Monitoring Business Services

SL1 version 12.2.0

Table of Contents

Chapter

1

Introduction to Business Services

Overview

This manual describes how to use SL1 to create and manage business services for your company. Business services let you gauge the availability, health, and risk of your services and the devices that provide those services.

NOTE: Business services are available as part of an SL1 Standard solution. To upgrade, contact ScienceLogic Customer Support. For more information, see https://sciencelogic.com/pricing.

NOTE: Business services and IT services created in the classic SL1 user interface are *not* included in the new business services, and "classic" business services and IT services are not related in any way to the new business services, IT services, and device services. For more information about the classic versions, see the ***Service Provider Utilities (formerly Business Services)*** and ***IT Services (Classic)*** manuals.

To view a case study of using business services to diagnose and resolve service-impacting issues, watch the video at https://sciencelogic.com/product/resources/diagnose-resolve-service-impacting-issues.

Use the following menu options to navigate the SL1 user interface:

- To view a pop-out list of menu options, click the menu icon (☰).
- To view a page containing all of the menu options, click the Advanced menu icon (⋯).

This chapter covers the following topics:

What is a Business Service?

A ***business service*** includes one or more technical services that provide value to internal or external customers. Some examples of business services include verifying Internet access or website hosting, online banking, remote backups, and remote storage. Usually a business service includes an associated Service Level Agreement (SLA) that specifies the terms of the service.

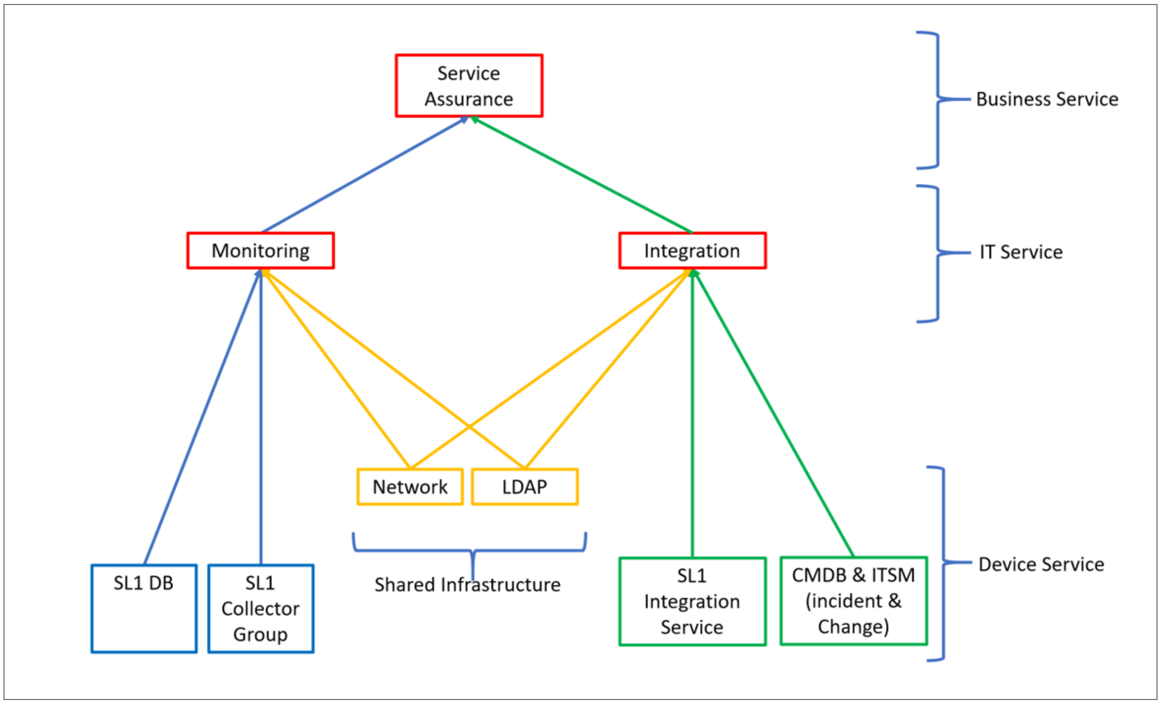
There are two methods by which you can create business services in SL1:

Option 1:

You can create the following types of services on the **Business Services** page, in the following order:

1. ***Device Service***. Monitors a set of related IT infrastructure components (devices) that deliver a discrete function, such as a DNS or Collector Group, or all devices in a specific region.
2. ***IT Service***. Monitors a service that IT provides to your organization. An IT Service provides a way to define how a set of related Device Services work together to power a given IT service, such as a DNS plus Collector Group plus a database.
3. ***Business Service***. Monitors a service your organization provides to your customers. A business service consists of one or more IT services.

