VERITAS

NetBackup™ API: Splunk Integration

Configure Splunk Enterprise[™] to collect NetBackup Jobs data using the NBU API.

Background

With the NetBackup[™] API maturing in every new release, we are presented with more and more opportunities to access and leverage NetBackup data in new and exciting ways. From lightweight UIs and flexible system monitors to sophisticated machine automation, the potential for managing, retrieving and integrating NetBackup data into popular third-party tools is growing rapidly. This whitepaper will endeavor to highlight this growing potential by detailing a solution for configuring Splunk Enterprise[™] to talk to NetBackup using the NBU API.

The problem we will be solving involves a company that wants to provide their employees with a customizable view of the NetBackup Activity Monitor without making everyone a NetBackup admin, as that would require training on how to safely use the NetBackup consoles, among other concerns. They also want to have the backup jobs metadata available in the same system they already use to collect and analyze their system logs, which will help them to limit the number of tools their systems analysts need to use to detect and solve problems in their heterogeneous IT environment.

Prerequisites

Preliminary NetBackup Configuration

The minimum recommended NetBackup version is 8.2, however, 8.1.2 also works if you are comfortable using basic authentication (ie with password in clear text). For this whitepaper, we'll assume the NetBackup version is 8.2 or later.

- From the NetBackup WebUI (<u>https://<masterserver>/webui/login</u>), navigate to Security > API keys and create a new key with an expiration that satisfies your requirements. Refer to the <u>NetBackup™ Web UI Security Administrator's</u> <u>Guide</u> for additional information related to this step.
- 2. Save the API key for later reference.

Preliminary Splunk Configuration

Splunk should normally be kept at the latest maintenance release. For the proof of concept described in this document, we used Splunk Enterprise version 8.0.3.

- 1. Install Add-on: REST API Modular Input.
 - a. In the Splunk GUI, goto Apps > Find More Apps.



- b. Search for "API".
- c. Locate the REST API Modular Input tile and click Install.



- 2. Register the Add-on and obtain a temporary evaluation key.
 - a. From the GUI menu bar, select Settings > Data Inputs.



b. Find the "REST" Data Input type in the list and select '+ Add New'

Data inputs - Settings Splunk × +					-	
\leftrightarrow \rightarrow C (i) localhost:8000/en-US	/manager/launcher/datainputstats				☆	Θ:
splunk>enterprise Apps •		🚯 Administrator 🔻 Messages 🕶	Settings Activity	Help 🔻 🛛 Fi	nd	٩
Data inputs Set up data inputs from files and directorie	es, network ports, and scripted inputs. If you want to set up forwarding and receiving betw	een two Splunk instances, go to Forwarding	g and receiving.			
Lo	ocal inputs					
	Туре	Inputs	Actions			
	Local event log collection Collect event logs from this machine.		Edit			
	Remote event log collections Collect event logs from remote hosts. Note: this uses WMI and requires a domain accord	1 unt.	+ Add new			
	Files & Directories Index a local file or monitor an entire directory.	9	+ Add new			
	Powershell v3 Modular Input Execute PowerShell scripts v3 with parameters as inputs.	0	+ Add new			
	REST REST API input for polling data from RESTful endpoints	2 B	+ Add new			
	Local Windows host monitoring Collect up-to-date hardware and software (Computer, Operating System, Processor, Se about this machine.	0 rvice, Disk, Network Adapter and Applicatio	+ Add new n) information			
	Local Windows network monitoring This is an input for Splunk Network Monitor.	0	+ Add new			
	Local Windows print monitoring Collect information about printers, printer jobs, print drivers, and print ports on this mac	0 hine.	+ Add new			
	Showing 1-5 of 5 modular inputs					

c. From the **Add Data** Input screen find the link that takes you to the activation page and complete the registration.

Add Data	Select Source Done	<back next=""></back>
	REST API Input	
WMI and	Name *	Name of this REST API Input
irectory.	Activation Key *	Visit http://www.baboonbones.com/#activation to obtain a non-
ver HTTP or	Endpoint URL *	URL to send the HTTP request to

d. Save your activation key for later reference.

