

# Integration Service: ServiceNow Incident Synchronization PowerPack

Version 3.0.0

## Table of Contents

Introduction to the ServiceNow Incident Synchronization PowerPack	7
Architecture Overview for ServiceNow Synchronization PowerPacks	8
SL1 and ServiceNow Terminology	9
Dependency Map for ServiceNow Synchronization PowerPacks	9
Prerequisites for ServiceNow Synchronization PowerPacks	9
Integration Applications Included in the Synchronization PowerPack	11
Integration Applications	11
Integration Application (Internal)	. 11
Installing and Configuring the Incident Synchronization PowerPack	12
Downloading, Importing, and Installing the ServiceNow Incident Synchronization PowerPack	13
Downloading the Synchronization PowerPack	. 13
Importing the Synchronization PowerPack	13
Installing the Synchronization PowerPack	. 14
Allowing Cross-Scoped Access in ServiceNow	14
Installing the ScienceLogic SL1: CMDB & Incident Automation Application in ServiceNow	16
Installing the ServiceNow Base Pack PowerPack in SL1	17
Validating Network Communications	18
Checking DNS	18
Checking HTTPS and JSON	. 19
HTTP Codes	. 19
Creating a ServiceNow Group	20
Creating a ServiceNow User	22
Configuring Integrations for the Incident Synchronization PowerPack	24
Event Data Flow Between Integration Service and ServiceNow	26
Event Data Flow: Integration Service to ServiceNow	26
Event Data Flow: SL1 to Integration Service	28
Overview of the Run Book Automation for Incident Sync	. 29
Configuring Incident Sync	31
Creating and Aligning a Configuration Object	31
Creating a Configuration Object	32
Aligning a Configuration Object	. 34
Creating a ServiceNow Credential in SL1	36
Enabling the Run Book Automation Policies	38
Enabling and Customizing the Run Book Action Policy	. 39
Customizing the Snippet Code in the Input Parameters Pane	40
Customizing Logging in the Run Book Action	. 43
Sending Custom Data to ServiceNow Using the Passthrough Option	43
Passing Custom Data to ServiceNow	44
Snippet Code Example	46
Configuring the "ServiceNow: Click to Create Incident" Automation Policy	47
Viewing Incidents and Events	49
Incident Topology Suppression	50
Hyperlinking Events	56
ServiceNow Hyperlinking	57
Viewing the Incident Import Table in ServiceNow	. 57
ServiceNow, ScienceLogic Event, and Incident Priority Matrix	
Adding Additional Fields to the Transform Map	60
I roubleshooting the Incident Synchronization PowerPack	
Initial I roubleshooting Steps	6/
Integration Service	6/

ServiceNow	67
Resources for Troubleshooting	67
Useful Integration Service Ports	67
Helpful Docker Commands	68
Viewing Container Versions and Status	68
Restarting a Service	68
Stopping all Integration Service Services	68
Restarting Docker	68
Viewing Logs for a Specific Service	69
Clearing RabbitMQ Volume	69
Viewing the Process Status of All Services	70
Deploying Services from a Defined Docker Compose File	70
Dynamically Scaling for More Workers	70
Completely Removing Services from Running	70
Diagnosis Tools	70
Retrieving Additional Debug Information (Debug Mode)	71
Frequently Asked Questions	72
Why are Incidents not getting created in ServiceNow?	72
What if my Incident does not have a CI?	73
What if the Integration Service user interface is unresponsive and Incidents are not being generated in	
ServiceNow?	74
Why are Incident numbers not populated in SL1 on Incident creation in ServiceNow?	74
Why am I not getting any Incidents after disabling the firewall?	74
Checklists for Deployment	75
CMDB-Only ServiceNow Integration with Single SL1, no Domain Separation in ServiceNow	76
Sync Devices from SL1 to ServiceNow	76
Discover Devices from ServiceNow in SL1	77
Sync Business Services from SL1 to ServiceNow	77
Sync File Systems from SL1 to ServiceNow	77
Sync Network Interfaces from SL1 to ServiceNow	77
Sync Installed Software from SL1 to ServiceNow	78
Sync Maintenance Schedules from ServiceNow to SL1	78
Sync Advanced Topology from SL1 to ServiceNow	78
CMDB-Only ServiceNow Integration with Single SL1 and Domain-Separated ServiceNow	79
Sync Devices from SL1 to ServiceNow	79
Discover Devices from ServiceNow in SL1	80
Sync Business Services from SL1 to ServiceNow	80
Sync File Systems from SL1 to ServiceNow	81
Sync Network Interfaces from SL1 to ServiceNow	81
Sync Installed Software from SL1 to ServiceNow	81
Sync Maintenance Schedules from ServiceNow to SL1	81
Sync Advanced Topology from SL1 to ServiceNow	82
CMDB-Only ServiceNow Integration with Multiple SL1 Systems, no Domain-Separated ServiceNow	83
Sync Devices from SL1 to ServiceNow	84
Discover Devices from ServiceNow in SL1	84
Sync Business Services from SL1 to ServiceNow	85
Sync File Systems from SL1 to ServiceNow	85
Sync Network Interfaces from SL1 to ServiceNow	85
Sync Installed Software from SL1 to ServiceNow	86
Sync Maintenance Schedules from ServiceNow to SL1	86
Sync Advanced Topology from SL1 to ServiceNow	86
Incident-Only ServiceNow Integration with Single SL1, no Domain Separation in ServiceNow	87

Certified Application Objects	8
Roles	69
Tables	0'
Table Columns (cmdb_ci)	0'
Table Columns (core_company)	1'
Table Columns (cmdb group)	1
Script Includes	1
	1
Scripted Actions	2'
Data Lookup Definitions	2'
System Properties	2'
Catalog Item	3
Catalog UI Policies	3
Variable Sets	3
Catalog Client Scripts	<i>4</i>
Workflows	<i>4</i>
Scripted REST Resources	<i>י</i> 5
Transform Maps	<i>7</i> י
Transform Scripts	7
erviceNow API Endpoints	8
Business Services	0
HTTP Method	0
Pagination	0
Resource Path	0
Default Resource Path	0
Example (Request URL)	0
Example (Response)	)]
Chanae Requests	)2
HTTP Method	)2
Resource Path	)2
Default Resource Path	)2
Fixed Internal Query	)3
Example	)3
Example (Response)	)3
Classification version 1	)4
HTTP Method	)4
Pagination	)4
Resource Path	)4
Default Resource Path	)4
Fixed Internal Query	)5
Example 10	)5
Example (Response)	)5
Classification version 2	)7
HTTP Method	)7
Pagination 10	)7
Resource Path	)7
Default Resource Path	)7
Fixed Internal Query	8(
Example 10	8
Example (Response)	8(
CMDB Group 11	0
HTTP Method	0

Pagination	1	10
Resource Path	1	10
Default Resource Path	1	10
Example (Request URL	1	10
Example (Body)	1	10
Example (Response)	1	11
Companies	1	12
, HTTP Method	1	12
Pagination	1	12
Resource Path	1	12
Default Resource Path	1	12
Fixed Internal Querv	1	13
Example	1	13
Example (Response)	1	13
Device Identification Engine	1	1.5
HTTP Method	1	15
Pagingtion	1	15
Resource Path	1	15
Default Persource Path	1	15
Example (Paquest LIPL)	1	15
Example (Request OKL)	1 1	15
Example (Dody)	1	12
Example Dusiness Service (Dody)	1	10
	1	17
	1	10
	1	10
Pagination	1	18
Resource Path	1	18
Detault Resource Path	1	18
Fixed Internal Query	1	19
Example	.	19
Example (Response)		19
File Systems	12	20
HTTP Method	12	20
Pagination	12	20
Resource Path	12	20
Default Resource Path	12	20
Fixed Internal Query	12	21
Example	12	21
Example (Response)	12	21
Import Set	12	22
HTTP Method	12	22
Resource Path	12	22
Default Resource Path	12	22
Example (Request URL)	12	22
Example (Body)	12	22
Incidents	12	24
HTTP Method	12	24
Pagination	12	24
Resource Path	12	24
Default Resource Path	12	24
Fixed Internal Query	12	25
Example	12	25

Example (Response)	.125
Installed Software	. 127
HTTP Method	.127
Pagination	. 127
Resource Path	.127
Default Resource Path	.127
Fixed Internal Query	128
Example (Request URL)	.128
Manufacturer	130
HTTP Method	130
Pagingtion	130
Resource Path	130
Default Resource Path	130
Example (Request URI )	130
Example (Body)	130
Example (Response)	131
Model	132
HTTP Method	132
Resource Path	132
Default Resource Path	132
Example (Request URI )	132
Example (Body)	132
Example (Response)	133
Network Adapters	134
HTTP Method	134
Pagingtion	134
Resource Path	134
Default Resource Path	.134
Fixed Internal Query	.135
Example (Request URL)	.135
Example (Response)	135
Service Requests	.136
HTTP Method	.136
Pagination	136
Resource Path	136
Default Resource Path	136
Fixed Internal Query	137
Example	137
Example (Response)	.137
	/

# Chapter

## Introduction to the ServiceNow Incident Synchronization PowerPack

#### Overview

This chapter describes the ServiceNow Incident Synchronization PowerPack, which is the ScienceLogic integration with the ServiceNow Incident Management Module.

This Synchronization PowerPack automatically logs, de-duplicates, correlates, updates, and appends ServiceNow Incidents, reducing the amount of time to resolve critical service issues. This Synchronization PowerPack covers the entire Incident life cycle, providing a bi-directional integration between SL1 events and ServiceNow Incidents, while providing a granular view into both the event and the associated Incident.

**NOTE**: The label "SyncPack" is used in place of "Synchronization PowerPack" in the Integration Service user interface.

This chapter covers the following topics:

Architecture Overview for ServiceNow Synchronization PowerPacks	8
SL1 and ServiceNow Terminology	9
Dependency Map for ServiceNow Synchronization PowerPacks	9
Prerequisites for ServiceNow Synchronization PowerPacks	9
Integration Applications Included in the Synchronization PowerPack	1

## Architecture Overview for ServiceNow Synchronization PowerPacks

The following diagram details the various elements that are contained in SL1 and the Integration Service, and how the Integration Service sits between the core SL1 platform and an external data platform:



The following diagram provides an example of the high-level architecture of an Integration Service system with High Availability, Disaster Recovery, and a proxy configured:



## SL1 and ServiceNow Terminology

The following table lists the different names for the shared elements in SL1 and ServiceNow:

SL1	ServiceNow
Device	Cl (Configuration Item)
Discovery Session	Service Catalog Request
Event	Incident
Organization	Company/Domain
Schedule	Maintenance Schedule
Тороlоду	Dependency

#### Dependency Map for ServiceNow Synchronization PowerPacks

The following graphic describes which Synchronization PowerPacks depend on other Synchronization PowerPacks:



TIP: For more information about the Standard Base Steps Synchronization PowerPack, see the Integration Service Platform manual.

## Prerequisites for ServiceNow Synchronization PowerPacks

This section describes the prerequisites for the ServiceNow Synchronization PowerPacks. For more information about the specific software versions required by a ServiceNow Synchronization PowerPack, see the release notes for that Synchronization PowerPack.

To install any of the ScienceLogic ServiceNow Synchronization PowerPacks, you must have administrator access to both SL1 and ServiceNow. Specifically, you will need:

- ScienceLogic root SSH access
- SSH access to the Integration Service
- ScienceLogic administrator access to the Administration Portal
- ServiceNow administrator access

Additional information related to uploading, installing, and upgrading the ServiceNow Synchronization PowerPacks:

- If you want to upload and install multiple ServiceNow Synchronization PowerPacks at the same time, you should upload *all* of the Synchronization PowerPacks first, and then install them to address any dependencies between the Synchronization PowerPacks.
- If you are upgrading from version 1.8.4 of the Integration Service, you can first move to version 2.5.0 of the ServiceNow Synchronization PowerPack, then upgrade to version 2.0 of the Integration Service, and finally move to version 3.0.0 or later of the relevant ServiceNow Synchronization PowerPacks.
- If you made customizations to version 2.5.0 or earlier of the ServiceNow Synchronization PowerPack, you must make a copy of that Synchronization PowerPack and save it as a new Synchronization PowerPack to keep your customizations. For more information, see the *Integration Service for Developers* manual.
- If you are starting out with version 2.0.0 of the Integration Service platform, you should skip version 2.5.0 of the ServiceNow Synchronization PowerPack and instead install version 3.0.0 of the relevant ServiceNow Synchronization PowerPacks.
- There is no backwards compatibility after you upgrade a ServiceNow Synchronization PowerPack from version 2.5.0 to 3.0.0.

**NOTE**: ScienceLogic highly recommends that you disable all firewall session-limiting policies. Firewalls will drop HTTPS requests, which results in data loss.

Source IP	Integration Service Destination	Integration Service Source Port	Destination Port	Requirement
Integration Service	SL1 API	Any	TCP 443	SL1 API Access
Integration Service	ServiceNow API	Any	TCP 443	ServiceNow API Access
SL1 Run Book Action	Integration Service	Any	TCP 443	Send SL1 data to Integration Service
Integration Service	SL1 Database	Any	ТСР 7706	SL1 Database Access

The following table lists the port access required by the Integration Service and this Synchronization PowerPack:

## Integration Applications Included in the Synchronization PowerPack

This section lists the contents of the ServiceNow Incident Synchronization PowerPack.

#### Integration Applications

The following integration applications are included with the ServiceNow Incident Synchronization PowerPack:

- Create or Update ServiceNow Incident from SL1 Event. Reads SL1 events and creates or updates the corresponding ServiceNow Incident.
- Sync Incident State from ServiceNow to SL1 Event. Clears or updates SL1 events when the related ServiceNow Incident is updated.
- Update ServiceNow Incident when SL1 Event is Acknowledged. Updates the synced ServiceNow incident when the corresponding SL1 event is acknowledged.
- Update ServiceNow Incident when SL1 Event is Cleared. Updates the synced ServiceNow Incident when the corresponding SL1 event is cleared.

#### Integration Application (Internal)

To view the internal integration application, click the Filter icon ( $\overline{\phantom{a}}$ ) on the **Integrations** page and select Show Hidden Integrations. Internal integration applications are hidden by default. The following integration application is "internal" and should not be run directly. Instead, it is automatically run by applications from the previous list:

• Bulk Update SL1 Events. Bulk updates SL1 events with a given payload.

# Chapter

# 2

## Installing and Configuring the Incident Synchronization PowerPack

#### Overview

This chapter describes the how to install and configure the ServiceNow Incident Synchronization PowerPack and the components used by the Synchronization PowerPack.

The following workflow covers how to install and configure this Synchronization PowerPack:

- 1. In the Integration Service, download, import, and install the ServiceNow Incident Synchronization PowerPack.
- 2. In ServiceNow, enable cross-scoped access and install the "ScienceLogic SL1: CMDB & Incident Automation" application.
- 3. In SL1, install the ServiceNow Base Pack PowerPack.
- 4. Validate network communications.
- 5. Create a ServiceNow group and user account.

These installation and configuration steps are covered in the following topics:

$Downloading, \ \textit{Importing}, \ \textit{and Installing the ServiceNow Incident Synchronization PowerPack} \ .$	13
Allowing Cross-Scoped Access in ServiceNow	14
Installing the ScienceLogic SL1: CMDB & Incident Automation Application in ServiceNow	16
Installing the ServiceNow Base Pack PowerPack in SL1	17
Validating Network Communications	18
Creating a ServiceNow Group	20
Creating a ServiceNow User	22

#### Downloading, Importing, and Installing the ServiceNow Incident Synchronization PowerPack

A Synchronization PowerPack file has the .**whl** file extension type. You can download the Synchronization PowerPack file from the ScienceLogic Support site.

WARNING: If you are upgrading to this version of the Synchronization PowerPack from a previous version, make a note of any settings you made on the **Configuration** pane of the various integration applications in this Synchronization PowerPack, as these settings are *not* retained when you upgrade.

#### Downloading the Synchronization PowerPack

A Synchronization PowerPack file has the .**whl** file extension type. You can download the Synchronization PowerPack file from the ScienceLogic Support site.

To locate and download the Synchronization PowerPack:

- 1. Go to the ScienceLogic Support site at https://support.sciencelogic.com/s/.
- 2. Click the **Product Downloads** tab, select *PowerPacks*, and then click the "Synchronization" link. The **Synchronization PowerPack Downloads** page appears.
- 3. Click the name of the Synchronization PowerPack you want to install. The PowerPack page appears.
- 4. In the **Files** list, locate the Synchronization PowerPack **.whl** file, click the down arrow button, and select *Download*.

**NOTE:** Synchronization PowerPacks do not require a specific license. After you download a Synchronization PowerPack, you can import it to your Integration Service using the Integration Service user interface.

#### Importing the Synchronization PowerPack

**NOTE**: You must import and install the ServiceNow Base Synchronization PowerPack before uploading and installing any of the other ServiceNow Synchronization PowerPacks.

To import a Synchronization PowerPack in the Integration Service user interface:

- 1. On the **SyncPacks** page of the Integration Service user interface, click **[Import SyncPack]**. The **Import SyncPack** page appears.
- 2. Click [Browse] and select the .whI file for the Synchronization PowerPack you want to install.

TIP: You can also drag and drop a .whI file to the SyncPacks page.

- 3. Click **[Import]**. The Integration Service registers and uploads the Synchronization PowerPack. The Synchronization PowerPack is added to the **SyncPacks** page.
- **NOTE:** You cannot edit the content package in a Synchronization PowerPack published by ScienceLogic. You must make a copy of a ScienceLogic Synchronization PowerPack and save your changes to the new Synchronization PowerPack to prevent overwriting any information in the original Synchronization PowerPack when upgrading.

#### Installing the Synchronization PowerPack

To install a Synchronization PowerPack in the Integration Service user interface:

1. On the **SyncPacks** page of the Integration Service user interface, click the **[Actions]** button (<sup>‡</sup>) for the Synchronization PowerPack you want to install and select *Activate & Install*. The **Activate & Install SyncPack** modal appears.

TIP: By default, the SyncPacks page displays only activated and installed PowerPacks. If you do not see the PowerPack that you want to install, click the toggle icon ( ) on the SyncPacks page and select Show All SyncPacks to see a list of the uninstalled PowerPacks.

- Click [Yes] to confirm the activation and installation. When the Synchronization PowerPack is activated, the SyncPacks page displays a green check mark icon (<sup>SO</sup>) for that Synchronization PowerPack. If the activation or installation failed, then a red exclamation mark icon (<sup>O</sup>) appears.
- 3. For more information about the activation and installation process, click the check mark icon (<sup>≤</sup>) or the exclamation mark icon (<sup>●</sup>) in the **Activated** column for that Synchronization PowerPack. For a successful installation, the "Activate & Install SyncPack" integration application appears, and you can view the Step Log for the steps. For a failed installation, the **Error Logs** window appears.

#### Allowing Cross-Scoped Access in ServiceNow

When using custom tables that are extended from the cmdb\_ci table, you must configure cross-scope access for any custom tables created outside of the base ServiceNow deployment.

The following examples contain errors that might occur when cross-scope access is required.

Example of an API response:

```
{"results":[{"error":
{"message":"com.glide.script.fencing.access.ScopeAccessNotGrantedException: read
access to ui_test_hardware not granted","detail":""},"status":"failure"}
```

Example of navigating to a URL directly from a web browser when cross-scope access is required:



In this example, the table requires that you grant access to the ScienceLogic Scope to allow the API call to run correctly. In the above example, the target table is **u\_test\_hardware**.

NOTE: A ServiceNow account with System Administrator is required.

To grant access to the ScienceLogic Scope in ServiceNow:

- 1. Log in to your ServiceNow instance.



3. From the **Application** drop-down list, select ScienceLogic ServiceNow Integration.

4. Close the **Developer System Settings** window and navigate to the **Cross scope privileges** page (System Applications > Application Cross-Scope Access).

**NOTE:** Make sure you are in the ScienceLogic ServiceNow Application scope and track these updates in an update set.

5. Click the **[New]** button to create a new record on the **Cross scope privileges** page:

< E Cross scope New record	e privilege			Ø	ŧ	000	Submit
* Source Scope	ScienceLogic ServiceNow Integration		Application	ScienceLogic ServiceNow Integration	()		^
* Target Scope	Global Q	0	* Operation	Read ~			
* Target Name	cmd_ci_endpoint_storage_fc		Status	Allowed ~			
* Target Type	Table ~						
Submit							

- 6. Verify that the **Source Scope** and **Application** fields are set to ScienceLogic ServiceNow Integration. If they are not, repeats steps 2-3.
- 7. Complete the following fields:
  - Target Scope. Specify the scope of the target table, such as Global.
  - Operation. Select Read.
  - Target Name. Specify the name of the target table.
  - Status. Select Allowed.
  - Target Type. Select Table.
- 8. Click the [Submit] button.

For more information, see <u>https://docs.servicenow.com/bundle/madrid-application-</u>development/page/build/applications/reference/c CrossScopePrivilegeRecord.html.

#### Installing the ScienceLogic SL1: CMDB & Incident Automation Application in ServiceNow

The ServiceNow Incident Synchronization PowerPack uses the "ScienceLogic SL1: CMDB & Incident Automation Application" to sync incident status update from ServiceNow back to SL1.

You must install the "ScienceLogic SL1: CMDB & Incident Automation" application on your ServiceNow instance to enable this Synchronization PowerPack. The "ScienceLogic SL1: CMDB & Incident Automation" application is also known as the "Certified Application" or the "Scoped Application".

- **NOTE**: You must have a ServiceNow HI Service Account to request this application and download it onto your ServiceNow instance.
- WARNING: Integration Service instances running version 2.0.0 or later of the ServiceNow integration applications are not backwards-compatible with the previous ServiceNow update sets or with SyncServer. After you install the "ScienceLogic SL1: CMDB & Incident Automation" application on your ServiceNow instance, you need to upgrade your ServiceNow integration applications to version 2.0.0 or later on all Integration Service instances. The "ScienceLogic SL1: CMDB & Incident Automation" application is also not backwards-compatible with SyncServer. This change cannot be reverted.

You must first request the "ScienceLogic SL1: CMDB & Incident Automation" application from the ServiceNow Store, and then you can install it.

To request and install the Certified Application:

- 1. Go to the ServiceNow Store at <a href="https://store.servicenow.com">https://store.servicenow.com</a> and search for "ScienceLogic SL1".
- 2. Select the "ScienceLogic SL1: CMDB & Incident Automation" application. The detail page for the application appears.
- 3. Click the [Get] button and log in with your HI credentials.
- 4. After the request is approved, log in to ServiceNow as an administrator and navigate to **Application Manager** (System Applications > Applications or My Company Applications).
- 5. Click [Downloads] in the menu header or search for "ScienceLogic".
- 6. Click the version drop-down for the "ScienceLogic ServiceNow Integration" application listing to make sure you are using the correct version of the application that is compatible with your version of this Synchronization PowerPack.
- 7. Click the **[Install]** button for the "ScienceLogic ServiceNow Integration" application. The installation is complete when the button changes to **[Installed]**.
- 8. In the filter navigator, search for "ScienceLogic" and locate the application in the left-hand navigation menu to verify that the application was installed.

## Installing the ServiceNow Base Pack PowerPack in SL1

The ServiceNow Base Pack PowerPack monitors the ServiceNow Incident and CMDB tables, and it returns information about Incident types, priorities, and states, displaying the information in an easy-to-consume dashboard. The PowerPack also returns information about the CI records that are actively being synced between SL1 and ServiceNow via the Integration Service, including basic CI metadata as well as an overall count.

Also, this PowerPack is a critical component of the Incident Sync Integration with ServiceNow, using Run Book Automations to integrate with the ServiceNow Incident Management module. TIP: By default, installing a new version of a PowerPack overwrites all content in that PowerPack that has already been installed on the target system. You can use the *Enable Selective PowerPack Field Protection* setting in the **Behavior Settings** page (System > Settings > Behavior) to prevent new PowerPacks from overwriting local changes for some commonly customized fields. For more information, see the *System Administration* manual.

To install the ServiceNow Base Pack PowerPack:

- 1. Download the latest version of the PowerPack from the Customer Portal to a local computer.
- 2. In SL1, log in and go to the **PowerPack Manager** page (System > Manage > PowerPacks).
- 3. Click [Actions] and select Import PowerPack.
- 4. Click [Browse] and navigate to the ServiceNow Base Pack PowerPack file from step 1.
- 5. Select the PowerPack file and click [Import]. The PowerPack Installer modal page displays a list of the PowerPack contents.
- 6. Click [Install]. After the installation is complete, the ServiceNow Base Pack PowerPack appears on the **PowerPack Manager** page.

#### Validating Network Communications

All communication between SL1 and ServiceNow is done through TCP port 443. To allow communication between SL1 and ServiceNow, the SL1 Database Server, Data Collector, or All-In-One Appliance must have external access to the ServiceNow instance. No inbound TCP ports are required to be open to the SL1 server. Outbound communication may use NAT or be direct.

**NOTE:** All firewall session-limiting policies must be disabled. If firewall session-limiting policies are enabled, HTTPS requests might be dropped by the firewall, resulting in data loss. Check with your security or firewall administrator to make sure there are no session limiting policies on TCP port 443 for your SL1 servers.

#### Checking DNS

Because ServiceNow is a cloud-based service, DNS must be configured on all SL1 servers that communicate with your ServiceNow instance.

**NOTE**: ServiceNow instances are generally named as: *your-instance.service-now.com*, where *your-instance* is the name of your ServiceNow server. The examples below use *mycompany.service-now.com*. Your instance name will be unique to your subscription.

To validate that your SL1 server has proper DNS name resolution configured, test network connectivity and name resolution using the nmap command, which is available from the command line of any SL1 server:

nmap -sT -p 443 mycompany.service-now.com

If the test was successful, you will see a message similar to the following:

Starting Nmap 5.51 ( http://nmap.org ) at 2013-11-12 20:22 UTC Nmap scan report for mycompany.service-now.com (199.91.136.100) Host is up (0.067s latency). PORT STATE SERVICE 443/tcp open https

If domain name resolution fails, you will see a message similar to:

Failed to resolve given hostname/IP: mycompany.service-now.com.

#### Checking HTTPS and JSON

You can administer a simple test to determine if the ServiceNow JSON Plug-in web service is configured and operating using the Basic Authentication method on your ServiceNow instance. To do so, run the following command from the ScienceLogic Central Database or All-In-One Appliance:

**NOTE**: In the example below, replace the admin:admin username and password key/value pair with your ServiceNow administrator username and password and mycompany.service-now.com with your ServiceNow instance name.

```
curl --location -vu admin:admin -H "Accept: application/json" -H "Content-Type:
application/json"
'https://mycompany.service-now.com/api/now/table/incident'
```

If not successful, the following message appears:

HTTP/1.1 401 Unauthorized

If successful, a JSON encoded string starting with the "result" variable appears:

{"result":[{"upon\_approval":"","location":"1083361cc611227501b682158cabf646",....