The following figure shows an example of how your business services may be organized.



Option 2:

Alternatively, if you require more flexibility in modeling your business service, you can create a custom ***Service Model*** based upon how your organization defines its structure.

This option, which is also called an "N-tier" service model, uses a wizard to walk you through the process of building custom service models with multiple nested or connected service levels, each of which you can label to match the terminology used in your business. This enables you to create service hierarchies with a custom number of tiers that accurately reflect your service structures within your organization, rather than being confined to the three-tier business service/IT service/device service model.

NOTE: SL1 PowerFlow users can use custom service models and the applications in the *ServiceNow Configuration Management Database (CMDB)* SyncPack to sync business services between SL1 and ServiceNow.

Using this method, you can create, update, or delete services in ServiceNow and it will be reflected in SL1, or vice versa.

However, services that you want to sync between the two systems must either be built entirely in ServiceNow or entirely in SL1; you cannot merge services between the two.

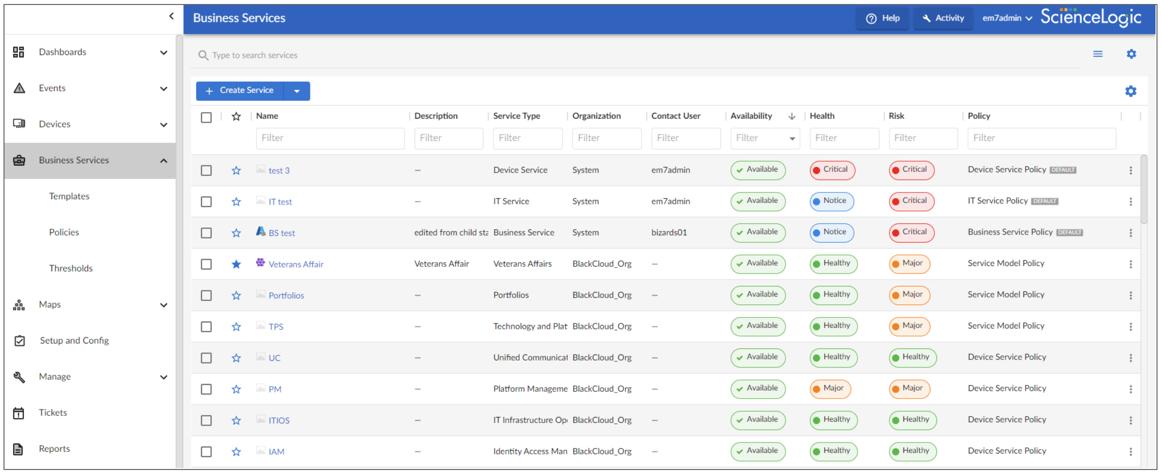
ScienceLogic recommends syncing services from ServiceNow into SL1 rather than building custom service models in SL1 and syncing them into ServiceNow.

For more information, see the section on "Syncing Business Services" in the ***ServiceNow CMDB SyncPack*** manual.

The Business Services Page

The **Business Services** page displays a list of the business, IT, and device services that you have access to, as well as some basic info and the health, availability, and risk metrics for each service.

To navigate to the **Business Services** page, click the **Business Services** icon (💼):



Name	Description	Service Type	Organization	Contact User	Availability	Health	Risk	Policy
test 3	–	Device Service	System	em7admin	✓ Available	● Critical	● Critical	Device Service Policy DEFAULT
IT test	–	IT Service	System	em7admin	✓ Available	● Notice	● Critical	IT Service Policy DEFAULT
BS test	edited from child sta	Business Service	System	bizards01	✓ Available	● Notice	● Critical	Business Service Policy DEFAULT
Veterans Affair	Veterans Affair	Veterans Affairs	BlackCloud_Org	–	✓ Available	● Healthy	● Major	Service Model Policy
Portfolios	–	Portfolios	BlackCloud_Org	–	✓ Available	● Healthy	● Major	Service Model Policy
TPS	–	Technology and Plat	BlackCloud_Org	–	✓ Available	● Healthy	● Major	Service Model Policy
UC	–	Unified Communicat	BlackCloud_Org	–	✓ Available	● Healthy	● Healthy	Device Service Policy
PM	–	Platform Manageme	BlackCloud_Org	–	✓ Available	● Major	● Major	Device Service Policy
ITIOS	–	IT Infrastructure Op	BlackCloud_Org	–	✓ Available	● Healthy	● Healthy	Device Service Policy
IAM	–	Identity Access Man	BlackCloud_Org	–	✓ Available	● Healthy	● Healthy	Device Service Policy