Configuring the REST API Modular Input

Data Input GUI Form

- 1. From the GUI menu bar, select **Settings > Data Inputs**.
- 2. Find the "REST" Data Input type in the list and select **'+ Add New'**
- 3. Fill in the remaining form fields using the table below for reference:

Field Name	Value
REST API Input Name	A unique name for the Data Input
	Example: NBU_API_with_handler
Activation Key	<your_rest_api_modular_input_activation_key></your_rest_api_modular_input_activation_key>
(see prerequisites above)	
Endpoint URL	https:// <your_nbu_master_hostname>:1556/netbackup/admin/jobs</your_nbu_master_hostname>
HTTP Method	GET
Authentication Type	none
HTTP Header Properties	Authorization=< <i>your_NBU_API_Key</i> >
(see prerequisites above)	Example: Authorization=eyJ0eXAiOiJKV1QiL
URL Arguments	sort=endTime,filter=(jobType eq 'BACKUP' or jobType eq 'DBBACKUP') and state eq
(see notes II and III below)	'DONE' and endTime gt 1970-01-01T00:00:00.000000Z
Response Type	JSON
Response Handler	Choose a name for the response handler class. step.
	Example: NBU_Job_Handler
Set sourcetype	Manual
Source Type	Choose another name for the event data source type within the Splunk index.
	Example: nbu_api

Data Input Form Notes:

- I. Any field not referenced in the table above can be left blank on the GUI form. The above settings should be considered a baseline for proven and acceptable functionality but is not intended to represent the best method for every situation.
- II. Filter terms inside the parenthesis may be modified as needed to pre-filter the collected data. Refer to <u>NetBackup™ 8.2 API Getting</u> <u>Started guide</u> for a detailed description of the available filters and other URL arguments.
- III. endTime date can also be modified as needed to limit the initial data input, however, once the API input is enabled and running, the endTime date in the URL arguments is self-adjusting to ensure no repeat data is gathered.

4. Save the form using the Save button at the bottom of the form.

API Response Handler Configuration

- 1. Locate and open the REST API Modular Input responsehandler.py file.
 - a. splunk/etc/apps/rest_ta/bin
- 2. Insert the following Python class code below the default handler class in responsehandler.py. Note: Ensure that the class name matches the name you entered in the Data Input form's Response Handler field.

```
class NBU Job Handler:
   def init (self,**args):
       pass
        call (self, response object, raw response output, response type, req args, endpoint):
   def
       if response type == "json":
           output = json.loads(raw_response_output)
           last job indexed endtime =
           datetime.strptime('1970-01-01T00:00:00.000Z', "%Y-%m-%dT%H:%M:%S.%fZ")
           for item in output["data"]:
               print_xml_stream(json.dumps(item))
               if "endTime" in item["attributes"]:
                   job endtime = \setminus
                   datetime.strptime(item["attributes"]["endTime"], "%Y-%m-%dT%H:%M:%S.%fZ")
               if job endtime > last job indexed endtime:
                   last job indexed endtime = job endtime
           if not "params" in req_args:
               req args["params"] = {}
           if last job indexed endtime != \
           datetime.strptime('1970-01-01T00:00:00.000Z', "%Y-%m-%dT%H:%M:%S.%fZ"):
               req args["params"]["filter"] = \
               "(jobType eq 'BACKUP' or jobType eq 'DBBACKUP') and state eq 'DONE' and \
               endTime gt {}".format(last job indexed endtime.strftime("%Y-%m-%dT%H:%M:%S.%f" + "Z"))
               req args["params"]["sort"] = "endTime"
       else:
           print xml stream(raw response output)
```

3. Save the responsehandler.py file.

Splunk Event Source Type Configuration

- 1. Locate and open the Splunk props.conf file.
 - a. splunk/etc/system/local
- 2. Insert the following event properties configuration below the [default] entry in props.conf.

```
[nbu_api]
TIME_PREFIX = endTime": "
TIME_FORMAT = %Y-%m-%dT%H:%M:%S.%3NZ
```

3. Save the props.conf file

Final Configuration Steps

- 1. Restart the splunkd service.
- 2. When the service is back up and running again, log back in to the Splunk GUI.
- 3. From the menu bar, select Settings > Data Inputs.
- 4. Find the "REST" Data Input type and click on the **REST** hyperlink.