#### HTTP Codes

HTTP codes are necessary for identifying specific problems. The following table lists typical HTTP codes that might occur when testing the ServiceNow JSON Web Service.

Code	Definition
401	Unauthorized. Check that the username and password are correct and properly formatted.
403	Forbidden. ServiceNow understood the request, but either the URL is incorrect, or the user account does not have permission to see the requested object.

Code	Definition
404	The ServiceNow server has not found anything matching the requested URL. Check to make sure there is data in the target table.
200	Success.
201	Success. Data is posted.

**TIP**: For more information about the ServiceNow JSON Web Service and the Table API, see <a href="http://wiki.servicenow.com/index.php?title=Table\_API">http://wiki.servicenow.com/index.php?title=Table\_API</a>. If you continue to have problems, please contact either ScienceLogic or ServiceNow customer support.

## Creating a ServiceNow Group

For best practice and security, create a dedicated ServiceNow account that has restricted access to only the groups, access control lists (ACLs), and roles needed for ScienceLogic incident management.

To create a ServiceNow Account for ScienceLogic Incident management:

- 1. In ServiceNow, search in the filter navigator for "groups".
- 2. On the Groups page (System Security > Groups), click [New]. A New record page appears.
- 3. In the **New record** page, type the group name and any additional information. **Name** is the only required field.

<			Ŵ	submit
Name	Sciencelogic Service Accounts	Group email	8	
Manager	System Administrator Q	① Parent	Q	
Description				
Submit				

4. Right-click the gray header and click Save to save the record.

<		Save		Ø	submit
Name	Sciencelogic Service Accounts	Configure > Export >	Group email	8	
Manager	System Administrator Q (i	Create Favorite	Parent	Q	
Description		Copy URL Copy sys_id Reload form			

5. At the bottom of the Group form, select the [Roles] tab and click [Edit].

Roles	Group Members	Groups				
	Roles Edit	Go to Created 💌	Search			Ð
$\bigtriangledown$	Group = Science	logic Service Accounts				
袋	Q	Created	<b>≡</b> Role	Granted by	≡ Inherits	

6. Search for x\_sclo\_scilogic.Admin and move it to the **Roles List** column using the arrow buttons.

Add Filter Run filter ?			
choose field 🔻	oper	•	value
Collection		Roles List IS4 - Service Acco	unts
action_designer activity_admin activity_creator admin agent_admin api_analytics_read app_service_admin app_service_user approval_admin approver_user assessment_admin asset assignment_rule_admin atf_test_admin atf_test_designer	>	x_sclo_scilogic	.Admin
	Cancel	Save	

7. Click [Save]. Your ServiceNow Group now has an assigned Role:

Group	ce Accounts			R	<b>₩</b> ••••	Update	Delete	• •
Name	IS4 - Service Accounts		Group email					
Manager		Q	Parent			Q		
Description								
Update Delete								
Roles (1) Group Me	embers (1) Groups							
■ Roles Edit.	Go to Created 🔻 Sea	arch		44	•	1 to 1 of		Ξ
Group = IS4 -	Service Accounts							
ø; Q ≡	■ Created	<b>≡</b> Role	≡ Gi	ranted by		≡ Inheri	ts	
(i) <u>2</u>	019-01-15 12:09:31	<u>x sclo scilogic.Admin</u>	(emp	ty)		true		
Actions on se	elected rows \$			••	• •	1 to 1 o	f1 🕨 🍽	

8. Next, create a ServiceNow user to use with this Group. See the following procedure for the details.

#### Creating a ServiceNow User

**NOTE**: The ServiceNow user you create in this procedure will *not* be able to log into the ServiceNow user interface with the username and password you give this user. However, you will use the username and password in the relevant configuration objects in the Integration Service user interface to run integration applications. For more information about configuration objects, see Creating and Aligning a Configuration Object.

To create a ServiceNow Account for ScienceLogic Incident management:

- 1. In ServiceNow, search in the filter navigator for "users".
- 2. On the Users page (System Security > Users), click [New]. A New record page appears.
- 3. Complete the following fields:
  - User ID. Type a user ID. Required.
  - First Name. Type the user's first name.
  - Last Name. Type the user's last name.
  - Password. Type a password. Required.
  - Active. Select this checkbox. Required.
  - Web Service Access Only. Select this checkbox. Required.

- Time Zone. Select GMT. Required.
- Date Format. Select System (yyyy-MM-dd).
- 4. Right-click the gray header and click Save to save the user.
- 5. Select the **[Groups]** tab at the bottom of the record and click the **[Edit]** button:

Roles	Groups	Delegates	Subscriptions	Manage	Subscriptions	
	Groups	New Edi	it Go to	Group 🔻	Search	-

6. Find the group you created previously and move the group to the right-hand column using the arrow buttons.

Collection	Groups List
Q sciencelogic	Service Account
None	Sciencelogic Service Accounts
	Cancel Save
Name Sciencelogic	Service Accounts

7. Click **[Save]**. After the user has been added to the group, you can see their Roles and Groups at bottom of the record:

Roles (18)	Groups (1)	Delegate	s Subscriptions	Manage Subscriptions			
Rol	es Edit	Go to	Role 🔻	Search	▲ ▲ 1 to 18 of 18	• •	••

**NOTE:** As a best practice, you should use a non-administrator ServiceNow user for the Integration Service configuration object.

## Chapter



## Configuring Integrations for the Incident Synchronization PowerPack

#### Overview

This chapter describes the how to configure and run the various Integration Service integration applications and Run Book Automations contained in the ServiceNow Incident Synchronization PowerPack.

An *integration application* is a JSON object that includes all the information required for executing an integration on the Integration Service platform. In this Synchronization PowerPack, the integration applications are aligned with an SL1*Run Book Automation* that you can configure to ensure that whenever SL1 detects a new, acknowledged, or cleared Event, a corresponding Incident is created or updated in ServiceNow.

This chapter covers the following topics:

Event Data Flow Between Integration Service and ServiceNow	26
Overview of the Run Book Automation for Incident Sync	29
Configuring Incident Sync	31
Creating and Aligning a Configuration Object	31
Creating a ServiceNow Credential in SL1	36
Enabling the Run Book Automation Policies	38
Enabling and Customizing the Run Book Action Policy	
Sending Custom Data to ServiceNow Using the Passthrough Option	43
Configuring the "ServiceNow: Click to Create Incident" Automation Policy	47
Viewing Incidents and Events	
Incident Topology Suppression	50
Hyperlinking Events	56

Viewing the Incident Import Table in ServiceNow	57
ServiceNow, ScienceLogic Event, and Incident Priority Matrix	59
Adding Additional Fields to the Transform Map	60

#### Event Data Flow Between Integration Service and ServiceNow

#### Event Data Flow: Integration Service to ServiceNow

The following chart and steps illustrate the event data flow from the Integration Service to a ServiceNow instance:



- 1. Workers are subscribed to the Integration Service task queue.
- 2. When a new event to be synced is placed in the Integration Service task queue, it is assigned and pushed to a worker.
- 3. The worker processes and transforms the necessary SL1 event data into a ServiceNow incident and POSTs the incident to the ServiceNow endpoint.
  - If the resulting status code matches the expected status code for the request, the original message is acknowledged and removed from the queue.
  - If the worker crashes while processing the event, the queue senses the unexpected disconnect, and the same event message is re-delivered to a new worker.

**NOTE**: The above results are performed through the "late acknowledgment" of tasks. With this setting enabled, an Integration Service worker will not remove a message from the queue until the message has been fully processed by the worker. This setting can be enabled or disabled with the environment variable "task\_acks\_late".

4. If ServiceNow responds with an unexpected status code when POSTing the incident, the message will be placed back in the queue with specified re-try parameters.

**NOTE**: You can configure re-try parameters on a per-task basis. You may want to manually alter your re-try parameters for tasks depending on the action the task is taking. The configuration of retries includes the maximum number of times a task is retried after consistently failing, and the delay length between retries.

#### Event Data Flow: SL1 to Integration Service

The following chart and steps illustrate the event data flow from SL1 to the Integration Service:



- 1. Through a Run Book Automation, SL1 identifies an event that should be synced to ServiceNow.
- 2. A Run Book Action executes a POST action to the Integration Service API to let the Integration Service know that an integration should be run to sync the event.
  - If the Run Book Action is successful and the POST responds with a 200, then the event data is stored in the Integration Service queue for syncing.
  - If the POST does not respond with a 200, then the Run Book Action inserts the missed event into a table in the SL1 database so that it can be retrieved later.
- 3. In parallel, a scheduled Integration Service event continuously checks the SL1 database for any missed events. If any missed events are found, they will be pulled from the database and inserted into the Integration Service queue.

**NOTE**: The Integration Service queue is persistently saved to disk, so if the service stops, any events that existed in the queue before to the failure will still exist in the queue after the service is running again.

4. Missed events are not removed from the SL1 database until after they are inserted into the queue.

## Overview of the Run Book Automation for Incident Sync

You can configure a Run Book Automation to ensure that whenever SL1 detects a new, acknowledged, or cleared event, a corresponding incident is created or updated in ServiceNow:



The "ServiceNow: Add/Update/Clear Incident" Run Book Action policy is responsible for sending the SL1 payload to the Integration Service. The Integration Service then sends that payload to ServiceNow and creates, updates, acknowledges, or clears an incident, as needed.

SL1 features three Run Book Automation policies that facilitate this process:

- ServiceNow: Add/Update Incident
- ServiceNow: Event Acknowledged
- ServiceNow: Event Cleared

**NOTE**: A fourth Run Book Automation policy, "ServiceNow: Click to Create Incident" lets you manually create an incident in ServiceNow by clicking the life-preserver icon (<sup>1</sup>) in SL1. For more information, see Configuring the "ServiceNow: Click to Create Incident" Automation Policy.

**NOTE:** The "Sync Incident State from ServiceNow to SL1 Event" integration application does not have an associated Run Book Action that triggers Incident Sync. You must schedule this integration application to run every minute, or to a time suitable for your requirements. You can use a cron job to trigger this schedule, or you can use the Integration Service user interface to schedule the application. For more information about scheduling, see .

Each Run Book Automation policy calls a single action in SL1. Ensure that the integration application in the Integration Service points to the relevant SL1 system and ServiceNow instance. The action then calls an integration application on the Integration Service that determines the workflow to execute.

Events in SL1 frequently occur and resolve due to fluctuations in the network and other changing conditions. However, the Run Book Automation policies above use a de-duplication algorithm to ensure that only a single open ServiceNow incident exists per device. As a result, if a device already has an existing ServiceNow incident, the following updates are made to the ServiceNow incident record:

- The "Work Notes" activity log in the incident record is updated with information about the secondary event(s).
- If a secondary event is of a higher severity than the event that originally created the ServiceNow incident, then the *Impact*, *Urgency*, and *Priority* fields are updated automatically in the ServiceNow incident record. If the secondary event is of a lesser severity, those fields are not updated.
- If an event is cleared in SL1 and then later reoccurs before the incident has been "Closed" in ServiceNow, then the subsequent events appear in the original ServiceNow incident record for that device. If an incident record has been "Closed," then ServiceNow will create a new incident record when a cleared event reoccurs in SL1.
- By default, if an event is acknowledged in SL1, the ServiceNow incident record will be updated with the work notes and the acknowledging user. Clearing an SL1 event will move the ServiceNow incident record state to "Resolved". If all SL1 events associated with a ServiceNow incident record are clear, the ServiceNow incident record will, by default, move to a "Resolved" state.

**NOTE**: You can edit the Run Book Action Snippet code to adjust the behavior for changing states when an SL1 event is acknowledged or cleared.

## Configuring Incident Sync

This workflow covers how to set up the Run Book Automation to run Incident Sync:

- 1. Create a configuration object in the Integration Service user interface
- 2. Align the new configuration file with the following integration applications:
  - "Create or Update ServiceNow Incident from SL1 Event"
  - "Sync Incident State from ServiceNow to SL1 Event"
  - "Update ServiceNow Incident when SL1 Event is Acknowledged"
  - "Update ServiceNow Incident when SL1 Event is Cleared"
- 3. Create a ServiceNow credential in SL1
- 4. Enable the following Run Book Automation Policies:
  - "ServiceNow: Add/Update Incident"
  - "ServiceNow: Event Acknowledged"
  - "ServiceNow: Event Cleared
- 3. Enable and customize the "ServiceNow: Add/Update/Clear Incident" Run Book Action Policy
- 4. Optionally, send custom data to ServiceNow using the Passthrough Option
- 5. Optionally, enable and configure the "ServiceNow: Click to Create Incident" Policy

## Creating and Aligning a Configuration Object

A configuration object supplies the login credentials and other required information needed to execute the steps

for an integration application in the Integration Service. The **Configurations** page (<sup>©</sup>) of the Integration Service user interface lists all available configuration objects for that system.

You can create as many configuration objects as you need. An integration can only use one configuration object at a time, but you can use (or "align") the same configuration object with multiple integration applications.

To use the ServiceNow Incident Synchronization PowerPack, you will need to create a new configuration object in the Integration Service user interface and align that configuration object to the relevant integration applications that are triggered by the Run Book Actions in SL1.

**TIP**: Depending on your SL1 and ServiceNow environments, you might be able to use the same configuration object with other Integration Service: ServiceNow Synchronization PowerPacks.

#### Creating a Configuration Object

For this Synchronization PowerPack, you can make a copy of the "ServiceNow SyncPack" configuration object, which is the sample configuration file that was installed with the ServiceNow Base Synchronization PowerPack.

To create a configuration object based on the "ServiceNow SyncPack" configuration object:

- 1. In the Integration Service user interface, go to the **Configurations** page (\*\*).
- 2. Click the **[Actions]** button (<sup>‡</sup>) for the "ServiceNow SyncPack" configuration object and select *Edit*. The **Configuration** pane appears:

≡	Configurations				isadmin ~ 🔨 Sciencelogic
55	Q Search			ServiceNow SyncPack	×
•	CONFIG NAME	VER AUTHOR	MODIFIED (UTC -5) DESCRIF	Description Sample Configuration file for the ServiceNow SyncPack	Toggle JSON Editor
	Certified Application	1.3.3.7	Oct 22, 2019 10:56:01	Version 1.1.0	
٠	IS - System Backup Configuration Example	1.0.0 ScienceLogic	Oct 30, 2019 15:45:11 Examp	Configuration Data	
	IS - System Diagnostic Configuration Example	1.0.0 ScienceLogic	Oct 30, 2019 15:45:11 Examp	1 - 1 2 - 3 "encrypted": false,	î
	IS - System Backup Configuration	1.0.0 ScienceLogic	Oct 30, 2019 11:14:23 Examp	4 "name": "Sl1_host", 5 value": "em7.sciencelogic.com" 6 }, 7 - {	
	ServiceNow SyncPack	1.1.0 ScienceLogic	Oct 17, 2019 13:54:22 Sample	8 "encrypted": true, 9 "name": "Sllpassword", 10 "value": "d4fUXDjeDs+96ylhkOpBDeLnqxcooh2d8fwvnT6X6ck="	
	Aligned Integrations			12 - { 13 - { 14 "encrypted": false, 15 "encrypted": false, 16 "encrypted": false, 17 - encrypted": false, 18 - encrypted": false, 19 - encrypted: false, 19 -	
	NONE			16 }, 17~ {	
	Test Host Settings	1.0.0 ScienceLogic	Oct 09, 2019 A test 14:39:05	18 "encrypted": false, 19 "name": "\$l_db.host", 20 "value": "\${config.sli_host}" 21 },	
	ven01767	1.3.3.7	Oct 10, 2019 10:31:50 Domai	22- { "encrypted": false, "name": "511db_user", "value": "root"	
	ven01770	1.2.3 ScienceLogic	Oct 21, 2019 11:01:44 Sample	26 }, 27 - { 28 "encrypted": true,	
				<pre>29 "name": "S1_db_password", 30 "value": "X3Wz66e/MMwhiWHbjgXX06bfLNpFpdFQ/SZc2rCCYNY=" 31 }, 32 - (</pre>	
				33 "encrypted": false, 34 "name": "snow.host", 35 "value": "sciencelogic.service-now.com"	
				<pre>36 }, 37 - { 38 "encrypted": false, "name": "snow user".</pre>	
				expects type: json	
					Convas
					Copy as Save

3. Click [Copy as]. The Create Configuration pane appears:

Create Configuration			×
			Toggle JSON Edit
Friendly Name			
Description			
Author	Version		
Configuration Data Values			
Name	Value	_	~
sl1_host	em7.sciencelogic.com	Encrypted	^
Name	Value	_	~
sl1_password	SVh9nTCUEffef1edepEljW8NrgF	Encrypted	^
Name	Value		~
sl1_user	em7admin	Encrypted	~
Name	Value		~
sl1_db_host	\${config.sl1_host}	Encrypted	^
Name	Value		×
sl1_db_user	root	Encrypted	~
Name	Value		×
sl1_db_password	IDPx5IwLIX5HOQzsg6niL4FpSgc	Encrypted	~
Name	Value	_	~
snow_host	sciencelogic.service-now.com	Encrypted	×
			Save

- 4. Complete the following fields:
  - Friendly Name. Name of the configuration object that will display on the Configurations page.
  - **Description**. A brief description of the configuration object.
  - Author. User or organization that created the configuration object.
  - Version. Version of the configuration object.
- 5. Click [Toggle JSON Editor] to show the JSON code.
- 6. In the **Configuration Data** field, be sure to include the required block of code to ensure that the integration applications aligned to this configuration object do not fail:

```
{
  "encrypted": false,
  "name": "sl1_db_host",
  "value": "${config.sl1_host}"
}
```

For example:

```
{
  "encrypted": false,
  "name": "sll_db_host",
  "value": "10.2.11.42"
}
```

- **NOTE**: If you are using SL1 with an External Database (SL1 Extended architecture or a cloud-based architecture), update the "value" of that block of code to be the host of your database. This field accepts IP addresses. For example: "value": "db.sciencelogic.com". If you are *not* using the SL1 Extended architecture or a cloud-based architecture, you do not need to make any changes to the block of code other than pasting the code into the configuration object.
- 7. In the **Configuration Data** field, update the default variable definitions to match your Integration Service configuration.

**TIP**: The "ServiceNow SyncPack" configuration object contains all of the required variables. Simply update the variables from that object to match your SL1 and ServiceNow settings.

NOTE: The *region* value is a user-defined variable that will identifies your SL1 instance within ServiceNow.

- 8. To create a configuration variable, define the following keys:
  - **encrypted**. Specifies whether the value will appear in plain text or encrypted in this JSON file. If you set this to "true", when the value is uploaded, the Integration Service encrypts the value of the variable. The plain text value cannot be retrieved again by an end user. The encryption key is unique to each Integration Service system. The value is followed by a comma.
  - **name**. Specifies the name of the configuration file, without the JSON suffix. This value appears in the user interface. The value is surrounded by double-quotes and followed by a comma.
  - **value**. Specifies the value to assign to the variable. The value is surrounded by double-quotes and followed by a comma.
- 9. Click [Save]. You can now align this configuration object with one or more integration applications.

#### Aligning a Configuration Object

To run Incident Sync, you must "align" the configuration object to run with the following integration applications:

- "Create or Update ServiceNow Incident from SL1 Event"
- "Update ServiceNow Incident when SL1 Event is Acknowledged"
- "Update ServiceNow Incident when SL1 Event is Cleared"
- "Sync Incident State from ServiceNow to SL1 Event"

**NOTE:** The "Sync Incident State from ServiceNow to SL1 Event" integration application is the only application for Incident Sync that can be run manually or scheduled. The other three applications should only be triggered by Run Book Automations.

To align the configuration object with the relevant integration applications:

1. On the **Integrations** page of the Integration Service user interface, open an "incident" integration application and click **[Configure]** (. The **Configurations** pane for that application appears:

Create or Update ServiceNow Incident from SL1 Event Cancel Save							
Align configuration and sa	ve						
Configuration scopped-app-conf		-					
snow_hostname ven01056.service-no	snow_user is4User1	Ê	snow_password	sl1_hos 10.2.1	tname l 1.41	ê	
\${config.snow host}	\${config.snow user}			\${config	sl1 host}		
sl1_user em7admin	sl1_password						
\${config.sl1 user}							
eventDetails 1							
expects type: ison							
region	snow_state						
QARegion10	2						
\${config.region}							
passthrough							
expects type: json correlation_type 5						•	
discard	assignmentGroup		retry_max 0				

- 2. From the **Configurations** drop-down, select the configuration object you want to use.
- 3. Click **[Save]** to align that configuration with the integration application.
- 4. Wait until you see the "App & Confg modifications saved" pop-up message before proceeding.
- 5. Repeat this process for every integration application you want to use.

NOTE: The values for eventDetails and the other parameters that appear in the Configuration pane with a padlock icon (a) are populated either by the configuration object you aligned with the integration application or by the Run Book Action. Do not modify these values. If you encounter an error, make sure your Run Book Action is configured properly.

## Creating a ServiceNow Credential in SL1

To configure SL1 to communicate with ServiceNow, you must first create a SOAP/XML credential. This credential allows the Run Book Automation scripts and the Dynamic Applications in the ServiceNow Base Pack PowerPack to connect with your ServiceNow instance. These Run Book Automations are responsible for sending the SL1 event data to the Integration Service, which ultimately sends the data to a ServiceNow Incident.

The **ServiceNow RBA - Example** credential from the ServiceNow Base Pack PowerPack is an example SOAP/XML credential that you can configure for your own use.

To configure the ServiceNow RBA - Example credential:

- 1. In SL1, go to the **Credential Management** page (System > Manage > Credentials).
- 2. Locate the ServiceNow RBA Example credential and click its wrench icon (<sup>J</sup>). The Edit SOAP/XML Credential page appears:

Credential Editor [85]							
Edit SOAP/XML Credential #85 New Reset							
Basic Settings         Profile Name       Content Encoding       Method       HTTP Version         [ServiceNow RBA - Example       [text/xml] <ul> <li>[POST]</li> <li>[HTTP/1.1]</li> <li>URL [https://INTEGRATIONSERVICEHOSTNAME</li> <li>HTTP Auth User</li> <li>HTTP Auth Password</li> <li>Timeout (seconds)</li> <li>[USERNAME</li> </ul> <ul> <li>[ServiceNome]</li> <li>[HTTP Auth Password</li> <li>[ServiceNome]</li> <li>[ServiceNome]</li> <li>[ServiceNome]</li> </ul> <ul> <li>[HTTP Auth Password</li> <li>[ServiceNome]</li> <li>[ServiceNome]</li> </ul> <ul> <li>[ServiceNome]</li> <li>[ServiceNome]</li> <li>[ServiceNome]</li> <li>[ServiceNome]</li> <li>[ServiceNome]</li> <li>[ServiceNome]</li> </ul>	Soap Options Embedded Password [%P] Embed Value [%1] Embed Value [%1] Embed Value [%2] Embed Value [%3] Embed Value [%4]						
Proxy Settings Hostname/IP Port User	HTTP Headers + Add a header						
CURL Options CAINFO CAPATH CLOSEPOLICY CONNECTTIMEOUT COOKIE COOKIEFILE COOKIEJAR COOKIELIST CRLF CUSTOMREQUEST DNSCACHETIMEOUT							
Save Save As							

- 3. Complete the following fields:
  - Profile Name. Type a new name for the ServiceNow credential.
  - Content Encoding. Make sure text/xml is selected.
  - Method. Make sure POST is selected.
  - HTTP Version. Select HTTP/1.1.
  - URL. Type the URL for your Integration Service instance.
  - HTTP Auth User. Type the username of your Integration Service instance.
- HTTP Auth Password. Type the password of your Integration Service instance.
- Timeout. Type "5".
- 4. Click [Save As].
- 5. When the confirmation message appears, click **[OK]**.
- 6. On the **Credential Management** page (System > Manage > Credentials), make a note of the value in the **ID** column for the credential you just created:

Credential Management   Credentials Fo	ound [1]									Actions	Reset	Guide
Profile Name +	Organization	RO Use	<u>RW</u> <u>Use</u>	DA Use	Type Credential User	Host	Port	Timeout (ms		Last Edited	Edited By	
1. 🤌 ServiceNow RBA - Example	🙀 [all orgs]				SOAP/XML Host USERNAME	INTEGRATIONSERVICEHOSTNAME	443	5000	107	2019-07-15 11:10:54	em7admin	
										•		

You will use this value with the "sl1\_credential\_id" parameter when you **enable and customize the** snippet code of the "ServiceNow: Add/Update/Clear Incident" Run Book Action:

Policy Editor   Editing Action [50]       Reset         Action Name       Action State         ServiceNow: Add/Updates/Clear Incident       [Enabled]         Description         Adds and Updates Incidents in ServiceNow.       Description         Adds and Updates Incidents in ServiceNow.       Organization         Organization       Action Type         [System]       ServiceNow: Create, Update, Clear Incident (1.0)         Execution Environment       Action Run Context         [Default: ServiceNow Base Pack]       [Database]         Input Parameters       [         {       "sell credential_id": "",         "debug": false,       "         "configuration": "",       "debug": false,         "is_app_name_new": "incident_sync_update_create",       ^         "is_app_name_clear": "event_acknowledged",       "         "is_app_name_clear": "event_cleared",       "         "servicenow_state_ack": "",       "         "servicenow_state_clear": "6",       "         "correlation_type": "5",       "         "assignment_group_new": "",       "	ction Editor	
Action Name     Action State       ServiceNow: Add/Update/Clear Incident     [Enabled]       Description       Adds and Updates Incidents in ServiceNow.       Organization     Action Type       [[System]       ServiceNow: Create, Update, Clear Incident (1.0)       Execution Environment     Action Run Context       [-Default: ServiceNow Base Pack]     [Database]       *     "sl1_credential_id": "", "debug": false, "configuration": "", "debug": false, "is_app_name_new": "incident_sync_update_create", "is_app_name_clear": "event_cleared", "servicenow_state_new": "1", "servicenow_state_clear": "6", "correlation_type": "5", "assignment_group_new": "", "assignment_group_new": "", "assignment_group_new": "",	Policy Editor   Editing Action [50]	Reset
ServiceNow: Add/Update/Clear Incident       [Enabled]         Description         Adds and Updates Incidents in ServiceNow.         Organization       Action Type         [System]       ServiceNow: Create, Update, Clear Incident (1.0)         Execution Environment       Action Run Context         [Default: ServiceNow Base Pack]       [Database]         Input Parameters       [         "sll_credential_id": "",       "debug": false,         "configuration": "",       "uqueue": "",         "debug": false,       "is app_name_new": "incident_sync_update_create",         "is_app_name_ack": "event_cleared",       "is_app_name_ack": "event_cleared",         "servicenow_state_new": "1",       "servicenow_state_clear": "6",         "correlation_type": "5",       "assignment_group_new": "",         "assignment_group_new": "",       "assignment_group_new": "",	Action Name	Action State
Description         Adds and Updates Incidents in ServiceNow.         Organization       Action Type         [System]       ServiceNow: Create, Update, Clear Incident (1.0)         Execution Environment       Action Run Context         [Default: ServiceNow Base Pack]       [Database]         Input Parameters       [         "sl1_credential_id": "", "debug": false, "configuration": "", "queue": "", "discard_if_no_ci": false, "is_app_name_new": "incident_sync_update_create", "is_app_name_clear": "event_cleared", "is_app_name_clear": "event_cleared", "servicenow_state_new": "1", "servicenow_state_ack": "", "servicenow_state_ack": "", "assignment_group_new": "", "assignment_group_new": "", "assignment_group_new": "",	ServiceNow: Add/Update/Clear Incident	[Enabled]
Action Type         Organization       Action Type         [System]       ServiceNow: Create, Update, Clear Incident (1.0)         Execution Environment       Action Run Context         [Default: ServiceNow Base Pack]       [Database]         Input Parameters       [Input Parameters         {       "sl1_credential_id": "", "debug": false, "configuration": "", "gueue": "", "discard_if_no_ci": false, "is_app_name_new": "incident_sync_update_create", "is_app_name_clear": "event_cleared", "is_app_name_clear": "event_cleared", "servicenow_state_new": "1", "servicenow_state_lear": "6", "correlation_type": "5", "assignment_group_new": "", "assignment_group_new": "",       v	Descri	iption
Organization       Action Type         [System]       ServiceNow: Create, Update, Clear Incident (1.0)         Execution Environment       Action Run Context         [Default: ServiceNow Base Pack]       [Database]         Input Parameters       [action figuration": "", "debug": false, "configuration": "", "ducue": "", "discard_if_no_ci": false, "is_app_name_new": "incident_sync_update_create", "is_app_name_new": "incident_sync_update_create", "is_app_name_clear": "event_cleared", "servicenow_state_new": "1", "servicenow_state_lear": "6", "correlation_type": "5", "assignment_group_new": "", "assignment_group_new": "",		A stine Time
Execution Environment       Action Run Context         [Default: ServiceNow Base Pack]       [Database]         Input Parameters         {         "sll_credential_id": "",         "debug": false,         "configuration": "",         "queue": "",         "discard_if_no_ci": false,         "is_app_name_new": "incident_sync_update_create",         "is_app_name_clear": "event_cleared",         "servicenow_state_ack": "",         "servicenow_state_lear": "6",         "correlation_type": "5",         "assignment_group_new": "",         "assignment_group_new": "",	[System]	ServiceNow: Create, Update, Clear Incident (1.0)
Execution Environment       Action Run Context         [Default: ServiceNow Base Pack]       [Database]         Input Parameters         {         "sll_credential_id": "", "debug": false, "configuration": "", "queue": "", "discard_if_no_ci": false, "is_app_name_new": "incident_sync_update_create", "is_app_name_ack": "event_acknowledged", "is_app_name_clear": "event_cleared", "servicenow_state_new": "1", "servicenow_state_clear": "6", "correlation_type": "5", "assignment_group_new": "", "assignment_group_new": "",	(	
<pre>[Default: ServiceNow Base Pack]</pre>	Execution Environment	Action Run Context
<pre>Input Parameters {     "sll_credential_id": "",     "debug": false,     "configuration": "",     "gueue": "",     "discard_if_no_ci": false,     "is_app_name_new": "incident_sync_update_create",     "is_app_name_ack": "event_acknowledged",     "is_app_name_clear": "event_cleared",     "servicenow_state_new": "1",     "servicenow_state_lear": "6",     "correlation_type": "5",     "assignment_group_new": "",     "assignment_group_new": "",</pre>	[ Default: ServiceNow Base Pack ]	[Database]
<pre>{     "sll_credential_id": "",     "debug": false,     "configuration": "",     "gueue": "",     "discard_if_no_ci": false,     "is_app_name_new": "incident_sync_update_create",     "is_app_name_ack": "event_acknowledged",     "is_app_name_clear": "event_cleared",     "servicenow_state_new": "1",     "servicenow_state_lear": "6",     "correlation_type": "5",     "assignment_group_new": "",     "assignment_</pre>	Input Para	ameters
	<pre>"sl1_credential_id": "",    "debug": false,    "configuration": "",    "discard_if_no_ci": false,    "is_app_name_new": "incident_sync_upda    "is_app_name_ack": "event_acknowledged    "is_app_name_clear": "event_cleared",    "servicenow_state_new": "1",    "servicenow_state_ack": "",    "servicenow_state_clear": "6",    "correlation_type": "5",    "assignment_group_new": "",    "assignment_group_ack": "", </pre>	te_create", ",

# Enabling the Run Book Automation Policies

Before you can run the "ServiceNow: Add/Update/Clear Incident" Run Book Action, you must enable the three related Run Book Automation policies in SL1:

- ServiceNow: Add/Update Incident
- ServiceNow: Event Acknowledged
- ServiceNow: Event Cleared

To enable the three ServiceNow Run Book Automation policies:

- 1. In SL1, go to the Automation Policy Manager page (Registry > Run Book > Automation).
- 2. Locate the "ServiceNow: Add/Update Incident" automation policy and click its wrench icon (*P*). The **Automation Policy Editor** page appears:

Automation Policy Editor   Editir	ng Automation P	olicy [43]		Reset
Policy Name ServiceNow: Add/Update Incident Criteria Logic [Severity >=] V [Notice,] V	Policy Type [Active Events] Match Logic [Text search]	Policy State [Enabled]	Policy Priority [High]	Organization [System] 🗸
[ and no time has elapsed ]       ~         [ since the first occurrence, ]       ~         [ and event is NOT cleared ]       ~         [ and all times are valid ]       ~         ✓       Trigger on Child Rollup	Repeat	t Time	Align \ [Devices] ices (organizations, ass	Vith v
Available Devices System ScienceLogic, Inc.: EM7 All-In-One: auto-tes ScienceLogic, Inc.: EM7 All-In-One: em7-ao ScienceLogic, Inc.: EM7 All-In-One: em7-ao ScienceLogic, Inc.: EM7 All-In-One: em7-ao	st -40 -37 -39	Aligned Devices (All devices)		
Available Events [3569] Critical: AKCP: AC Voltage sensor de [3578] Critical: AKCP: DC Voltage sensor Lb [3579] Critical: AKCP: DC Voltage sensor Lb [3568] Critical: AKCP: Dry Contact Sensor L [3574] Critical: AKCP: Smoke Detector Alert! [3572] Critical: AKCP: Water Sensor has de	stects no current gh Critical w Critical ow Critical tected water	Aligned Events (All events)		< >
Available Actions SNIMP Trap [1]: EM7 Event Trap Snippet [5]: AWS: Disable Instance By Tag Snippet [5]: AWS: Biscover from EC2 IP Snippet [5]: AWS: Get EC2 Instance Config Snippet [5]: AWS: Merge Physical with Com Snippet [5]: AWS: Anish Terminated EC2 In Snippet [5]: Classe: ACI Davise Class Design	iration ponent stances	Aligned Actions	eate, Update, Clear Incid	ent [100]: Si
	Save	Save As		

- 3. Update the following fields:
  - **Policy State**. Select Enabled.
  - **Policy Priority**. Select High to ensure that this Integration Service automation policy is added to the top of the queue.
  - Available Actions. If it is not already selected, select the corresponding ServiceNow Run Book Action policy.

TIP: By default, the "ServiceNow: Add/Update Incident" automation policy will create ServiceNow incidents for all devices. You can limit the devices affected by making changes to the Organization, Severity, Match Logic, Aligned Devices, and/or Aligned Events fields.

WARNING: ScienceLogic highly recommends that you do not make changes to the **Policy Type**, **Repeat Time**, or **Align With** fields or the And event is NOT acknowledged setting.

- 4. Click [Save].
- 5. Repeat steps 2-4 for the "ServiceNow: Event Acknowledged" and "ServiceNow: Event Cleared" Run Book Automation policies.

# Enabling and Customizing the Run Book Action Policy

The "ServiceNow: Add/Update/Clear Incident" Run Book Action policy contains several default values in the snippet code for the policy that you can customize for Incident Sync. You can edit these values in the **Input Parameters** pane of the **Action Policy Editor** page for this policy.

For example, the **Correlation Type** is a value that you can use to correlate an SL1 event with a ServiceNow incident. For the Correlation Type, which is also called the "Correlation ID", you can choose a number of different ways in which an incident can be created. The default setting is "correlation\_type": "5", which means that this Run Book Action correlates all events by device ID and event policy ID, and if the event matches and the state is active, the Action updates the existing incident. The Action creates a *new* incident if the event does *not* match by device ID and event policy ID. As a result, the Correlation Type helps determine which events get rolled up under an incident. All Run Book Action scripts should use the same Correlation Type value, otherwise correlation will fail.

To enable and customize the Run Book Automation policies:

- 1. In SL1, go to the **Action Policy Manager** page (Registry > Run Book > Actions).
- 2. Locate the ServiceNow: Add/Update/Clear Incident policy and click its wrench icon (*P*). The Action Policy Editor page appears:

Action Editor	×								
Policy Editor   Editing Action [50]	Reset								
Action Name	Action State								
ServiceNow: Add/Update/Clear Incident									
Description									
Adds and Updates Incidents in ServiceNow.									
Organization	Action Type								
[System]	ServiceNow: Create, Update, Clear Incident (1.0)								
Execution Environment	Action Run Context								
[ Default: ServiceNow Base Pack ]	[Database]								
<pre>#putrak {     "sll_credential_id": "",     "debug": false,     "configuration": "",     "discard_ifn_coi": false,     "is_app_name_new": "incident_sync_upda     "is_app_name_clear": "event_cleared",     "servicenow_state_ack": "",     "servicenow_state_clear": "6",     "correlation_type": "5",     "assignment_group_new": "",     "assignment_group_new: "",</pre>	ameters								

- 3. For the Action State filed select Enabled.
- 4. In the **Input Parameters** pane, edit the snippet code as necessary, using the information in the **Customizing the Snippet Code in the Input Parameters Pane** section, below. When you are finished, click **[Save]**.

#### Customizing the Snippet Code in the Input Parameters Pane

SL1 Run Book Action snippets are written in Python. In the event of a syntax error, the policies will no longer run. As a result, you must ensure that all edits adhere to Python standards. True and False options are case-sensitive and must not contain quotes.

**NOTE**: Previous SyncServer users had three separate Run Book Action scripts for add/update, acknowledge, and clear. These have been rolled into a single Run Book Action in the Integration Service, but there are still three Automation policies.

You can customize the following values in the "ServiceNow: Add/Update/Clear Incident" Run Book Action snippet code:

- *sl1\_credential\_id*. Specifies the ID of the credential object. You can find this value in the **ID** column of the **Credentials** page (System > Manage > Credentials of SL1.
- **debug**. A true/false value that determines if the action is logged in SL1 and if the application is run in Debug Mode on the Integration Service. Troubleshooting logs are written to **/data/tmp/servicenow\_rba.log**.
- configuration. Specifies the ID of the configuration object used on the Integration Service. The configuration ID is all lower-case, with spaces in the configuration object "friendly" name replaced by underscores. For example: "configuration": "servicenow\_syncpack\_configs"

**NOTE**: To find the configuration ID with the API, make a GET request on this endpoint: https://<Integration\_Service\_hostname>/api/v1/configurations.

- queue. Specifies the worker queue on which the application runs. Leave this as default.
- **discard\_if\_no\_ci**. Specifies whether the Integration Service should create incidents in ServiceNow for devices that do not have a matching CI record. The default is *false*. Your options include:
  - true. If a device is not mapped to a CI, the Integration Service will not create an incident in ServiceNow, and SL1 is not updated. The following log message appears: "No CI found".
  - false. If a device is not mapped to a CI, the Integration Service will create an incident in ServiceNow and update SL1.

#### • servicenow\_state\_new:

- 1. Incident state is "New". This is the default value.
- 2. Incident state is "In Progress".
- 3. Incident state is "On Hold".
- 6. Incident state is "Resolved".
- 7. Incident state is "Closed".
- 8. Incident state is "Canceled".
- servicenow\_state\_ack:
  - 1. Incident state is "New". There is no default value.
  - 2. Incident state is "In Progress".
  - 3. Incident state is "On Hold".
  - 6. Incident state is "Resolved".
  - 7. Incident state is "Closed".
  - 8. Incident state is "Canceled".

#### • servicenow\_state\_clear:

- 1. Incident state is "New".
- 2. Incident state is "In Progress".
- 3. Incident state is "On Hold".
- 6. Incident state is "Resolved". This is the default value.
- 7. Incident state is "Closed".
- 8. Incident state is "Canceled".
- correlation\_type. Correlates an SL1 event with a ServiceNow incident. For this value, which is also called the "Correlation ID", you can choose a number of different ways in which an incident can be created. The default setting is "correlation\_type": "5", which means that this Run Book Action correlates all events by device ID and event policy ID, and if the event matches and the state is active, the Action updates the existing incident. The Action creates a *new* incident if the event does *not* match by device ID and event policy ID. As a result, the Correlation Type helps determine which events get rolled up under an incident. All Run Book Action scripts should use the same Correlation Type value, otherwise correlation will fail.

The possible Correlation Type values include the following:

- 1. Correlate all duplicate incidents by SL1 ID only.
- 2. Correlate all duplicate incidents by event policy ID only.
- 3. Correlate all duplicate incidents by device ID only.
- 4. Correlate all duplicate incidents by Interface ID only. This correlation requires that the SL1 event has an interface aligned. If there is no interface aligned to the event, the returned Interface ID will be 0.
- 5. Correlate all duplicate incidents by device ID and event policy ID. This is the default Correlation Type value.
- 6. Correlate all duplicate incidents by device ID, event policy ID, and event sub entity ID.
- 7. Correlate all duplicate incidents by device ID, event policy ID, region, and event ID. Please note that using this correlation type will result in all events triggering new incidents.
- 8. Correlate all events to the root device ID of the component device into one incident. Please note
  that using this correlation type might lead to undesirable behavior, as not all events generated on a
  child device indicate a problem on the root device. As a result, ScienceLogic recommends that you
  only use this correlation type against specific event policies.
- You can assign the assignment group to one of the new, acknowledged, or cleared incidents that are mapped. To disable this feature, ensure that no values are set. After an incident is created, the assignment group value will not be changed by the Run Book Action. To assign an assignment group, set the variable value to the **sys\_id** of the ServiceNow Assignment Group. In the following example, the assignment group is assigned to incidents that are *cleared*:

```
"assignment_group_new": "",
"assignment_group_ack": "",
"assignment_group_clear": "sys_id"
```

## Customizing Logging in the Run Book Action

You can customize the following logging-related items in the "ServiceNow: Add/Update/Clear Incident" Run Book Action snippet code:

- logfile = /data/tmp/ServiceNow\_add\_update\_clear\_incident.log
  - Location for logging output.
  - Will be created if it does not exist.
  - Will be appended with each Run Book job.
  - Is case-sensitive.
- do\_debug\_logging = True
  - True is on, False is off.
  - Is case-sensitive.
  - For troubleshooting, these can be enabled or changed.
  - Writes logs to /data/tmp/servicenow\_rba.log.

# Sending Custom Data to ServiceNow Using the Passthrough Option

You can use the "ServiceNow: Add/Update Incident" Run Book Automation and the "ServiceNow: Add/Update/Clear Incident" Run Book Action to "pass through" custom data to ServiceNow. For example, you might want to use the passthrough functionality to overwrite the impact and urgency of a ServiceNow Incident, which is the only way to change the priority of the Incident.

To pass custom data to ServiceNow:

- Create a new Run Book Action that pulls the relevant data and adds it to a dictionary called EM7\_RESULT.
- Add the new Run Book Action to the "ServiceNow: Add/Update Incident" Run Book Automation Policy, ahead of the "ServiceNow: Add/Update/Clear Incident" Run Book Action so that the new Action runs first, and then is consumed by the ServiceNow Action.

The following procedure describes how to configure the passthrough functionality.

## Passing Custom Data to ServiceNow

To pass custom data to ServiceNow:

1. In SL1, go to the **Action Policy Manager** page (Registry > Run Book > Actions) and click **[Create]** to create a new Run Book Action policy:

Action Name       Action State         Example Passthrough EM7_RESULT       [Enabled]         Description       Passthrough data using EM7_RESULT disctionary         Organization       Action Type         [System]       Run a Snippet         Snippet Credential       Action Run Context         Execution Environment       [Default Environment]         Snippet Code       Snippet Code         EM7_RESULT = {"work_notes": "This is a new note"}	Policy Editor   Creating New Action				Reset
Example Passthrough EM7_RESULT       [Enabled]         Description         Passthrough data using EM7_RESULT disctionary         Organization       Action Type         [System]       Run a Snippet         Snippet Credential       Action Run Context       Execution Environment         (None)       Database       [Default Environment]         Snippet Code       EM7_RESULT = {"work_notes": "This is a new note"}	Action Name				
Description         Passthrough data using EM7_RESULT disctionary         Organization       Action Type         [System]       Run a Snippet         Snippet Credential       Action Run Context       Execution Environment         (None)       Database       [Default Environment]         Snippet Code       EM7_RESULT = {"work_notes": "This is a new note"}	Example Passthrough EM7_RESULT		[Enabled]		$\sim$
Passthrough data using EM7_RESULT disctionary       Organization       Action Type       [System]       Image: Snippet Credential       Action Run Context       Execution Environment       (None)       Image: Database       Snippet Code       EM7_RESULT = {"work_notes": "This is a new note"}		Descr	ription		
Organization     Action Type       [System]     Run a Snippet       Snippet Credential     Action Run Context     Execution Environment       (None)     Database     [Default Environment]       Snippet Code     Snippet Code       EM7_RESULT = {"work_notes": "This is a new note"}	Passthrough data using EM7_RESULT disc	tionary			
[System]       Image: Construction of the system of the syst	Organization			Action Type	
Snippet Credential       Action Run Context       Execution Environment         (None)       Database       [Default Environment]         Snippet Code       EM7_RESULT = {"work_notes": "This is a new note"}	[System]	$\sim$	Run a Snippet		~
(None) Database Contract Excellent Environment] Snippet Code EM7_RESULT = {"work_notes": "This is a new note"}	Snippet Credential	Action Pu	in Context	Execution Environ	ment
Snippet Code EM7_RESULT = {"work_notes": "This is a new note"}	(None)	Database	~	[ Default Environment]	~
<pre>EM7_RESULT = {"work_notes": "This is a new note"}</pre>		Snippe	t Code		

- 2. Complete the following fields:
  - Action Name. Type a unique name for the Action.
  - Action State. Select Enabled.
  - Action Type. Select Run a Snippet.
  - Execution Environment. Select ServiceNow Base Pack.
  - Complete the other fields as needed.

3. In the **Snippet Code** pane, add the snippet code you want to include for the EM7\_RESULT dictionary. For example, the following snippet code lets you override the ServiceNow Incident work notes with a hardcoded note:

```
EM7 RESULT = { "work notes": "This is a new note" }
```

Additional notes about the structure of the EM7\_RESULT dictionary:

- EM7\_RESULT = is required for the dictionary, and the formatting of the keys should match the example above.
- All keys defined in the EM7\_RESULT dictionary need to map to field IDs on the **ScienceLogic Events** table in ServiceNow.
- You can hard-code the values in the EM7\_RESULT dictionary, or you can use variables and functions, like the "Snippet Code Example", below.
- As a best practice, avoid sending null passthrough values to ServiceNow. If you must send 'null' or 'NULL' values to ServiceNow, pass through that value as an empty string, such as "location":"". Also, only pass through values that you need. For example, instead of sending {"location": "", "work\_notes": "stuff"}, simply send {"work\_notes": "stuff"}.
- A long snippet might delay the ticket being created
- 4. Click [Save].
- 5. Go to the **Automation Policy Manager** page (Registry > Run Book > Automation) and open the "ServiceNow: Add/Update Incident" Run Book Automation Policy.

6. In the **Available Actions** section, add the new Run Book Action before the "ServiceNow: Create, Update, Clear Incident" Run Book Action:

Policy Name		Policy Type	Policy State		Policy Pri	ority	Organization
ServiceNow: Add/Update Incident		[Active Events] *	[Enabled]		[High]		[System]
Criteria Logic		Match Looic		_	Match Su	otax	
Severity >= 1 T Major 1	•	[Text search ] Y	10	-	interest of	THEA.	
and no time has elapsed 1				-		0213	02201
I since the first occurrence 1		Rep	eat Time	n With			
and event is NOT cleared 1		[ Only once ]		•	[Devices]		
[ and all times are valid ]	Include events fo	r entities other than	devi	ces (organizati	ons, ass	ets, etc.)	
Trigger on Child Rollup							
vailable Devices			Aligned Device	5			
			(All devices)	-			
servicewow, instance: venu1056			«				
vailable Events			Aligned Events				
			(All events)				
3569] Critical: AKCP: AC Voltage sen 3576] Critical: AKCP: DC Voltage sen 3579] Critical: AKCP: DC Voltage sen 3569] Critical: AKCP: Dry Contact Ser 3574] Critical: AKCP: Smoke Detector 3572] Critical: AKCP: Water Sensor h	sor dete sor High sor Low nsor Low r Alerti as detec	cts no current A Critical Critical V Critical ded water V	2				
vailable Actions			Aligned Actions	8			
Snippet [5]: Cisco: VOS Component to Snippet [5]: Cisco: VOS Node Classific Snippet [5]: Dell EMC: Unity Classify R Snippet [5]: Dell EMC: VMAX Unisphet Snippet [5]: EM7 Ping Snippet	Physica cation ar loct Dev re Class	al Merge d Cluster Crea foe Class ify Root Device	1 Snippet [5] 2. ServiceNow *	Cre	nple Passifivou sate, Update, C	igh EM7 lear Inci	RESULT A

- **NOTE:** The output of this new Run Book Action will be consumed by the "ServiceNow: Create, Update, Clear Incident" Run Book Action, ensuring that the EM7\_RESULT dictionary is passed through to ServiceNow. The "ServiceNow: Create, Update, Clear Incident" Run Book Action automatically populates the passthrough values with any values from EM7\_LAST\_RESULT. The passthrough overwrites any other previously defined fields, such as assignment group.
- 7. You can add additional Run Book Actions to the Run Book Automation Policy for any additional workflows that you might want to run. The Automation Policy execute these Actions in a sequential, top-down order. However, the "ServiceNow: Create, Update, Clear Incident" Run Book Action only consumes the EM7\_RESULT dictionary from the Run Book Action directly above it.

## Snippet Code Example

The following snippet code example shows how to pull additional information and make it available for passthrough. All of the additional information that is going to be sent is contained in a dictionary variable called EM7\_RESULT. You can pass through multiple items through in a single Run Book Action by adding additional keys to the EM7\_RESULT dictionary.

This example lets you assign assignment groups to an Incident based on certain criteria, such as event policy IDs:

```
from future.utils import iteritems
def invert mappings (mappings):
    .....
    Invert received one-to-many mappings and converts it into a one-to-one
    mapping.
    Args:
       mappings (dict): Dictionary of mapped values
   Returns:
        dict: inverted dictionary.
    .....
    inverted_mappings = dict()
    for key, values in iteritems(mappings):
        for sub value in values:
           invert mappings[sub value] = key
    return inverted mappings
# Example of assignment group to list of event policy ids mapping.
assignment_groups to event policies = {
    "sys_id_1": [1, 2, 3, 4, 5],
    "sys id 2": [6, 7, 8, 9, 10],
# which sys id to use if the current event policy id isn't mapped
default sys id = "sys id 3"
# invert the mappings
event_policy_to_assignment_group = invert_mappings(assignment_groups_to_event_
policies)
# Send assignment group sys id to IS RBA
EM7 RESULT = \{
    "assignment_group": event_policy_to_assignment_group.get(
        EM7 VALUES["%3"], default sys id
    )
}
```

# Configuring the "ServiceNow: Click to Create Incident" Automation Policy

The "ServiceNow: Click to Create Incident" Run Book Automation policy lets you manually create an incident in ServiceNow by clicking the life-preserver icon (<sup>1)</sup>) in SL1. This policy is available in the ServiceNow Base Pack PowerPack.

To configure the "ServiceNow: Click to Create Incident" policy:

- 1. In SL1, go to the Behavior Settings page (System > Settings > Behavior) and set the **Event Console Ticket** Life Ring Button Behavior option to Create/View External Ticket.
- 2. Click **[Save]** to save your changes.
- 3. Go to the Automation Policy Manager page (Registry > Run Book > Automation).
- 4. Locate the ServiceNow: Click to Create Incident policy and click its wrench icon (*P*). The Automation Policy Editor page appears:

Automation Policy Editor   Editing Automation F	Policy [59] Reset
Policy Name     Policy Type       ServiceNow: Click to Create Incident     [Active Events] v       Criteria Logic     Match Logic       [Severity >= ] v     [Minor,] v       [and no time has elapsed] v     Repe       [and external ticket IS requested] v     Include events fo       [and all times are valid] v     Include events fo	Policy State Enabled V Policy Priority Organization [Default] V Match Syntax at Time Satisfied V r entities other than devices (organizations, assets, etc.)
Available Devices	Aligned Devices
Bananaquit AWS: Service: JEM-Virtual Cardinal Microsoft: Windows Server 2008 R2 Domain Controller: VPW NET-SNMP: Linux: sctest NET-SNMP: Linux: sctest NET-SNMP: Linux: sctest NET-SNMP: Linux: sctest NET-SNMP: Linux: sctest NET-SNMP: Linux: sctest	(All devices)
Available Events	Aligned Events
[3186] Critical: AKCP: AC Voltage sensor detects no current [3195] Critical: AKCP: DC Voltage sensor High Critical [3196] Critical: AKCP: DC Voltage sensor Low Critical [3183] Critical: AKCP: Dry Contact Sensor Low Critical [3191] Critical: AKCP: Norke Detector Alert [3193] Critical: AKCP: Water Sensor has detected water [3153] Critical: AKCP: Water Sensor has detected water	(All events)
Available Actions	Aligned Actions
SNMP Trap [1]: EM7 Event Trap Snippet [5]: AWS: Disable Instance By Tag Snippet [5]: AWS: Discover from EC2 IP Snippet [5]: AWS: det EC2 Instance Configuration Snippet [5]: AWS: Merge Physical with Component Snippet [5]: AWS: Vanish Terminated EC2 Instances Science 1: Clines: ACI During Clines Dealingment	1. ServiceNow: Create, Update, Clear Incident [106]: Si ∧ ≫ «
Save	Save As

- 5. Update the following fields:
  - Policy State. Select Enabled.
  - **Repeat Time**. Specify the frequency at which SL1 should execute the automation policy while the conditions are still met. The choices range from "every 30 seconds until satisfied" to "every 2 hours until satisfied", or "only once". By default, the policy only runs once.
  - Available Actions. If it is not already selected, select the corresponding ServiceNow Run Book Action policy to add it to the Aligned Actions field.
- 6. Click [Save].