These business services let you gauge the health, availability, and risk of your services or the devices that provide those services. On the **Business Services** page, these values display in the following format and order:

1. ***Availability***: The availability of a Device Service is derived from the availability rules. This may or may not be linked to device availability. A service or device is considered unavailable if SL1 is not able to collect data from the device or service, or if a device is usable or not usable. A value of *0* means a device or service is unavailable, and a value of *1* means a device is available. Availability uses the following icons:

✓ Available	⊘ Unavailable
1	0

2. ***Health***: Indicates the current status of a Device Service—for example, the rate of processing or throughput for the devices in the Device Service. In the case of SL1 CDB devices, the Rows Behind presentation objects can provide a good measure of how effectively the CDB is processing Collector data. Health is represented by a color-coded "severity" icon that corresponds to a numerical value between 0 and 100. For example, the Health value could indicate when a device is intermittently unavailable because of a power problem, thereby falling below the required level of performance. Health uses the following icons by default:

● Critical	● Major	● Minor	● Notice	● Healthy
0 - 20	21 - 40	41 - 60	61 - 80	81 - 100

3. ***Risk***: Displays a percentage value between 0 and 100 that indicates how close a service is to being in an undesirable state. Use risk for data that is known to cause issues if left unchecked, such as critical events, swap usage, or low database logging space. The safest possible risk value is 0%, while the worst risk value is 100%.

These values are computed in this order because SL1 uses *Availability* values to compute *Health*, and then uses both *Availability* and *Health* values to compute *Risk*.

You can define metrics for *device services* based on:

- availability
- latency
- event count
- event severity
- device state
- Dynamic Application performance data collected by SL1
- collection label metrics (for example, CPU, Memory, or Swap)

NOTE: IT services created in the classic user interface are *not* included in the new user interface, and "classic" IT services are not related in any way to the new business services, IT services, and device services.

The **Business Services** page displays the following about each service:

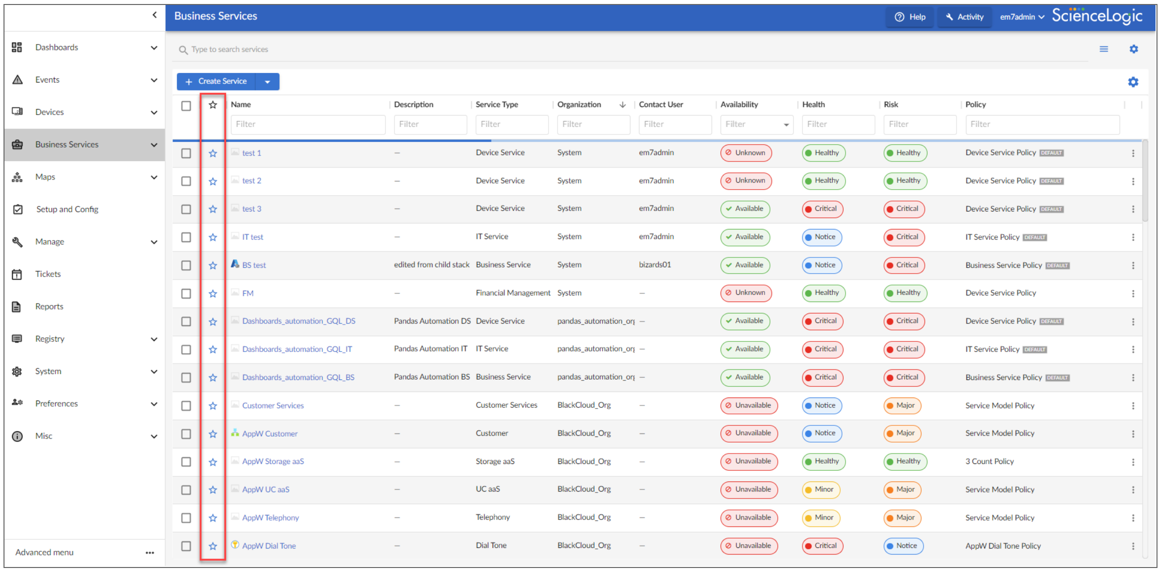
- ***Name***. The name of the service.
- ***Description***. A description of the service.
- ***Service Type***. Indicates the service type. Values include *Business Service*, *IT Service*, *Device Service*, or a custom service type.
- ***Organization***. The organization that owns the service.
- ***Contact Organization***. The organization that should by contacted with any questions about the service.
- ***Contact User***. The user who should be contacted with any questions about the service.
- ***Availability***. The service's current availability value.
- ***Health***. The service's current health value.
- ***Risk***. The service's current risk value.
- ***Policy***. The service policy associated with the service.
- ***Date Updated***. The date and time at which the service was last updated.
- ***Last Updated By***. The username of the user who last updated the service.
- ***RCA Options***. Indicates whether Root Cause Analysis is enabled or disabled for the service.