Data inputs - Settings Splunk	× +			- 0
\leftrightarrow \rightarrow C (i) localhost:8	000/en-US/manager/launcher/datainputstats			☆ (
splunk>enterprise Ap Data inputs	ps ▼	nistrator 🔻 🕄 Messag	jes ▼ Settings ▼ Activity ▼	Help - Find
er up data inputs nom mes an	Local inputs	unk instances, go to Poly	vording and receiving.	
	Туре	Inputs	Actions	
	Local event log collection Collect event logs from this machine.		Edit	
	Remote event log collections Collect event logs from remote hosts. Note: this uses WMI and requires a domain account.	1	+ Add new	
	Files & Directories Index a local file or monitor an entire directory.	9	+ Add new	
	Powershell v3 Modular Input Execute PowerShell scripts v3 with parameters as inputs.	0	+ Add new	
	REST API input for polling data from RESTful endpoints	2	+ Add new	
	Local Windows host monitoring Collect up-to-date hardware and software (Computer, Operating System, Processor, Service, Disk, N about this machine.	0 Network Adapter and App	+ Add new dication) information	
	Local Windows network monitoring This is an input for Splunk Network Monitor.	0	+ Add new	
	Local Windows print monitoring Collect information about printers, printer jobs, print drivers, and print ports on this machine.	0	+ Add new	
	Showing 1-5 of 5 modular inputs			

- 5. From the Data Inputs list, Enable your NBU REST API Data Input.
 - a. Note: This action will begin the process of indexing NBU jobs data as new events in Splunk.

> Settings Splunk	× +						- 🗆 X
\leftrightarrow \rightarrow C (i) localhos	st:8000/en-US/manager,	launcher/data/inputs/rest?search=NBU_API_with_handler&count=25					☆ \varTheta :
splunk>enterprise	Apps 🔻		🚺 Administrator 🕶 🛛	<mark>3)</mark> Messages ▼	Settings 🔻	Activity - Help	▼ Find Q
REST Data inputs » REST Showing 1-1 of 1 item filter	Q						New 25 per page 🔹
REST API Input Name +	Activation Key \$	Endpoint URL 🕈	Authentication Type 🕈	Source type +	App \$	Status 🕈	Actions
NBU_API_with_handler		https://winmaster:1556/netbackup/admin/jobs	none	nbu_api	search	Disabled Enable	5 Delete
4							Þ

Verification Steps

- 1. From the Splunk GUI menu bar, choose Apps > Search & Reporting.
- 2. Under "What to Search", click on Data Summary.

Search Splunk 8.0.3 × +	- 0	×
← → C (i) localhost:8000/en-US/app/search/search	* 0	:
splunk>enterprise App: Search & Reporting -	🚯 Administrator 🕶 🌀 Messages 👻 Settings 💌 Activity 👻 Help 👻 🛛 Find	
Search Analytics Datasets Reports Alerts Dashboards	Search & Reportir	g
Search		
enter search here	Last 24 hours • Q	
No Event Sampling •	₹ Smart Mode ▼	
How to Search If you are not familiar with the search features, or want to learn more, see one of the following resources. Documentation [2] Tutorial [2]	What to Search 58 Events 4 days ago 11 minutes ago INDEXED EARLIEST EVENT LATEST EVENT	
> Search History		

- 3. On the Data Summary dialog...
 - a. Select the SourceTypes Tab
 - b. Click on your NBU API source type to start a new search.

Data Summary				×
Hosts (1) Sources (1)	Sourcetypes (1)	A		
filter	Q	-		
Sourcetype 🗘	al	Count \$	Last Update 💲	
nbu_api B	al 💌	58	6/5/20 4:09:45.000 PM	

4. On the search results screen, confirm NetBackup jobs are being separated into unique events and event times reflect the Job endTime values.