# Viewing Incidents and Events

To view SL1-created incidents in ServiceNow, go to the **Incidents** page (Incident > Open) in ServiceNow:

	service <b>nuw</b>	Serv	vice A	uton	nation							Se	arch Q -	
laugator	Welcome: em7 admin 💄 🔒		lene lene lene lene lene lene lene lene											
And Form	☆ Type filter text	≡ ^		ncidents	New Go to	lumber v :	Search				v	• •• • 1 to	44 of 44 🕨 🕨	
	Incident													
agged	🏫 Create New		7 /	All> Acti	ive = true									
uments	Assigned to me	- 11	49	Q	■ Number ▼	≡ Caller	Short description	■ Category	$\equiv$ Correlation ID	■ Priority	≡ State	■ Assignment group	$\equiv$ Assigned to	
okmarks	Copen - Unassigned				Search	Search	Search	Search	Search	Search	Search	Search	Search	
0	☆ Resolved ☆ Closed			(i)	INC0010677		It-esxi-demo3.sciencelogic.local: GeneralHostWarningEvent: Issue Detected On It-	Monitoring	EM7+EVENT+107	3 - Moderate	Awaiting Evidence			
tark and sated UI sep	★ All ☆ Overview			<b>(i)</b>	INC0010676		TCPREPLAY: Device Failed Availability Check: Component Device 209 Is Not Availab	Monitoring	EM7+EVENT+209	• 2 - High	New			
m Logs >	Critical Incidents Map Problem	- 5		(i)	INC0010675		TCPREPLAY: Device Failed Availability Check: Component Device 208 Is Not Availab	Monitoring	EM7+EVENT+208	• 2 - High	Awaiting Evidence			
istem nžion > Han Rules	Change			(i)	INC0010674		PlixerSCILOBD: Device Failed Availability Check: Component Device 206 Is Not Ava	Monitoring	EM7+EVENT+206	• 2 - High	Awaiting Evidence			
	Business Services			0	INC0010673		JPLDemoTest: Device Failed Availability Check: Component Device 205 Is Not Avail	Monitoring	EM7+EVENT+205	• 2 - High	Awaiting Evidence			
	Groups     Application Servers			<b>(i)</b>	INC0010672		Lab-xen01.acme.com: Filesystem Unavailable: /var/run/sr-mount/1ca767c5-3008-558	Monitoring	EM7+EVENT+88	3 - Moderate	Awaiting Evidence			
	★ All ☆ Tomcat	*		0	INC0010671		CUCM10-01.qa.sciencelogic.local: Device Failed Availability Check: UDP - SNMP	Monitoring	EM7+EVENT+204	• 2 - High	Awaiting Evidence			
	☆ BEA Weblogic ☆ IBM Websphere			i	INC0010670		Svcnowdemo_db: Physical Memory Has Exceeded Threshold: (80%) Currently (81%)	Monitoring	EM7+EVENT+164	3 - Moderate	Awaiting Evidence			
	☆ Java ☆ JBoss			0	INC0010669		Svcnowdemo_col1: Physical Memory Has Exceeded Threshold: (80%) Currently (85%)	Monitoring	EM7+EVENT+163	3 - Moderate	Awaiting Evidence			
	Domino  Web Servers  Servere	ers C		(i)	INC0010668		NTNX-15SM65260085-C-CVM: Nutanix: CVM Exceeded High Memory Threshold: 100%	Monitoring	EM7+EVENT+191	3 - Moderate	New			
	★ All ★ Linux			(i)	INC0010667		Dc2bhntxclst01: Nutanix Cluster Alert [Warning]: Wall Clock Time Has Drifted By	Monitoring	EM7+EVENT+166	3 - Moderate	Awaiting Evidence			
	☆ Windows ☆ Unix			<b>(i)</b>	INC0010666		NTNX-15SM65260085-A-CVM: Nutanix: CVM Exceeded High Memory Threshold: 100%	Monitoring	EM7+EVENT+187	3 - Moderate	New			
	★ ESX			()	INC0010665		NTNX-15SM65260085-8-CVM: Nutanix: CVM Exceeded High Memory Threshold: 100%	Monitoring	EM7+EVENT+179	3 - Moderate	New			
	☆ AIX ☆ HPUX			()	INC0010664		CS420GX23XX.acme.com: Device Failed Availability Check: UDP - SNMP	Monitoring	EM7+EVENT+37	• 2 - High	Awaiting Evidence			
	☆ OS X ★ Netware			()	INC0010663		Generic-printer-XeroX3210-2: Device Failed Availability Check: UDP - SNMP	Monitoring	EM7+EVENT+66	• 2 - High	Awaiting Evidence			

All SL1 incidents use the event message from the SL1 **Events** page as the incident description in ServiceNow. The SL1 **Events** page also links to the Incident record if you click the life-preserver icon (<sup>(E)</sup>) under the **External Ticket** column. Note that you might need to enable the **External Ticket** column by modifying the Console preferences.

SL1 and ServiceNow use slightly different methods for designating the severity or priority of an event or incident. A custom data lookup table handles the conversion by translating the SL1 event severity into ServiceNow *Impact*, *Urgency*, and *Priority* fields. This severity data lookup table for automatically deploys with the "ScienceLogic SL1: CMDB & Incident Automation Application", also called the Scoped or Certified Application:

≡ Severity	≡ Impact	≡ Urgency	
Search	Search	Search	
1	1		2
2	2		2
3	2		3
4	3		3

If a second event for the same incident occurs, that event will update the *Impact* and *Urgency* values, based on the severity lookup table.

When the SL1 Run Book Automation creates a ServiceNow incident, the action taken depends on the **Correlation Type** you specified in the "ServiceNow Add/Update/Clear Incident" Run Book Action. If one or more events are aligned to the same incident, those events will show up in the **[Events]** tabs at the bottom of the Incident record in ServiceNow. All event-specific information for an incident is listed on this page:

Task SL	sk SLAs Affected Cls Impacted Services/Cls Child Incidents Events (13)										
	E Events Now Search Event created 🔹 Search										
7	▼ mcdent=btC013377										
\$	Q	■ Action policy	■ Active	$\equiv$ Automation policy	$\equiv$ Correlation	$\equiv$ Device	≡ Event count	Event created <b>v</b>	≡ Event ID	Event policy	≡ Hyperlink
	<b>(i)</b>	ServiceNow: Add/Update /Clear Incident	false	ServiceNow: Add/Update Incident	fsundemo89+DEV+2197+EVENT+1705	(empty)	1	2019-09-19 09:23:16	•	Poller: Network Latency Exceeded Threshold	http://em7.mydomain.com/em7/index.em7?exec=events& q_type=aid&q_arg=1176592&q_sev=1&q_sort=0&q_oper=0
	(j)	ServiceNow: Add/Update /Clear Incident	false	ServiceNow: Add/Update Incident	fsundemo89+DEV+2197+EVENT+1705	(empty)	1	2019-09-19 08:28:17	• 1176551	Poller: Network Latency Exceeded Threshold	http://em7.mydomain.com/em7/index.em7?exec=events& q_type=aid&q_arg=1176557&q_sev=1&q_sort=0&q_oper=0
	(i)	ServiceNow: Add/Update /Clear Incident	false	ServiceNow: Add/Update Incident	fsundemo89+DEV+2197+EVENT+1705	(empty)	1	2019-09-19 08:18:16	• • • • • •	Poller: Network Latency Exceeded Threshold	http://em7.mydomain.com/em7/index.em7?exec=events& g_type=aid&q_arg=1176549&q_sev=1&q_sort=0&q_oper=0
	i	ServiceNow: Add/Update /Clear Incident	false	ServiceNow: Add/Update Incident	fsundemo89+DEV+2197+EVENT+1705	(empty)	1	2019-09-19 07:33:17	• 1176520	Poller: Network Latency Exceeded Threshold	http://em7.mydomain.com/em7/index.em7?exec=events& q_type=aid&q_arg=1176520&q_sev=1&q_sort=0&q_oper=0
	(i)	ServiceNow: Add/Update /Clear Incident	false	ServiceNow: Add/Update Incident	fsundemo89+DEV+2197+EVENT+1705	(empty)	1	2019-09-19 07:13:16	•	Poller: Network Latency Exceeded Threshold	http://em7.mydomain.com/em7/index.em7?exec=events& q_type=aid&q_arg=1176505&q_sev=1&q_sort=0&q_oper=0
	<b>(i)</b>	ServiceNow: Add/Update /Clear Incident	false	ServiceNow: Add/Update Incident	fsundemo89+DEV+2197+EVENT+1705	(empty)	1	2019-09-19 07:03:18	• 1176404	Poller: Network Latency Exceeded Threshold	http://em7.mydomain.com/em7/index.em7?exec=events& q_type=aid&q_arg=1176498&q_sev=1&q_sort=0&q_oper=0

TIP: If the [Events] tab does not display at the bottom of the Incident record, you can add it by opening the Incident record, clicking the Additional actions icon (=), and selecting Configure > Related Lists. Add Event > Incident to the Selected column and click [Save].

For more information about ServiceNow incident management, see <a href="https://docs.servicenow.com/bundle/newyork-it-service-management/page/product/incident-management/concept/c">https://docs.servicenow.com/bundle/newyork-it-service-management/page/product/incident-management/concept/c</a> IncidentManagement.html.

## Incident Topology Suppression

*Incident topology suppression* is used when ServiceNow incidents that have been synced with SL1 devices occur on devices that have a parent/child relationship. If you choose to enable incident topology suppression in SL1, child events synced with ServiceNow incidents do not appear in the SL1 **Event Console** as separate events. Instead, the child events are nested under the parent event.

NOTE: The steps in this process use the Classic user interface for SL1.

To enable incident topology suppression:

1. In SL1, navigate to the **Event Policy Manager** page (Registry > Events > Event Manager) and click the **[Create]** button. The **Event Policy Editor** modal appears:

Event Policy Editor   Editing Event Policy [4895]		New	Reset Guide
Policy Advanced Suppressions			
Event Source	Policy Name		
API V V Topology Suppress			9
Operational State	Event Message		
Event Severity			•
Critical Use Modifier 💡			.::
Polic	Description		
Start typing			
5ave	Save As		

- 2. On the **[Policy]** tab, update the following fields:
  - Event Source: Select API.
  - Operational State: Select Enabled.
  - Event Severity: Select Critical as the severity of the event.
  - **Policy Name**. Type the name of the event. Can be any combination of alphanumeric characters, up to 48 characters in length
  - Event Message. Type the message that will appear when this event occurs.

3. Click the [Advanced] tab.

Event Policy Editor   Policy Successfully Saved [48	95]   Editing Event Policy [4895]	New	Reset	Guide	
Policy Advanced Suppressions					
Occurrence Count	First Regular Expression				٦
[Disabled]	CRITICAL				0
Occurrence Time	Second Regular Expression				
[[Disabled]]					9
[ Disabled ]	Identifier Pattern		Override Ytype		
Detection Weight		🕑 [None]		$\sim$	<u>  </u>
20 - Last 🗸 🗸	Identifier Format				a
Component Type					"
[N/A]	Auto-Clear		Topology Suppression	n	
External Event Id		🕑 🛛 Both		$\sim$	0
	[ None Selected ] A Healthy: AKCP: AC Voltage sensor now reporting Normal Status [3192]		Category		
External Category	Healthy: AKCP: DC Voltage sensor returned to Normal Status [3199]	Etterne Co	la stad 3		<u>   </u>
	Healthy: AKCP: Dry contact sensor now Normal [3190] Healthy: AKCP: Smoke detector now Normal Status [3187]	[ None Se	lected j		
Match Logic	Healthy: AKCP: Water sensor now Normal [3188] Healthy: Alteon: Primary Power Supply Healthy [3013]				
Regex Match 🗸 😧	Healthy: Alteon: Redundant Power Supply Healthy [3015]				
🗌 Use Multi-match 😧	Healthy: APC: Batteries Do Not Need Replacement [1516]				
🗹 Use Message-match 🚱	Healthy: APC: Battery Charge Normal [1524] Healthy: APC: Battery Run Time Remaining No Longer Critical [1518]				
	Healthy: APC: Calibration Test Completed [1537]				
	Healthy: APC: Diagnostic Test Passed [1534]				
	Healthy: APC: Diagnostics Schedule Set [1530] Healthy: APC: Percent Battery Remaining No Longer Critical [1520]				
	Healthy: APC: Temperature has returned to normal [1539]				
	Healthy: APC: UPS Not on Battery [1526] Healthy: APC: UPS Not Running on Battery [1522]				
	Healthy: APC: Zero Defective Battery Packs [1514] Healthy: Automatic Windows Service is now running [3508]				
	Healthy: AWS: StorageGateway WorkingStorageUsed Has Returned To No				
	Healthy: AWS: API 4XX Error Has Returned To Normal [4658] Healthy: AWS: API 5XX Error Has Returned To Normal [4660]				
	Healthy: AWS: API Count Has Returned To Normal [4664]			v	_
	Save Save As				

- 4. On the [Advanced] tab, update the following fields:
  - **Detection Weight**. Select 20 Last. If two event definitions are very similar, the weight field specifies the order in which SL1 should match messages against the similar event definitions. The event definition with the lowest weight will be matched first. This field is most useful for events that use expression matching. Options range from 0 (first) 20 (last).
  - Match Logic. Select Regex Match. Specifies whether SL1 should process the First Match String field and Second Match String as regular expressions or as simple text matches. Because you selected Regex Match, you cannot define a "match all" expression by leaving the First Match String and Second Match String fields empty.
  - Use Message-match. Select this option. If SL1 has generated an event and then a second log message or alert matches the same event policy for the same entity, SL1 will not generate a second event, but will increase the count value for the original event. This behavior will occur only if the log messages or alerts contain the same message.
  - *First Regular Expression*. Type "CRITICAL" as the string used to correlate the event with a log message.
  - **Topology Suppression**. Select Both. If this event occurs on a parent device, it behaves as a suppressing event. If this event occurs on a child device, it behaves as a suppressible event.

- 5. Click [Save] and close the Event Policy Editor modal.
- 6. Next, go to the **Device Groups** page (Registry > Device Groups) and click the **[Create]** button. A **Device Group Editor** page appears:

Device Group Editor   Creating new group   Clie	ck Save to commit ch	anges			Guide	Reset
Device Group Name		Force Child Visibility?		Sharin	g Permissions	
All Devices	[ No ]		~	[ Private (visible to you only) ]	-	~
lcon		Visibility		Pern	ission Keys	
	Mags/Vews Conting Boldsaw/Buke Ede Notification/Automation Discovery Device Schedules Event Suppression RSS Feeds		~	EM7 System Administration Grant All Basic User Privileges PowerPack Administration Provisioning Access Admin Portal UI Access Subscription Management IT Services - View IT Services - View	1	*
Static Devices and Groups   Devices [0]   Groups	ups [0]					Del Add
Device Name • Class   Sub-class	D Organization	2	Device Group	Name • ID	Devices Groups	Rules 📝
No devices in current device g	roup.		N	io sub-groups in current device g	itentity	
Dynamic Rules   Rules Found [1]   Adding rule	es [1]					Del Add
Selector Type 1.1. OP Device Name *		Selector Targets		Devices n	Ma 9 atched for rule 1: 9	Matched
		Save				

- 7. Complete the following fields, and leave the default settings for the remaining fields:
  - Template Name. Specify the name of the new device group.
  - Force Child Visibility. Select "No".
  - Visibility. Select Config Policies/Bulk Edit to let you configure all the devices in the new device group using a device template.

8. Click the **[Save]** button and then click the **[Add]** button in the **Dynamic Rules** pane to add dynamic rules to the new device group. The Device Group Rule Editor modal page appears:

Add Rule							2
Device Group Rule Editor   Active S	election					Res	et
Active Selectors         Organization         Device Class         Device Category         Device Name         Device State         Collector Group         Open TCP Ports         Running Process         Windows Service         Subscribed Product         Active Event	Selector (1 Operators e term* term term term term1, term	Definitions Device Name Begins with "term" Ends with "term" Is "term", "teem" Is not "term" 2 is "term" or "term2"					
Matched Devices [9]	0.1				0	Collection	^
1. 10.2.11.66	Unknown	Ping   Generic Linux	9	System	<u>OrganitZation</u>	Active	
2. 10.2.11.68	Unknown	Ping   Generic Linux	10	System		Active	
3. milairlocks	Unknown	Ping   Generic Linux	11	System		Active	
4. MAZURE Device	Service	Microsoft   Azure Services	3	System		Active	
5. 🎢 em7ao	EM7	ScienceLogic, Inc.   EM7 All-In-0	1	System		Active	
6. <u>M</u> em7ao	EM7	ScienceLogic, Inc.   EM7 All-In-0	2	System		Active	
7. Integration Service Docs	EM7	ScienceLogic   Integration Serv	5	System		Active	
					Select related de	evices OK	

- 9. In the Active Selectors pane, select Device Name.
- 10. Optionally, in the **Selector Definitions** pane, type an asterisk (\*) in the **Device Name** field. Using the \* includes all devices by Device Name. In the **Matched Devices** pane, a list of all devices appears.
- 11. Click **[OK]** to close the modal page.
- 12. On the Device Group Editor modal page, click [Save] and close the page.

 Next, create a Device Group Template that will disable Event Masking for all devices in the new Device Group. Click the building blocks icon (<sup>(A)</sup>) for the new device group. A **Device Template Editor** page appears:

emplate New / One-off	Template	Save Whe	en Applied & Confin	med Template Na	ame 🦳		
Config	Inter fa ce	CV Policies	Port Policies	Svc Policies	Proc Polic	cies Dyn Apps	Logs
cess & Monitoring						Device Preferences	
Device Organization	Acme Inc		$\sim$			Auto-Clear Events	Scan All IPs
SNMP Read	Cisco SNMPv2 -	Example	SNMP Write	None	$\sim$		
Availability Protocol	TCP		Avail Port	ICMP	$\sim$	Accept All Logs	Dynamic Discovery
Latency Protocol	TCP		Latency Port	ICMP	$\sim$		
Avail+Latency Alert	Disabled		$\sim$			Daily Port Scans	Preserve Hostname
Collection	Enabled		Collector Grp	CUG	$\sim$		
Coll. Type	Standard		~			Auto-Update	Disable Asset Update
Critical Ping	Disabled		$\sim$				
Event Mask	Disabled		~			Bypass Interface Inventory	
vice Retention & Bas	ic Thresholds			Daily Rollup Bandwidth			
oysion Euron	7 • <b>1</b>	· · ·	100 ms	Data			730 days
				Hourly Rollup Bandwidth Data	-	1	120 days
Availability Packet Siz	<sup>20</sup>	1	56 bytes	Raw Performance		1	7 days
Availability Ping Cou	nt 🔟		1 pings	Daily Rollup Performance Data			730 days
erface Inventory Set	tings						
Interface Invent	tory date	1 1	ms	Maximum Allowed	dia.	1	10000 interfaces

- 14. Because all of the fields are disabled (grayed-out) by default, click the **Event Mask** field name to enable the field. Use the default setting of *Disabled*.
- 15. Click [Apply] and click [Confirm] on the Device Template Editor page.
- 16. Next, turn off the Trigger on Child Rollup option on the "ServiceNow: Add/Update Incident" Run Book Automation. Go to the Automation Policy Manager page (Registry > Run Book > Automation) and click the wrench icon () for the "ServiceNow: Add/Update Incident" Run Book Automation. The Automation Policy Editor page appears:

rice Template Editor   emplate New / One-off	Applying Template	to Devices   Clic	k [Save] to com	mit changes   Config 1	Name	ttings (Click field labels to	enable/dist Reset
Config	Inter face	CV Policies	Port Policies	Svc Policies	Proc Poli	cies Dyn Apps	Logs
ccess & Monitoring						Device Preferences	
Device Organization	Acme Inc	~				Auto-Clear Events	Scan All IPs
SNMP Read	Cisco SNMPv2 - Exa	mple	SNMP Write	None	$\sim$		
Availability Protocol	TCP	~	Avail Port	ICMP	$\sim$	Accept All Logs	Dynamic Discovery
Latency Protocol	TCP	~	Latency Port	ICMP	$\sim$		
Avail+Latency Alert	Disabled	~	/			Daily Port Scans	Preserve Hostname
Collection	Enabled	~	Collector Grp	CUG	$\sim$		
Coll. Type	Standard	~	/			Auto-Update	Disable Asset Upda
Critical Ping	Disabled	~	·				
Event Mask	Disabled	~				Bypass Interface Inventory	
vice Retention & Bas	ic Thresholds			Daily Rollup Bandwidth			
o yotom zatom	- <b>-</b>		100 ms	Data	<u> </u>		730 days
				Hourly Rollup Bandwidth Data	÷	1 1	120 days
Availability Packet Siz			56 bytes	Raw Performance		1	7 days
Availability Ping Cou	nt 🔟		1 pings	Daily Rollup Performance Data	-	· · · · ·	730 days
terface Inventory Set	tings						
Interface Invent	tory Lat	I I	me	Maximum Allowe	ad	I	10000 interfaces

17. Make sure the *Trigger on Child Rollup* option is not selected and click **[Save]**. Close the **Automation Policy Editor** page.

# Hyperlinking Events

Both ServiceNow and SL1 provide mechanisms for hyperlinking to multiple active events and incidents. This section describes those processes.

## ServiceNow Hyperlinking

Each incident in ServiceNow will have one or more events aligned with it through the Related List of events, which you can view in the **[Events]** tab at the bottom of the Incident record.

By default the *Hyperlink* field appears on the custom event table provided with the Certified application (x\_sclo\_ scilogic\_event). Each event shown in the **[Events]** tab at the bottom of the Incident record will have its own URL associated. The following image shows the Event record for an event aligned with an Incident:

$\leftarrow$ $\equiv$ Event 315			/ 🛃 👓 Up	date Delete 🛧 🗸
Incident	INC0010020 Q	(i) Device	em7-ao-47	Q (j)
Region	region6341	Organization	System	Q (j)
Event ID	315	Severity	Minor	$\sim$
Event policy	Dynamic App Snippet Exception	Event created	2019-10-30 13:00:19	iii
Automation policy	ServiceNow: Click to Create Incident	Last detected	2019-10-30 13:00:19	iii
Action policy	ServiceNow: Add/Update/Clear Inciden	Event count		1
Message	em7-ao-47: App: 90, Snippet: 110 reporte walkbulk to query .1.3.6.1.2.1.25.2.3.1.2)	d a collection problem (Explanation: SNMP error	returned: Timeout. Location: Using	
Hyperlink	http://em7.mydomain.com/em7/index.em	7?exec=events&q_type=aid&q_arg=315&q_sev=1	<u>l&amp;q_sort=0&amp;q_oper=0</u>	æ
Update Delete				
				Ċ

TIP: If the [Events] tab does not display at the bottom of the Incident record, you can add it by opening the Incident record, clicking the Additional actions icon (=), and selecting Configure > Related Lists. Add Event->Incident to the Selected column and click [Save].

## Viewing the Incident Import Table in ServiceNow

Each time SL1 creates or changes an incident in ServiceNow, data is inserted into a temporary import table on the ServiceNow system. This table displays all inbound data from SL1 and is a useful tool to determine what data is being sent and imported. The incident import table is created automatically when you install the ScienceLogic Certified (Scoped) Application.

