

Splunk Admin On-Demand Service Catalog

Admin on Demand Service Catalog

The Services that can be provided through Admin on Demand together with full descriptions of the capabilities and limitations of each service can be found below:

TASK	CREDITS
Build a lookup	1
Create/Manage indexes	1
Extract a new field	1
Build a Dashboard	2
Build a Search	1
Create a Drilldown	1
Create a Macro, Tag or Eventtype	1
Create Workflows	1
Install a Cloud Certified App (Cloud Only)	1
Assist with Data On-Boarding	1
Ask an Expert – 1 hour	1
Ask an Expert – 2 hours	2

TASK	DEFINITION	INFO. REQUIRED FROM USER
BUILD A LOOKUP Create lookup tables to enrich indexed data.	<ul style="list-style-type: none"> Create a single csv or kv store based lookup Enable automatic lookups if required 	<ul style="list-style-type: none"> Csv to be used for lookup Sourcetype to be used Linked values within datasources
CREATE/MANAGE INDEXES Creation of indexes to organize ingested data within Splunk for searching.	<ul style="list-style-type: none"> Create up to 5 indexes Manage retention and access policies for up to 5 indexes Assist with deployment of app 	<ul style="list-style-type: none"> Index names Retention and Access requirements
EXTRACT A NEW FIELD Helping clients properly extract particular fields from datasets.	<ul style="list-style-type: none"> Extract up to 5 new fields via regular expression or key values 	<ul style="list-style-type: none"> Example dataset & data definition Field names required

TASK	DEFINITION	INFO. REQUIRED FROM USER
<p>BUILD A DASHBOARD (2 credits)</p> <p>Build a simple dashboard to utilize ingested Splunk data in a visual format</p>	<ul style="list-style-type: none"> • Up to 4 unique charts or panels • Based on a single new search and any number of existing searches • Up to 2 custom dashboard inputs (i.e. text boxes or drop-down lists) • Does not include sub searches, commands that require sub-searches, custom visualizations, javascript modifications, or CSS customizations. • Data already exists in the system (no data onboarding or field extractions) 	<ul style="list-style-type: none"> • Detailed description of search and dashboard requirements
<p>BUILD A SEARCH</p> <p>Help with building or debugging simple searches of indexed Splunk data.</p>	<ul style="list-style-type: none"> • Build a single search with up to 3 data sources • Data already exists in the system (no data onboarding or field extractions) • Does not include sub-searches or new data model creation 	<ul style="list-style-type: none"> • Detailed Description of search requirements
<p>CREATE A DRILLDOWN</p> <p>Help with creation of a drilldown on an existing dashboard to provide deeper data visibility.</p>	<ul style="list-style-type: none"> • Add up to 5 drilldowns to existing dashboard 	<ul style="list-style-type: none"> • Current Dashboard • Drilldown definition
<p>CREATE A MACRO, TAG OR EVENTTYPE</p> <p>Help customers with creation of knowledge objects to facilitate the index of data.</p>	<ul style="list-style-type: none"> • Create up to 5 macros, tags, or eventtypes • Assumes search already defined 	<ul style="list-style-type: none"> • Definition of items to be created
<p>CREATE WORKFLOWS</p> <p>Enable interactions between indexed or extracted data to other web resources.</p>	<ul style="list-style-type: none"> • Create up to 5 workflows • Limited to 1 field per workflow 	<ul style="list-style-type: none"> • Data source type • Target of workflow action • Fields to be provided to target
<p>INSTALL A CLOUD CERTIFIED APP (Cloud Only)</p> <p>Installation of apps that are not available via self-service.</p>	<ul style="list-style-type: none"> • Install up to 5 indexer or search head Cloud Certified Apps • No additional configuration 	<ul style="list-style-type: none"> • Apps to be installed

TASK	DEFINITION	INFO. REQUIRED FROM USER
<p>ASSIST WITH DATA ON-BOARDING</p> <p>Assistance in getting new data sources ingesting into Splunk.</p>	<ul style="list-style-type: none"> • Build necessary props & transforms to enable best practices for new data onboarding • Build necessary inputs.conf configurations necessary to onboard data • Assist with deploying app • Does not include field extractions which can be requested separately • Because this task is flexible in nature it is not to exceed 2 hours per session 	<ul style="list-style-type: none"> • Example dataset & data definition
<p>ASK AN EXPERT – 1 HOUR</p> <p>A one-hour one-on-one session with a Splunk Core Fundamentals Accredited consultant to answer adoption and best practice questions.</p>	<ul style="list-style-type: none"> • Discussion with a technical consultant regarding any adoption activity • Assist customer with best practices approach to adoption • May or may not include hands-on keyboard activities by the technical consultant based on customer demand • Up to 1-hour session 	<ul style="list-style-type: none"> • Question/Discussion to be answered
<p>ASK AN EXPERT – 2 HOURS (2 credits)</p> <p>A two-hour one-on-one session with a Splunk Core Fundamentals Accredited consultant to answer adoption and best practice questions.</p>	<ul style="list-style-type: none"> • Discussion with a technical consultant regarding any adoption activity • Assist customer with best practices approach to adoption • May or may not include hands-on keyboard activities by the technical consultant based on customer demand • Up to 2-hour session 	<ul style="list-style-type: none"> • Question/Discussion to be answered

Terms and Conditions

This document is for informational purposes only. Payment is due within thirty (30) days of the Splunk invoice. All Admin on Demand Services are annual subscriptions unless agreed otherwise. Admin on Demand Service Credits can be used only for items specifically listed in this Service Catalog and not for any other purpose. Each Admin on Demand Service Credit is expected to be able to be completed within 1 hour of work – in any event, if the work required takes longer than 2 hours Splunk reserves the right to require the use of additional Service Credits. Notwithstanding anything to the contrary in an agreement, Admin on Demand credits reset on the 1st of each calendar month, and any unused credits for the previous month expire. There are no refunds or credits for Admin on Demand Services not used. SPLUNK MAKES NO WARRANTIES, EXPRESSED OR IMPLIED, IN THIS FACT SHEET. All of the Admin on Demand service engagements are governed by the Splunk Agreement for Professional Services (PSA) [http://www.splunk.com/en_us/legal/professional-services-agreement.html] except for the payment, refund and credit terms identified above shall control for the Admin on Demand services. All references to SOWs in the PSA mean this FACT SHEET. However, the agreement noted above does not apply to the extent there is a separate, mutually signed agreement for or includes Professional Services.