NOTE: To delete one or more services, select the check boxes of the services you want to delete from the **Business Services** page and then click **[Delete Services]**. Alternatively, you can delete a single service by clicking the **Actions** button (···) for that service and then selecting *Delete*.

Favorite a Business Service

In SL1, you can select one or more services so that they always display at the top of the list on the **Business Services** page. This process is called ***favoriting*** services or ***favorite*** service.

For example, on the Business Services page pictured below, click the ***Favorite Service*** star icon (☆) to add or remove the service from your favorites list. Click the icon (★) again to remove the favorite status.



☐	☆	Name	Description	Service Type	Organization	Contact User	Availability	Health	Risk	Policy
Filter		Filter	Filter	Filter	Filter	Filter	Filter	Filter	Filter	Filter
☐	☆	test 1	–	Device Service	System	em7admin	Unknown	Healthy	Healthy	Device Service Policy DEFAULT
☐	☆	test 2	–	Device Service	System	em7admin	Unknown	Healthy	Healthy	Device Service Policy DEFAULT
☐	☆	test 3	–	Device Service	System	em7admin	Available	Critical	Critical	Device Service Policy DEFAULT
☐	☆	IT test	–	IT Service	System	em7admin	Available	Notice	Critical	IT Service Policy DEFAULT
☐	☆	BS test	edited from child stack	Business Service	System	bizards01	Available	Notice	Critical	Business Service Policy DEFAULT
☐	☆	FM	–	Financial Management	System	–	Unknown	Healthy	Healthy	Device Service Policy
☐	☆	Dashboards_automation_GQL_DS	Pandas Automation DS	Device Service	pandas_automation_or	–	Available	Critical	Critical	Device Service Policy DEFAULT
☐	☆	Dashboards_automation_GQL_IT	Pandas Automation IT	IT Service	pandas_automation_or	–	Available	Critical	Critical	IT Service Policy DEFAULT
☐	☆	Dashboards_automation_GQL_BS	Pandas Automation BS	Business Service	pandas_automation_or	–	Available	Critical	Critical	Business Service Policy DEFAULT
☐	☆	Customer Services	–	Customer Services	BlackCloud_Org	–	Unavailable	Notice	Major	Service Model Policy
☐	☆	AppW Customer	–	Customer	BlackCloud_Org	–	Unavailable	Notice	Major	Service Model Policy
☐	☆	AppW Storage aaS	–	Storage aaS	BlackCloud_Org	–	Unavailable	Healthy	Healthy	3 Count Policy
☐	☆	AppW UC aaS	–	UC aaS	BlackCloud_Org	–	Unavailable	Minor	Major	Service Model Policy
☐	☆	AppW Telephony	–	Telephony	BlackCloud_Org	–	Unavailable	Minor	Major	Service Model Policy
☐	☆	AppW Dial Tone	–	Dial Tone	BlackCloud_Org	–	Unavailable	Critical	Notice	AppW Dial Tone Policy

You can then sort your Business Services by their favorite status.

With favorite services, you can:

- View your favorite service at the top of the **Business Services** page by default.
- Include favorites in the multi-sort function.
- Filter services by favorite.