To view the data and the status of the import process, go to the **Import Incidents** page (ScienceLogic > Event > Events) in ServiceNow:

Sciencelogic		8		mport Inci	idents New	Search	Updated v :	Search							44 4 🔲 1 t	to 100 of 1,310 🕨 🕨
8	*	0	7	All												
Favorites		^	4	Q	≡ Event ID		■ Created		≡ Incident	CMDB CI	≡ Updated ▼		≡ State	Incident state	■ Created by	≡ Import set run
					Search		Search	Search	Search	Search	Search	Search	Search	Search	Search	Search
i scienceLogic	- Dependents			()		1176595	2019-09-19 09:33:21	fsundemo89+DEV+2196+EVENT+1705	INC0013376	(empty)	2019-09-19 09:33:21	Event: 1176595	Updated	Resolved	fsun	(empty)
ScienceLogic				0		1176595	2019-09-19 09:33:21	fsundemo89+DEV+2196+EVENT+1705	INC0013376	(empty)	2019-09-19 09:33:21	Incident: INC0013376	Updated	Resolved	fsun	(empty)
Support				•												
▼ Event				0		1176595	2019-09-19 09:28:27	fsundemo89+DEV+2196+EVENT+1705	INC0013376	(empty)	2019-09-19 09:28:27	Event: 1176595	Inserted	In Progress	fsun	(empty)
Event Propertie	es			()		1176595	2019-09-19 09:28:27	fsundemo89+DEV+2196+EVENT+1705	INC0013376	(empty)	2019-09-19 09:28:27	Incident: INC0013376	Updated	In Progress	fsun	(empty)
Severity Looku	ıp Rules			0		1176592	2019-09-19 09:28:26	fsundemo89+DEV+2197+EVENT+1705	INC0013377	(empty)	2019-09-19 09:28:26	Incident: INC0013377	Updated	Resolved	fsun	(empty)
Events				()		1176592	2019-09-19 09:28:26	fsundemo89+DEV+2197+EVENT+1705	INC0013377	(empty)	2019-09-19 09:28:26	Event: 1176592	Updated	Resolved	fsun	(empty)
Device				()		1176592	2019-09-19 09:23:22	fsundemo89+DEV+2197+EVENT+1705	INC0013377	(empty)	2019-09-19 09:23:22	Event: 1176592	Inserted	In Progress	fsun	(empty)
Device Properti	les			()		1176592	2019-09-19 09:23:22	fsundemo89+DEV+2197+EVENT+1705	INC0013377	(empty)	2019-09-19 09:23:22	Incident: INC0013377	Updated	In Progress	fsun	(empty)
Automations				()		1176577	2019-09-19 09:03:34	fsundemo89+DEV+2196+EVENT+1705	INC0013376	(empty)	2019-09-19 09:03:34	Event: 1176577	Updated	Resolved	fsun	(empty)
Automation Pre	operties			()		1176577	2019-09-19 09:03:34	fsundemo89+DEV+2196+EVENT+1705	INC0013376	(empty)	2019-09-19 09:03:34	Incident: INC0013376	Updated	Resolved	fsun	(empty)
Sessions Prope	erties			۵.		1176577	2019-09-19 08-58:30	fsundemo89+DEV+2196+EVENT+1705	INC0013376	(empty)	2019-09-19 08:58:30	Incident: INC0013376	Updated	In Progress	fsun	(empty)
Dependents		*														
Tasks				()		1176577	2019-09-19 08:58:30	fsundemo89+DEV+2196+EVENT+1705	INC0013376	(empty)	2019-09-19 08:58:30	Event: 1176577	Inserted	In Progress	tsun	(empty)
Catalog Templa	ates			<b>(i)</b>		1176570	2019-09-19 08:53:35	fsundemo89+DEV+2196+EVENT+1705	INC0013376	(empty)	2019-09-19 08:53:35	Incident: INC0013376	Updated	Resolved	fsun	(empty)
V Maintenance				(j)		<u>1176570</u>	2019-09-19 08:53:35	fsundemo89+DEV+2196+EVENT+1705	INC0013376	(empty)	2019-09-19 08:53:35	Event: 1176570	Updated	Resolved	fsun	(empty)
Maintenance P	roperties			(j)		1176570	2019-09-19 08:48:31	fsundemo89+DEV+2196+EVENT+1705	INC0013376	(empty)	2019-09-19 08:48:31	Incident: INC0013376	Updated	In Progress	fsun	(empty)
V Supporting Im	ports			<b>(i)</b>		1176570	2019-09-19 08:48:31	fsundemo89+DEV+2196+EVENT+1705	INC0013376	(empty)	2019-09-19 08:48:31	Event: 1176570	Inserted	In Progress	fsun	(empty)
Organization				()		1176556	2019-09-19 08:38:32	fsundemo89+DEV+2196+EVENT+1705	INC0013376	(empty)	2019-09-19 08:38:32	Incident: INC0013376	Updated	Resolved	fsun	(empty)

You can view a complete audit of all import data and transforms by going to the **Transform Histories** page (System Import Sets > Advanced > Transform History):

	Transforr	n Histories	Go to Started	▼ Se	arch							• • •	1 to 1	100 of 20440 🕨 🕨
$\bigtriangledown$	All													
蓉	Q	$\equiv$ Started	≡ State	$\equiv$ Completed	$\equiv$ Run time	≡ Set	≡ Import set table	■ Total	≡ Inserts	$\equiv$ Updates	$\equiv$ Ignored	≡ Skipped	≡ Errors	■ Transform Map
	(i)	2016-09-04 04:00:50	<ul> <li>Complete</li> </ul>	2016-09-04 04:00:50	0 Seconds	ISET0013291	ScienceLogic File System [u_sciencelogic_file_system]		1	0	0	1	0	ScienceLogic File System T-Map
	i	<u>2016-09-01</u> <u>12:00:27</u>	<ul> <li>Complete</li> </ul>	2016-09-01 12:00:27	0 Seconds	ISET0013275	ScienceLogic Network Interfaces [u_sciencelogic_adapters]		1	0	0	1	0	ScienceLogic Adapter <u>T-Map</u>
	(j)	2016-09-02 14:00:12	<ul> <li>Complete</li> </ul>	2016-09-02 14:00:12	0 Seconds	ISET0013278	ScienceLogic Hardware Models [u_sciencelogic_hardware_models]		1	0	0	1	0	ScienceLogic Hardware Model T- Map
	(j)	<u>2016-09-01</u> <u>16:00:44</u>	Complete	2016-09-01 16:00:44	0 Seconds	ISET0013276	ScienceLogic File System [u_sciencelogic_file_system]		1	0	0	1	0	ScienceLogic File System T-Map
	i	<u>2016-08-31</u> <u>18:01:16</u>	<ul> <li>Complete</li> </ul>	2016-08-31 18:01:16	0 Seconds	ISET0013271	ScienceLogic File System [u_sciencelogic_file_system]		1	0	0	1	0	ScienceLogic File System T-Map
	(j)	2016-09-02 03:00:28	<ul> <li>Complete</li> </ul>	2016-09-02 03:00:28	0 Seconds	ISET0013280	ScienceLogic File System [u_sciencelogic_file_system]		1	0	0	1	0	ScienceLogic File System T-Map
	(j)	2016-09-01 20:01:03	<ul> <li>Complete</li> </ul>	2016-09-01 20:01:03	0 Seconds	ISET0013276	ScienceLogic File System [u_sciencelogic_file_system]		1	0	0	1	0	<u>ScienceLogic File</u> System T-Map
	i	<u>2016-09-03</u> <u>02:01:22</u>	<ul> <li>Complete</li> </ul>	2016-09-03 02:01:22	0 Seconds	ISET0013286	ScienceLogic File System [u_sciencelogic_file_system]		1	0	0	1	0	ScienceLogic File System T-Map
	i	2016-09-01 12:00:59	<ul> <li>Complete</li> </ul>	2016-09-01 12:00:59	0 Seconds	ISET0013275	ScienceLogic Network Interfaces [u_sciencelogic_adapters]		1	0	0	1	0	ScienceLogic Adapter <u>T-Map</u>
	i	<u>2016-09-03</u> <u>12:00:12</u>	<ul> <li>Complete</li> </ul>	2016-09-03 12:00:12	0 Seconds	ISET0013283	ScienceLogic Hardware Models [u_sciencelogic_hardware_models]		1	0	0	1	0	ScienceLogic Hardware Model T- Map
	i	2016-09-04 22:00:33	<ul> <li>Complete</li> </ul>	2016-09-04 22:00:33	0 Seconds	ISET0013290	ScienceLogic Network Interfaces [u_sciencelogic_adapters]		1	0	0	1	0	ScienceLogic Adapter T-Map
	i	<u>2016-09-01</u> <u>16:01:17</u>	<ul> <li>Complete</li> </ul>	2016-09-01 16:01:17	0 Seconds	ISET0013276	ScienceLogic File System [u_sciencelogic_file_system]		1	0	0	1	0	ScienceLogic File System T-Map

# ServiceNow, ScienceLogic Event, and Incident Priority Matrix

By default, when SL1 triggers an event, it is sent to ServiceNow through the Integration Service. The following mappings are currently in place for mapping an SL1 Event to a ServiceNow Incident (ScienceLogic > Event > Severity Lookup Rules):

≡ Severity	≡ Impact	≡ Urgency	
Search	Search	Search	
1		1	2
2		2	2
3		2	3
4		3	3

NOTE: This severity lookup table handles all Severity conversions.

A **transformation script** that translates the SL1 event severity into the ServiceNow **Impact**, **Urgency**, and **Priority** fields automatically deploys with the ScienceLogic Certified (Scoped) Application.

By default, the **Priority** field is read-only and must be set by selecting the **Impact** and **Urgency** values.

Impact	Urgency	Priority
1 - High	1 - High	1 - Critical
1 - High	2 - Medium	2 - High
1 - High	3 - Low	3 - Moderate
2 - Medium	1 - High	2 - High
2 - Medium	2 - Medium	3 - Moderate
2 - Medium	3 - Low	4 - Low
3 - Low	1 - High	3 - Moderate
3 - Low	2 - Medium	4 - Low
3 - Low	3 - Low	5 - Planning

Priority is calculated according to the following data lookup rules:

# Adding Additional Fields to the Transform Map

If you require additional mandatory fields to be filled out to resolve an incident, you can add those fields to the *transform map* in ServiceNow.

For example, if you require four mandatory fields in the ServiceNow Incident—Assignment Group, IT Service, Service Component, and Description—to be filled out before that incident can be resolved in SL1, you would perform the following steps.

1ain D	etails* Notes Related Rec	ords Resolution Information	Admin			
	* Caller	Science Logic	Q	efa	(i) Contact type	web \$
	Behalf of user		Q		Impact	Some Users \$
JIP	* Company	Motorpoint Limited		i	Urgency	3 - Low \$
	Location		Q		Priority (?)	4 - Low
	★ IT service		Q		Major incident state	
	★ Service component		Q		Owning group	Q
	Symptom		Q		Assignment group	Q
	Configuration item		Q		Assigned to	Q
	* Short description	mp-sql-2014-01: Host Resource	e: Storage I	Utilizati	n (E:\ Label:Data Serial Number d01ef7f2) has exceeded th	reshold 90%, currently 90.02%
	* Description				Related Search Results >	

To add an assignment group:

- 1. Navigate to **User Administration > Groups** and select the assignment group you want to add. The Group record appears.
- 2. Right-click the gray task bar at the top and select **Copy sys** id.

Croup Access Requests		Save	
Name	Access Requ	Insert Insert and Stay	
Manager		Configure > Export >	Q
Group email	support@n	View >	
Parent		Create Favorite Copy URL	Q
Updated	04-05-2018	Copy sys_id	
Туре	A	Show XML History >	
Description	Access Requ	Reload form	

- 3. In SL1, open to the "ServiceNow: Add/Update/Clear Incident" Run Book Action (Registry > Run Book > Actions).
- 4. Edit the Input Parameters of the Run Book Action to add the sys\_id to the relevant parameter or parameters to assign the assignment group to one of the new, acknowledged, or cleared incidents that are mapped. After an incident is created, the assignment group value will not be changed by the Run Book Action.

In the following example, the assignment group is assigned to incidents that are cleared:

```
"assignment_group_new": "",
"assignment_group_ack": "",
"assignment group clear": "sys id"
```

The *IT Service*, *Service Component*, and *Description* fields in our example must be filled in before an Incident can be closed. To do this, changes must be made in the transform maps that are provided in the form of update sets from ScienceLogic.

**TIP:** For more information about mapping new fields and other mappings options, see <u>https://docs.servicenow.com/bundle/newyork-platform-administration/page/script/server-scripting/concept/c\_MappingOptions.html</u>.

To add the **Description** field:

- 1. In ServiceNow, search for "transform map" in the filter navigator. Click **Transform Maps**.
- 2. In the list of transform maps, search for "ScienceLogic" in the field above the **Name** column.

3. Open the "ScienceLogic Incident" map:

	lanagemen	nt			Sc	ienceLogic 💠 🛛 SA Sy	stem Administrato	r• Q⊄	57 (?) (\$\$
( Transform map	= Tal	ble Trans	sform Maps New	Go to Order 💌	Search		44 4	1 to 8	of 8 🕨 🕨
<b>⊡ ★</b> (0)	Al								
System Import Sets	103 103	Q	Name	Source table	Target table	Run business rules	Count	= Active	
Create Transform Map		_	Search	Search	Search	Search	Search	Search	Search
▼ Administration		i	<u>ScienceLogic</u> Incident	ScienceLogic Incident Import [u_imp_silo_incidents]	Incident [incident]	true	100	true	2018-05-18 20:44:15
Transform Maps 🥒 🖒		(i)	Notification	Notification [imp_notification]	Incident [incident]	true	100	true	2008-12-28 22:08:39
System LDAP		i	User	User [imp_user]	User [sys_user]	true	100	true	2015-07-07 07:32:42
Transform Maps		i	Location	Location [imp_location]	Location [cmn_location]	true	100	true	2015-07-07 07:30:52
		(j)	Computer	Computer [imp_computer]	Computer [cmdb_ci_computer]	true	100	true	2015-07-07 07:29:19
		i	LDAP User Import	label [ldap_import]	User [sys_user]	true	100	true	2011-04-11 16:17:55
		i	LDAP Group Import	label [ldap_group_import]	Group [sys_user_group]	true	100	true	2009-11-12 09:33:59
		i	<u>ScienceLogic</u> <u>Event</u>	ScienceLogic Incident Import [u_imp_silo_incidents]	ScienceLogic Events [u_silo_events]	true	200	true	2018-05-18 21:27:35

- 4. The **Field Maps** table at the bottom of the page allows you to edit or create mappings from the ScienceLogic Incident Import table to the ServiceNow Incident table. Click **[New]** to create a new field mapping.
- 5. The **Source table** field should contain the ScienceLogic Incident Import and the **Target table** should include the ServiceNow Incident table:

Field Map New record			Ø ==
Мар	ScienceLogic Incident Q	(i) Application	Global
Source table	ScienceLogic Incident Import [u_imp_s V	Target table	Incident [incident]
Source field	Action Policy	Target field	Active
Use source script		Coalesce	

- 6. To create a new mapping to copy the contents of the **Short description** field to the **Description** field, select Short description from the **Source field** drop-down menu.
- 7. In the **Target field** drop-down menu, select Description.
- 8. Click **Update** to save your changes.

The *IT Service* and *Service Component* fields in our example are set in the Transform Script in the "ScienceLogic Event" transform map. To set the fields:

- 1. In ServiceNow, make sure you have the *sys\_id* value for the target fields. If a field contains a magnifying glass, it will require a *sys\_id*. If a field has a drop-down, type in the field you wish to apply from the drop-down. In the case of our example, the *sys\_id* values of the two fields are required.
- 2. In your ServiceNow instance, navigate to the Transform Maps table and select "ScienceLogic Event".

3. In the ScienceLogic Event transform map page, click the **[Transform Script]** tab and open the "onAfter" script.

< ≡ Table Transform Map        Copy       ScienceLogic Event         Copy									
Current View: Default view (cl	lick me for other views)	Application	ScienceLogic	G					
* Source table	ScienceLogic Incident Import [u_imp_s ▼	Created	2018-05-18 21:27:35						
Active	$\checkmark$	* Target table	ScienceLogic Events [u_silo_events]						
Run business rules	$\checkmark$	Order		200					
Enforce mandatory fields	No	Run script							
Copy empty fields									
Update Copy De	elete								
Related Links									
Auto Map Matching Fields Transform	Auto Map Matching Fields Transform								
	Index Coalesce Fields								
Field Maps (16) Transfo	orm Scripts (2)								
Transform Scripts	New Go to Order V Search		44 4	1 to 2 of 2 <b>&gt; &gt;</b>					
Map = ScienceLog	gic Event								
Q ≡ wi	hen		E Order						
(i) onAfter	er (function runTransformSo	cript(source, map		100 true					
i onBet	fore (function runTransformSi	cript(source, map		100 true					

4. Add the following under the "//Update target record when the Event was cleared from Sciencelogic" text:

```
sl_INT.(target field) = '[sys_id of the source field]'; //(IT service field)
sl_INT.(target field) = '[sys_id of the source field]'; //(Service component)
```

When 🥐	onAfter	Application ScienceLogic								
		Active 🖌								
		Order 100								
of this script a	nd the globals	s available to it vary depending on when the script is set to run. For more information, see the Wiki. See also the article about the recommended								
Script ⑦	🤞 📮									
	1 . (	(function runTransformScript(source, map, log, target /*undefined onStart*/ ) {								
	2	······································								
	3	event_state_management();								
	4	Function quart state management ()								
	6	//Check Sciencelogic Events to see, if the Incident can be closed.								
	7	<pre>var sl events = new GlideRecord('u silo events');</pre>								
	8	<pre>8 sl events.addEncodedOuerv('u active=true^u silo task=' + source.u task);</pre>								
	9	9 sl_events.query();								
	10 *	10 v if(sl_events.getRowCount() == 0){								
	11	<pre>11 var sl_INT = new GlideRecord('incident');</pre>								
	12	<pre>sl_INT.get(target.u_silo_task);</pre>								
	13 •	<pre>if(source.u_incident_state == 6 &amp;&amp; sl_INT.close_code.nil()){</pre>								
	14	//update target record when the Event was cleared from Sciencelogic.								
	15	st_lnt.close_code='tlosed/Resolved by Caller';								
	17	16 s_INI.close_notes=source.u_work_notes;								
	18 *	$17$ $S_{\pm}(1), State= 0;$ late if (course u incident state == 6.85 Ls] INT close code nil())/								
	19	//Update target record when Event was cleared From ServiceNow.								
	20	<pre>sl INT.close notes= sl INT.close notes + " (" + source.u work notes + ")";</pre>								
	21	}								
	22	<pre>sl_INT.update();</pre>								
	23	}								
	24	return;								
	25	Ų.								
	26									
	27	<pre>})(source, map, log, target);</pre>								

5. To find the target field, make a temporary mapping to see what the target field is. This mapping can be deleted once you know the target field.

Field Maps (14) Transform Scripts (3) Versions (1)						
Field Maps New						
ວັ The Source field	Target field					
(i) <u>u short description</u>	sh <mark>p</mark> rt_description					
(i) <u>u contact type</u>	contact_type					
(i) <u>u active</u>	active					
(i) <u>u short description</u>	description					
(i) <u>u assignment group</u>	ass <mark>i</mark> gnment_group					
i <u>u correlation id</u>	correlation_id					
i sys updated by	cal <mark>l</mark> er_id					
i <u>u urgency</u>	urgancy					
(i) <u>u cmdb ci</u>	cm <mark>d</mark> b_ci					
(i) <u>u work notes</u>	work_notes					
(i) <u>u impact</u>	u_service_component					
(i) <u>u_impact</u>	impact					
(i) [Script]	company					
i [Script]	location					
Actions on selected rows						

6. Click **[Update]** to save your changes. The selected fields will be added into an Incident on closure.

# Chapter

# 4

# Troubleshooting the Incident Synchronization PowerPack

## Overview

This chapter contains troubleshooting resources, procedures, and the answers to frequently asked questions to use with the ServiceNow Incident Synchronization PowerPack.

This chapter covers the following topics:

Initial Troubleshooting Steps	67
Resources for Troubleshooting	67
Frequently Asked Questions	72

# Initial Troubleshooting Steps

The Integration Service acts as a middle server between data platforms. For this reason, the first steps should always be to ensure that there are no issues with the data platforms with which the Integration Service is talking. There might be additional configurations or actions enabled on ServiceNow or SL1 that result in unexpected behavior. For detailed information about how to perform the steps below, see **Resources for Troubleshooting**.

## Integration Service

1. Run the following command:

docker service ls

- 2. Note the Docker container version, and verify that the Docker services are running.
- 3. If a certain service is failing, make a note the service name and version.
- 4. If a certain service is failing, run docker service ps <service\_name> to see the historical state of the service and make a note of this information. For example: docker service ps iservices\_contentapi.
- 5. Make a note of any logs impacting the service by running docker service logs <service\_name>. For example: docker service logs iservices\_couchbase.

## ServiceNow

- 1. Make a note of the ServiceNow version and Synchronization PowerPack version, if applicable.
- 2. Make a note of whether the user is running an update set or the Certified Application (also called the "ScienceLogic SL1: CMDB & Incident Automation" application).
- 3. Make a note of the ServiceNow integration application that is failing on the Integration Service.
- 4. Make a note of what step is failing in the integration application, try running the application in debug mode, and capture any traceback or error messages that occur in the step log.

## **Resources for Troubleshooting**

This section contains port information for the Integration Service and troubleshooting commands for Docker, Couchbase, and the Integration Service API.

## **Useful Integration Service Ports**

- http://<IP of Integration Service>:8081. Provides access to Docker Visualizer, a visualizer for Docker Swarm.
- https://<IP of Integration Service>:8091. Provides access to Couchbase, a NoSQL database for storage and data retrieval.
- https://<IP of Integration Service>:15672. Provides access to the RabbitMQ Dashboard, which you can use to monitor the service that distributes tasks to be executed by Integration Service workers.

 https://<IP of Integration Service>/flower. Provides access to Flower, a tool for monitoring and administrating Celery clusters.

## Helpful Docker Commands

The Integration Service is a set of services that are containerized using Docker. For more information about Docker, see the <u>Docker tutorial</u>.

Use the following Docker commands for troubleshooting and diagnosing issues with the Integration Service:

#### Viewing Container Versions and Status

To view the Integration Service version, SSH to your Integration Service instance and run the following command:

docker service ls

In the results, you can see the container ID, name, mode, status (see the *replicas* column), and version (see the *image* column) for all the services that make up the Integration Service:

<pre>(root@fsunis4lab ~}# docker service 1s</pre>								
ID	NAME	MODE	REPLICAS	IMAGE	PORTS			
ommihuj5v30i	iservices_gui	replicated		repository.auto.sciencelogic.local:5000/is-gui:1.7.0	*:80->80/tcp,*:443->443/tcp			
i0vs9ltlwnh3	iservices redis	replicated	1/1	redis:4.0.2				
jlm6hljtumlf	iservices flower	replicated	1/1	repository.auto.sciencelogic.local:5000/is-worker:1.7.0	*:5555->5555/tcp			
lh3pt2181rsf	iservices_scheduler	replicated	1/1	repository.auto.sciencelogic.local:5000/is-worker:1.7.0				
ntimltvg6xhx	iservices contentapi	replicated	1/1	repository.auto.sciencelogic.local:5000/is-api:1.7.0	*:5000->5000/tcp			
ryln9qgsudmi	iservices rabbitmq	replicated	1/1	rabbitmq:3				
xlul9h8jsfs6	iservices visual	replicated	2/1	dockersamples/visualizer:latest	*:8081->8080/tcp			
ycy38w8buauw	iservices_couchbase	replicated		repository.auto.sciencelogic.local:5000/is-couchbase:1.7.0	*:8091->8091/tcp,*:8092->8092/			
3->8093/tcp,*:8094-	3->8093/tcp,*:8094->8094/tcp,*:11210->11210/tcp							
zlbxstxoz7uf	iservices_steprunner	replicated	5/5	repository.auto.sciencelogic.local:5000/is-worker:1.7.0				

#### Restarting a Service

Run the following command to restart a single service:

```
docker service update --force <service_name>
```

#### Stopping all Integration Service Services

Run the following command to stop all Integration Service services:

docker stack rm iservices

#### **Restarting Docker**

Run the following command to restart Docker:

```
systemctl restart docker
```

**NOTE:** Restarting Docker does not clear the queue.

#### Viewing Logs for a Specific Service

You can use the Docker command line to view the logs of any current running service in the Integration Service cluster. To view the logs of any service, run the following command:

docker service logs -f iservices <service name>

Some common examples include the following:

docker service logs -f iservices\_couchbase docker service logs -f iservices\_steprunner docker service logs -f iservices\_contentapi

**NOTE:** Application logs are stored on the central database as well as on all of the Docker hosts in a clustered environment. These logs are stored at **/var/log/iservices** for both single-node or clustered environments. However, the logs on each Docker host only relate to the services running on that host. For this reason, using the Docker service logs is the best way to get logs from all hosts at once.

#### Clearing RabbitMQ Volume

RabbitMQ is a service that distributes tasks to be executed by Integration Service workers. This section covers how to handle potential issues with RabbitMQ.

The following error message might appear if you try to run an integration application via the API:

```
Internal error occurred: Traceback (most recent call last):\n File \"./content_
api.py\", line 199, in kickoff_application\n task_status = ... line 623, in _on_
close\n (class_id, method_id), ConnectionError)\nInternalError: Connection.open: (541)
INTERNAL ERROR - access to vhost '/' refused for user 'guest': vhost '/' is down
```

First, verify that your services are up. If there is an issue with your RabbitMQ volume, you can clear the volume with the following commands:

docker service rm iservices\_rabbitmq
docker volume rm iservices\_rabbitdb

If you get a message stating that the volume is in use, run the following command:

docker rm <id of container using volume>

Re-deploy the Integration Service by running the following command:

docker stack deploy -c /opt/iservices/scripts/docker-compose.yml iservices

**NOTE**: Restarting Docker does not clear the queue, because the queue is persistent. However, clearing the queue with the commands above might result in data loss due to the tasks being removed from the queue.

#### Viewing the Process Status of All Services

Run the following command:

docker ps

#### Deploying Services from a Defined Docker Compose File

Run the following command:

docker stack deploy -c <compose-file> iservices

#### Dynamically Scaling for More Workers

Run the following command:

docker service scale iservices\_steprunner=10

#### Completely Removing Services from Running

Run the following command:

docker stack rm iservices

## **Diagnosis** Tools

Multiple diagnosis tools exist to assist in troubleshooting issues with the Integration Service platform:

- **Docker PowerPack**. This PowerPack monitors your Linux-based Integration Service server with SSH (the Integration Service ISO is built on top of an Oracle Linux Operating System). This PowerPack provides key performance indicators about how your Integration Service server is performing. For more information on the Docker PowerPack and other PowerPacks that you can use to monitor the Integration Service, see the "Using SL1 to Monitor the Integration Service" chapter in the **Integration Service Platform** manual.
- *Flower*. This web interface tool can be found at the /flower endpoint. It provides a dashboard displaying the number of tasks in various states as well as an overview of the state of each worker. This tool shows the current number of active, processed, failed, succeeded, and retried tasks on the Integration Service platform. This tool also shows detailed information about each of the tasks that have been executed on the platform. This data includes the UUID, the state, the arguments that were passed to it, as well as the worker and the time of execution. Flower also provides a performance chart that shows the number of tasks running on each individual worker.
- **Debug Mode**. All applications can be run in "debug" mode via the Integration Service API. Running applications in debug mode may slow down the platform, but they will result in much more detailed logging information that is helpful for troubleshooting issues. For more information on running applications in Debug Mode, see *Retrieving Additional Debug Information*.
- Application Logs. All applications generate a log file specific to that application. These log files can be found at /var/log/iservices and each log file will match the ID of the application. These log files combine all the log messages of all previous runs of an application up to a certain point. These log files roll over and will get auto-cleared after a certain point.

- Step Logs. Step logs display the log output for a specific step in the application. These step logs can be accessed via the Integration Service user interface by clicking on a step in an integration application and bringing up the Step Log tab. These step logs display just the log output for the latest run of that step.
- Service Logs. Each Docker service has its own log. These can be accessed via SSH by running the following command:

```
docker service logs -f <service name>
```

## Retrieving Additional Debug Information (Debug Mode)

The logs in the Integration Service use the following loglevel settings, from most verbose to least verbose:

- 10. Debug Mode.
- 20. Informational.
- 30. Warning. This is the default settings if you do not specify a loglevel.
- 40. Error.

WARNING: If you run integration applications with "loglevel": 10, those integration applications will take longer to run because of increased I/O requirements. Enabling debug logging using the following process is the only recommended method. ScienceLogic does not recommend setting "loglevel": 10 for the whole stack with the docker-compose file.

To run an application in Debug Mode, POST the following to the API endpoint:

```
https://<integration_service>/api/v1/applications/run
```

Request body:

```
{
   "name": "<application_name>",
   "params": {
      "loglevel": 10
   }
}
```

After running the integration application in Debug Mode, go back to the Integration Service user interface and review the step logs to see detailed debug output for each step in the integration application. When run in Debug Mode, the step log output shows additional debug statements such as "Saved data for next step", which displays the data being sent from one step to the next.

