple Object Access Protocol (SOAP)-based, firewall-friendly protocol that allows hardware and operating systems, from different vendors, to interoperate.
- The WinRM Python module must be installed on the Ansible Tower Control Node(s)
- WinRM must be set up on the target Windows hosts
 - https://docs.ansible.com/ansible/latest/user_guide/windows_setup.html#winrm-setup
 - WinRM has already been set up for the Windows hosts in this session
- Control Nodes will need remote network access to managed Windows hosts on TCP port 5986
- Password authentication is used to manage target Windows hosts in this session



```
ansible_user: 'dtu.training'
```

```
ansible_password: '@dynatrace2020'
```

```
ansible_connection: winrm # used to tell Ansible Tower to manage this host with WinRM  
ansible_winrm_server_cert_validation: ignore # used to tell Ansible Tower to ignore SSL  
certificate warnings
```

Do not copy the comments.

These variables will be passed/used by all hosts belonging to this group

Add Your Target Hosts: Windows

The screenshot shows the Ansible Inventory Manager interface. The URL in the browser is `INVENTORIES / hot-inv-instructor / ALL GROUPS / windows / ASSOCIATED HOSTS`. The main navigation bar has tabs for `DETAILS`, `GROUPS`, and `HOSTS`. The `HOSTS` tab is currently selected. Below the tabs is a search bar with a magnifying glass icon and a key icon. To the right of the search bar are buttons for `SEARCH` and `KEY`. The main content area is titled `windows` and contains two columns: `HOSTS` and `DESCRIPTION`. At the bottom right of the content area is a green button with a plus sign and the text `Add a host`. A purple callout box with an arrow points to the `HOSTS` tab with the text `Switch to the HOSTS tab`. Another purple callout box with an arrow points to the green `+ Add a host` button with the text `Click the + to add a host`.

Confidential 21

Add Your Target Hosts: Windows

The screenshot shows a web-based interface for creating a new host in an Ansible inventory. The URL in the address bar is `INVENTORIES / hot-inv-instructor / ALL GROUPS / windows / ASSOCIATED HOSTS / CREATE HOST`. The main title is "Add Your Target Hosts: Windows".

The form has three tabs: "DETAILS" (selected), "FACTS", and "GROUPS". A purple callout box points to the "HOST NAME" input field, which contains "w.x.y.z". The input field is labeled "Enter the DNS host name or IP address of your Windows host".

Below the input fields are sections for "DESCRIPTION" (empty) and "VARIABLES" (YAML tab selected, showing a single variable "1").

At the bottom right are "CANCEL" and "SAVE" buttons. A purple callout box points to the "SAVE" button, with the text "Click SAVE".

At the bottom right of the page, there are links for "Confidential" and "22".

Add Your Target Hosts: Windows

INVENTORIES / hot-inv-instructor / ALL GROUPS / windows / ASSOCIATED HOSTS

windows

HOSTS

SEARCH

KEY

HOSTS ▲

DESCRIPTION ▲

ADD

Existing Host

New Host

Repeat this process and add the remaining Windows hosts you have been provided

Add a host

Confidential 23

Inventory Complete

The screenshot shows the Ansible Tower inventory interface for the 'hot-inv-instructor' inventory. The 'HOSTS' tab is selected. A purple callout box highlights the message: 'Validate that all (4) of your hosts are added to the Inventory'. The table lists five hosts:

HOSTS	DESCRIPTION	RELATED GROUPS	ACTIONS
35.161.215.215		linux	
35.35.76		linux	
Validate that all (4) of your hosts are added to the Inventory		windows	
		windows	
		linux	

ITEMS 1 - 5

Confidential

24

Ansible Tower: Credentials

Confidential 25

Credential: EC2-Credential

The screenshot shows a web-based interface for creating a new credential. The title bar says "Credential: EC2-Credential". The main form is titled "ec2-credential". It has tabs for "DETAILS" (selected) and "PERI".
DETAILS Section:

- * NAME:
- DESCRIPTION:
- * CREDENTIAL TYPE: (with a dropdown arrow pointing to "Choose 'Machine' Credential Type")
- ORGANIZATION:

TYPE DETAILS Section:

USERNAME: <input type="text" value="dtu.training"/>	PASSWORD: <input type="text"/> (with a dropdown arrow pointing to "Enter the Linux host credentials you have been provided")	<input type="checkbox"/> Prompt on launch
	ENCRYPTED: <input type="checkbox"/>	(eye icon)

Buttons:
Click SAVE

Confidential 26

Custom Credential Types

- Ansible allows you to define a custom credential type in a standard format using a YAML/JSON-like definition, allowing the assignment of new credential types to jobs and inventory updates.
 - For example, you could create a custom credential type that injects an API token for a third-party web service into an environment variable, which your playbook or custom inventory script could consume.
 - In this session, we will use a custom credential type 'dt-api-token' that will be used to pass our Dynatrace API token to our Playbooks
- Custom credential types are created by system administrators and can be used by Organization administrators
- Using an Ansible custom credential type can be more secure than passing tokens in plain text

Custom Credential Types

CREDENTIAL TYPES / dt-api-token

dt-api-token

* NAME: dt-api-token

DESCRIPTION: Dynatrace API Token

INPUT CONFIGURATION YAML JSON

```
1 fields:
2   - id: api_token
3   type: string
4   label: api-token
5   secret: true
6 required: .....
```

Credential contains a single string field

INJECTOR CONFIGURATION YAML JSON

```
1 extra_vars:
2   dt_api_token: '{{ api_token }}'
3
```

The string value will be injected as an extra variable 'dt_api_token'

CANCEL SAVE

Confidential

28

Credential: Dynatrace Install Token

The screenshot shows a 'Create Credential' form for a 'Dynatrace Install Token'. The form has tabs for 'DETAILS' (selected) and 'PERMISSIONS'. The 'NAME' field is set to 'dynatrace-install-token', 'DESCRIPTION' is empty, and the 'ORGANIZATION' is 'hot-org-instructor'. The 'CREDENTIAL TYPE' is set to 'dt-api-token', and the 'TYPE DETAILS' section shows an 'API-TOKEN' field containing a redacted string. The right side of the form has 'CANCEL' and 'SAVE' buttons. A large purple callout box highlights the 'NAME' field with the text 'Name your Credential 'dynatrace-install-token''. Another purple callout box highlights the 'CREDENTIAL TYPE' dropdown with the text 'Choose 'dt-api-token' Credential Type'. A third purple callout box highlights the 'ORGANIZATION' field with the text 'Assign your Credential to your Organization'. A fourth purple callout box highlights the 'API-TOKEN' field with the text 'Enter the Dynatrace Install token string you have been provided'. A fifth purple callout box highlights the 'SAVE' button with the text 'Click SAVE'.

CREDENTIALS / CREATE CREDENTIAL

NEW CREDENTIAL

DETAILS PERMIS

Name your Credential 'dynatrace-install-token'

* NAME

DESCRIPTION

ORGANIZATION

* CREDENTIAL TYPE

Choose 'dt-api-token' Credential Type

TYPE DETAILS

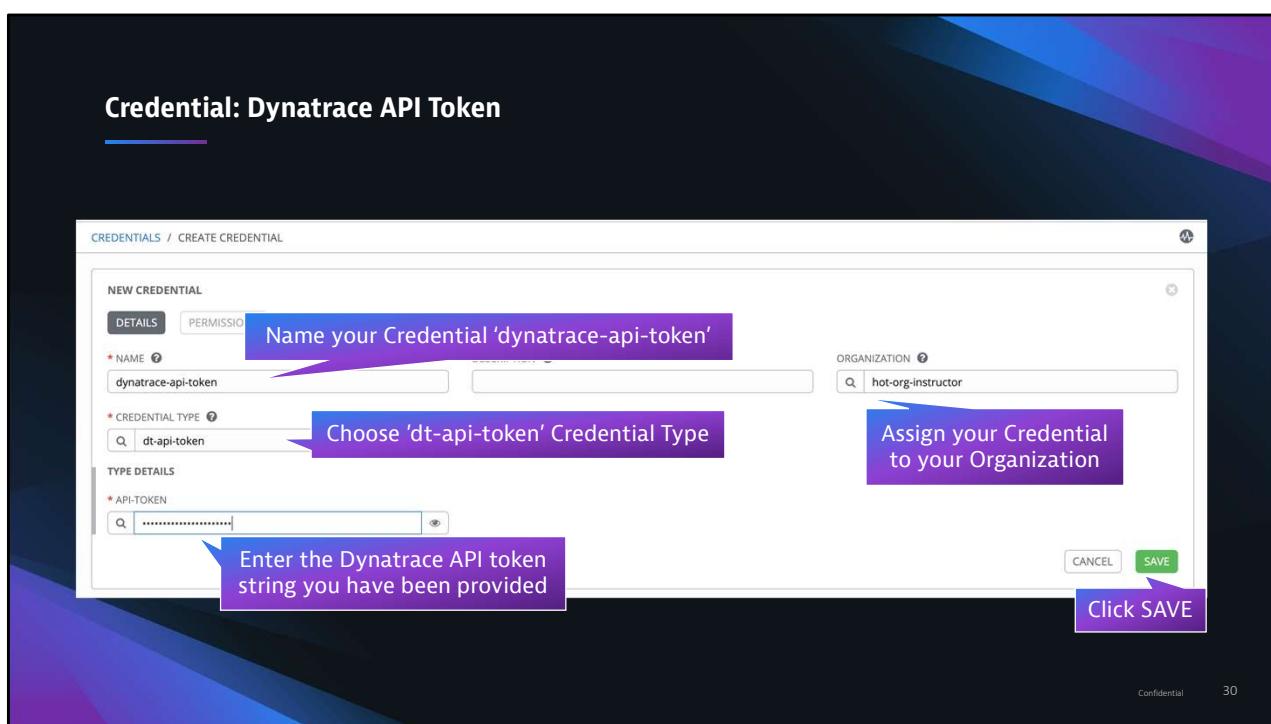
* API-TOKEN

Enter the Dynatrace Install token string you have been provided

CANCEL SAVE

Click SAVE

Credential: Dynatrace API Token



Confidential

30

Credential: SMTP Email

NEW CREDENTIAL

DETAILS **PERMISSION**

Name your Credential 'smtp-aws'

* NAME DESCRIPTION

ORGANIZATION

* CREDENTIAL TYPE

Choose 'smtp-email' Credential Type

TYPE DETAILS

* SMTP HOST * SMTP PORT * SMTP USER NAME

* SMTP PASSWORD

Enter the SMTP details you have been provided

CANCEL **SAVE**

Assign your Credential to your Organization

Click SAVE

Credentials Complete

The screenshot shows a list of credentials in a dark-themed interface. At the top left, it says "CREDENTIALS 4". Below that is a search bar and a "KEY" button. A green "+" button is in the top right corner. The main area has a table with columns: NAME, KIND, OWNERS, and ACTIONS. The entries are:

NAME	KIND	OWNERS	ACTIONS
dynatrace-api-token	dt-api-token	admin, hot-org-instructor	
dynatrace-install-token	dt-api-token	admin, hot-org-instructor	
ec2-credential	Machine	admin, hot-org-instructor	
smtp-aws	smtp-email	admin, hot-org-instructor	

At the bottom right of the table, it says "ITEMS 1-4".

Ansible Tower: Job Templates

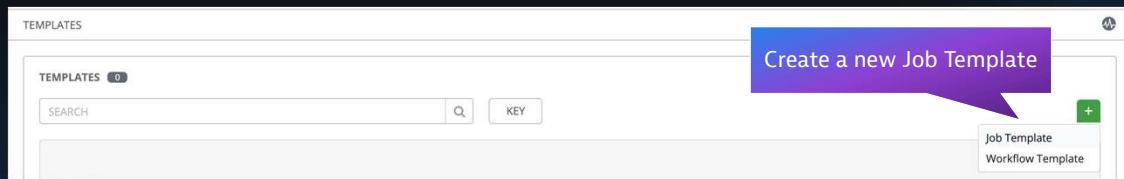
Session Automation Goals

- OneAgent Deployment
 - Deploy the Dynatrace OneAgent to target host(s) and assign a Host Group
- RUM Web Application + Detection Rule via Dynatrace API
 - Create a RUM Web Application and a URL-based detection rule using the Dynatrace API
- Management Zone via Dynatrace API
 - Create a Management Zone containing Host Group entities using the Dynatrace API
- Alerting Profile via Dynatrace API
 - Create an Alerting Profile & Notification for the Management Zone entities using the Dynatrace API
- Dashboard via Dynatrace API
 - Clone an existing Dashboard template using the Dynatrace API

OneAgent Deployment

Confidential 35

OneAgent Deployment: Linux



OneAgent Deployment: Linux

NEW JOB TEMPLATE

DETAILS PERMISSION

Name your Template based on your participant identifier

* NAME: instructor-dt-oneagent-install-linux

DESCRIPTION:

* INVENTORY: hot-inv-instructor

PROMPT ON LAUNCH:

* PROJECT: hot-proj-instructor

PROMPT ON LAUNCH:

* JOB TYPE: Run

PROMPT ON LAUNCH:

* PLAYBOOK: dt-oneagent-install-linux.yml

PROMPT ON LAUNCH:

CREDENTIALS: ec2-credential, dynatrace-install-token

PROMPT ON LAUNCH:

FORKS: 0

LIMIT:

PROMPT ON LAUNCH:

VERBOSITY: 0 (Normal)

PROMPT ON LAUNCH:

SKIP TAGS:

PROMPT ON LAUNCH:

LABELS:

JOB SLICING: 1

PROMPT ON LAUNCH:

TIMEOUT: 0

PROMPT ON LAUNCH:

SHOW CHANGES:

PROMPT ON LAUNCH:

OPTIONS

ENABLE PRIVILEGE ESCALATION

ENABLE PROVISIONING CALLBACKS

ENABLE WEBHOOK

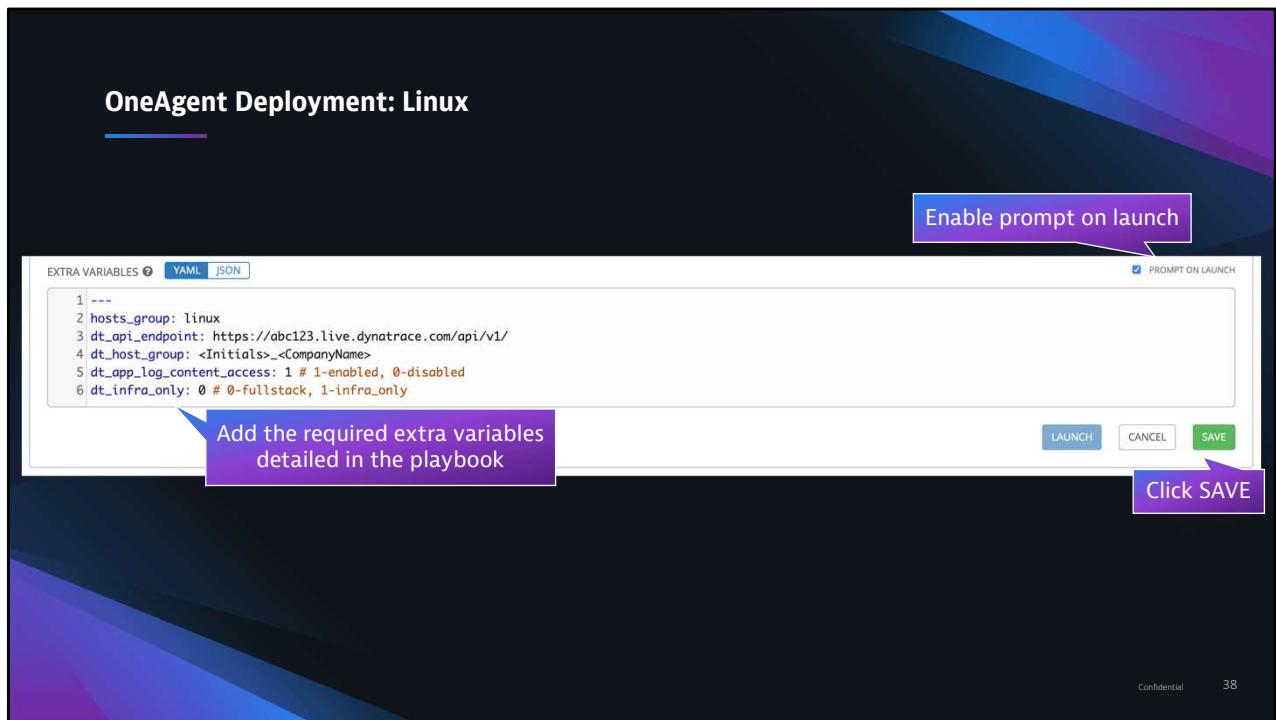
ENABLE CONCURRENT JOBS

ENABLE FACT CACHE

Select the Linux install playbook

Select your Inventory, Project, EC2 Credential, and Dynatrace Install Token

Confidential 37



```
---  
hosts_group:  
dt_api_endpoint:  
dt_host_group:  
dt_app_log_content_access: 1 # 1-enabled, 0-disabled  
dt_infra_only: 0 # 0-fullstack, 1-infra_only
```

OneAgent Deployment: Linux

INSTRUCTOR-DT-ONEAGENT-INSTALL-LINUX

OTHER PROMPTS PREVIEW

JOB TYPE Playbook Run

CREDENTIAL dynatrace-install-token ↗ ec2-credential

INVENTORY hot-inv-instructor

VERBOSITY 0 (Normal)

SHOW CHANGES OFF

EXTRA VARIABLES

```
1 ---  
2 hosts_group: linux  
3 dt_api_endpoint: https://abc123.live.dynatrace.com/api/v1/  
4 dt_host_group: <Initials>_<CompanyName>  
5 dt_app_log_content_access: 1 # 1-enabled, 0-disabled  
6 dt_infra_only: 0 # 0-fullstack, 1-infra_only
```

CANCEL LAUNCH

Click LAUNCH

Confidential 39

OneAgent Deployment: Linux

The screenshot displays the Ansible Tower interface for a job titled "instructor-dt-oneagent-install-linux".

Job Details:

- STATUS: Successful
- STARTED: 1/18/2020 5:24:41 PM
- FINISHED: 1/18/2020 5:25:20 PM
- JOB TEMPLATE: instructor-dt-oneagent-install-linux
- JOB TYPE: Run
- LAUNCHED BY: hot-user-instructor
- INVENTORY: hot-inv-instructor
- PROJECT: hot-proj-instructor
- REVISION: 40cb3ab
- PLAYBOOK: dt-oneagent-install-linux.yml
- CREDENTIAL: dynatrace-install-token, ec2-credential
- ENVIRONMENT: /var/lib/awx/venv/ansible
- EXECUTION NODE: localhost
- INSTANCE GROUP: tower
- EXTRA VARIABLES: YAML, JSON

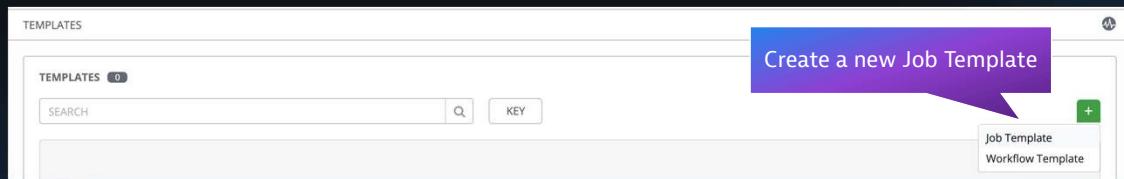
Playbook Output:

```
instructor-dt-oneagent-install-linux
PLAYS 0 TASKS 6 HOSTS 3 ELAPSED 00:00:38
SEARCH
PLAY RECAP
  35.161.215.215 : ok=5    changed=3    unreachable=0    failed=0    skipped=0
  44.225.35.76   : ok=5    changed=3    unreachable=0    failed=0    skipped=0
  54.68.143.241 : ok=5    changed=3    unreachable=0    failed=0    skipped=0
```

A purple callout bubble points to the play recap section with the text: "Validate successful execution on all Linux hosts".

40

OneAgent Deployment: Windows



OneAgent Deployment: Windows

NEW JOB TEMPLATE

DETAILS PERMISSIONS

Name your Template based on your participant identifier

* NAME: instructor-dt-oneagent-install-windows

DESCRIPTION:

* INVENTORY: hot-inv-instructor

PROMPT ON LAUNCH:

* PROJECT: hot-proj-instructor

PROMPT ON LAUNCH:

CREDENTIALS: ec2-credential, dynatrace-install-token

PROMPT ON LAUNCH:

FORKS: 0

PROMPT ON LAUNCH:

* VERBOSITY: 0 (Normal)

LABELS:

TIMEOUT: 0

SHOW CHANGES:

PROMPT ON LAUNCH:

* JOB TYPE: Run

ON LAUNCH:

* PLAYBOOK: dt-oneagent-install-windows.yml

PROMPT ON LAUNCH:

LIMIT:

PROMPT ON LAUNCH:

SKIP TAGS:

PROMPT ON LAUNCH:

JOB SLICING: 1

PROMPT ON LAUNCH:

OPTIONS

ENABLE PRIVILEGE ESCALATION

ENABLE PROVISIONING CALLBACKS

ENABLE WEBHOOK

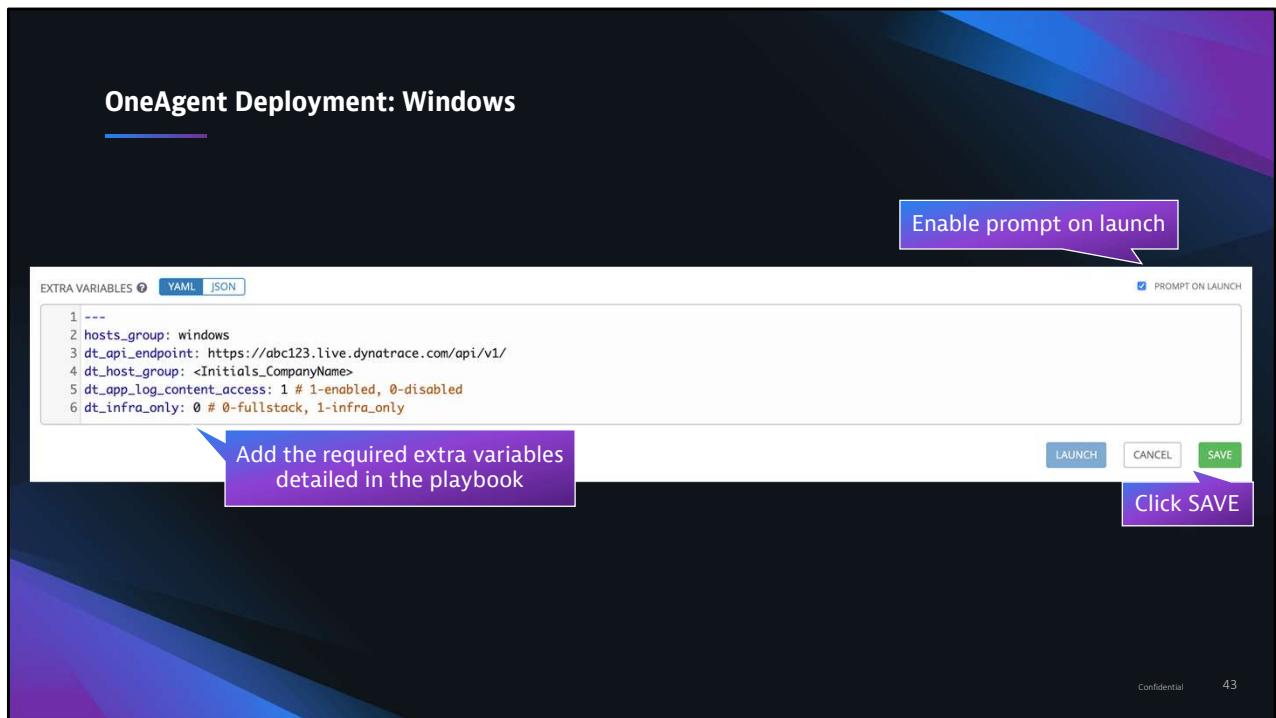
ENABLE CONCURRENT JOBS

ENABLE FACT CACHE

Confidential 42

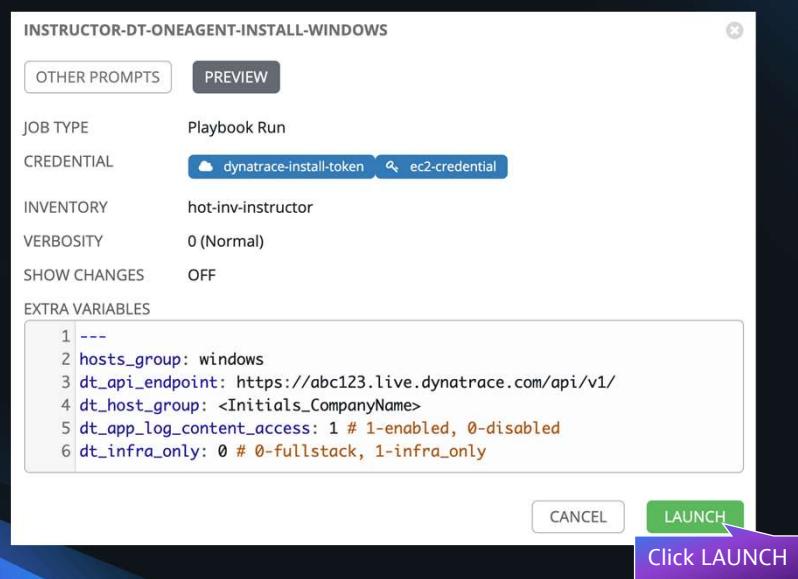
Select the Windows install playbook

Select your Inventory, Project, EC2 Credential, and Dynatrace Install Token



```
---
hosts_group: windows
dt_api_endpoint: https://abc123.live.dynatrace.com/api/v1/
dt_host_group: <Initials_CompanyName>
dt_app_log_content_access: 1 # 1-enabled, 0-disabled
dt_infra_only: 0 # 0-fullstack, 1-infra_only
```

OneAgent Deployment: Windows



Confidential

44

OneAgent Deployment: Windows

The screenshot shows the Ansible web interface for a job titled "instructor-dt-oneagent-install-windows".

Job Details:

- STATUS: Successful
- STARTED: 1/18/2020 5:34:09 PM
- FINISHED: 1/18/2020 5:35:02 PM
- JOB TEMPLATE: instructor-dt-oneagent-install-windows
- JOB TYPE: Run
- LAUNCHED BY: hot-user-instructor
- INVENTORY: hot-inv-instructor
- PROJECT: hot-proj-instructor
- REVISION: 40cb3ab
- PLAYBOOK: dt-oneagent-install-windows.yml
- CREDENTIAL: dynatrace-install-token, ec2-credential
- ENVIRONMENT: /var/lib/awx/venv/ansible
- EXECUTION NODE: localhost
- INSTANCE GROUP: tower

EXTRA VARIABLES:

```
2 dt_app_log_content_access: 1
3 dt_host_group: ABC_MyCompany
4 dt_infra_only: 0
5 hosts_group: windows
6
```

Playbook Log:

```
instructor-dt-oneagent-install-windows
PLAYS 1 TASKS 7 HOSTS 2 ELAPSED 00:00:52
SEARCH
17 TASK [download oneagent install file] *****
18 changed: [44.232.37.39]
19 changed: [44.226.4.8]
20
21 TASK [install: execute oneagent install file] *****
22 changed: [44.226.4.8]
23 changed: [44.232.37.39]
24
25 TASK [update: uninstall existing oneagent package] *****
26 skipping: [44.232.37.39]
27 skipping: [44.226.4.8]
28
29 TASK [update: execute oneagent install file] *****
30 skipping: [44.232.37.39]
31 skipping: [44.226.4.8]
32
33 PLAY RECAP *****
34 44.226.4.8 : ok=5    changed=2    unreachable=0    failed=0    skipped=2
35 44.232.37.39 : ok=5    changed=2    unreachable=0    failed=0    skipped=0
36
```

Validation Note: Validate successful execution on all Windows hosts

45

(Re)start Application Processes

Starting easyTravel on Linux

```
Last login: Mon Jan  6 20:35:37 UTC 2020 on pts/0
Last failed login: Mon Jan  6 20:45:01 UTC 2020 from 49.88
There were 15 failed login attempts since the last success.
[root@ip-10-0-0-181 ~]# cd /opt/easyTravel-Docker/
[root@ip-10-0-0-181 easyTravel-Docker]# docker-compose up -d
mongodb is up-to-date
backend is up-to-date
frontend is up-to-date
www is up-to-date
loadgen is up-to-date
[root@ip-10-0-0-181 easyTravel-Docker]# docker-compose down
Stopping loadgen ... done
Stopping www ... done
Stopping frontend ... done
Stopping backend ... done
Stopping mongodb ... done
Removing loadgen ... done
Removing www ... done
Removing frontend ... done
Removing backend ... done
Removing mongodb ... done
[root@ip-10-0-0-181 easyTravel-Docker]# docker-compose up -d
Creating mongodb ... done
Creating backend ... done
Creating frontend ... done
Creating www ... done
Creating loadgen ... done
[root@ip-10-0-0-181 easyTravel-Docker]#
```