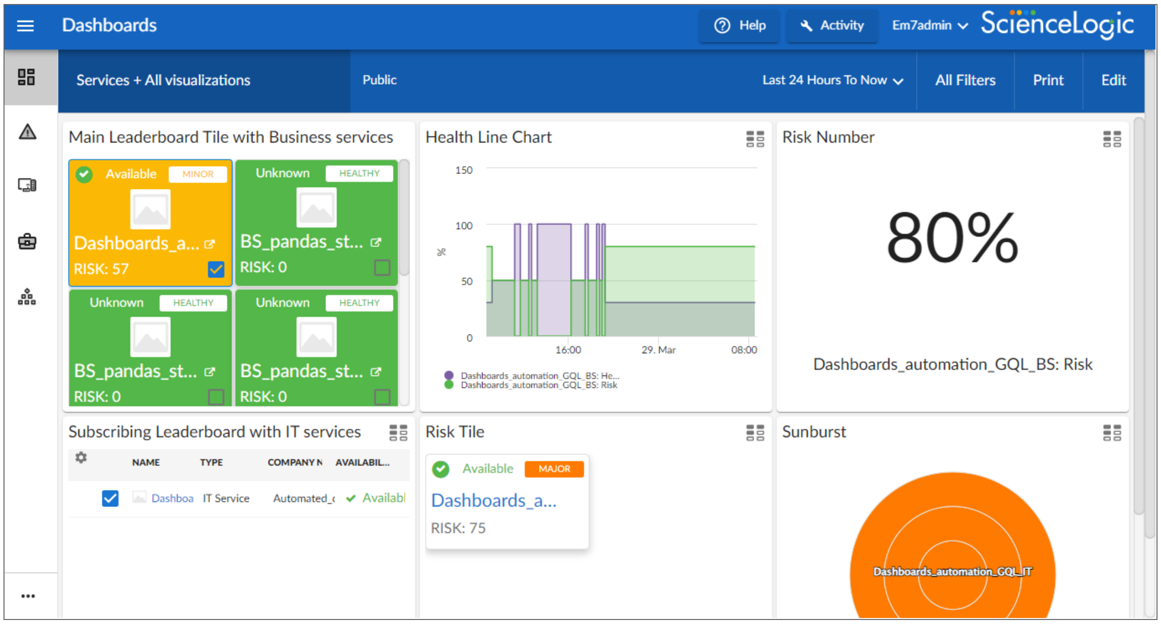
Business Service Dashboards

SL1 includes three default dashboards relating to business services on the **Dashboards** page (▦):

- NOC Overview dashboard
- Business Services dashboard
- Business Service Details dashboard

For more information about these dashboards, see the ***Dashboards*** manual.

In addition to these default dashboards, you can also choose to create your own custom dashboards for business services. For more information, see the ***Dashboards*** manual.



Example: Retail Banking

Using SL1 to monitor a business service lets you quickly see whether the service is available and working as expected for a customer or end user. For example, a banking company wants to ensure that its retail banking service is available around the world. It would use the following workflow to set up its services in SL1:

1. Because the company has offices around the world, it creates multiple ***device services*** that organize devices based on location or region. The company adds all of its devices to the relevant device services.
2. The company then creates multiple ***IT services*** to monitor the device services (from step 1), including separate IT services for online banking, teller systems, and ATM networks.
3. Next, the company creates a ***business service*** for its retail banking business, and this business service includes all of the IT services (from step 2) that deal with retail banking.

NOTE: As needed, the banking company repeats steps 1-3 to create additional business services (made up of IT services and device services) to monitor their commercial banking and investment banking devices and services.

Chapter

2

Creating Services and Service Policies

Overview

This chapter describes how to create and monitor business services, IT services, and devices services, as well as custom service models. This chapter also describes how to create and use policies for each service to assist with monitoring those services.