This information is especially helpful when trying to understand why an integration application or step failed:

Integ	rations Configurations	Reports					Account ?
NVD	To Events				Reports	Edit Configure	Run Now
<	Run: failure			GetDataXML	GetInstalledSoftware	Marin .	
Logs							•
6	MySqlSelect	15 Oct, 2018 11:00:21, 626	INFO	Loaded parameter value: root, type <type 'str'=""> for</type>	parameter: username		*
7	MySqlSelect	15 Oct, 2018 11:00:21, 629	INFO	Loaded parameter value: em7admin, type <type 'st<="" td=""><td>tr'&gt; for parameter: password</td><td></td><td>- 1</td></type>	tr'> for parameter: password		- 1
8	MySqlSelect	15 Oct, 2018 11:00:21, 630	INFO	Loaded parameter value: SELECT did, title FROM r	master_dev.device_packages;, type <type 'str'=""> for parameter: select_query</type>		
9	MySqlSelect	15 Oct, 2018 11:00:21, 633	INFO	Loaded parameter value: *, type <type 'str'=""> for par</type>	rameter: fields		
10	MySqlSelect	15 Oct, 2018 11:00:21, 633	INFO	Loaded parameter value: 7706, type <type 'int'=""> for</type>	r parameter: port		
11	BaseStep	15 Oct, 2018 11:00:21, 733	ERROR	Error when connecting to DB Host: 'http://192.168. -21 Name or service not known'n	32.188', Username: 'root', database: 'master_dev' - (2003, "Can't connect to MySQL server on 'http	//192.168.32.188' ([Ermo	

You can also run an integration in debug using curl via SSH:

- 1. SSH to the Integration Service instance.
- 2. Run the following command:

```
curl -v -k -u isadmin:em7admin -X POST "https://<your_
hostname>/api/v1/applications/run" -H 'Content-Type: application/json' -H 'cache-
control: no-cache' -d '{"name": "interface_sync_sciencelogic_to_
servicenow","params": {"loglevel": 10}}'
```

# Frequently Asked Questions

This section contains a set of frequently asked questions (FAQs) and the answers to address those situations.

## Why are Incidents not getting created in ServiceNow?

- 1. In SL1, go to the **[Events Console]** (Classic user interface) or the **Events** page (SL1 user interface) and locate the event that was created.
  - In the SL1 user interface, click the **[Actions]** button (\*\*\*) for that event and select View Automation Actions.
  - In the Classic user interface, click the **View Notification Log** mailbox icon (A) for that event.
The Event Actions Log window appears:



- 2. On the **Event Actions Log** window, verify that the Run Book Action was triggered, and that the Run Book Action successfully posted to the Integration Service.
- 3. In the "Add/Update Incident action" pane, locate the Integration Service run ID, which is the first six or seven characters of the "isapp" integration ID associated with that run of the integration. For example: *isapp*-a7805e58.
- 4. In the Integration Service user interface, go to the **Integrations** page and open the "Create or Update ServiceNow Incident from SL1 Event" integration application.
- 5. Click the **[Timeline]** button () to locate the run that contains the Integration Service run ID associated with that run of the integration (from step 3, above).
- 6. Click [View Run] for that run on the Timeline and review the logs in the Step Log panel to see where the integration application failed.

### What if my Incident does not have a CI?

For an incident with an active event:

- 1. In SL1, go to the **[Events Console]** (classic user interface) or the **Events** page (new user interface) and locate the event that was created.
  - In the SL1 user interface, click the **[Actions]** button (\*\*\*) for that event and select View Automation Actions.

• In the Classic user interface, click the **View Notification Log** mailbox icon (<sup>(A)</sup>) for that event.

The Event Actions Log window appears

- 2. On the **Event Actions Log** window, locate the Integration Service run ID, which is the first six or seven characters of the "isapp" integration ID associated with that run of the integration. For example: *isapp*-a7805e58.
- 3. In the Integration Service user interface, go to the **Integrations** page and open the integration application that used that run.
- 4. Review the Step Log and confirm that the device class was mapped in the "Sync Devices from SL1 to ServiceNow" integration application.
- 5. Confirm that the "Sync Devices from SL1 to ServiceNow" integration application is running at least every 24 hours, and that the "Sync Devices from SL1 to ServiceNow" integration application has run within 24 hours of that event sync run.

### What if the Integration Service user interface is unresponsive and Incidents are not being generated in ServiceNow?

If the Integration Service user interface is unresponsive, and Incidents are not being generated in ServiceNow, this might mean that during the deployment process, a change to the firewall rules for monitoring broke the ingress network for Docker.

To address this issue, run the following command to restart Docker every time you make a firewall or network configuration change:

systemctl restart docker

# Why are Incident numbers not populated in SL1 on Incident creation in ServiceNow?

If an incident exists in ServiceNow, but incident data is not getting back to SL1, and the "Sync ServiceNow Incident State to SL1 Event" integration application fails on the "Get Incident" step (with a 404 error) and eventually times out, the issue might be because the ServiceNow API is overloaded.

### Why am I not getting any Incidents after disabling the firewall?

If you disabled the firewall to enable SNMP monitoring on the Integration Service, but were not able to connect, you should add the additional rule you need.

# Appendix



### **Checklists for Deployment**

### Overview

This appendix describes the checklists for deploying the Integration Service and the ServiceNow Synchronization PowerPacks, based on your environment and configuration.

This appendix includes the following topics:

CMDB-Only ServiceNow Integration with Single SL1, no Domain Separation in ServiceNow	76
CMDB-Only ServiceNow Integration with Single SL1 and Domain-Separated ServiceNow	79
CMDB-Only ServiceNow Integration with Multiple SL1 Systems, no Domain-Separated ServiceNow	83
Incident-Only ServiceNow Integration with Single SL1, no Domain Separation in ServiceNow	87

### CMDB-Only ServiceNow Integration with Single SL1, no Domain Separation in ServiceNow

- 1. Deploy the Integration Service ISO:
  - IP address, Netmask, Gateway, DNS, Hostname provided
  - Root password provided (this is the root user for the OS)
  - Start Docker services after installation:

/opt/iservices/scripts/pull\_start\_iservices.sh

• Validate that iservices are running:

docker service ls

- 2. Activate the Configuration Management For Scoped Apps (CMDB) Plugin.
- 3. Install the ScienceLogic Certified Application and create a ServiceNow group and user account:
  - Username
  - Password
  - Web Service Access Only
  - GMT Time Zone
  - x\_sclo\_scilogic.Admin role assigned
- 4. Install the ServiceNow Synchronization PowerPacks on the Integration Service.
- 5. Create the Integration Service configuration object using the "ServiceNow SyncPack" configuration object as a template.

#### Sync Devices from SL1 to ServiceNow

- 1. Align the configuration object to the following integration applications:
  - Cache ServiceNow Cls and SL1 Device Classes
  - Sync Devices from SL1 to ServiceNow
- 2. Run "Cache ServiceNow Cls and SL1 Device Classes" to retrieve all device class information from SL1 and ServiceNow. This will populate the device class mapping in the following step. This integration should be run at least every 23 hours.
- 3. Configure class and attribute mappings in "Sync Devices from SL1 to ServiceNow".
- 4. Run "Generate Required CI Relations for ServiceNow" to see if you are missing any service rules or class mappings and create any required maps, containment rules, and hosting rules.
- 5. Run "Sync Devices from SL1 to ServiceNow" either manually or on a schedule. This integration should be run at least every 23 hours. See documentation for more information.

### Discover Devices from ServiceNow in SL1

- 1. Align the configuration object to the following integration applications:
  - Sync Discovery Requirements
  - Sync Discovery Session Requests from ServiceNow to SL1
  - Sync Discovery Session Status from SL1 to ServiceNow
- 2. Set additional configuration variables for each of the integrations applications above in the respective **Configuration** pane.
- 3. Run "Sync Discovery Requirements" to sync all discovery-dependent information from SL1 to ServiceNow.
- 4. Make sure that the Discovery request RITM is successfully created and approved in ServiceNow using the provided Service Catalogs.
- 5. Run "Sync Discovery Session Requests from ServiceNow to SL1" either manually or on a schedule to create and execute the discovery session in SL1.
- 6. After the discovery session has completed in SL1, run "Sync Discovery Session Status from SL1 to ServiceNow" either manually or on a schedule to update the status of the RITM in ServiceNow.

**NOTE:** The following integration applications only sync CIs that are aligned with the devices that are already synced with ServiceNow. Before syncing any of the CIs below, you must first sync devices between SL1 and ServiceNow.

### Sync Business Services from SL1 to ServiceNow

- 1. Align the configuration object to the following integration application:
  - Sync Business Services from SL1 to ServiceNow
- 2. Configure the service classification mappings in "Sync Business Services from SL1 to ServiceNow". These are defined in the **Configuration** pane.
- 3. Run "Sync Business Services from SL1 to ServiceNow" either manually or on a schedule.

### Sync File Systems from SL1 to ServiceNow

- 1. Align the configuration object to the following integration application:
  - Sync File Systems from SL1 to ServiceNow
- 2. The parent CI must be synced in order to see these related CIs.
- 3. Run "Sync File Systems from SL1 to ServiceNow" either manually or on a schedule.

### Sync Network Interfaces from SL1 to ServiceNow

1. Align the configuration object to the following integration application:

- Sync Network Interfaces from SL1 to ServiceNow
- 2. Determine additional filters for syncing network interfaces using the **adapter\_sync** variable defined in the **Configuration** pane.
- 3. The parent CI must be synced in order to see these related CIs.
- 4. Run "Sync Network Interfaces from SL1 to ServiceNow" either manually or on a schedule. This integration application should be run at least every 23 hours if you would like to sync interface-level relationships with "Sync Advanced Topology from SL1 to ServiceNow".

### Sync Installed Software from SL1 to ServiceNow

- 1. Align the configuration object to the following integration application:
  - Sync Software Packages from SL1 to ServiceNow
  - Sync Installed Software from SL1 to ServiceNow
- 2. The parent CI must be synced in order to see these related CIs.
- 3. First, run "Sync Software Packages from SL1 to ServiceNow". Verify that the integration has run successfully.
- 4. Run "Sync Installed Software from SL1 to ServiceNow" either manually or on a schedule.

#### Sync Maintenance Schedules from ServiceNow to SL1

- 1. Align the configuration object to the following integration application:
  - Sync Maintenance Schedules from ServiceNow to SL1
- 2. The parent CI must be synced in order to see these related CIs. The affected CI must have **SL1 Monitored** set to *True*.
- 3. If needed, configure the **Request** and **Task state** IDs in the **Configuration** pane. This is needed if the customer has custom IDs for certain change request or change task states.
- 4. Run "Sync Maintenance Schedules from ServiceNow to SL1" either manually or on a schedule.

### Sync Advanced Topology from SL1 to ServiceNow

- 1. Align the configuration object to the following integration application:
  - Sync Advanced Topology from SL1 to ServiceNow
- The parent CI must be synced in order to see these related CIs. Syncing Interface-level relationships (Layer 2, LLDP, and CDP) will require that "Sync Network Interfaces from SL1 to ServiceNow" is set to run at least every 23 hours.
- 3. Run "Sync Advanced Topology from SL1 to ServiceNow" either manually or on a schedule.

# CMDB-Only ServiceNow Integration with Single SL1 and Domain-Separated ServiceNow

- 1. Deploy the Integration Service ISO:
  - IP address, Netmask, Gateway, DNS, Hostname provided
  - Root password provided (this is the root user for the OS)
  - Start Docker services after installation:

/opt/iservices/scripts/pull\_start\_iservices.sh

• Validate that iservices are running:

docker service ls

- 2. Activate the Configuration Management For Scoped Apps (CMDB) Plugin.
- 3. Install the ScienceLogic Certified Application and create a ServiceNow group and user account:
  - Username
  - Password
  - Web Service Access Only
  - GMT Time Zone
  - x\_sclo\_scilogic.Admin role assigned
- 4. Install the ServiceNow Synchronization PowerPacks on the Integration Service.
- 5. Create the Integration Service configuration object using the "ServiceNow SyncPack" configuration object as a template.

#### Sync Devices from SL1 to ServiceNow

- 1. Align the configuration object to following integration applications:
  - Sync Organizations from SL1 to ServiceNow Companies
  - Cache ServiceNow Cls and SL1 Device Classes
  - Sync Devices from SL1 to ServiceNow
- 2. In "Sync Organizations from SL1 to ServiceNow Companies" **Configuration** pane, set the **Source\_of\_** *Truth* to ServiceNow and set the **Domain\_Separation** flag to True.
- 3. Run "Sync Organizations from SL1 to ServiceNow Companies".
- Run "Cache ServiceNow Cls and SL1 Device Classes" to retrieve all device class information from SL1 and ServiceNow. This will populate the device class mapping in the following step. This integration application should be run at least every 23 hours.

- 5. Configure class and attribute mappings in "Sync Devices from SL1 to ServiceNow". Set **Domain\_** Separation to True.
- 6. Run "Generate Required CI Relations for ServiceNow" to see if you are missing any service rules or class mappings, and then create any required maps, containment rules, and hosting rules.
- 7. Run "Sync Devices from SL1 to ServiceNow" either manually or on a schedule. This integration application should be run at least every 23 hours.

#### Discover Devices from ServiceNow in SL1

- 1. Align Configuration Object to following integration applications:
  - Sync Discovery Requirements
  - Sync Discovery Session Requests from ServiceNow to SL1
  - Sync Discovery Session Status from SL1 to ServiceNow
- 2. In "Sync Discovery Requirements" **Configuration** pane, set the **Source\_of\_Truth** to ServiceNow. Set **Domain\_Separation** to True.
- 3. Run "Sync Discovery Requirements" to sync all discovery-dependent information from SL1 to ServiceNow and back to SL1.
- 4. Set additional configuration variables for each of the other integration applications above in the respective **Configuration** pane.
- 5. Discovery request RITM is successfully created and approved in ServiceNow using the provided Service Catalogs.
- 6. Run "Sync Discovery Session Requests from ServiceNow to SL1" either manually or on a schedule to create and execute the discovery session in SL1.
- 7. After the discovery session completes in SL1, run "Sync Discovery Session Status from SL1 to ServiceNow" either manually or on a schedule to update the status of the RITM in ServiceNow.
- **NOTE:** Domain separation requires that "Sync Organizations from SL1 to ServiceNow Companies" is configured with **Domain\_Separation** enabled and **Source\_of\_Truth** set to ServiceNow. In a domain-separated ServiceNow environment, this integration application must be properly configured and run successfully before syncing any additional CI items. SL1 organizations that are linked to a ServiceNow company will have the **crm\_id** populated with the ServiceNow Company **sys\_id**.

**NOTE:** The following integrations only sync CIs that are aligned with the devices that are already synced with ServiceNow. Before syncing any of the CIs below, you must first sync devices between SL1 and ServiceNow.

### Sync Business Services from SL1 to ServiceNow

1. Align the configuration object to the following integration application:

- Sync Business Services from SL1 to ServiceNow
- 2. Configure the service classification mappings in "Sync Business Services from SL1 to ServiceNow". These are defined in the **Configuration** pane.
- 3. Ensure that **Domain\_Separation** is set to True in the **Configuration** pane.
- 4. Run "Sync Business Services from SL1 to ServiceNow" either manually or on a schedule.

### Sync File Systems from SL1 to ServiceNow

- 1. Align the configuration object to the following integration application:
  - Sync File Systems from SL1 to ServiceNow
- 2. Ensure that **Domain\_Separation** is set to True in the **Configuration** pane.
- 3. The parent CI must be synced in order to see these related CIs.
- 4. Run "Sync File Systems from SL1 to ServiceNow" either manually or on a schedule.

### Sync Network Interfaces from SL1 to ServiceNow

- 1. Align the configuration object to the following integration application:
  - Sync Network Interfaces from SL1 to ServiceNow
- 2. Determine additional filters for syncing network interfaces using the **adapter\_sync** variable defined in the **Configuration** pane.
- 3. Ensure that **Domain\_Separation** is set to True in the **Configuration** pane.
- 4. The parent CI must be synced in order to see these related CIs.
- 5. Run "Sync Network Interfaces from SL1 to ServiceNow" either manually or on a schedule. This integration application should be run at least every 23 hours if you would like to sync interface-level relationships with "Sync Advanced Topology from SL1 to ServiceNow".

### Sync Installed Software from SL1 to ServiceNow

- 1. Align the configuration object to the following integration application:
  - Sync Software Packages from SL1 to ServiceNow
  - Sync Installed Software from SL1 to ServiceNow
- 2. The parent CI must be synced in order to see these related CIs.
- 3. First, run "Sync Software Packages from SL1 to ServiceNow". Verify that the integration has run successfully.
- 4. Run "Sync Installed Software from SL1 to ServiceNow" either manually or on a schedule.

### Sync Maintenance Schedules from ServiceNow to SL1

1. Align the configuration object to the following integration application:

- Sync Maintenance Schedules from ServiceNow to SL1
- 2. The parent CI must be synced in order to see these related CIs. The affected CI must have **SL1 Monitored** set to True.
- 3. If needed, configure the **Request** and **Task state** IDs in the **Configuration** pane. This is needed if the customer has custom IDs for certain change request or change task states.
- 4. Run "Sync Maintenance Schedules from ServiceNow to SL1" either manually or on a schedule.

### Sync Advanced Topology from SL1 to ServiceNow

- 1. Align the configuration object to the following integration application:
  - Sync Advanced Topology from SL1 to ServiceNow
- 2. Ensure that **Domain\_Separation** is set to True in the **Configuration** pane.
- The parent CI must be synced in order to see these related CIs. Syncing Interface-level relationships (Layer 2, LLDP, and CDP) will require that "Sync Network Interfaces from SL1 to ServiceNow" is set to run at least every 23 hours.
- 4. Run "Sync Advanced Topology from SL1 to ServiceNow" either manually or on a schedule.

### CMDB-Only ServiceNow Integration with Multiple SL1 Systems, no Domain-Separated ServiceNow

**NOTE**: Depending on the size of your SL1 stacks and the number of SL1 stacks you have, you may need to consider a "multi-tenant" configured IS. This is a more advanced deployment model. Please contact a ScienceLogic representative for more information.

- 1. Deploy the Integration Service ISO:
  - IP address, Netmask, Gateway, DNS, Hostname provided
  - Root password provided (this is the root user for the OS)
  - Start Docker services after installation:

/opt/iservices/scripts/pull\_start\_iservices.sh

• Validate that iservices are running:

docker service ls

- 2. Activate the Configuration Management For Scoped Apps (CMDB) Plugin.
- 3. Install the ScienceLogic Certified Application and create a ServiceNow group and user account:
  - Username
  - Password
  - Web Service Access Only
  - GMT Time Zone
  - x\_sclo\_scilogic.Admin role assigned
- 4. Install the ServiceNow Synchronization PowerPacks on the Integration Service.
- 5. Create the Integration Service configuration object using the "ServiceNow SyncPack" configuration object as a template.

**NOTE:** The key difference between integrating a single SL1 stack on the Integration Service and integrating multiple SL1 stacks on the Integration Service is how you run the integration application. Running the integration application with multiple SL1 stacks involves creating an individual configuration object for each SL1 stack. Then, create an individual schedule for each configuration object. Each schedule should use a configuration object that is specific to a single SL1 stack.

When creating the schedule, populate the custom parameters with the configuration object ID. For example:

Cache_cis_and_devclasses			÷
SL1Stack A	Runs: 0	Type: crontab	~
SL1 Stack B	Runs: 0	Type: crontab	^
"23:00 every day" Cron Expression: 0 23 * * *			
Custom Parameters			
1 * K 2 "configuration": "SL1_stack_B" 3 }			
expects type: json			
		Del	lete

### Sync Devices from SL1 to ServiceNow

- 1. Create a schedule for each SL1 stack for the following Integrations following the note above:
  - Cache ServiceNow CIs and SL1 Device Classes
  - Sync Devices from SL1 to ServiceNow
- 2. Wait for the "Cache ServiceNow CIs and SL1 Device Classes" to retrieve all device class information from SL1 and ServiceNow. This will populate the device class mapping in the following step. This integration should be run at least every 23 hours.
- 3. Configure class and attribute mappings in "Sync Devices from SL1 to ServiceNow". If each SL1 stack has different class and attribute mapping requirements, you will need to specify the mappings in each schedule's custom parameters for this application.
- 4. Run "Generate Required CI Relations for ServiceNow" to see if you are missing any service rules or class mappings and create any required maps, containment rules, and hosting rules. By default, these will pull from the mappings set in "Sync Devices from SL1 to ServiceNow". If you have defined different mappings for each SL1 stack, you will need to also specify these mappings in each schedule's custom parameters for this application.
- 5. Run "Sync Devices from SL1 to ServiceNow" with a schedule where each schedule uses the configuration object for a SL1 stack. This integration application should be run at least every 23 hours.

### Discover Devices from ServiceNow in SL1

- 1. Create a schedule for each SL1 stack for the following integration applications:
  - Sync Discovery Requirements
  - Sync Discovery Session Requests from ServiceNow to SL1

- Sync Discovery Session Status from SL1 to ServiceNow
- 2. If any additional configuration variables are needed, these will need to be set in the custom parameters section for each schedule
- 3. Run "Sync Discovery Requirements" on a schedule to sync all discovery-dependent information from SL1 to ServiceNow.
- 4. Verify that the discovery request RITM is successfully created and approved in ServiceNow using the provided Service Catalogs.
- 5. Run "Sync Discovery Session Requests from ServiceNow to SL1" on a schedule where each schedule uses the configuration object for a SL1 stack to create and execute the discovery session in SL1.
- 6. Once the discovery session has completed in SL1, run "Sync Discovery Session Status from SL1 to ServiceNow" via schedule where each schedule uses the configuration object for a SL1 stack to update the status of the RITM in ServiceNow.

The following integration applications only sync CIs that are aligned with the devices that are already synced with ServiceNow. Before syncing any of the CIs below, you must first sync devices between SL1 and ServiceNow.

#### Sync Business Services from SL1 to ServiceNow

- 1. Create a schedule for each SL1 stack for the following integration application:
  - Sync Business Services from SL1 to ServiceNow
- 2. Configure service classification mappings in "Sync Business Services from SL1 to ServiceNow" application. These are defined in the **Configuration** pane.
- 3. Run "Sync Business Services from SL1 to ServiceNow" on a schedule where each schedule uses the configuration object for a SL1 stack.

### Sync File Systems from SL1 to ServiceNow

- 1. Create a schedule for each SL1 stack for the following integration application:
  - Sync File Systems from SL1 to ServiceNow
- 2. The parent CI must be synced in order to see these related CIs.
- 3. Run "Sync File Systems from SL1 to ServiceNow" on a schedule where each schedule uses the configuration object for a SL1 stack.

#### Sync Network Interfaces from SL1 to ServiceNow

- 1. Create a schedule for each SL1 stack for the following integration application:
  - Sync Network Interfaces from SL1 to ServiceNow

- 2. Determine additional filters for syncing network interfaces using the **adapter\_sync** variable defined in the **Configuration** pane.
- 3. The parent CI must be synced in order to see these related CIs.
- 4. Run "Sync Network Interfaces from SL1 to ServiceNow" on a schedule where each schedule uses the configuration object for a SL1 stack. This integration application should be run at least every 23 hours if you would like to sync interface-level relationships with "Sync Advanced Topology from SL1 to ServiceNow".

### Sync Installed Software from SL1 to ServiceNow

- 1. Create a schedule for each SL1 stack for the following integration application:
  - Sync Software Packages from SL1 to ServiceNow
  - Sync Installed Software from SL1 to ServiceNow
- 2. The parent CI must be synced in order to see these related CIs.
- 3. "Sync Software Packages from SL1 to ServiceNow" must run on a schedule before "Sync Installed Software from SL1 to ServiceNow". Verify that the software packages have been synced before continuing.
- 4. After the software packages have been synced, run "Sync Installed Software from SL1 to ServiceNow" on a schedule where each schedule uses the configuration object for a SL1 stack.

### Sync Maintenance Schedules from ServiceNow to SL1

- 1. Create a schedule for each SL1 stack for the following integration application:
  - Sync Maintenance Schedules from ServiceNow to SL1
- 2. The parent CI must be synced in order to see these related CIs. The affected CI must have the **SL1** Monitored field set to True.
- 3. If needed, configure the **Request** and **Task state** IDs in the **Configuration** pane. This is needed if the customer has custom IDs for certain change request or change task states.
- 4. Run "Sync Maintenance Schedules from ServiceNow to SL1" on a schedule where each schedule uses the configuration object for a SL1 stack.

### Sync Advanced Topology from SL1 to ServiceNow

- 1. Create a schedule for each SL1 stack for the following integration application:
  - Sync Advanced Topology from SL1 to ServiceNow
- The parent CI must be synced in order to see these related CIs. Syncing Interface-level relationships (Layer 2, LLDP, and CDP) will require that you set "Sync Network Interfaces from SL1 to ServiceNow" to run at least every 23 hours.
- 3. Run "Sync Advanced Topology from SL1 to ServiceNow" on a schedule where each schedule uses the configuration object for a SL1 stack.

### Incident-Only ServiceNow Integration with Single SL1, no Domain Separation in ServiceNow

- 1. Deploy the Integration Service ISO:
  - IP address, Netmask, Gateway, DNS, Hostname provided
  - Root password provided (this is the root user for the OS)
  - Start Docker services after installation: /opt/iservices/scripts/pull\_start\_iservices.sh
  - Validate that iservices are running: docker service ls
- 2. Install the ScienceLogic Certified Application and create a ServiceNow group and user account:
  - Username
  - Password
  - Web Service Access Only
  - GMT Time Zone
- 3. Install the ServiceNow Synchronization PowerPacks on the Integration Service.
- 4. Create the Integration Service configuration object using the "ServiceNow SyncPack" configuration object as a template:
  - Align the configuration object to the following integration applications:
    - Create or Update ServiceNow Incident from SL1 Event
    - Update ServiceNow Incident when SL1 Event is Acknowledged
    - Update ServiceNow Incident when SL1 Event is Cleared
    - Sync Incident State from ServiceNow to SL1 Event
  - Only the following Integration should be run manually or scheduled:
    - Sync Incident State from ServiceNow to SL1 Event
- 5. Install the ServiceNow Base PowerPack and configure SL1:
  - Use the "ServiceNow RBA Example" credential as a template to create a new credential that points to the Integration Service instance.
  - Align the newly-created credential to the "ServiceNow Add/Update/Clear Incident" Run Book Action.
  - Ensure that all Run Book Actions and Run Book Policies are enabled.