Switch to root user

Switch to the easyTravel-Docker directory

Start easyTravel containers

(optional) Stop containers

(optional) Start containers

Become root user:

sudo su -

Switch to easyTravel-Docker directory:

cd /opt/easyTravel-Docker

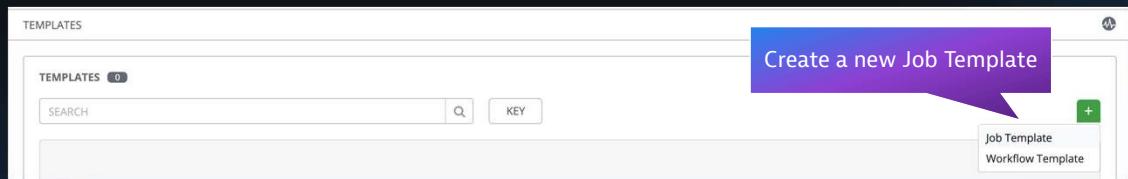
Start easyTravel containers:

docker-compose up -d

(optional) Stop easyTravel containers:

docker-compose down

Start (or Restart) easyTravel on Linux



Confidential 48

Start (or Restart) easyTravel on Linux

Start (or Restart) easyTravel on Linux

NEW JOB TEMPLATE

Name your Template based on your participant identifier

* NAME: instructor-dt-easytravel-start-linux

DESCRIPTION:

* INVENTORY: hot-inv-instructor

PROMPT ON LAUNCH:

* PROJECT: hot-proj-instructor

PROMPT ON LAUNCH:

CREDENTIALS:

PROMPT ON LAUNCH:

FORKS: 0

* VERBOSITY: 0 (Normal)

PROMPT ON LAUNCH:

LABELS:

INSTANCE GROUPS:

PROMPT ON LAUNCH:

TIMEOUT: 0

SHOW CHANGES:

PROMPT ON LAUNCH:

Select the easyTravel start Linux playbook

* JOB TYPE: Run

PROMPT ON LAUNCH:

* PLAYBOOK: dt-easytravel-start-linux.yml

PROMPT ON LAUNCH:

LIMIT:

Skip Tags:

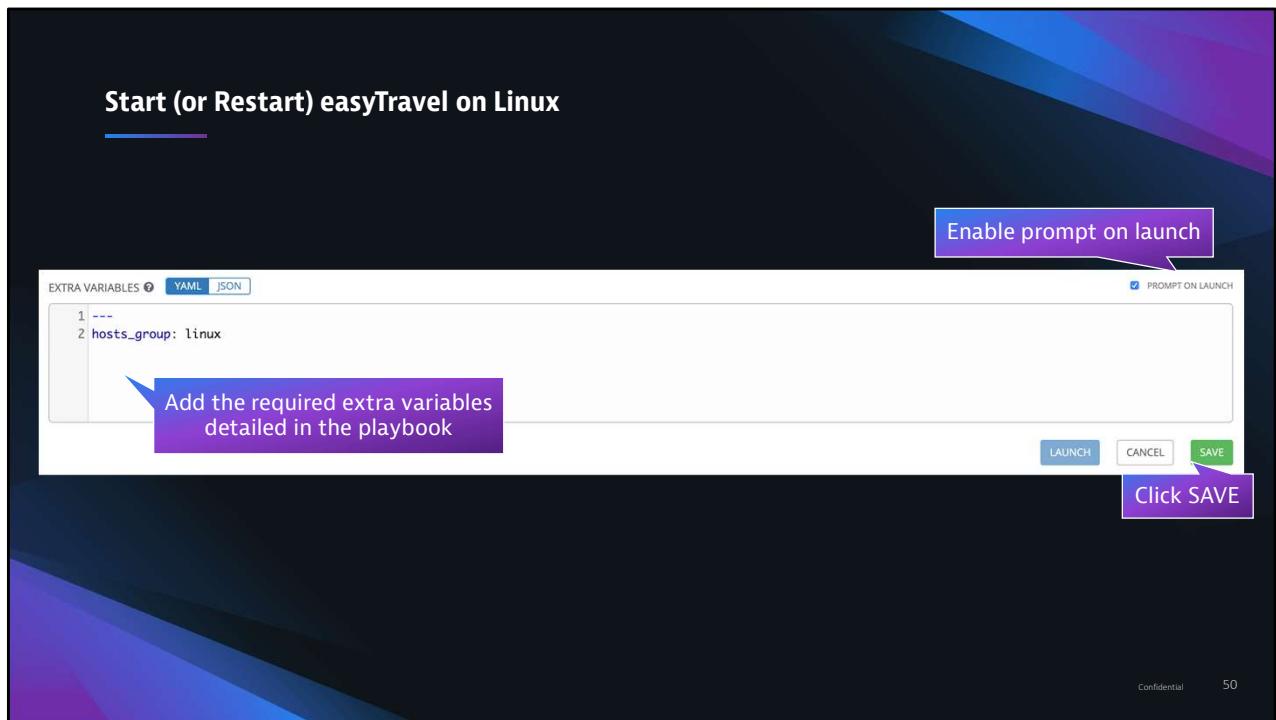
PROMPT ON LAUNCH:

Job Slicing:

1

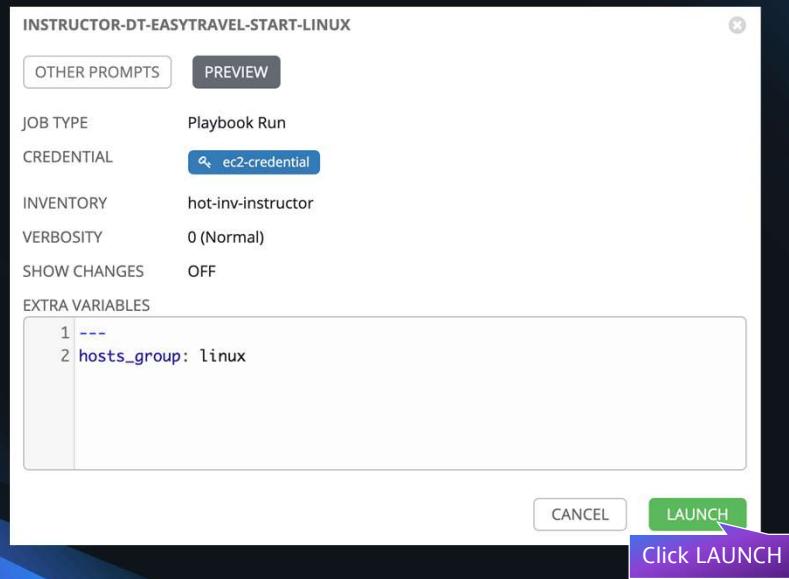
OPTIONS:

- ENABLE PRIVILEGE ESCALATION
- ENABLE PROVISIONING CALLBACKS
- ENABLE WEBHOOK
- ENABLE CONCURRENT JOBS
- ENABLE FACT CACHE

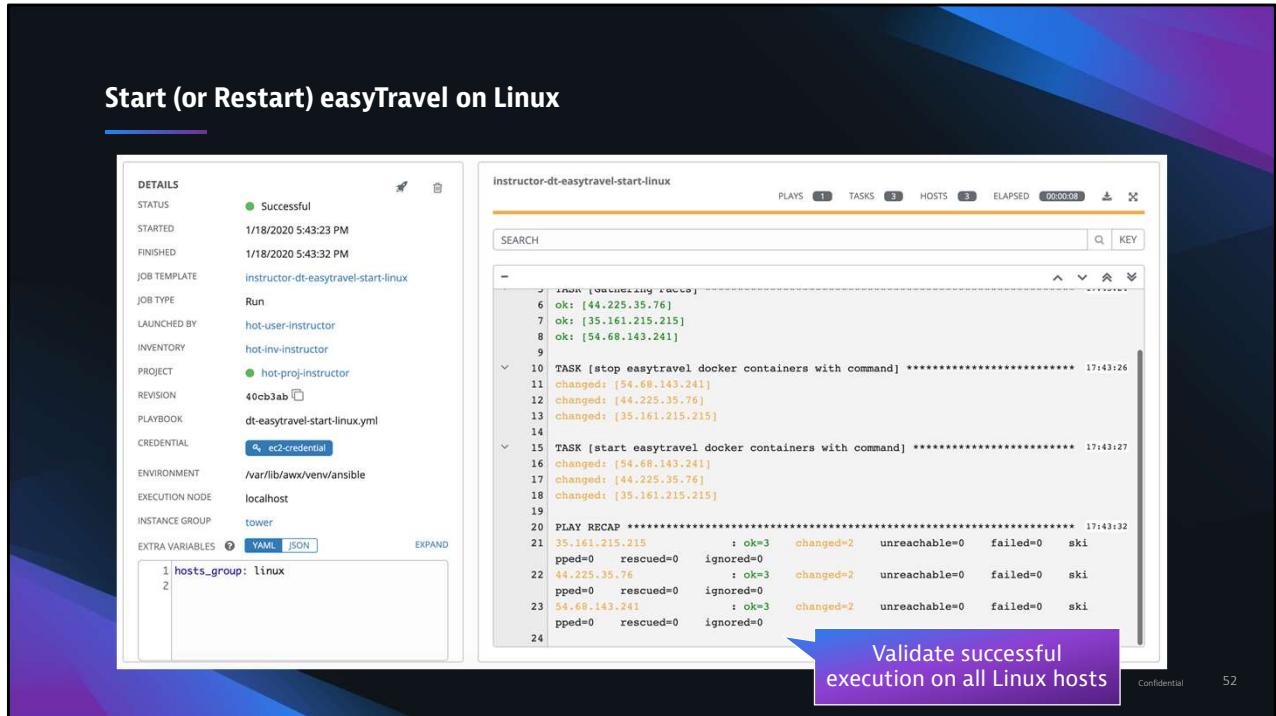


hosts_group:

Start (or Restart) easyTravel on Linux



Start (or Restart) easyTravel on Linux



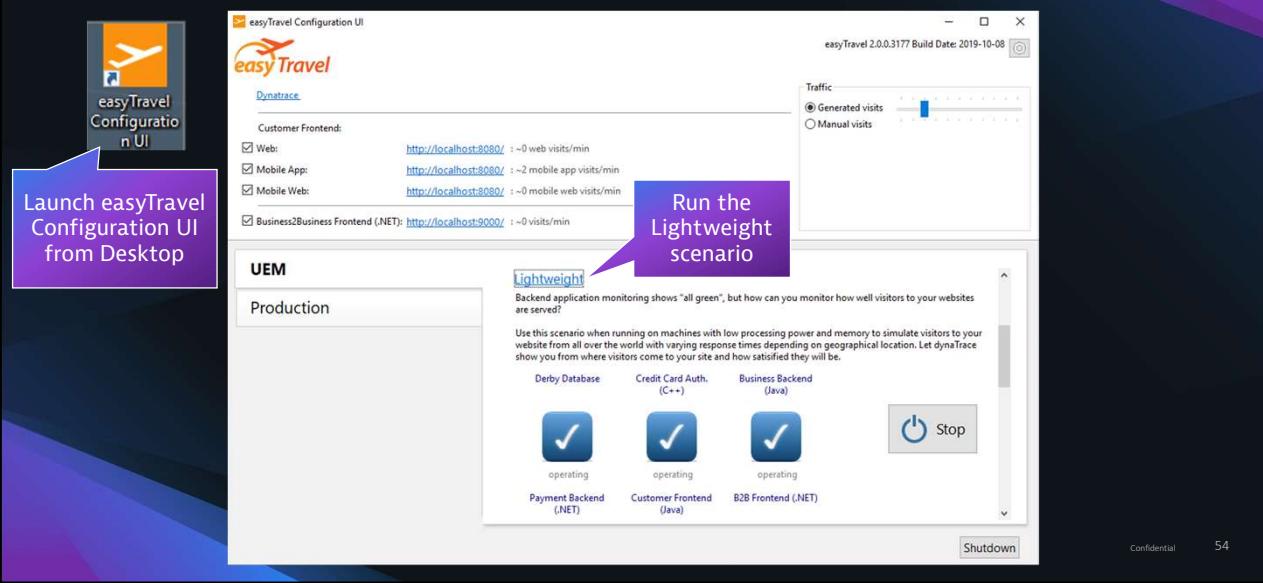
Starting easyTravel on Linux

Access easyTravel from
your browser on port 80

The screenshot shows a web browser window displaying the easyTravel website. The URL in the address bar is 44.229.124.145. The page features a header with the easyTravel logo and links for Home, Special Offers, About, Contact, Terms of Use, Privacy Policy, and Login. A purple speech bubble on the right side of the header contains the text "Access easyTravel from your browser on port 80". Below the header, there's a large image of a tropical beach with palm trees and a "Travel to Hawaii" banner. To the right of the banner is a photo of a smiling couple. The main search form is titled "Your Journey" and includes fields for Trip Destination, From Date, and To Date, with a "Search" button. Below the search form is a section titled "Recommendations" featuring two travel deals: "Davey - Bahia Blanca" for \$1110.30 and "Silver Star - VILLA CANALES" for \$265.80. Each deal includes a small image, a brief description, and a "Book Now" button.

Confidential 53

Starting easyTravel on Windows



Starting easyTravel on Windows

Access easyTravel from your browser on port 8080

44.227.211.234:8080

The screenshot shows the easyTravel website running on a Windows system. The header includes the easyTravel logo, navigation links for Home, Special Offers, About, Contact, Terms of Use, Privacy Policy, and Login, along with social media icons. A banner on the left features a beach scene with a starfish and the text "Travel to Paris". A banner on the right features a couple in swimwear. Below these are sections for "Your Journey" (with fields for Trip Destination, From Date, To Date, and a Search button) and "Recommendations" (listing two travel packages: Brasstown - Marina and Bloomville - La Rue). Each recommendation includes a thumbnail image, the destination name, the price (\$954.80 or \$1611.30), a brief description, and a "Book Now" button.