Use the following menu options to navigate the SL1 user interface:

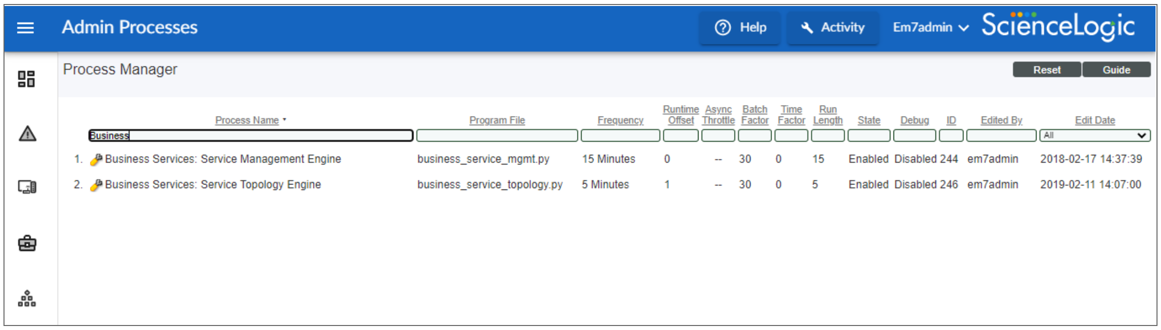
- To view a pop-out list of menu options, click the menu icon (☰).
- To view a page containing all of the menu options, click the Advanced menu icon (⋯).

This chapter covers the following topics:

Administrative Processes for Business Services

Two administrative processes (System > Settings > Admin Processes) are used to calculate business service values:

- ***Business Services: Service Management Engine***. This process aggregates all of the metric information from your devices and services to create the Health, Availability, and Risk values. This is a long-running process which typically runs every 15 minutes. You should only run it more frequently if you have a robust Collector Database (CDB) with room to support the more frequent collection.
- ***Business Services: Service Topology Engine***. This process calculates the relationships between your services and your devices. By default, this process runs every 5 minutes. If your services and device relationships are relatively static, you can decrease the frequency to every 15 minutes.



	Process Name	Program File	Frequency	Runtime Offset	Async Throttle	Batch Factor	Time Factor	Run Length	State	Debug	ID	Edited By	Edit Date
	Business												All
1.	Business Services: Service Management Engine	business_service_mgmt.py	15 Minutes	0	--	30	0	15	Enabled	Disabled	244	em7admin	2018-02-17 14:37:39
2.	Business Services: Service Topology Engine	business_service_topology.py	5 Minutes	1	--	30	0	5	Enabled	Disabled	246	em7admin	2019-02-11 14:07:00

Understanding Health, Availability, and Risk

> NOTE: None of the metrics described in these examples actually pinpoint the exact cause of the unavailability, degradation in health, or increase in risk, but they do bring it to your attention quickly and with a minimal level of administration. When you use key performance indicators (KPI) for responsiveness or availability, you may find it much easier than trying to model every way a service can break

Understanding Availability

Availability assesses whether something is reachable or is performing at a level to be useful. Here are a few examples to help you understand availability:

- **Website**. The URL for a website must be responsive, that is, it must respond either with the expected page or with an error page indicating that the site is unreachable (up/down). The web site's response also needs to be fast enough that users will not leave the page due to a slow response time. This should be considered when defining availability.

- **Cluster of database servers**. Assume one database server can process 1,000 transactions per second with good response times. To maintain those response times with 3,000 transactions per second, four equivalently configured database servers are put into a cluster. This method allows for any one database server to be down without losing acceptable throughput and responsiveness. If three servers in the database cluster become unavailable, the one remaining database server will not be able to maintain throughput or responsiveness, so the cluster is effectively unavailable.
- **Processes**. Consider that Process A passes work to Process B by way of a queue. If the queue depth sits at zero, it indicates that Process A is not passing any new work and is considered to be unavailable. If the queue grows to a specified threshold, it indicates that Process B is not pulling work from the queue and is considered to be unavailable.

Understanding Health

A decline in health for a given service or device means that one or more key performance indicators (KPI) are degrading. Left unchecked, this can be expected to degrade throughput or responsiveness. Here are a few examples of issues that impact health:

- **Database Server**. On an SL1 Database Server, a key database function is to retrieve and store events and Dynamic Applications data. You can create Device Service policies that degrade health as the volumne of high frequency (HF) rows climbs, as this indicates the CDB is becoming overloaded or slow to process incoming data. This could lead to delays in events from Collectors being presented to automation actions or the Events page, and can impact overall system performance.
- **Windows server**. In some cases, the CPU Queue depth on a Windows server starts to increase, indicating the CPU has insufficient bandwidth to process its workload. When this happens, all processes or applications running on the Windows server will run slowly, impacting either responsiveness or throughput. You can build a policy that lets you know if this is happening on any Windows servers.
- **Website**. A website that is the face of an application has increasing web URL response times, indicating stress in the delivery of the URL. If it is known that the URL becomes functionally unavailable at 5 seconds, meaning that your customer may give up and goes to another vendor, then setting health to degrade for 1 to 4 seconds will give notice that the service health is degrading and investigations and resolution can be performed before the URL reaches an unavailable state.