# Appendix

# B

### **Certified Application Objects**

### Overview

This appendix describes the tables, endpoints, and roles that were created in ServiceNow as part of the "ScienceLogic SL1: CMDB & Incident Automation" application. This application is also known as the "Certified Application" or the "Scoped Application".

This appendix includes the following topics:

Roles	89
Tables	90
Table Columns (cmdb_ci)	90
Table Columns (core_company)	91
Table Columns (cmdb_group)	91
Script Includes	91
Event Registry	91
Scripted Actions	92
Data Lookup Definitions	92
System Properties	92
Catalog Item	93
Catalog UI Policies	93
Variable Sets	93
Catalog Client Scripts	94
Workflows	94
Scripted REST Resources	

Transform Maps	. 97
Transform Scripts	. 97

### Roles

Two Roles were added with the ScienceLogic update set, Admin (x\_sclo\_scilogic.Admin) and User (x\_sclo\_ scilogic.User). Both give access to SL1.

Role	Inherited Roles	Other Inherited Roles	Role Definition
x_sclo_scilogic.Admin			Role for ScienceLogic Service Accounts.
	itil		Can perform standard actions for an ITIL help desk technician. This is the default "Technician" role. Can open, update, close incidents, problems, changes, config management items. By default, only users with the itil role can have tasks assigned to them
		Dependency_view	A special role to be applied both on the \$ngbsm UI page and on the BSMProcessor. This role is required to access the dependency views module. By default, ITIL includes this role to avoid regressions.
		cmdb_query_builder	Can access the CMDB Query Builder application to create, run, and save queries on the CMDB.
		template_editor	
		view_changer	Can switch active views.
		app_service_user	Can view and retrieve information using API from application service maps (cmdb_ci_service_discovered).
		certification	Can work on Certification tasks.
	import_ transformer		Can manage Import Set Transform Maps and run transforms.
x_sclo_scilogic.User			General user account that allows read- only access to SL1.

### Tables

Name	Label	Extends	Comments
x_sclo_scilogic_event	Event	(empty)	Event information
x_sclo_scilogic_event_ severity	Event Severity Look Rules	Data Lookup Matcher Rules	Look up table for event Severity
x_sclo_scilogic_incident	Import Incident	Import Set Row	Import / staging events before transform to Event and Incident
x_sclo_scilogic_import_ installed_software	Import Installed Software	Import Set Row	Import / staging events before transform to Software Instance
x_sclo_scilogic_org_ven_ mfg	Import ORG VEN MFG	Import Set Row	Import / staging events before transform to core_company
x_sclo_scilogic_import_ discovery_dependent	Import Discovery Dependent	Import Set Row	Import / staging events before transform to Discovery Dependent table
x_sclo_scilogic_discovery_ dependent	Discovery Dependent	(empty)	Discovery Dependent Information
x_sclo_scilogic_catalog_ item_templates	Catalog item Templates	(empty)	Templates use to fill out catalog items
x_sclo_scilogic_import_ service_request	Import Service Request	Import Set Row	Import / staging events before transform to Service Requests

# Table Columns (cmdb\_ci)

Name	Label	Туре	Comments
x_sclo_scilogic_id	SL1 ID	Integer	Unique ID
x_sclo_scilogic_region	SL1 Region	String	Unique String of SL1 Platform
x_sclo_scilogic_url	SL1 URL	URL	URL to SL1 Platform
x_sclo_scilogic_monitored	SL1 Monitored	True/False	Device currently synced with SL1 Platform

### Table Columns (core\_company)

Name	Label	Туре	Comments
x_sclo_scilogic_id	SL1 ID	String	Unique ID
x_sclo_scilogic_region	SL1 Region	String	Unique String of SL1 Platform
x_sclo_scilogic_monitored	SL1 Monitored	True/False	Organization currently synced with SL1 Platform

### Table Columns (cmdb\_group)

Name	Label	Туре	Comments
x_sclo_scilogic_id	SL1 ID	String	Unique ID
x_sclo_scilogic_region	SL1 Region	String	Unique String of SL1 Platform

### Script Includes

Name	API Name	Comments
CatalogUtils	x_sclo_scilogic.catalogUtils	Catalog Script include scripts
ChangeUtils	x_sclo_scilogic.changeUtils	Change Script include scripts
DeviceUtils	x_sclo_scilogic.DeviceUtils	Device Script include scripts
EventUtils	x_sclo_scilogic.EventUtils	Event Script include scripts
GeneralUtils	x_sclo_scilogic.GeneralUtils	General Script include scripts

### Event Registry

Suffix	Event name	Table	Comments
device_monitoring	x_sclo_scilogic.device_	Configuration Item [cmdb_	Event for Device
	monitoring	ci]	Monitoring
Remove_	x_sclo_scilogic.remove_	Configuration Item [cmdb_	Event for Remove
monitoring	monitoring	ci]	Monitoring

### Scripted Actions

Name	Event name	Comments
Device Monitoring Catalog item	x_sclo_scilogic.device_ monitoring	Action used to submit Catalog item via Event.
Device Removal Catalog item	x_sclo_scilogic.remove_ monitoring	Action used to submit Catalog item via Event.

### Data Lookup Definitions

Name	Source Table	Matcher Table	Comments
Event	Import Incident [x_sclo_	Event Severity Lookup Rules [x_sclo_	Lookup for ScienceLogic Severity to
Severity	scilogic_incident]	scilogic_event_severity]	Impact and Urgency

### System Properties

Suffix	Name	Comments
CatalogItemDiscovery	x_sclo_ scilogic.CatalogItemDiscovery	Unique value (sys_id)
CatalogItemRemove	x_sclo_scilogic.CatalogItemRemove	Unique value (sys_id)
closeCode	x_sclo_scilogic.closeCode	Value to use for Close Code for Incident Transform
Contact type	x_sclo_scilogic.Contact Type	Value to use for Contact type for Incident Transform
deviceLogging	x_sclo_scilogic.deviceLogging	Turn on Logging
deviceLoggingParam	x_sclo_scilogic.deviceLoggingParm	Add additional parameters beyond the default errors
discoverySource	x_sclo_scilogic.discoverySource	Discovery Source to be used by Integration Service
notResolved	x_sclo_scilogic.notResolved	Value of Reopened Incident
stateNew	x_sclo_scilogic.stateNew	Value of New Incident
StateResolved	x_sclo_scilogic.stateResolved	Value of Resolved Incident

### Catalog Item

Name	Comments
Device Discovery	Role for ScienceLogic Service Accounts.
Monitoring Removal	General user account that allows read only access to ScienceLogic Application.

### Catalog UI Policies

Catalog item	Short description	Comments
Device Discovery	Catalog Template	Updates form based on Select template
Device Discovery	Create Virtual Device	Updates form based on Request type
Device Discovery	Create Virtual Device (Retired)	
Device Discovery	Device Discovery	Updates form based on Request type
Device Discovery	Device Discovery (Retired)	
Monitoring Removal	Hide Overview variables not required	Hide variables not required for the Monitoring Removal request
Device Discovery	Port Scan	Hide scan ports that are not default
Device Discovery	Port Scan (Retired)	
Device Discovery	Region	Updates form based on Organization
Device Discovery	Region (Retired)	
Monitoring Removal	Region via Organization	Updates form based on Organization
Device Discovery	Save as Template	Updates form based on Save as template

### Variable Sets

Title	Internal name	Comments
Create_virtual_device	create_virtual_device	
Discovery Overview	discovery_overview	

Title	Internal name	Comments
Discovery Sesion - Basic Settings	discovery_sesion_basic_settings	
Discovery Session - Detection and Scanning	discovery_session_detection_and_scanning	
Discovery Session - IP & Credentials	discovery_session_ip_credentials	
Monitoring Removal	monitoring _removal	
Service Catalog item Template	service_catalog_item_template	

## Catalog Client Scripts

Name	Catalog item	Туре	Comments
Hide Request Type Options	Monitoring Removal	onLoad	Shared variable hide options that don't apply
Hide Request Type Options	Device Discovery	onLoad	Shared variable hide options that don't apply
Region	Monitoring Removal	onChange	Update Region field based on Company Region
Region	Monitoring Removal	onChange	Update Region field based on Company Region

### Workflows

Name	Table	Comments
SL1 Monitoring Removal	Requested Item [sc_req_item]	Workflow for Removal of devices from SL1 process
SL1 Discovery Session	Requested Item [sc_req_item]	Workflow for Discovery session process

## Scripted REST Resources

Name			Comments
Business Services	/api/x_sclo_ scilogic/v1/sciencelogic/business_service	GET	This GET api will pull all ScienceLogic monitored Configuration items specific to Business Services class from the CMDB. It will be ordered via the sys_id field to ensure the same order every time.
CMDB Group	/api/x_sclo_scilogic/v1/sciencelogic/cmdb_ group	post	Use this API to create cmdb_groups & add a CI to them.
Change Requests	/api/x_sclo_ scilogic/v1/sciencelogic/change_requests	GET	This GET api will pull Active Change Requests or Change Tasks based on the record_type supplied that have ScienceLogic monitored CI attached. It will be ordered via the sys_id field to ensure the same order every time.
Classification	/api/x_sclo_ scilogic/v1/sciencelogic/classification	GET	This GET api will pull all required CMDB information to build JSON payloads.
Companies	/api/x_sclo_ scilogic/v1/sciencelogic/companies	GET	This GET api will pull all Active Companies that are ScienceLogic monitored. It will be ordered via the sys_id field to ensure the same order every time.
Configuration Items	/api/x_sclo_ scilogic/v1/sciencelogic/configuration_Items	GET	This GET api will pull all ScienceLogic monitored Configuration items from the CMDB. It will be ordered via the sys_id field to ensure the same order every time.
Device IdentificationEngine	/api/x_sclo_ scilogic/v1/sciencelogic/IdentificationEngine	POST	Use this API to create or update configuration items within the CMDB via ScienceLogic.

Name			Comments
File Systems	/api/x_sclo_scilogic/v1/sciencelogic/file_ systems	GET	This GET api will pull all ScienceLogic monitored Configuration items specific to File systems class from the CMDB. It will be ordered via the sys_id field to ensure the same order every time.
Import Set	/api/x_sclo_ scilogic/v1/sciencelogic/import_set		This POST API will post to the target import set table and create a record for each cmdb_ci.
Incidents	/api/x_sclo_ scilogic/v1/sciencelogic/incidents	GET	This GET api will pull all incidents. It will be ordered via the sys_id field to ensure the same order every time.
Installed Software	/api/x_sclo_ scilogic/v1/sciencelogic/installed_software	GET	This GET api will pull all Servicenow Software packages and installed instances from the CMDB. It will be ordered via the sys_id field to ensure the same order every time.
Manufacture	/api/x_sclo_ scilogic/v1/sciencelogic/manufactures	POST	This POST API will pull all Manufactures.
Model	/api/x_sclo_scilogic/v1/sciencelogic/models	POST	This POST API will pull all Model.
Network Adapters	/api/x_sclo_ scilogic/v1/sciencelogic/network_adapters	GET	This GET api will pull all ScienceLogic monitored Configuration items specific to Network Adapter class from the CMDB. It will be ordered via the sys_id field to ensure the same order every time.
Service Request	/api/x_sclo_ scilogic/v1/sciencelogic/service_request	GET	This GET api will pull all ServiceRequest items from the CMDB associated with Device Discovery Catalog item. It will be ordered via the sys_id field to ensure the same order every time.
Classification	/api/x_sclo_ scilogic/v2/sciencelogic/classification	GET	This GET api will pull all required CMDB information to build JSON payloads.

# Transform Maps

Name	Source Table	Target Table	Comments
ScienceLogic Discovery	Import Discovery	Discovery	Import / staging table for Catalog
Dependent	Dependent	Dependent	Dependents
ScienceLogic Event	Import Incident	Event	Import / staging table for Events.
ScienceLogic Incident	Import Incident	Incident [incident]	Import / staging table for Incident
ScienceLogic Organization	Import ORG VEN	Company [core_	Import / staging table for
	MFG []	company]	Organization
ScienceLogic Service	Import Service	Request Item [sc_	Import / staging table for Request
Request	Request []	req_item]	item

### Transform Scripts

Name	Transform Map	Order	Comments
onBefore	ScienceLogic Event	100	Check Action
onAfter	ScienceLogic Event	100	Check Action; Get Resolved Validation script include
onBefore	ScienceLogic Incident	100	Check Action, event workflow script include
onAfter	ScienceLogic Incident	100	Check Action, Affected CI script include

# Appendix

# C

### **ServiceNow API Endpoints**

### Overview

This appendix describes the customized ServiceNow API Endpoints that were created for the Integration Service ServiceNow Synchronization PowerPacks. These scripted endpoints reduce the amount of REST calls that the Integration Service makes to ServiceNow.

Please note that for pagination, the following Query parameters are not required: sysparm\_limit. The default settings are:

- sysparm\_offset=0
- sysparm\_limit = ServiceNow defines the default upper limits for data export. It will check the following properties at System Properties > Import Export: glide.json.export.limit, glide.ui.export.limit, and then glide.ui.export.war.threshold.

For example, if you have 200 total records and you want to pull the records in 100-record chunks, then the first pull would be sysparm\_offset=0 & sysparm\_limit=100 and the second pull would be sysparm\_ offset=100 & sysparm\_limit=100. For more information, see the ServiceNow documentation for Export Limits.

This appendix includes the following topics:

Business Services	100
Change Requests	102
Classification version 1	104
Classification version 2	107
CMDB Group	110
Companies	112
Device Identification Engine	115

Discovery Dependents	
File Systems	120
Import Set	122
Incidents	124
Installed Software	
Manufacturer	130
Model	132
Network Adapters	134
Service Requests	136

### **Business Services**

### **HTTP Method**

GET

#### Pagination

Enabled

#### **Resource** Path

/api/x\_sclo\_scilogic/v1/sciencelogic/business\_service

### Default Resource Path

/api/x\_sclo\_scilogic/sciencelogic/business\_service

This operation pulls all the fields from just the Business Service (**cmdb\_ci\_service**) table. The return is ordered by **sys\_id**, so the results display in the same order every time. The results are filtered by the **SL1 monitored** and **SL1 ID** field on the ServiceNow side. This operation requires the region to be supplied by the requester, and it will only return region-supplied configuration items.

Headers	
Кеу	Value
Content-Type	application/json
Accept	application/json

Parameters	
Кеу	Value
region (required)	ScienceLogic
sysparm_offset	0
sysparm_limit	glide.json.export.limit, glide.ui.export.limit, glide.ui.export.war.threshold

### Example (Request URL)

https://<your Instance>.service-now.com/api/x\_sclo\_scilogic/v1/ sciencelogic/business\_ service

#### Example (Response)

```
{
    "results": [
        {
            "operational status": "1",
            "sys updated on": "2019-02-06 19:32:34",
            "discovery_source": "Other Automated",
            "first discovered": "2019-02-06 19:31:19",
            "sys updated by": "admin",
            "sys_created_on": "2019-02-06 19:31:19",
            "sys_domain": "global",
            "used_for": "Production",
            "sys created by": "is4user1",
            "sys_domain_path": "/",
            "install_status": "1",
            "name": "One Service to rule them",
            "subcategory": "Service",
            "busines_criticality": "1 - most critical",
            "last_discovered": "2019-02-06 19:31:19",
            "sys_class_name": "cmdb_ci_service",
            "sys id": "52da95dcdb6323009f7dd7a0cf961918",
            "sys_class_path": "/!!/#C",
            "comments": "Postman",
            "sys mod count": "1",
            "x_sclo_scilogic_id": "1570",
            "model id": "e8aaeb3f3763100044e0bfc8bcbe5d20",
            "cost cc": "USD",
            "x sclo scilogic monitored": "true",
            "category": "Business Service",
            "service classification": "Technical Service",
            "x_sclo_scilogic_region": "ScienceLogic"
        }
    ],
    "sysparm_offset": 0,
    "sysparm_limit": 100,
   "return_count": 1,
    "total count": 1
}
```

### Change Requests

### HTTP Method

GET

#### **Resource** Path

```
/api/x_sclo_scilogic/v1/sciencelogic/change_requests?record_type=change_
request&state=1&region=ScienceLogic
```

### Default Resource Path

```
/api/x_sclo_scilogic/v1/sciencelogic/change_requests?record_type=change_
request&state=1&region=ScienceLogic
```

This scripted API was built for pulling Change Requests or Change Tasks and formatting a JSON object response with the required information to create a maintenance schedule in SL1. The GET queries the **task\_ci** table to find configuration items that are monitored by SL1 and are the correct record type. The GET operation returns all records with their configuration items in formatted JSON strings that include planned start and end time.

Headers	
Кеу	Value
Content-Type	application/json
Accept	application/json

Parameters		
Кеу	Value	
record_type (required)	change_request	
state	-5	
region (required)	ScienceLogic	
sysparm_offset	0	
sysparm_limit	glide.json.export.limit, glide.ui.export.limit, glide.ui.export.war.threshold	

**HTTP Status** 

Code	Value
200	ОК
400	Query parameter \'region\' is not defined and is required.

### Fixed Internal Query

#### State:

```
`task.sys_class_name=' + recordType + `task.state=' + state + `^ci_item.x_sclo_
scilogic_monitored=true^ci_item.x_sclo_scilogic_region=' + region
```

#### Non-State:

```
`task.active=true^task.sys_class_name=' + recordType + `ci_item.x_sclo_scilogic_
monitored=true^ci_item.x_sclo_scilogic_region=' + region
```

### Example

```
https://<your Instance>.service-now.com/api/x_sclo_scilogic/v1/sciencelogic/change_
requests?record_type=change_request&state=-5&region=ScienceLogic
```

### Example (Response)

```
{
    "results": [
        {
            "sys id": "48ebaba0db962f00dc44f00fbf961961",
            "number": "CHG0030001",
            "state value": "-5",
            "state": "New",
            "short_description": "Test Change",
            "planned start date": "2019-01-01 06:00:01",
            "planned end_date": "2019-01-01 18:00:01",
            "device": [
                {
                    "sys id": "d83dac0adb4dab00dc44f00fbf961919",
                    "name": "Postman Test Server 11",
                    "id": "11",
                    "region": "ScienceLogic"
                }
            ]
       }
   ]
}
```

### Classification version 1

**NOTE:** This API Endpoint has been deprecated. The last version of the "ScienceLogic SL1: CMDB & Incident Automation" application" (also called the Certified or Scoped application), that used this endpoint was version 1.0.18.

### HTTP Method

GET

#### Pagination

Enabled

#### **Resource** Path

/api/x\_sclo\_scilogic/v1/sciencelogic/classification

### Default Resource Path

```
/api/x_sclo_scilogic/sciencelogic/classification
```

To support the identification and reconciliation framework, SL1 requires a large amount of information to know how to correctly fill out the JSON formatted string defined by the Identification Engine documentation. This operation uses the **getTableExtension()** function to find all the tables extended from the **cmdb\_ci** table and then goes through each table one by one. This operation collects information about each class, such as which fields are required to identify and if it is considers another class to help find uniqueness. This operation then finds all the associated metadata. Finally, the operation pulls a list of all field names from the table. By default the **criterion\_ attributes** and **attributes** are not included and require "action=attributes" as a parameter in the API call to be passed.

Headers	
Кеу	Value
Content-Type	application/json
Accept	application/json

Parameters	
Кеу	Value
action	attributes

Attributes require x\_sclo\_scilogic.Admin be added to **sys\_dictionary**.\* (read) ACL to allow the API to access field names on each class table.

### Fixed Internal Query

#### Example

```
https://<your Instance>.service-now.com/api/x_sclo_scilogic/sciencelogic/
classification
```

#### Example (Response)

```
{
 "results": [
   {
     "class label": "Storage Area Network",
     "class_table": "cmdb_ci_san",
      "criterion_attributes": [
       ....
     ],
      "independent": "false",
      "containment_rule": [
     ],
      "hosting_rule": [
      ],
      "reference_rule": [
      ],
      "attributes": [
       "asset",
        "asset_tag",
        "assigned",
        "assigned to",
        "assignment_group",
        "attributes",
        "can print",
        "category",
        "change_control",
        "checked in",
        "checked_out",
        "comments",
        "company",
        "correlation_id",
        "cost",
        "cost cc",
        "cost_center",
        "delivery_date",
        "department",
        "discovery_source",
        "dns_domain",
        "due",
        "due in",
        "fault_count",
```

"first\_discovered", "fqdn", "gl\_account", "install\_date", "install\_status", "invoice\_number", "ip address", "justification", "last\_discovered", "lease\_id", "location", "mac address", "maintenance\_schedule", "managed by", "manufacturer", "model id", "model\_number", "monitor", "name", "operational\_status", "order\_date", "owned\_by", "po\_number", "purchase date", "san\_id", "schedule", "serial number", "short description", "skip\_sync", "start date", "subcategory", "supported by", "support\_group", "sys class name", "sys\_class\_path", "sys\_created\_by", "sys\_created\_on", "sys\_domain", "sys\_domain\_path", "sys\_id", "sys\_mod\_count", "sys\_updated\_by", "sys\_updated\_on", "unverified", "vendor", "warranty\_expiration", "x\_sclo\_scilogic\_id", "x\_sclo\_scilogic\_monitored", "x sclo scilogic region", "x sclo scilogic url" ] }

] }

### Classification version 2

### HTTP Method

GET

### Pagination

Enabled

### **Resource** Path

/api/x\_sclo\_scilogic/v2/sciencelogic/classification

### Default Resource Path

/api/x\_sclo\_scilogic/sciencelogic/classification

To support the identification and reconciliation framework, SL1 requires a large amount of information to know how to correctly fill out the JSON formatted string defined by the Identification Engine documentation. This operation uses the **getTableExtension()** function to find all the tables extended from the **cmdb\_ci** table and then goes through each table one by one. This operation collects information about each class, such as which fields are required to identify and if it is considers another class to help find uniqueness. This operation then finds all the associated metadata. Finally, the operation pulls a list of all field names from the table. By default the **criterion\_ attributes** and **attributes** are not included and require "action=attributes" as a parameter in the API call to be passed.

Headers	
Кеу	Value
Content-Type	application/json
Accept	application/json

Parameters	
Кеу	Value
action	attributes
sysparm_offset	0
sysparm_limit	glide.json.export.limit, glide.ui.export.limit, glide.ui.export.war.threshold

Attributes require x\_sclo\_scilogic.Admin be added to **sys\_dictionary**.\* (read) ACL to allow the API to access field names on each class table.

### Fixed Internal Query

### Example

```
https://<your Instance>.service-now.com/api/x_sclo_scilogic/v2/sciencelogic/
classification
```

### Example (Response)

```
{
  "results": [
   {
      "class label": "Storage Area Network",
      "class_table": "cmdb_ci_san",
      "criterion_attributes": [
       ....
      ],
      "independent": "false",
      "containment_rule": [
      ],
      "hosting_rule": [
      ],
      "reference_rule": [
      ],
      "attributes": [
       "asset",
        "asset_tag",
        "assigned",
        "assigned to",
        "assignment_group",
        "attributes",
        "can print",
        "category",
        "change_control",
        "checked_in",
        "checked_out",
        "comments",
        "company",
        "correlation_id",
        "cost",
        "cost cc",
        "cost center",
        "delivery_date",
        "department",
        "discovery_source",
        "dns domain",
        "due",
        "due in",
        "fault_count",
        "first_discovered",
        "fqdn",
        "gl_account",
```
"install\_date", "install\_status", "invoice\_number", "ip\_address", "justification", "last\_discovered", "lease id", "location", "mac address", "maintenance\_schedule", "managed by", "manufacturer", "model\_id", "model\_number", "monitor", "name", "operational\_status", "order date", "owned\_by", "po\_number", "purchase\_date", "san\_id", "schedule", "serial\_number", "short\_description", "skip sync", "start date", "subcategory", "supported by", "support group", "sys\_class\_name", "sys\_class\_path", "sys\_created\_by", "sys\_created\_on", "sys\_domain", "sys\_domain\_path", "sys\_id", "sys mod count", "sys\_updated\_by", "sys\_updated\_on", "unverified", "vendor", "warranty\_expiration", "x\_sclo\_scilogic\_id", "x\_sclo\_scilogic\_monitored", "x sclo\_scilogic\_region", "x\_sclo\_scilogic\_url" ]

} ] }

# CMDB Group

### HTTP Method

POST

### Pagination

Enabled

#### **Resource** Path

/api/x\_sclo\_scilogic/v1/sciencelogic/cmdb\_group

# Default Resource Path

/api/x\_sclo\_scilogic/sciencelogic/cmdb\_group

This operation handles the intake of groups of devices from SL1 and converts the device groups to CMDB groups. This operation uses a standard formatted JSON string, and it checks for a **sys\_id** of the group first by searching for a matching group. This process creates a group if a group is not supplied or found, and then it passes the JSON object to the ServiceNow CMDBGroupAPI, which sets the manual CI list of the group.

Headers		
Кеу	Value	
Content-Type	application/json	
Accept	application/json	

# Example (Request URL

https://<your Instance>.service-now.com/api/x\_sclo\_scilogic/v1/sciencelogic/cmdb\_group

# Example (Body)

```
[
    {
        "items": [
            {
            "name": "test",
            "description": "",
            "group": "",
            "manualCIList": "d83dac0adb4dab00dc44f00fbf961919,2e6b7046db8dab00dc44f00fbf
        961929,7fb39667dba12380dc44f00fbf961901,77b39667dba12380dc44f00fbf961917,7bb
        39667dba12380dc44f00fbf96191c",
            "region": "Cisco",
            "id": "1"
        }
}
```

] } ]

```
{
 "result": [
   {
     "idList": [
     ],
     "partialCIListDueToACLFlag": false,
     "nextBatchStart": 0,
     "result": true
   },
   {
     "idList": [
     ],
     "partialCIListDueToACLFlag": false,
     "nextBatchStart": 0,
     "result": true
  }
 ]
}
```

# Companies

# HTTP Method

GET

# Pagination

Enabled

### **Resource** Path

/api/x\_sclo\_scilogic/v1/sciencelogic/companies

# Default Resource Path

/api/x\_sclo\_scilogic/sciencelogic/companies

This operation supports Domain Separation enabled or not enabled. This operation pulls all the fields for from the company table that are not NULL values. The return is ordered by **sys\_id**, so the results display in the same order every time. The results are filtered by the **SL1 Monitored** and **region** values. The region mus be supplied by the requester, and it will only return region-specific companies.

Headers	
Кеу	Value
Content-Type	application/json
Accept	application/json

Parameters		
Кеу	Value	
region (required)	ScienceLogic	
domainSep	false	
sysparm_offset	0	
sysparm_limit	glide.json.export.limit, glide.ui.export.limit, glide.ui.export.war.threshold	

HTTP Status		

Code	Value
200	ОК
400	Query parameter \'region\' is not defined and is required.