Your Journey

Trip Destination

From Date

To Date

Search

Recommendations

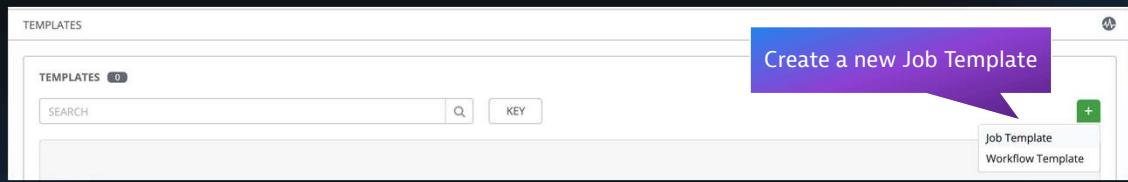
Brasstown - Marina \$ 954.80
Dai Reo
If you wish to stay in a hotel that has friendly staff and an inviting ambience that reminds you of home, then head to the Grand Hotel.
Mar 10 - Mar 17 [Book Now](#)

Bloomville - La Rue \$ 1611.30
If you wish to stay in a hotel that has friendly staff and an inviting ambience that reminds you of home, then head to the Grand Hotel.
Jan 11 - Jan 16 [Book Now](#)

Confidential 55

RUM Web Application

RUM Web Application + Detection Rule via Dynatrace API



Confidential 57

RUM Web Application + Detection Rule via Dynatrace API

NEW JOB TEMPLATE

DETAILS PERMISSIONS

Name your Template based on your participant identifier

* NAME: instructor-dt-api-application-config

DESCRIPTION:

* JOB TYPE: Run

* INVENTORY: hot-inv-instructor

PROMPT ON LAUNCH:

* PROJECT: hot-proj-instructor

CREDENTIALS: ec2-credential, dynatrace-api-token

PROMPT ON LAUNCH:

FORKS: 0

LIMIT: 0

PROMPT ON LAUNCH:

PLAYBOOK: dt-api-application-config.yml

Skip Tags:

PROMPT ON LAUNCH:

Job Slicing: 1

PROMPT ON LAUNCH:

Labels:

PROMPT ON LAUNCH:

TIMEOUT: 0

SHOW CHANGES:

PROMPT ON LAUNCH:

OPTIONS

ENABLE PRIVILEGE ESCALATION

ENABLE PROVISIONING CALLBACKS

ENABLE WEBHOOK

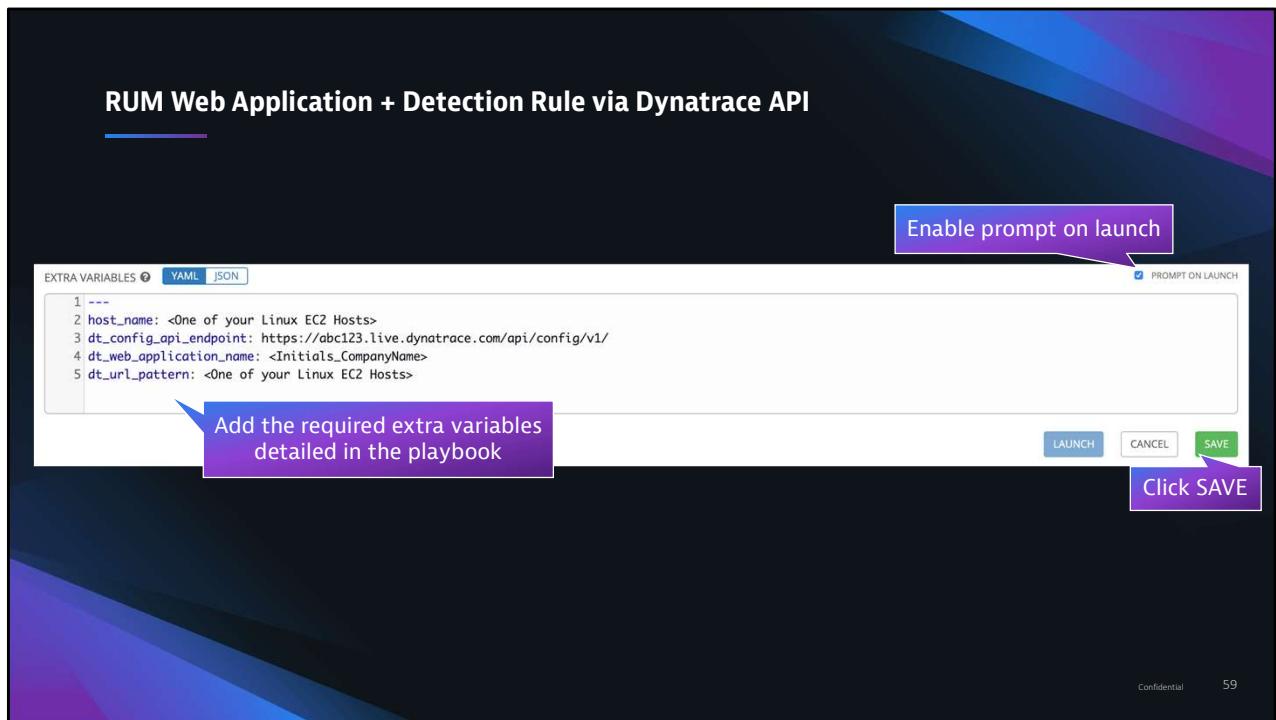
ENABLE CONCURRENT JOBS

ENABLE FACT CACHE

Select the application config playbook

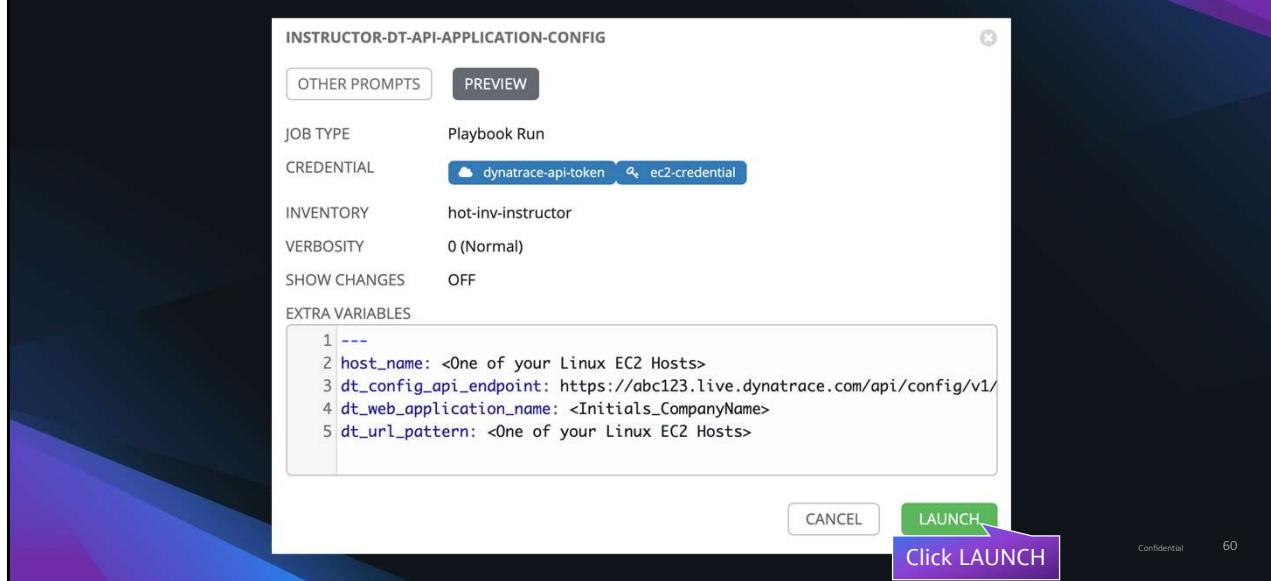
Select your Inventory, Project, EC2 Credential, and Dynatrace API Token

58



```
host_name: <One of your Linux EC2 Hosts>
dt_config_api_endpoint: https://abc123.live.dynatrace.com/api/config/v1/
dt_web_application_name: <Initials_CompanyName>
dt_url_pattern: <One of your Linux EC2 Hosts>
```

RUM Web Application + Detection Rule via Dynatrace API



Confidential

60

RUM Web Application + Detection Rule via Dynatrace API

The screenshot shows the Ansible Playbook execution interface. On the left, the 'DETAILS' panel displays the job status as 'Successful', with execution times from 1/19/2020 2:53:44 PM to 1/19/2020 2:53:52 PM. It also lists the job template ('instructor-dt-api-application-config'), job type ('Run'), launched by ('hot-user-instructor'), inventory ('hot-inv-instructor'), project ('hot-proj-instructor'), revision ('40cb3ab'), playbook ('dt-api-application-config.yml'), credential ('dynatrace-api-token' and 'ec2-credential'), environment ('/var/lib/awx/venv/ansible'), execution node ('localhost'), instance group ('tower'), and extra variables ('YAML' and 'JSON'). A purple callout points to the log output, which shows the creation of a detection rule payload and its output.

instructor-dt-api-application-config

PLAYS 0 TASKS 11 HOSTS 1 ELAPSED 00:00:08

SEARCH KEY

21: OK: [44.225.35.76]

22:

23: TASK [obtain web application id from json object] **** 14:53:50

24: ok: [44.225.35.76]

25:

26: TASK [validate application detection rule payload] **** 14:53:50

27: ok: [44.225.35.76]

28:

29: TASK [create application detection rule] **** 14:53:51

30: ok: [44.225.35.76]

31:

32: TASK [set web application id artifact] ** 14:53:52

33: ok: [44.225.35.76]

34:

35: TASK [output web application id] *** 14:53:52

36: ok: [44.225.35.76] => {

37: "msg": "APPLICATION-8B65341EB7E0B22D"

38: }

39:

Document web application id for future use

Validate successful execution

Confidential 61

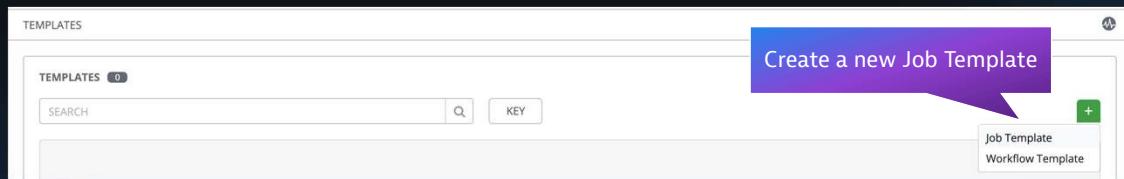


Management Zone

Confidential

62

Management Zone via Dynatrace API



Confidential 63

Management Zone via Dynatrace API

NEW JOB TEMPLATE

DETAILS **PERMISSIONS**

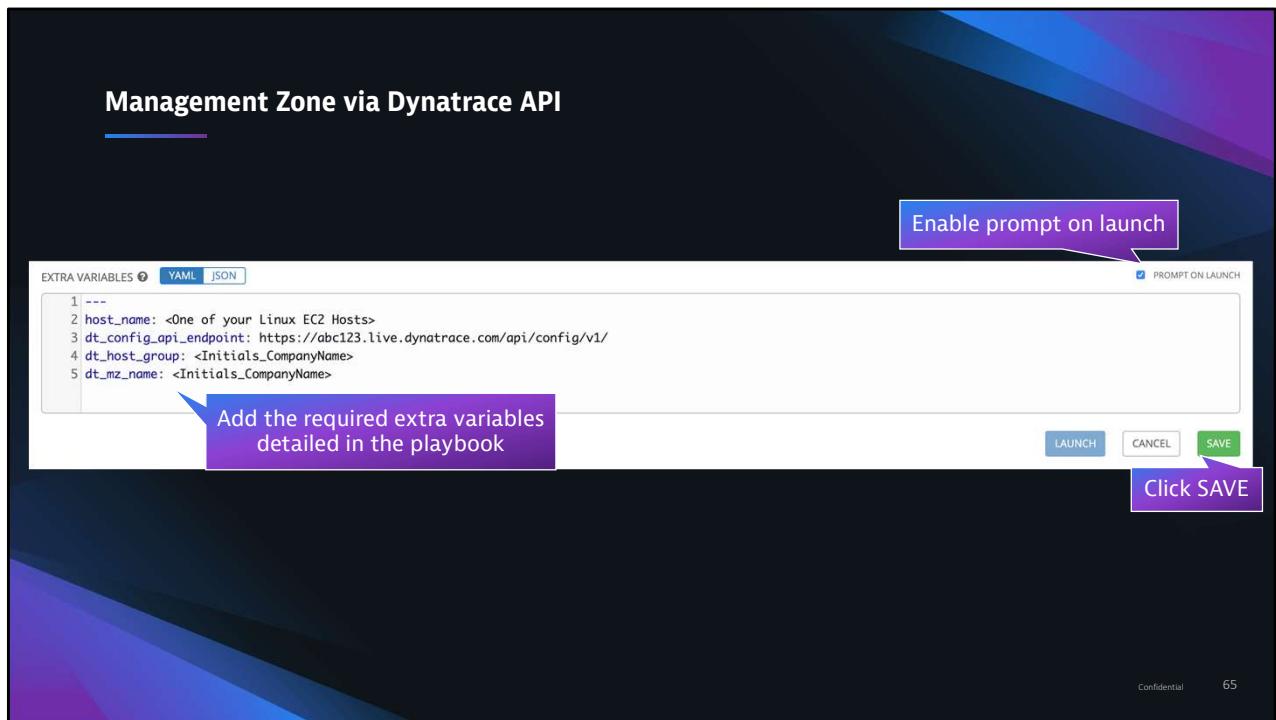
Name your Template based on your participant identifier

* NAME instructor-dt-api-management-zone	DESCRIPTION	* JOB TYPE Run
* INVENTORY hot-inv-instructor	PROMPT ON LAUNCH	* PROJECT hot-proj-instructor
CREDENTIALS ec2-credential, dynatrace-api-token	PROMPT ON LAUNCH	FORKS 0
* VERBOSITY 0 (Normal)	PROMPT ON LAUNCH	LIMIT PROMPT ON LAUNCH
LABELS	SKIP TAGS PROMPT ON LAUNCH	JOB SLICING 1
TIMEOUT 0	SHOW CHANGES PROMPT ON LAUNCH	OPTIONS
<input type="checkbox"/> ENABLE PRIVILEGE ESCALATION <input type="checkbox"/> ENABLE PROVISIONING CALLBACKS <input type="checkbox"/> ENABLE WEBHOOK <input type="checkbox"/> ENABLE CONCURRENT JOBS <input type="checkbox"/> ENABLE FACT CACHE		