Troubleshooting Tips

- No data is being indexed This is most likely due to problems in the python code or the remote master has
 rejected the REST API call, use the following search term in Splunk to check for these errors index=_internal
 error rest.py
- /var/log/splunk/splunkd.log can also be helpful for troubleshooting API related issues.
- Verify remote NetBackup master API functionality using API debugging tools such as Postman, Insomnia or Swagger.

Next Steps

Once you have NetBackup job events indexing in Splunk, the next thing you might want to do is to start using it to build reports, dashboards, monitors, etc. Since this is a very complex subject, worthy of its own dedicated documentation, we will just leave you with a sample of what can be done and allow you to explore from here on your own. Thank you for taking the time to review this document.

NetBackup Splunk 8.0.3 × +					- 🗆 ×
\leftrightarrow \rightarrow C () localhost:8000/en-US/app/search/netbackup?form.field1.earliest=%40d8	&form.field1.latest=now				☆ \varTheta :
splunk>enterprise App: Search & Reporting -		🚯 Administrator 👻 3 M	essages ▼ Settings ▼ Activity ▼	Help 🔻 Find	a a
Search Analytics Datasets Reports Alerts Dashboards				> Search	& Reporting
NetBackup				Edit Expo	rt 🔻 📖
Today + Hide Filters					
			_		
9			5		
Successful lobe			Eailed lobs		
JUCCESSIU JOUS			Falled JODS		
Peak Jobs		Status Code Distribution			
4					
ng			58		
2					
		150 -			
12:00 AM 2:00 AM 4:00 AM 6:00 AM 8:00 AM 10:00 AM 12:00 P	M 2:00 PM				
2020					
Activity Monitor					
jobId clientName policyName	scheduleName 🗢	startTime 🗢	endTime \$	status ≎	state 🗢
3361 win-5qndu309nuf SQL2012-Confluence	Full	2020-06-05T17:08:07.000Z	2020-06-05T17:15:44.000Z	58	DONE
3360 winmaster SQL2012-Confluence		2020-06-05T17:08:05.000Z	2020-06-05T17:15:44.000Z	58	DONE
3359 win2k8x64-clnt OpsCenter_DB	Full	2020-06-05T17:05:02.000Z	2020-06-05T17:10:42.000Z	150	DONE
3358 SLES11x64-client SLES11x64-client_SLP_ADV_TO_MSDP	FULL	2020-06-05T17:04:43.000Z	2020-06-05T23:08:46.000Z	150	DONE
3356 winmaster Catalog_Backup	Differential-Inc	2020-06-05T16:30:15.000Z	2020-06-05T16:30:34.000Z	0	DONE
3355 winmaster Catalog_Backup	Differential-Inc	2020-06-05T16:29:05.000Z	2020-06-05T16:30:02.000Z		DONE
3354 winmaster winmaster-filesystem old	Diff-Inc	0000 0C 0FT1C-00-F0 0007	0000 00 00710-00-00 0007		

ABOUT VERITAS

Veritas Technologies is a global leader in data protection and availability. Over 50,000 enterprises—including 99 of the Fortune 100—rely on us to abstract IT complexity and simplify data management. Veritas Enterprise Data Services Platform automates the protection and orchestrates the recovery of data everywhere it lives, ensures 24/7 availability of business-critical applications, and provides enterprises with the insights they need to comply with evolving data regulations. With a reputation for reliability at scale and a deployment model to fit any need, Veritas supports more than 500 data sources and over 150 storage targets, including 60 clouds. Learn more at www.veritas.com. Follow us on Twitter at @veritastechllc.

2625 Augustine Drive, Santa Clara, CA 95054 +1 (866) 837 4827 veritas.com For specific country offices and contact numbers, please visit our website.



Copyright © 2020 Veritas Technologies LLC. All rights reserved. Veritas, the Veritas Logo, and NetBackup are trademarks or registered trademarks of Veritas Technologies LLC or its affiliates in the U.S. and other countries. Other names may be trademarks of their respective owners.