#### Domain:

```
'x_sclo_scilogic_region=' + region + `^x_sclo_scilogic_monitored=true^sys_
domain!=global'
```

#### Non-Domain:

```
'x'_sclo_scilogic_monitored=true^x_sclo_scilogic_idISNOTEMPTY^x_sclo_scilogic_region''
+ region
```

### Example

```
https://<your instance>.service-now.com/api/x_sclo_scilogic/v1/sciencelogic/
companies?region=ScienceLogic&sysparm_offset=0&sysparm_limit=100
```

```
{
  "results": [
   {
     "country": "USA",
     "notes": "What's on your digital horizon?",
      "city": "San Jose",
      "sys updated on": "2018-11-30 16:03:45",
      "sys class name": "core company",
      "sys id": "lac84f95dbce2700dc44f00fbf9619c8",
      "sys_updated by": "is4user1",
      "market cap": "0",
      "street": "170 West Tasman Dr.",
      "sys created on": "2018-11-27 16:32:33",
      "state": "CA",
      "sys created by": "admin",
      "zip": "95134",
      "profits": "0",
      "revenue_per_year": "0",
      "sys_mod_count": "4",
      "x sclo scilogic id": "1",
      "x sclo scilogic monitored": "true",
      "phone": "18005532447",
      "name": "Cisco Systems, Inc.",
      "x sclo scilogic region": "Cisco"
    }
 ],
 "sysparm offset": 0,
 "sysparm_limit": 1,
 "return count": 1,
  "total count": 1
}
```

# Device Identification Engine

### HTTP Method

POST

#### Pagination

Enabled

#### **Resource** Path

/api/x\_sclo\_scilogic/v1/sciencelogic/IdentificationEngine

# Default Resource Path

/api/x\_sclo\_scilogic/sciencelogic/IdentificationEngine

This operation handles all creates and updates to the CMDB. This operation incorporates Identification Engine and uses the Identification and Reconciliation framework to properly import devices into the CMDB as a configurable discovery source. SL1 uses the classification GET to populate the JSON object.

Headers	
Кеу	Value
Content-Type	application/json
Accept	application/json

Parameters	
Кеу	Value
test	true

# Example (Request URL)

https://<your Instance>.service-now.com/api/x\_sclo\_scilogic/v1/sciencelogic/ IdentificationEngine?test=true

# Example (Body)

```
[
{
    "items": [
    {
        "className": "cmdb_ci_linux_server",
    }
}
```

```
"values": {
          "name": "Postman Test Server 1",
          "serial_number": "9876EFGH",
          "mac_address": "BF:D4:D6:6E:56:F1",
          "ip address": "10.10.10.4",
          "ram": "16000",
          "x sclo scilogic_region": "ScienceLogic",
          "x sclo_scilogic_id": "1"
        }
      }
    ]
 },
  {
    "items": [
      {
        "className": "cmdb ci linux server",
        "values": {
          "name": "Postman Test Server 2",
          "serial number": "HGFE6789",
          "mac_address": "87:54:3C:8C:2A:A3",
          "ip_address": "10.10.10.5",
          "ram": "16000",
          "x sclo scilogic region": "ScienceLogic",
          "x_sclo_scilogic_id": "2"
        }
      }
    ]
 }
]
```

# Example Business Service (Body)

```
[
{
"items": [
{
"className": "cmdb ci service",
"values": {
"name": "Integration Service",
"busines_criticality": "1 - most critical",
"used for": "Production",
"operational_status": "1",
"service_classification": "Technical Service",
"comments": "Postman",
"x sclo scilogic region": "ScienceLogic",
"x_sclo_scilogic_id": "1570"
}
},
{
"className": "cmdb ci linux server",
"values": {
"name": "Postman Test Server",
"serial number": "7MDvgrSNyd",
"manufacturer": "ScienceLogic, Inc.",
"model_id": "",
"mac address": "EE:D6:0B:79:32:C7",
```

```
"ip_address": "10.10.10.224",
"ram": "16000",
"x_sclo_scilogic_region": "ScienceLogic",
"x_sclo_scilogic_id": "10"
}
],
"relations": [
{
    "type": "Depends on::Used by",
    "parent": 0,
    "child": 1
}
]
```

```
{
  "result": [
    {
      "items": [
        {
          "className": "cmdb ci linux server",
          "operation": "NO CHANGE",
          "sysId": "7fb39667dba12380dc44f00fbf961936",
          "identifierEntrySysId": "fb27f69cc3000200d8d4bea192d3ae67",
          "identificationAttempts": [
            {
              "identifierName": "Hardware Rule",
              "attemptResult": "SKIPPED",
              "attributes": [
                "serial number",
                "serial_number_type"
              ],
              "searchOnTable": "cmdb serial number"
            },
            {
              "identifierName": "Hardware Rule",
              "attemptResult": "MATCHED",
              "attributes": [
                "serial_number"
              ],
              "searchOnTable": "cmdb_ci_hardware"
            }
          ]
        }
      ],
      "relations": [
     ]
   }
 ]
}
```

# **Discovery Dependents**

# HTTP Method

GET

### Pagination

Enabled

### **Resource** Path

/api/x\_sclo\_scilogic/v1/sciencelogic/discovery\_dependent

# Default Resource Path

/api/x\_sclo\_scilogic/sciencelogic/discovery\_dependent

This operation pulls all Discovery-dependent records that are tied to the **region** value, which is used for the catalog request process. Based on the request type, this operation returns a formatted JSON object. This operation pulls all the required information for both SL1 processes: Discovery Session and Create Virtual Device. Both requests require different information and are formatted accordingly.

The basic catalog item Device Discovery is set up as information collection to support the process within SL1. The Service Catalog has been simplified to its most basic form. The Service Catalog moves the request into the correct state to be picked up by the GET Request and then waits for its return before completing the workflow.

Headers	
Кеу	Value
Content-Type	application/json
Accept	application/json

Parameters		
Кеу	Value	
region (required)	ScienceLogic	
sysparm_offset	0	
sysparm_limit	glide.json.export.limit, glide.ui.export.limit, glide.ui.export.war.threshold	

HTTP Status		
Code	Value	
200	ОК	
400	Query parameter \'region\' is not defined and is required.	

Region Specific: 'region=' + region

### Example

```
https://<your instance>.service-now.com/api/x_sclo_scilogic/v1/sciencelogic/discovery_
dependent?region=del_test&sysparm_offset=0&sysparm_limit=100
```

```
{
    "results": [
        {
            "sys_updated_on": "2019-08-28 18:03:50",
            "type": "credential",
            "type label": "Credentials",
            "sys_id": "0491aae51b273f0045c8db1dcd4bcbc2",
            "hostname": "example.com",
            "sys updated by": "is4user1",
            "sys_created_on": "2019-08-28 18:03:50",
            "name": "AppDynamics Example",
            "id": "93",
            "category": "soapCredentials",
            "region": "del_test",
            "sys_created_by": "is4user1"
        }
    ],
    "sysparm_offset": 0,
    "sysparm_limit": 1,
    "return_count": 1,
    "total count": 150
}
```

# File Systems

# HTTP Method

GET

# Pagination

Enabled

### **Resource** Path

/api/x\_sclo\_scilogic/v1/sciencelogic/file\_systems

# Default Resource Path

/api/x\_sclo\_scilogic/sciencelogic/file\_systems

This operation pulls all the fields from the File System table. The return is ordered by **sys\_id**, so the results display in the same order every time. The results are filtered by the **SL1 monitored** and **SL1 ID** field on the ServiceNow side. This operation requires the region to be supplied by the requester, it returns only region-supplied configuration items.

Headers		
Кеу	Value	
Content-Type	application/json	
Accept	application/json	

Parameters		
Кеу	Value	
region (required)	ScienceLogic	
sysparm_offset	0	
sysparm_limit	glide.json.export.limit, glide.ui.export.limit, glide.ui.export.war.threshold	

HTTP Sto	atus
Code	Value

200	OK
400	Query Parameter \'region\' is not defined and is required.

`x\_sclo\_scilogic\_monitored=true^x\_sclo\_scilogic\_idISNOTEMPTY^x\_sclo\_scilogic\_region='
+ region

#### Example

```
https://<your Instance>.service-now.com/api/x_sclo_scilogic/v1/sciencelogic/file_
systems?region=ScienceLogic&sysparm offset=0&sysparm limit=100
```

```
{
  "results": [
   {
      "operational_status": "1",
      "sys updated on": "2018-11-12 21:59:52",
      "media type": "fixed",
      "sys created by": "admin",
      "sys domain path": "/",
      "sys class name": "cmdb ci file system",
      "computer": "d83dac0adb4dab00dc44f00fbf961919",
      "x_sclo_scilogic_monitored": "true",
      "x_sclo_scilogic_region": "ScienceLogic",
      "sys_updated_by": "admin",
      "sys_created_on": "2018-11-12 21:59:06",
      "sys_domain": "global",
      "install status": "1",
      "name": "/root",
      "subcategory": "File Share",
      "sys_id": "afd30ba0dbf5a380dc44f00fbf961951",
      "file system": "ntfs",
      "sys class path": "/!!/!K/!!",
      "mount point": "/root",
      "sys_mod_count": "3",
      "x sclo scilogic id": "31",
     "label": "/root",
      "cost cc": "USD",
      "category": "Resource"
   }
 ],
 "sysparm offset": 0,
 "sysparm limit": 100,
 "return count": 1,
  "total count": 1
}
```

# Import Set

# HTTP Method

POST

### **Resource** Path

/api/x\_sclo\_scilogic/v1/sciencelogic/import\_set

# Default Resource Path

```
/api/x_sclo_scilogic/sciencelogic/import_set
```

This operation handles the custom intake of import sets before it reaches the transform map staging table, such as x\_sclo\_scilogic\_import\_installed\_software. This operations is currently only used for importing installed software (x\_sclo\_scilogic\_import\_installed\_software).

Headers	
Кеу	Value
Accept	application/json
Content-Type	application/json

Parameters		
Кеу	Value	
record_type (required)	x_sclo_scilogic_import_installed_software	

# Example (Request URL)

https://<your Instance>.service-now.com/api/x\_sclo\_scilogic/v1/sciencelogic/import\_set

# Example (Body)

```
"c411a81edb1df300dc44f00fbf96195d",
    "7701a81edb1df300dc44f00fbf961922",
    "7b01681edb1df300dc44f00fbf9619e7",
    "fb01a81edb1df300dc44f00fbf961927"
    ],
    "active": true
    }
  ]
}
```

# Incidents

# HTTP Method

GET

# Pagination

Enabled

### **Resource** Path

/api/x\_sclo\_scilogic/v1/sciencelogic/incidents

# Default Resource Path

/api/x\_sclo\_scilogic/sciencelogic/incidents

This operation pulls all records from the incident table that are created by a specific **user\_id** and its related events. The results are ordered by the **sys\_id** of the incident, so the results display in the same order every time. This operation is also based on the incident being in an active state. This operation returns a pre-set of data and does not return everything on the Incident and Event (x\_sclo\_scilogic\_event) tables.

Headers		
Кеу	Value	
Content-Type	application/json	
Accept	application/json	

Parameters		
Кеу	Value	
user_id (required)	is4user]	
sysparm_offset	0	
sysparm_limit	glide.json.export.limit, glide.ui.export.limit, glide.ui.export.war.threshold	

HTTP Sto	atus
Code	Value

200	ОК
400	Query Parameter \'user_id\' is not defined and is required.

'sys\_created\_by=' + user\_id + 'active=true'

### Example

```
https://<your Instance>.service-now.com/api/x_sclo_
scilogic/v1/sciencelogic/incidents?user_id=is4user1&sysparm_offset=0&sysparm_limit=100
```

```
{
  "results": [
    {
      "sys id": "0141807bdbb16300dc44f00fbf9619fc",
      "number": "INC0010135",
      "state": "2",
      "state_label": "In Progress",
      "events": [
        {
          "event id": "16908",
          "device": {
            "sys_id": {
            }
          }
        },
        {
          "event id": "16874",
          "device": {
            "sys id": {
            }
          }
        },
        {
          "event id": "16865",
          "device": {
            "sys id": {
            }
          }
        }
      ]
   }
 ],
  "sysparm_offset": 0,
  "sysparm_limit": 1,
  "return_count": 1,
```

```
"total_count": 44
}
```

# Installed Software

### HTTP Method

GET

# Pagination

Enabled

#### **Resource** Path

/api/x\_sclo\_scilogic/v1/sciencelogic/installed\_software

# Default Resource Path

/api/x\_sclo\_scilogic/sciencelogic/installed\_software

This operation pulls all the fields from the software (cmdb\_ci\_spkg) table. The return is ordered by **sys\_id**, so the results display in the same order every time. The results are filtered by the **SL1 monitored** field on the ServiceNow side. This operation requires the **region** to filter the installed software on devices.

Headers		
Кеу	Value	
Content-Type	application/json	
Accept	application/json	

Parameters		
Кеу	Value	
region	ScienceLogic	
sysparm_offset	0	
sysparm_limit	glide.json.export.limit, glide.ui.export.limit, glide.ui.export.war.threshold	

HTTP Status	
Code	Value
200	ОК

400 G	Query parameter \'region\' is not defined and are required.
-------	--

'x sclo scilogic monitored=true'

#### Example (Request URL)

```
https://<your Instance>.service-now.com/api/x sclo scilogic/v1/sciencelogic/installed
software?sysparm offset=0&sysparm limit=100&region=ScienceLogic
Example (Response) {
"results": [
{
"operational status": "1",
"operational_status_label": "Operational",
"sys_updated_on": "2019-05-01 06:00:09",
"install count": "2",
"sys updated by": "system",
"sys_created_on": "2019-03-29 19:42:58",
"sys domain": "global",
"sys created by": "admin",
"sys domain path": "/",
"install_status": "1",
"install status label": "Installed",
"name": "Test 31",
"subcategory": "Package",
"sys class name": "cmdb ci spkg",
"sys class name label": "Software",
"sys id": "le9608fcdb2cb740dc44f00fbf961949",
"sys class path": "/!!/#$",
"key": "Test 31 ::: NULL",
"license available": "-2",
"sys mod count": "1",
"x_sclo_scilogic_id": "31",
"model id": "2c146728dbe8b740dc44f00fbf9619c6",
"model id label": "Unknown",
"cost cc": "USD",
"cost_cc_label": "USD",
"x sclo scilogic monitored": "true",
"package name": "Test 31",
"category": "Software",
"x sclo scilogic region": "AutoGenerateClass",
"installed on": [
{
"sys id": "5a271407dbfe6300dc44f00fbf96190f",
"id": "10",
"region": "ScienceLogic",
"monitored": "true"
},
{
"sys id": "5a271407dbfe6300dc44f00fbf96190f",
```

```
"id": "10",
"region": "ScienceLogic",
"monitored": "true"
}
]
}
],
"sysparm_offset": 0,
"sysparm_limit": 100,
"return_count": 4,
"total_count": 4
}
```

# Manufacturer

# HTTP Method

POST

### Pagination

Enabled

### **Resource** Path

/api/x\_sclo\_scilogic/v1/sciencelogic/manufacture

# Default Resource Path

/api/x\_sclo\_scilogic/sciencelogic/manufactures

This operation does not populate any data into ServiceNow. Instead, this operation takes an array of manufacturer names and attempts to line them up with manufacturers already in ServiceNow. Then the operation returns the sys\_ id of manufacturers it was able find based on matching name. If the Normalization Data Services Client is active on the target instance, this operation uses those tables to find a matching company record; otherwise the operation will match on whether name and manufacturer is true on the core\_company table.

Headers	
Кеу	Value
Content-Type	application/json
Accept	application/json

Parameters	
Кеу	Value
region (required)	ScienceLogic

# Example (Request URL)

https://<your Instance>.service-now.com/api/x\_sclo\_scilogic/v1/sciencelogic/ manufacture

# Example (Body)

```
{
  "manufactures": [
  "Cisco Systems Inc",
```

```
"Cisco Systems, Incorporated",
"CiscoSystems",
"American Power Conversion Inc.",
"APC Corp",
"Apc",
"IBM",
"IBM CORP",
"International Business Machines",
"Juniper Systems",
"Juniper Networks,Inc",
"Juniper Solutions"
]
```

}

```
{
"result": {
"Cisco Systems Inc": "",
"Cisco Systems, Incorporated": "",
"CiscoSystems": "",
"American Power Conversion Inc.": "",
"APC Corp": "",
"Apc": "",
"IBM": "",
"IBM CORP": "",
"International Business Machines": "",
"Juniper Systems": "",
"Juniper Networks, Inc": "",
"Juniper Solutions": ""
}
}
```

# Model

# HTTP Method

POST

# **Resource** Path

/api/x\_sclo\_scilogic/v1/sciencelogic/model

# Default Resource Path

/api/x\_sclo\_scilogic/sciencelogic/models

This operation does not populate any data into ServiceNow. Instead, this operation takes an array of model names and attempts to line them up with models already in ServiceNow and returns the sys\_id of models it was able to find based on matching name.

Headers	
Кеу	Value
Content-Type	application/json
Accept	application/json

Parameters	
Кеу	Value
region (required)	ScienceLogic

# Example (Request URL)

https://<your Instance>.service-now.com/api/x\_sclo\_scilogic/v1/sciencelogic/models

# Example (Body)

```
{
   "models": [
   "4331 ISR",
   "7206VXR",
   "7609S",
   "AS5300",
   "ASR5000",
   "Catalyst 3560G-24TS",
   "Catalyst 4948",
   "Catalyst 6509-CatOS",
   "BIG-IP Viprion B4300",
```

```
"F5 BIG-IP DNS",
"BIG-IP Wide IP Container",
"BIG-IP Data Center Container"
]
}
```

```
{
"result": {
"4331 ISR": "",
"7206VXR": "",
"7609S": "",
"AS5300": "",
"ASR5000": "",
"Catalyst 3560G-24TS": "",
"Catalyst 4948": "",
"Catalyst 6509-CatOS": "",
"BIG-IP Viprion B4300": "",
"F5 BIG-IP DNS": "",
"BIG-IP Wide IP Container": "",
"BIG-IP Data Center Container": ""
}
}
```

# Network Adapters

# HTTP Method

GET

### Pagination

Enabled

### **Resource** Path

/api/x\_sclo\_scilogic/v1/sciencelogic/network\_adapters

# Default Resource Path

/api/x\_sclo\_scilogic/sciencelogic/network\_adapters

This operation pulls all the fields from the network adapter table. The return is ordered by **sys\_id**, so the results display in the same order every time. The results are filtered by the **SL1 monitored** and **SL1 ID** field on the ServiceNow side. This operation requires the region to be supplied by the requester, and it only returns region-supplied configuration items.

Headers	
Кеу	Value
Content-Type	application/json
Accept	application/json

Parameters	
Кеу	Value
region (required)	ScienceLogic
sysparm_offset	0
sysparm_limit	glide.json.export.limit, glide.ui.export.limit, glide.ui.export.war.threshold

HTTP Status	
Code	Value

200	OK
400	Query Parameter \'region\' is not defined and is required.

`x\_sclo\_scilogic\_monitored=true^x\_sclo\_scilogic\_idISNOTEMPTY^x\_sclo\_scilogic\_region='
+ region

#### Example (Request URL)

```
https://<your Instance>.service-now.com/api/x_sclo_scilogic/v1/sciencelogic/network_
adapters?region=ScienceLogic&sysparm_offset=0&sysparm_limit=100
```

```
{
  "results": [
   {
      "operational_status": "1",
      "sys updated on": "2018-11-12 21:29:23",
      "sys_updated_by": "admin",
      "sys_created_on": "2018-11-12 21:27:48",
      "sys domain": "global",
      "sys created by": "admin",
      "cmdb ci": "d83dac0adb4dab00dc44f00fbf961919",
      "sys_domain_path": "/",
      "install status": "1",
      "name": "eth0",
      "subcategory": "Network",
      "sys_class_name": "cmdb_ci_network_adapter",
      "sys id": "33ac36acdbb5a380dc44f00fbf961963",
      "netmask": "255.255.255.0",
      "sys_class_path": "/!!/!8",
      "mac_address": "BF:D4:D6:6E:56:F1",
      "sys mod count": "3",
      "x sclo scilogic id": "20",
      "ip_address": "10.10.10.4",
      "cost cc": "USD",
      "x sclo scilogic monitored": "true",
      "category": "Hardware",
      "x sclo scilogic region": "ScienceLogic"
   }
 ],
  "sysparm offset": 0,
 "sysparm limit": 1,
 "return count": 1,
  "total count": 5
}
```

# Service Requests

# HTTP Method

GET

### Pagination

Enabled

### **Resource** Path

/api/x\_sclo\_scilogic/v1/sciencelogic/service\_request

# Default Resource Path

/api/x\_sclo\_scilogic/sciencelogic/service\_request

This operation pulls all service requests that are tied to specific catalog item. Based on the request type it returns a formatted JSON object. It pulls all the required information for an SL1 Discovery session and creating a virtual device in SL1. Both requests require different information and are formatted accordingly.

The basic catalog item Device Discovery is set up as information collection to support the process within SL1. The Service Catalog has been simplified to its most basic form. The workflow moves the request into the correct state to be picked up by the GET request and then waits for its return before completing the workflow.

Headers	
Кеу	Value
Content-Type	application/json
Accept	application/json

Parameters	
Кеу	Value
region (required)	ScienceLogic
state	2
sysparm_offset	0
sysparm_limit	glide.json.export.limit, glide.ui.export.limit, glide.ui.export.war.threshold

HTTP Status	
Code	Value
200	OK
400	Query Parameter \'region\' is not defined and is required.

#### State:

```
`request_item.active=true^request_item.cat_item=' + catalog + `^sc_item_option.item_
option_new.name=Region^sc_item_option.value=' + region
```

#### Non-State:

```
`request_item.active=true^request_item.cat_item=' + catalog + `^sc_item_option.item_
option_new.name=Region^sc_item_option.value=' + region + `^request_item.state=' +
state
```

### Example

```
https://<your Instance>.service-now.com/api/x_sclo_scilogic/v1/sciencelogic/ service_
request?region=Cisco
```

```
{
 "results": [
   {
     "number": "RITM0010018",
     "sysid": "00365de2db1a2340dc44f00fbf961941",
     "state": "2",
     "request type": "Discover Device",
     "region": "Cisco",
     "log all": "false",
     "ip_hostname_list": "167.132.14.15",
      "credentials": [
       {
          "Category": "Linux",
          "ID": "1"
        }
     ],
      "discover_non_snmp": "false",
      "model devices": "true",
     "dhcp": "false",
      "device model cache ttl h": "2",
      "collection_server": "1",
      "organization": "1",
      "add devices to device groups": [
       "test"
     ],
     "device_template": "1",
      "initial scan level": "System Default (Recommended)",
```

```
"scan throttle": "System Default (Recommended)",
  "scan_ports": "21,22,23,25,80",
  "port_scan_all": "System Default (Recommended)",
  "port scan timeout": "System Default (Recommended)",
  "interface_inventory_timeout": "600000",
  "maximum_allowed_interfaces": "10000",
  "bypass interface_inventory": "false"
},
{
  "number": "RITM0010016",
  "sysid": "194447e8db162f00dc44f00fbf96195b",
  "state": "2",
  "request_type": "Discover Device",
  "region": "Cisco",
  "log all": "false",
  "ip hostname list": "192.168.1.1",
  "credentials": [
    {
      "Category": "Linux",
      "ID": "1"
    }
  ],
  "discover non snmp": "false",
  "model devices": "false",
  "dhcp": "false",
  "device_model_cache_ttl_h": "2",
  "collection server": "1",
  "organization": "1",
  "add devices to device groups": [
  ],
  "device template": "1",
  "initial scan level": "System Default (Recommended)",
  "scan throttle": "System Default (Recommended)",
  "scan ports": "21,22,23,25,80",
  "port_scan_all": "System Default (Recommended)",
  "port scan timeout": "System Default (Recommended)",
  "interface inventory timeout": "600000",
  "maximum allowed interfaces": "10000",
  "bypass_interface_inventory": "false"
},
{
  "number": "RITM0010014",
  "sysid": "250dae2cdbd22f00dc44f00fbf961954",
  "state": "2",
  "request type": "create virtual device",
  "region": "Cisco",
  "collection_server": "1",
  "virtual device class": "1"
}
```

] }

#### © 2003 - 2020, ScienceLogic, Inc.

#### All rights reserved.

#### LIMITATION OF LIABILITY AND GENERAL DISCLAIMER

ALL INFORMATION AVAILABLE IN THIS GUIDE IS PROVIDED "AS IS," WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESS OR IMPLIED. SCIENCELOGIC <sup>™</sup> AND ITS SUPPLIERS DISCLAIM ALL WARRANTIES, EXPRESS OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE OR NON-INFRINGEMENT.

Although ScienceLogic<sup>™</sup> has attempted to provide accurate information on this Site, information on this Site may contain inadvertent technical inaccuracies or typographical errors, and ScienceLogic<sup>™</sup> assumes no responsibility for the accuracy of the information. Information may be changed or updated without notice. ScienceLogic<sup>™</sup> may also make improvements and / or changes in the products or services described in this Site at any time without notice.

#### Copyrights and Trademarks

ScienceLogic, the ScienceLogic logo, and EM7 are trademarks of ScienceLogic, Inc. in the United States, other countries, or both.

Below is a list of trademarks and service marks that should be credited to ScienceLogic, Inc. The ® and ™ symbols reflect the trademark registration status in the U.S. Patent and Trademark Office and may not be appropriate for materials to be distributed outside the United States.

- ScienceLogic<sup>™</sup>
- EM7<sup>™</sup> and em7<sup>™</sup>
- Simplify IT™
- Dynamic Application™
- Relational Infrastructure Management<sup>™</sup>

The absence of a product or service name, slogan or logo from this list does not constitute a waiver of ScienceLogic's trademark or other intellectual property rights concerning that name, slogan, or logo.

Please note that laws concerning use of trademarks or product names vary by country. Always consult a local attorney for additional guidance.

#### Other

If any provision of this agreement shall be unlawful, void, or for any reason unenforceable, then that provision shall be deemed severable from this agreement and shall not affect the validity and enforceability of any remaining provisions. This is the entire agreement between the parties relating to the matters contained herein.

In the U.S. and other jurisdictions, trademark owners have a duty to police the use of their marks. Therefore, if you become aware of any improper use of ScienceLogic Trademarks, including infringement or counterfeiting by third parties, report them to Science Logic's legal department immediately. Report as much detail as possible about the misuse, including the name of the party, contact information, and copies or photographs of the potential misuse to: legal@sciencelogic.com



800-SCI-LOGIC (1-800-724-5644)

International: +1-703-354-1010