Select the management zone playbook

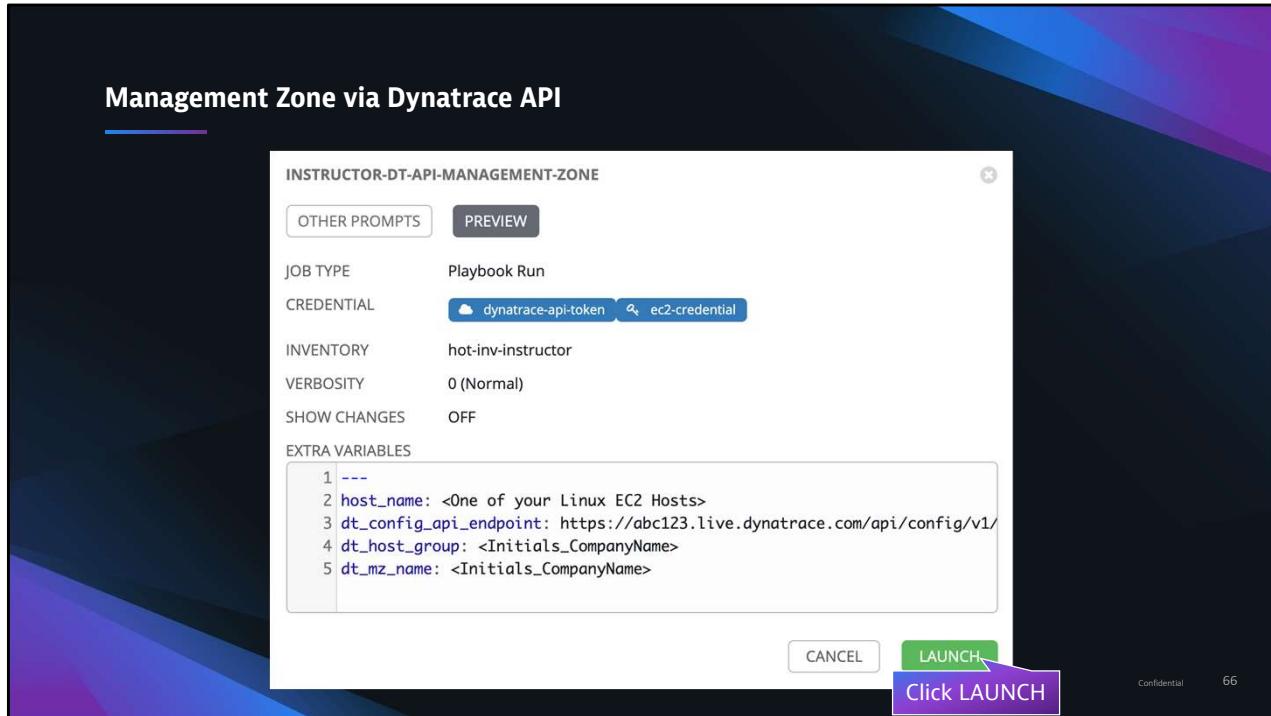
Select your Inventory, Project, EC2 Credential, and Dynatrace API Token

Confidential 64



```
---  
host_name: <One of your Linux EC2 Hosts>  
dt_config_api_endpoint: https://abc123.live.dynatrace.com/api/config/v1/  
dt_host_group: <Initials_CompanyName>  
dt_mz_name: <Initials_CompanyName>
```

Management Zone via Dynatrace API



Confidential

66

Management Zone via Dynatrace API

The screenshot shows the Ansible Playbook execution interface. On the left, the 'DETAILS' panel displays job information:

- STATUS: Successful
- STARTED: 1/19/2020 3:05:10 PM
- FINISHED: 1/19/2020 3:05:15 PM
- JOB TEMPLATE: instructor-dt-api-management-zone
- JOB TYPE: Run
- LAUNCHED BY: hot-user-instructor
- INVENTORY: hot-inv-instructor
- PROJECT: hot-proj-instructor
- REVISION: 40cb3ab
- PLAYBOOK: dt-api-management-zone.yml
- CREDENTIAL: [dynatrace-api-token](#), [ec2-credential](#)
- ENVIRONMENT: /var/lib/awx/venv/ansible
- EXECUTION NODE: localhost
- INSTANCE GROUP: tower
- EXTRA VARIABLES: [YAML](#), [JSON](#)

On the right, the 'instructor-dt-api-management-zone' log pane shows the playbook execution details:

```
PLAYS 1 TASKS 6 HOSTS 1 ELAPSED 00:00:05
SEARCH
1 OK! [44.225.35.76]
2
3
4
5
6
7
8 TASK [generate management zone 64 bit id] *****
9 ok: [44.225.35.76]
10
11 TASK [validate management zone 64 bit id is available] *****
12 ok: [44.225.35.76]
13
14 TASK [validate management zone payload] *****
15 ok: [44.225.35.76]
16
17 TASK [create management zone] *****
18 ok: [44.225.35.76]
19
20 TASK [output management zone id] *****
21 ok: [44.225.35.76] => {
22     "msg": "177494441883105950"
23 }
```

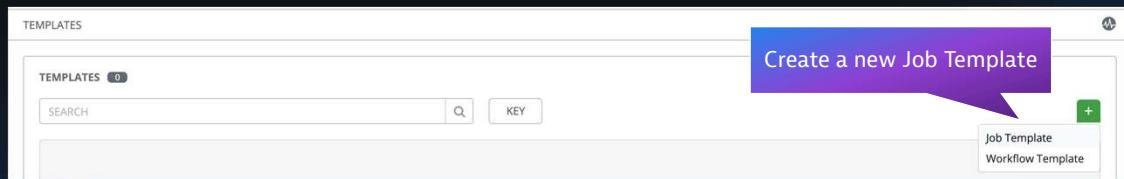
Annotations highlight specific log entries:

- A purple callout points to the line 'ok: [44.225.35.76]' with the text 'Document management zone id for future use'.
- A purple callout points to the line 'ok: [44.225.35.76]' with the text 'Validate successful execution'.

At the bottom right, the text 'Confidential' and '67' are visible.

Alerting Profile

Alerting Profile via Dynatrace API



Alerting Profile via Dynatrace API

NEW JOB TEMPLATE

DETAILS PERMISSIONS

Name your Template based on your participant identifier

* NAME: instructor-dt-api-alerting-profile

DESCRIPTION:

* INVENTORY: hot-inv-instructor

PROMPT ON LAUNCH:

* PROJECT: hot-proj-instructor

PROMPT ON LAUNCH:

CREDENTIALS: ec2-credential, dynatrace-api-token

PROMPT ON LAUNCH:

FORKS: 0

PROMPT ON LAUNCH:

* VERBOSITY: 0 (Normal)

PROMPT ON LAUNCH:

LABELS:

TIMEOUT: 0

PROMPT ON LAUNCH:

SHOW CHANGES:

PROMPT ON LAUNCH:

* JOB TYPE: Run

PROMPT ON LAUNCH:

* PLAYBOOK: dt-api-alerting-profile.yml

PROMPT ON LAUNCH:

LIMIT:

PROMPT ON LAUNCH:

SKIP TAGS:

PROMPT ON LAUNCH:

JOB SLICING: 1

PROMPT ON LAUNCH:

OPTIONS

ENABLE PRIVILEGE ESCALATION

ENABLE PROVISIONING CALLBACKS

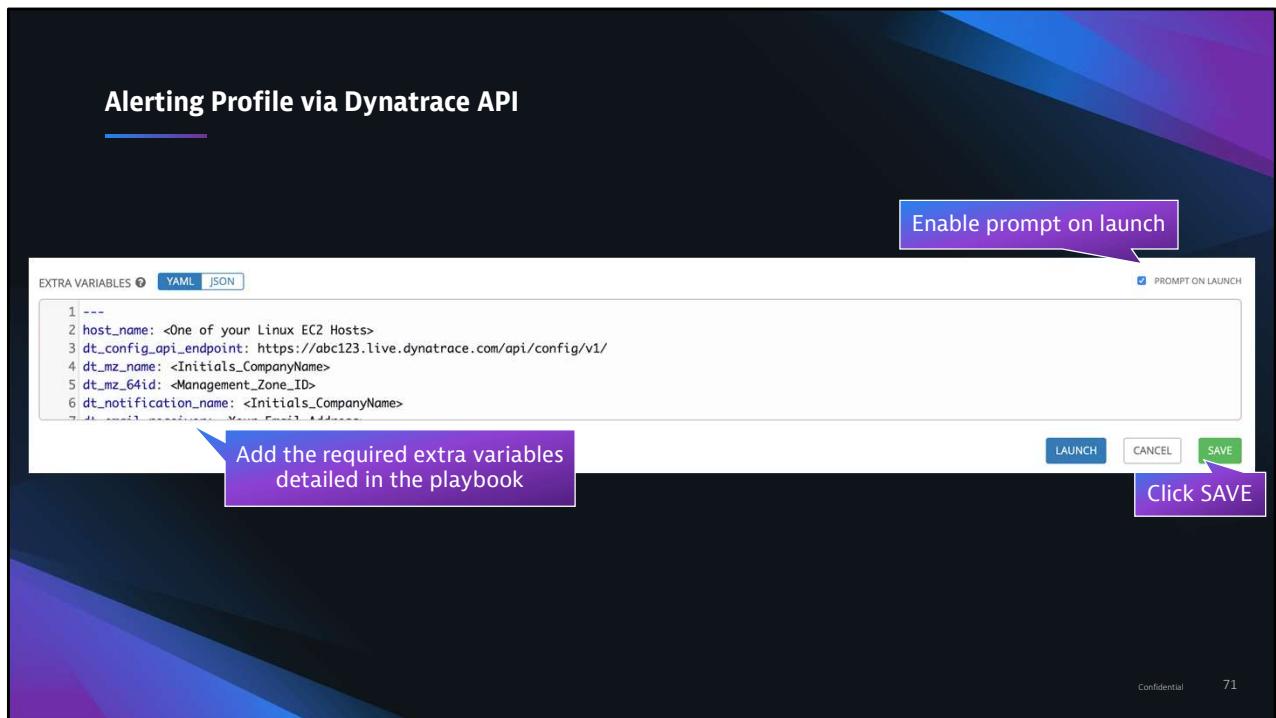
ENABLE WEBHOOK

ENABLE CONCURRENT JOBS

ENABLE FACT CACHE

Select the alerting profile playbook

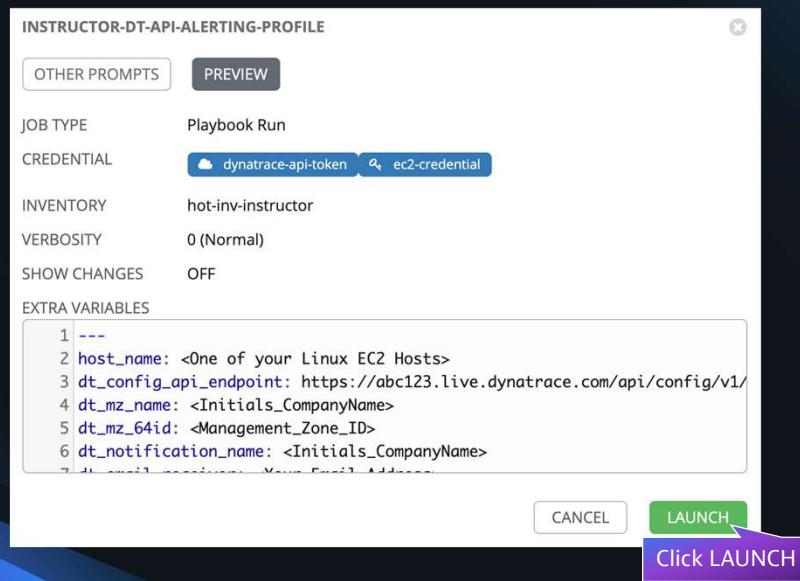
Select your Inventory, Project, EC2 Credential, and Dynatrace API Token



```

---
host_name: <One of your Linux EC2 Hosts>
dt_config_api_endpoint: https://abc123.live.dynatrace.com/api/config/v1/
dt_mz_name: <Initials_CompanyName>
dt_mz_64id: <Management_Zone_ID>
dt_notification_name: <Initials_CompanyName>
dt_email_receiver: <Your_Email_Address>
  
```

Alerting Profile via Dynatrace API



Confidential

72

Alerting Profile via Dynatrace API

Alerting Profile via Dynatrace API

DETAILS

STATUS	Successful
STARTED	1/19/2020 3:19:02 PM
FINISHED	1/19/2020 3:19:12 PM
JOB TEMPLATE	instructor-dt-api-alerting-profile
JOB TYPE	Run
LAUNCHED BY	hot-user-instructor
INVENTORY	hot-inv-instructor
PROJECT	hot-proj-instructor
REVISION	40cb3ab
PLAYBOOK	dt-api-alerting-profile.yml
CREDENTIAL	dynatrace-api-token ec2-credential
ENVIRONMENT	/var/lib/awx/venv/ansible
EXECUTION NODE	localhost
INSTANCE GROUP	tower
EXTRA VARIABLES	

EXPAND

instructor-dt-api-alerting-profile

PLAYS 1 TASKS 17 HOSTS 1 ELAPSED 00:00:09

SEARCH

```
41 TASK [create notification rule]
42 ok: [44.225.35.76]
43
44 TASK [convert response to json object] *****
45 ok: [44.225.35.76]
46
47 TASK [obtain notification uuid from json object] *****
48 ok: [44.225.35.76]
49
50 TASK [output alerting profile uuid] *****
51 ok: [44.225.35.76] => {
52     "msg": "3c0c401b-3e4f-504c-a5b6-978c6397a681"
53 }
54
55 TASK [output notification uid] *****
56 ok: [44.225.35.76] => {
57     "msg": "734c6b25-e9c8-53a2-873b-28bd8eae3a8f"
58 }
59
```

Document alerting profile id and notification id for future use

Validate successful execution

Dashboard

Confidential 74

 Amazon Web Services – Email Address Verification Request in region US East (N. Virginia)

Amazon Web Services <no-reply-aws@amazon.com>

Tuesday, December 24, 2019 at 1:29 PM

Pope-Cruz, Anthony

[Show Details](#)

Dear Amazon Web Services Customer,

We have received a request to authorize this email address for use with Amazon SES and Amazon Pinpoint in region US East (N. Virginia). following URL to confirm that you are authorized to use this email address:

[https://nam02.safelinks.protection.outlook.com/?url=https%3A%2F%2Femail-verification.us-east-1.amazonaws.com%2F%3FContext%3D087532670362Date%3D20191224T182953Z%26Identity.IdentityName%3Danthonyc_pope-cruz%2540dynatrace.com%26X-Amz-Algorithm%3DAWS4-HMAC-SHA256%26Identity.IdentityName%3Dhost%26X-Amz-Credential%3DAKIAJR7UVJEP5GNMLX6A%252F20191224X252Fus-east-1%252Fses%252Faws4_request%26Operation%3DConfirmSignature%3D9949880329ba6f23ec788d42279ac0e840fa050e5fc3f267cc723dd0ce1715&data=02%7C01%7Canthonyc_pope-cruz%40dynatrace.com%7C7f844e81b7da4f8c158e08d7889f4600%7C70ebe3a35b30435d9d677716d74ca190%7C1%7C1%7C637128089975493097&sdata=Pv6L%](https://nam02.safelinks.protection.outlook.com/?url=https%3A%2F%2Femail-verification.us-east-1.amazonaws.com%2F%3FContext%3D087532670362Date%3D20191224T182953Z%26Identity.IdentityName%3Danthonyc_pope-cruz%2540dynatrace.com%26X-Amz-Algorithm%3DAWS4-HMAC-SHA256%26Identity.IdentityName%3Dhost%26X-Amz-Credential%3DAKIAJR7UVJEP5GNMLX6A%252F20191224X252Fus-east-1%252Fses%252Faws4_request%26Operation%3DConfirmSignature%3D9949880329ba6f23ec788d42279ac0e840fa050e5fc3f267cc723dd0ce1715&data=02%7C01%7Canthonyc_pope-cruz%40dynatrace.com%7C7f844e81b7da4f8c158e08d7889f4600%7C70ebe3a35b30435d9d677716d74ca190%7C1%7C1%7C637128089975493097&sdata=Pv6L%2B)

Your request will not be processed unless you confirm the address using this URL. This link expires 24 hours after your original verification.

If you did NOT request to verify this email address, do not click on the link. Please note that many times, the situation isn't a phish, use our service, or someone setting up email-sending capabilities on your behalf as part of a legitimate service, but without having fully understood what's happening. If you're still concerned, please forward this notification to aws-email-domain-verification@amazon.com and let us know in the forward that you did not request this verification.

To learn more about sending email from Amazon Web Services, please refer to the Amazon SES Developer Guide at [https://nam02.safelinks.protection.outlook.com/?url=http%3A%2F%2Fdocs.aws.amazon.com%2Fses%2Flatest%2FDeveloperGuide%2FWelcome.html&data=02%7C01%7Canthonyc_pope-cruz%40dynatrace.com%7C7f844e81b7da4f8c158e08d7889f4600%7C70ebe3a35b30435d9d677716d74ca190%7C1%7C1%7C637128089975493097&sdata=Ph3W%](https://nam02.safelinks.protection.outlook.com/?url=http%3A%2F%2Fdocs.aws.amazon.com%2Fses%2Flatest%2FDeveloperGuide%2FWelcome.html&data=02%7C01%7Canthonyc_pope-cruz%40dynatrace.com%7C7f844e81b7da4f8c158e08d7889f4600%7C70ebe3a35b30435d9d677716d74ca190%7C1%7C1%7C637128089975493097&sdata=Ph3W%2B) and Amazon Pinpoint Developer Guide at [https://nam02.safelinks.protection.outlook.com/?url=http%3A%2F%2Fdocs.aws.amazon.com%2Fpinpoint%2Flatest%2Fuserguide%2Fwelcome.html&data=02%7C01%7Canthonyc_pope-cruz%40dynatrace.com%7C7f844e81b7da4f8c158e08d7889f4600%7C70ebe3a35b30435d9d677716d74ca190%7C1%7C1%7C637128089975493097&sdata=6UHym%](https://nam02.safelinks.protection.outlook.com/?url=http%3A%2F%2Fdocs.aws.amazon.com%2Fpinpoint%2Flatest%2Fuserguide%2Fwelcome.html&data=02%7C01%7Canthonyc_pope-cruz%40dynatrace.com%7C7f844e81b7da4f8c158e08d7889f4600%7C70ebe3a35b30435d9d677716d74ca190%7C1%7C1%7C637128089975493097&sdata=6UHym%2B)

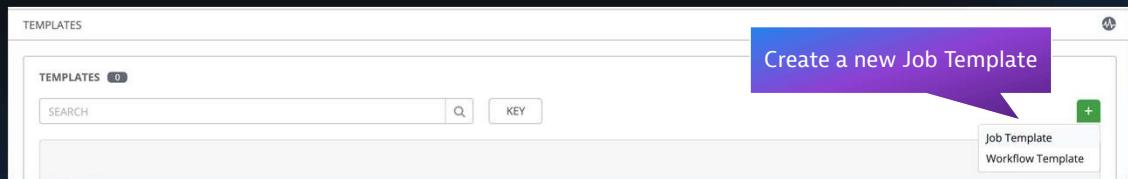
Sincerely,

The Amazon Web Services Team.

Complaint

75

Dashboard via Dynatrace API



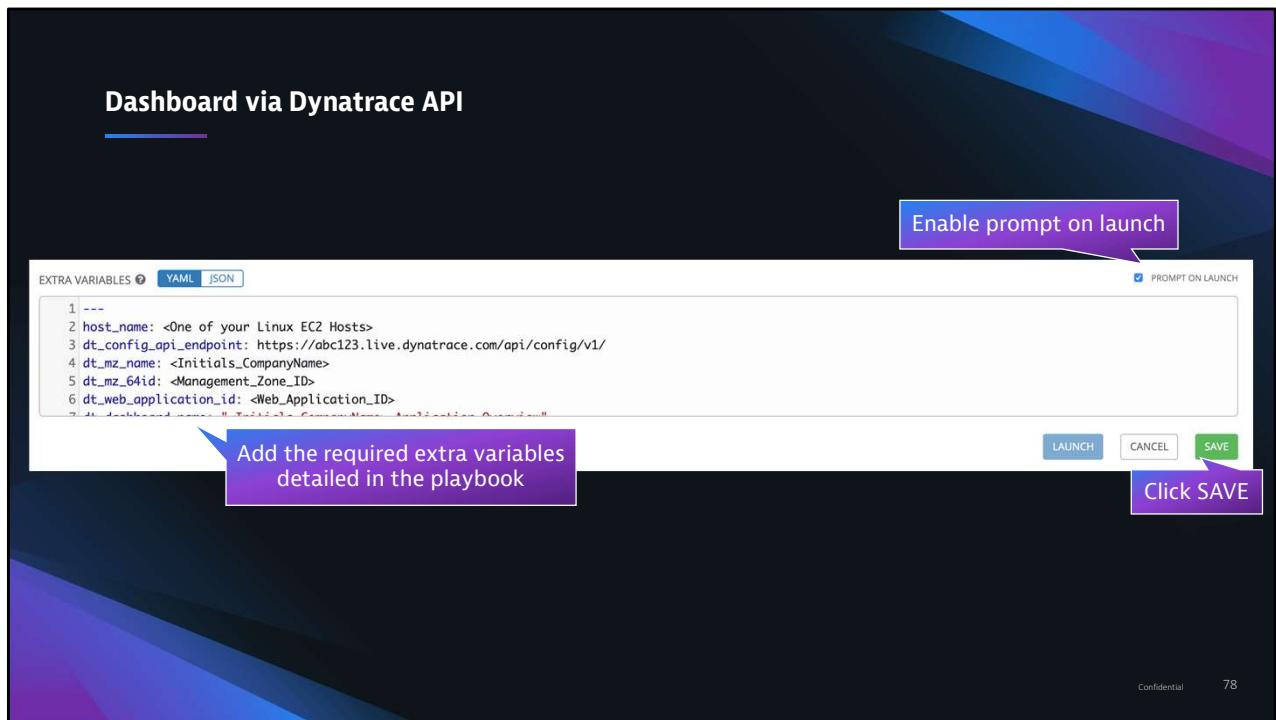
Dashboard via Dynatrace API

The screenshot shows a configuration interface for a dashboard clone. The main title is "Dashboard via Dynatrace API". The form has several sections:

- DETAILS** tab selected.
- PERMISSIONS** tab available.
- NAME**: instructor-dt-api-dashboard-clone
- DESCRIPTION**: (empty)
- INVENTORY**: hot-inv-instructor
- PROJECT**: hot-proj-instructor
- CREDENTIALS**:
 - dynatrace-api-token
 - ec2-credential
 - smtp-aws
- VERBOSITY**: 0 (Normal)
- LABELS**: (empty)
- TIMEOUT**: 0
- DESCRIPTION SURVEY**: (empty)
- JOB TYPE**: Run
- PLAYBOOK**: dt-api-dashboard-clone.yml
- LIMIT**: 0
- SKIP TAGS**: (empty)
- JOB SLICING**: 1
- OPTIONS**:
 - ENABLE PRIVILEGE ESCALATION
 - ENABLE PROVISIONING CALLBACKS
 - ENABLE WEBHOOK
 - ENABLE CONCURRENT JOBS
 - ENABLE FACT CACHE

Annotations highlight specific fields:

- A purple box labeled "Name your Template based on your participant identifier" covers the NAME field and the DESCRIPTION SURVEY area.
- A purple box labeled "Select the dashboard clone playbook" covers the PLAYBOOK field.
- A purple box labeled "Select your Inventory, Project, EC2 Credential, SMTP Credential and Dynatrace API Token" covers the CREDENTIALS section.



```

---
host_name: <One of your Linux EC2 Hosts>
dt_config_api_endpoint: https://abc123.live.dynatrace.com/api/config/v1/
dt_mz_name: <Initials_CompanyName>
dt_mz_64id: <Management_Zone_ID>
dt_web_application_id: <Web_Application_ID>
dt_dashboard_name: "<Initials_CompanyName> Application Overview"
dt_owner_id: <Your Email Address>
dt_clone_uuid: <Dashboard UUID You've Been Provided>
dt_base_url: https://abc123.live.dynatrace.com/
dt_email_receiver: <Your Email Address>

```

Dashboard via Dynatrace API

INSTRUCTOR-DT-API-DASHBOARD-CLONE

OTHER PROMPTS PREVIEW

JOB TYPE Playbook Run

CREDENTIAL **dynatrace-api-token** **ec2-credential** **smtp-aws**

INVENTORY hot-inv-instructor

VERBOSITY 0 (Normal)

SHOW CHANGES OFF

EXTRA VARIABLES

```
1 ---  
2 host_name: <One of your Linux EC2 Hosts>  
3 dt_config_api_endpoint: https://abc123.live.dynatrace.com/api/config/v1/  
4 dt_mz_name: <Initials_CompanyName>  
5 dt_mz_64id: <Management_Zone_ID>  
6 dt_web_application_id: <Web_Application_ID>
```

CANCEL LAUNCH

Click LAUNCH

Confidential

79

Dashboard via Dynatrace API

Dashboard via Dynatrace API

DETAILS

STATUS	Successful
STARTED	1/19/2020 3:42:49 PM
FINISHED	1/19/2020 3:43:03 PM
JOB TEMPLATE	instructor-dt-api-dashboard-clone
JOB TYPE	Run
LAUNCHED BY	hot-user-instructor
INVENTORY	hot-inv-instructor
PROJECT	hot-proj-instructor
REVISION	40cb5ab
PLAYBOOK	dt-api-dashboard-clone.yml
CREDENTIAL	dynatrace-api-token ec2-credential smtp-aws
ENVIRONMENT	/var/lib/awx/venv/ansible
EXECUTION NODE	localhost
INSTANCE GROUP	tower
EXTRA VARIABLES	YAML JSON

EXPAND

instructor-dt-api-dashboard-clone

PLAYS 1 TASKS 13 HOSTS 1 ELAPSED 00:00:13

SEARCH

```
-
  32 TASK [replace dashboard owner with dt_owner_id in json] *****
  33 ok: [44.225.35.76]
  34
  35 TASK [create new dashboard with modified json] *****
  36 [WARNING]: The value True (type bool) in a string field was converted to
  37 u'True' (type string). If this does not look like what you expect, quote the
  38 entire value to ensure it does not change.
  39
  40 ok: [44.225.35.76]
  41
  42 TASK [send email with dashboard link] ***
  43 ok: [44.225.35.76]
  44
  45 TASK [output dashboard uid] *****
  46 ok: [44.225.35.76] => {
  47   "msg": "9e9fea6f-7cc7-57eb-b195-492ccb8600d1"
  48 }
```

Document dashboard id for future use

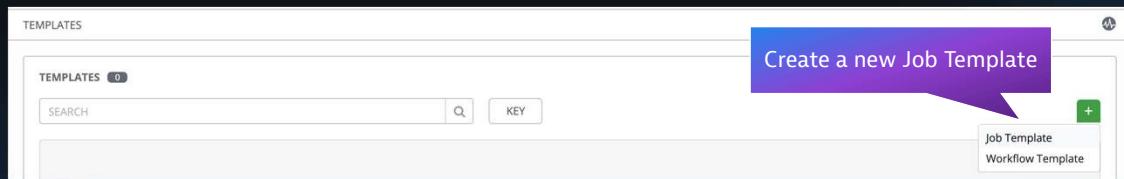
Validate successful execution

Ansible Tower: Workflow Template

Confidential

81

Workflow Template: Set Stats Job Template



Confidential

82

Workflow Template: Set Stats Job Template

NEW JOB TEMPLATE

DETAILS **PERMISSIONS** **COMPLETED JOBS**

Name your Template based on your participant identifier

* NAME <input type="text" value="instructor-dt-onboarding-workflow-set-stats"/>	DESCRIPTION <input type="text"/>	* JOB TYPE <input checked="" type="radio"/> Run	<small>PROMPT ON LAUNCH</small> <input type="checkbox"/>
* INVENTORY <input type="text" value="hot-inv-instructor"/>	<input type="checkbox"/> PROMPT ON LAUNCH	* PROJECT <input type="text" value="hot-proj-instructor"/>	<small>PROMPT ON LAUNCH</small> <input type="checkbox"/>
CREDENTIALS <input type="text" value="ec2-credential"/>	<input type="checkbox"/> PROMPT ON LAUNCH	FORKS <input type="text" value="0"/>	<small>PROMPT ON LAUNCH</small> <input type="checkbox"/>
* VERBOSITY <input type="text" value="0 (Normal)"/>	<input type="checkbox"/> PROMPT ON LAUNCH	INSTANCE GROUPS <input type="text" value=""/>	<small>PROMPT ON LAUNCH</small> <input type="checkbox"/>
LABELS <input type="text"/>	SHOW CHANGES <input type="checkbox"/>	JOB SLICING <input type="text" value="1"/>	<small>PROMPT ON LAUNCH</small> <input type="checkbox"/>
TIMEOUT <input type="text" value="0"/>	<input type="checkbox"/> PROMPT ON LAUNCH	OPTIONS <ul style="list-style-type: none"> <input type="checkbox"/> ENABLE PRIVILEGE ESCALATION <input type="checkbox"/> ENABLE PROVISIONING CALLBACKS <input type="checkbox"/> ENABLE WEBHOOK <input type="checkbox"/> ENABLE CONCURRENT JOBS <input type="checkbox"/> ENABLE FACT CACHE 	

Select the set stats playbook

*** PLAYBOOK**

LIMIT

SKIP TAGS

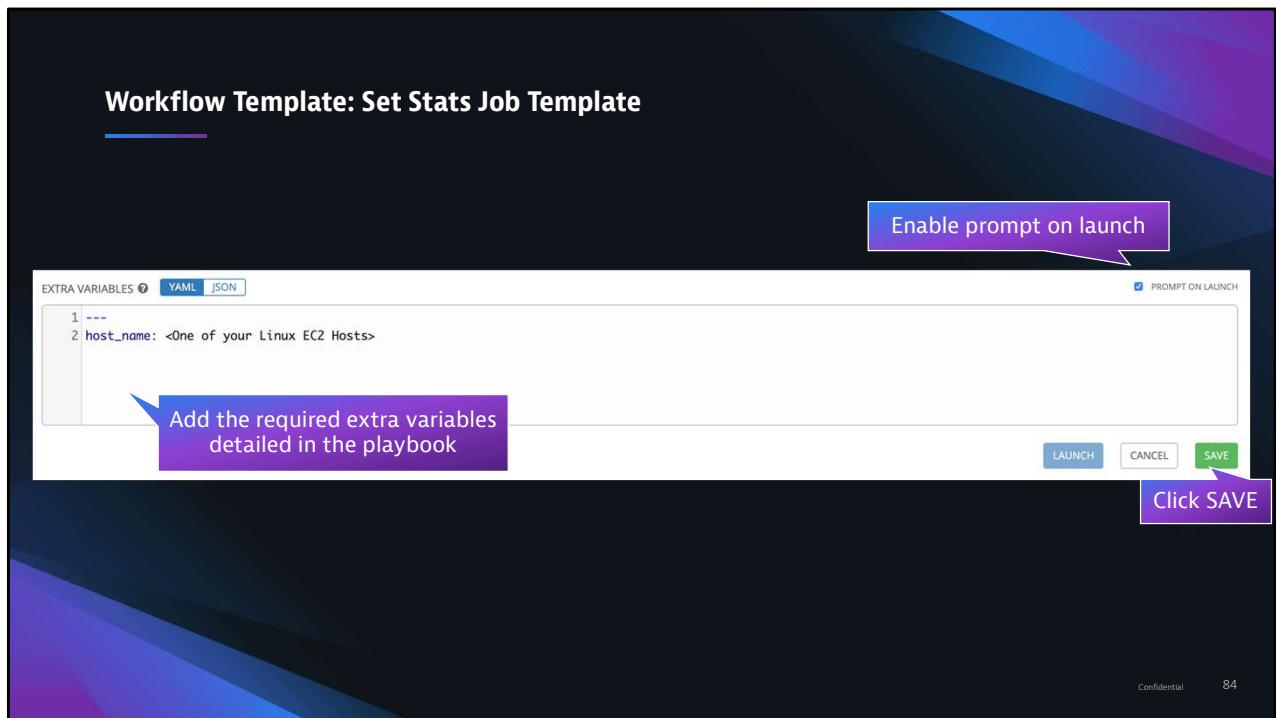
JOB SLICING

OPTIONS

- ENABLE PRIVILEGE ESCALATION
- ENABLE PROVISIONING CALLBACKS
- ENABLE WEBHOOK
- ENABLE CONCURRENT JOBS
- ENABLE FACT CACHE

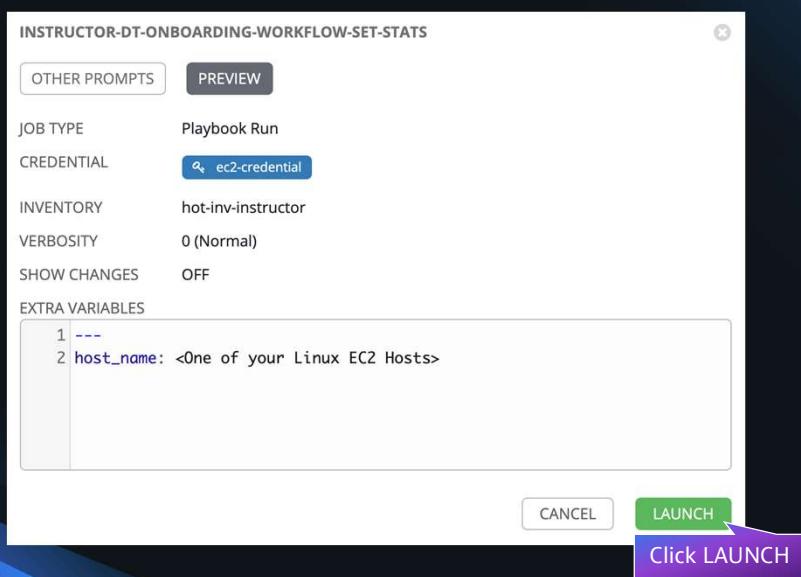
OPTIONS

- ENABLE PRIVILEGE ESCALATION
- ENABLE PROVISIONING CALLBACKS
- ENABLE WEBHOOK
- ENABLE CONCURRENT JOBS
- ENABLE FACT CACHE



```
host_name: <One of your Linux EC2 Hosts>
```

Workflow Template: Set Stats Job Template



Confidential

85

Workflow Template: Set Stats Job Template

DETAILS

STATUS	Successful
STARTED	1/19/2020 3:56:54 PM
FINISHED	1/19/2020 3:56:57 PM
JOB TEMPLATE	instructor-dt-onboarding-workflow-set-stats
JOB TYPE	Run
LAUNCHED BY	hot-user-instructor
INVENTORY	hot-inv-instructor
PROJECT	hot-proj-instructor
REVISION	40cb3ab
PLAYBOOK	dt-onboarding-workflow-set-stats.yml
CREDENTIAL	ec2-credential
ENVIRONMENT	/var/lib/awx/venv/ansible
EXECUTION NODE	localhost
INSTANCE GROUP	tower
EXTRA VARIABLES	YAML JSON

[EXPAND](#)

instructor-dt-onboarding-workflow-set-stats

PLAYS 0 TASKS 14 HOSTS 1 ELAPSED 00:00:03

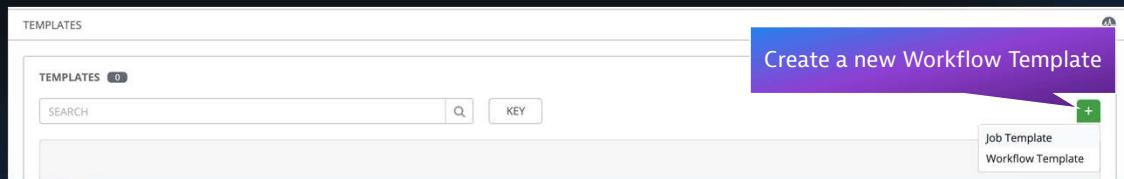
SEARCH Q KEY

29	TASK [set web application name] ****	15:56:57	
30	skipping: [44.225.35.76]		
31			
32	TASK [set dashboard name] ****	15:56:57	
33	skipping: [44.225.35.76]		
34			
35	TASK [set problem notification name] ****	15:56:57	
36	skipping: [44.225.35.76]		
37			
38	TASK [set web application url pattern] ****	15:56:57	
39	skipping: [44.225.35.76]		
40			
41	TASK [set notification email recipient] ****	15:56:57	
42	skipping: [44.225.35.76]		
43			
44	TASK [set dashboard owner] ****	15:56:57	
45	skipping: [44.225.35.76]		

Validate successful execution

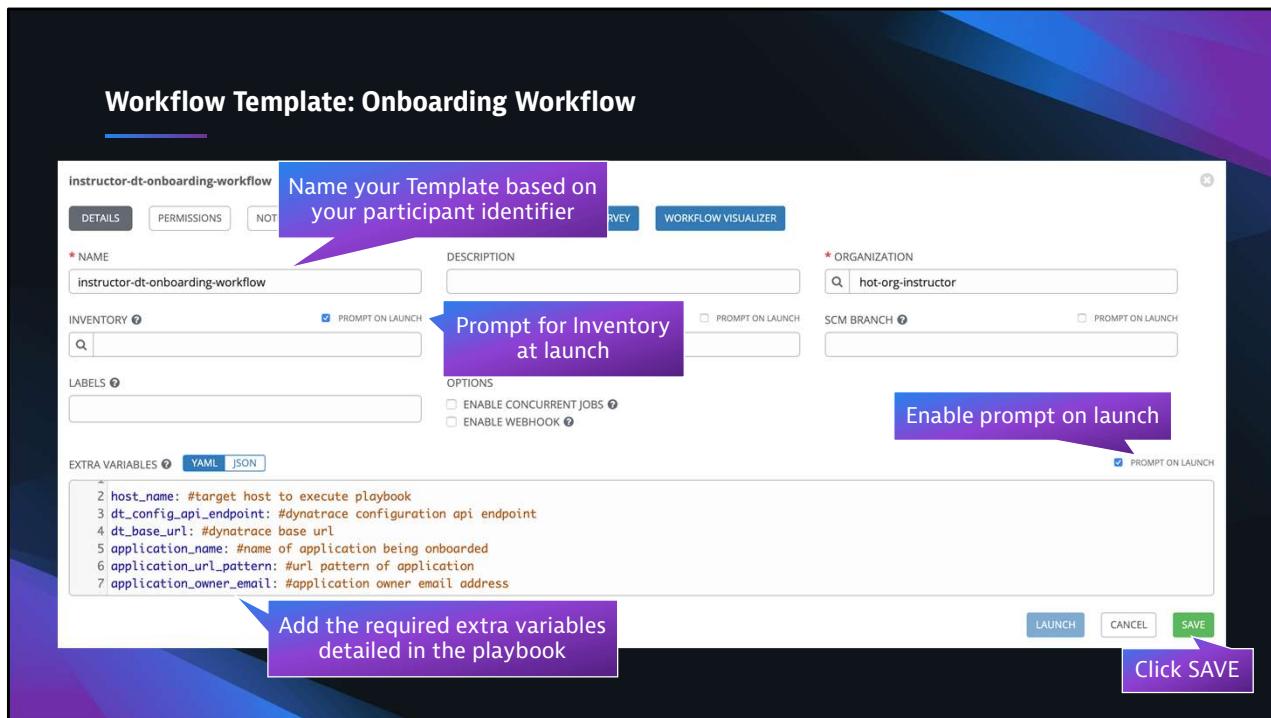
Confidential 86

Workflow Template: Onboarding Workflow



Confidential

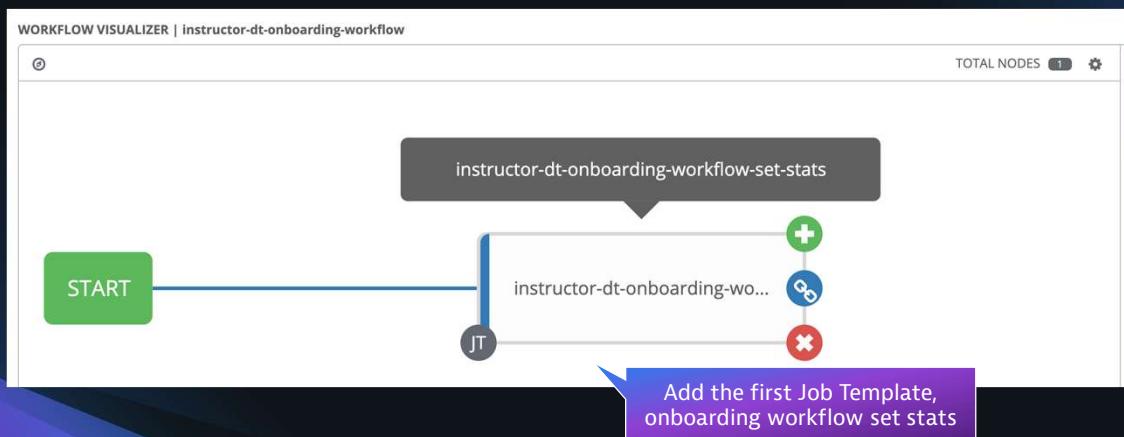
87



```

host_name: #target host to execute playbook
dt_config_api_endpoint: #dynatrace configuration api endpoint
dt_base_url: #dynatrace base url
application_name: #name of application being onboarded
application_url_pattern: #url pattern of application
application_owner_email: #application owner email address
dt_clone_uuid: #unique UUID id of the dynatrace dashboard to clone
    
```

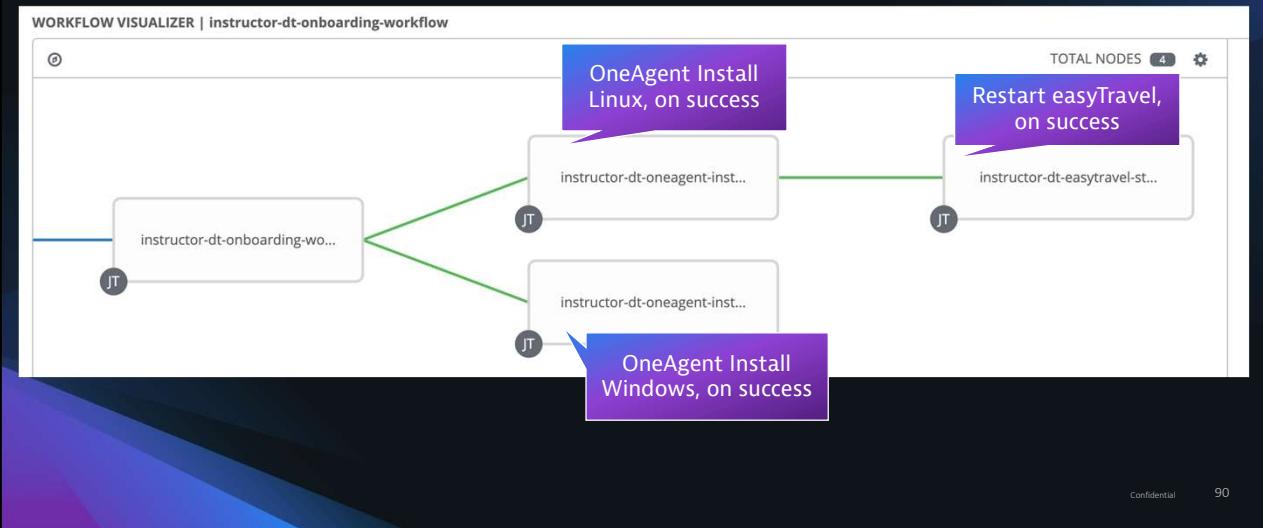
Workflow Template: Workflow Visualizer



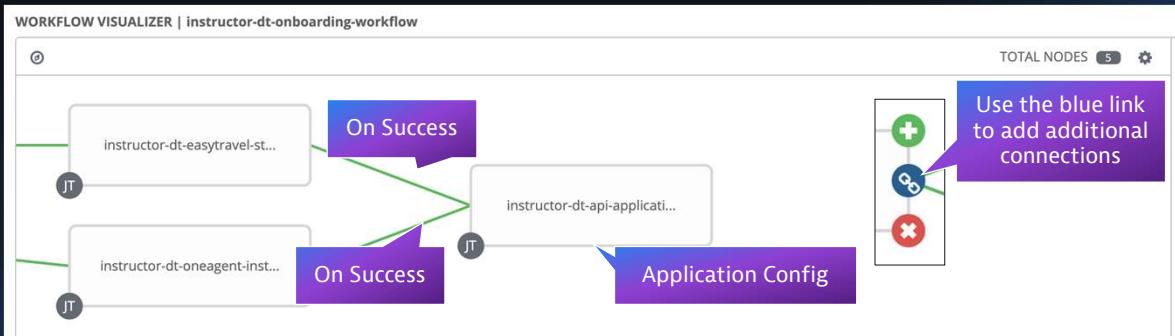
Confidential

89

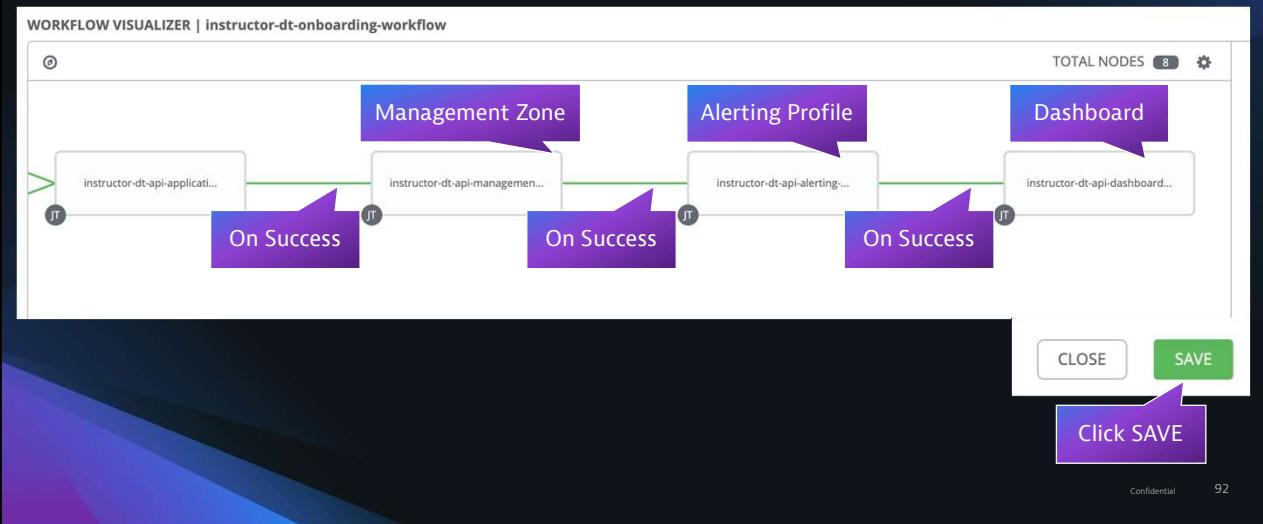
Workflow Template: Workflow Visualizer



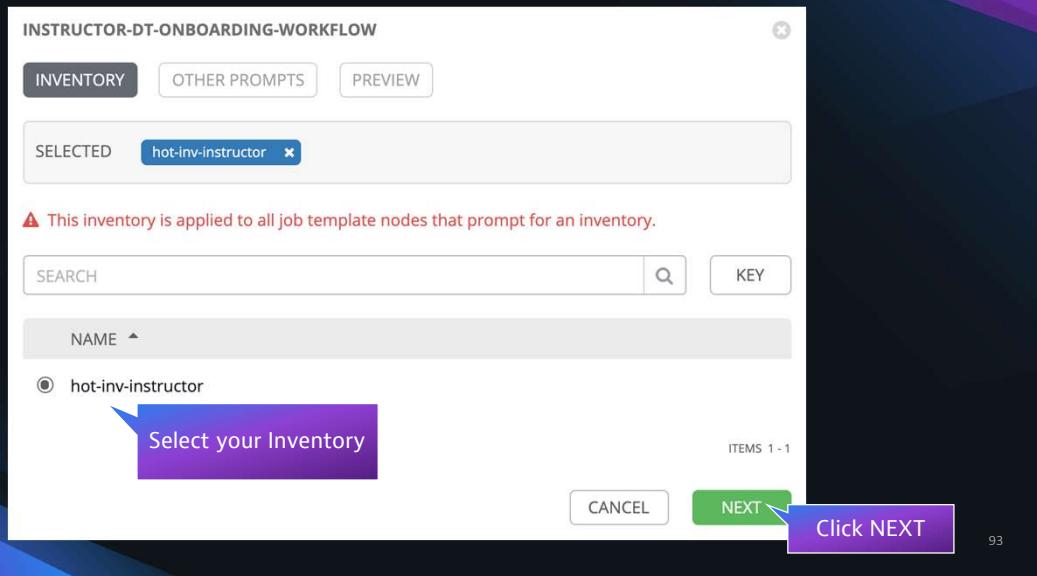
Workflow Template: Workflow Visualizer

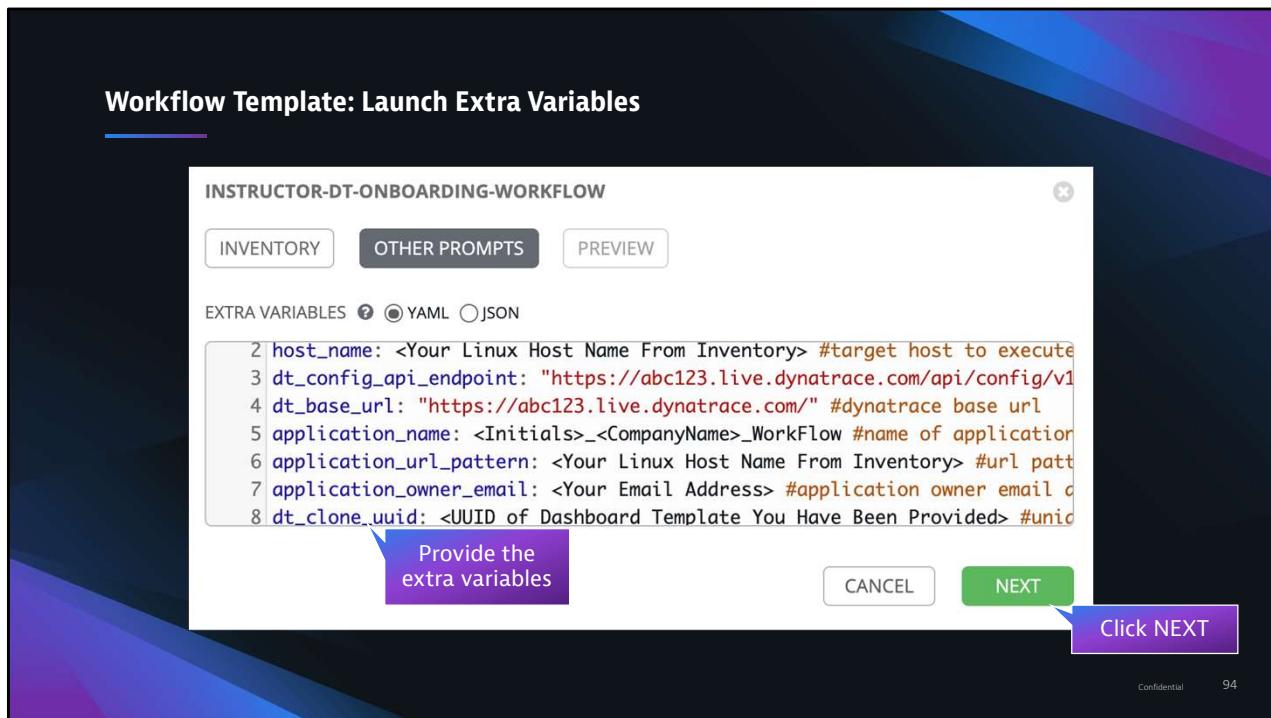


Workflow Template: Workflow Visualizer



Workflow Template: Launch Inventory





```
host_name: <One of your Linux EC2 Hosts> #target host to execute playbook
dt_config_api_endpoint: https://abc123.live.dynatrace.com/api/config/v1/ #dynatrace configuration api endpoint
dt_base_url: https://abc123.live.dynatrace.com/ #dynatrace base url
application_name: <Initials_CompanyName_Workflow> #name of application being onboarded
application_url_pattern: <One of your Linux EC2 Hosts> #url pattern of application
application_owner_email: <Your Email Address> #application owner email address
dt_clone_uuid: <UUID of Dashboard Template You Have Been Provided> #unique UUID id of the dynatrace dashboard to clone
```

Workflow Template: Launch Preview

INSTRUCTOR-DT-ONBOARDING-WORKFLOW

INVENTORY hot-inv-instructor

EXTRA VARIABLES

```
1 ---  
2 host_name: <Your Linux Host Name From Inventory> #target host to execute  
3 dt_config_api_endpoint: "https://abc123.live.dynatrace.com/api/config/v1  
4 dt_base_url: "https://abc123.live.dynatrace.com/" #dynatrace base url  
5 application_name: <Initials>_<CompanyName>_WorkFlow #name of application  
6 application_url_pattern: <Your Linux Host Name From Inventory> #url patt
```

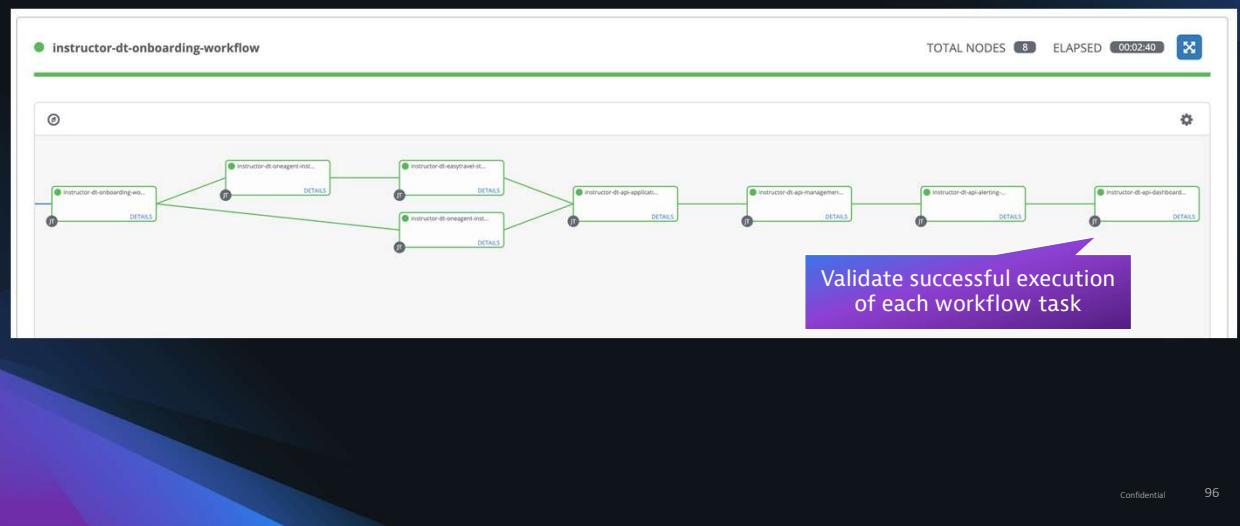
CANCEL LAUNCH

Click LAUNCH

Confidential

95

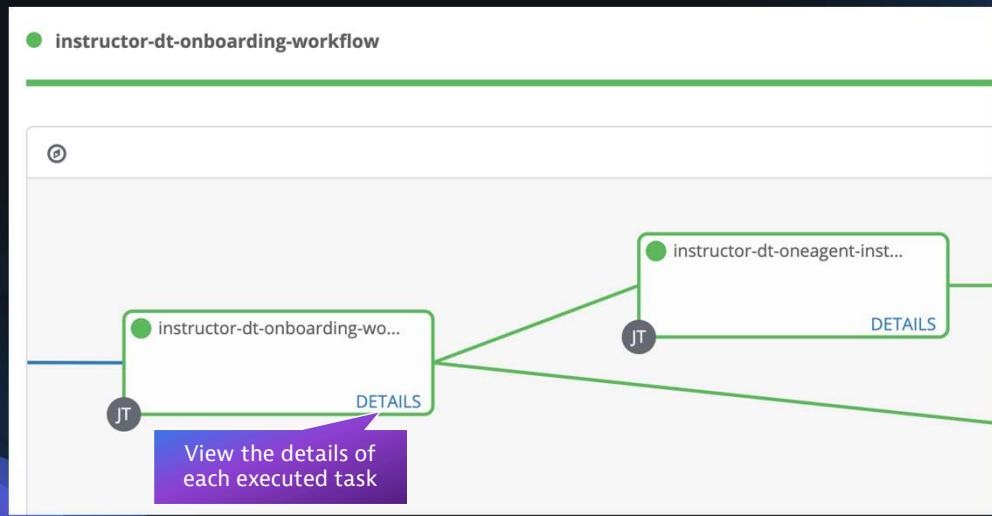
Workflow Template: Successful Execution



Confidential

96

Workflow Template: Successful Execution



Confidential

97