Understanding Risk

In considering risk, think of the consequences of a KPI degrading. If a selected KPI is known to indicate situations that, if left unaddressed, will impact Health or Availability, you will want to create a policy for that. Some examples:

- On an SL1 Database Server, if the InnoDB table runs out of space, MariaDB will stop, which leads the Database Server to become unavailable. A shrinking level of available InnoDB space will not degrade the responsiveness and throughput of MariaDB, and therefore the Database Server, but it can indicate that your Database Server availability is at risk.
- Another way to measure risk for devices in a service is by monitoring the level of severity for events. This provides a reasonable baseline for risk. For example, many critical events for a device either indicates a false positive that should be suppressed or that monitoring has found a condition that is deemed to be unacceptable.

Creating Services

You can create services in SL1 using one of two methods:

- You can create a ***three-tier service***, consisting of a business service, one or more IT services, and one or more device services.
- You can create a ***custom service model*** with a user-defined business hierarchy.

When designing your service structure, a good design principle is to begin with the end in mind. To create a new business service, you should first determine the following:

- *Stakeholders*. Who is the intended audience for the service?
- *Purpose*. What problem are you trying to solve for your stakeholders?
- *Visibility*. Who needs to see which services?
- *Workflow*. How are your stakeholders currently performing fault isolation?
- *Right-sizing*. What is the right number of services? Consider the following:
    - The devices that impact the business service
    - The IT services that impact the business service
    - The specific conditions that you want to monitor, based on your business processes

If you follow the design flow described above, you will have an outline of which model type to create and which specific services you need to build. For example, if you provide email service, then a failure of your primary SMTP server and backup SMTP server would constitute a Critical status.

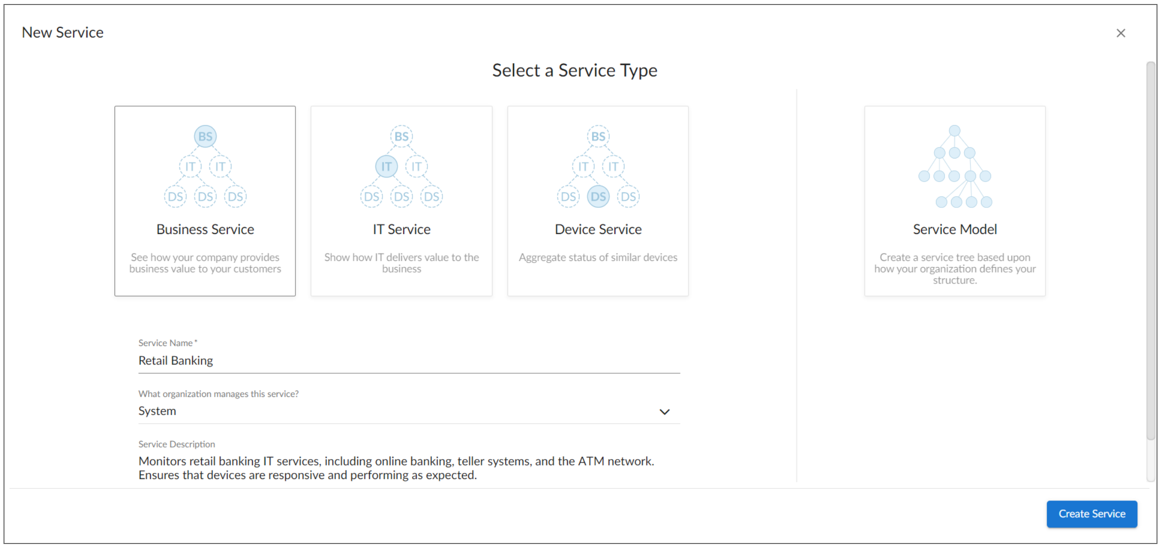
The next consideration is to determine which devices share a common description of health, availability, and risk rules. If two devices need different rules, you will need to create two Device Services.

TIP: You can copy an existing service on the **Business Services** page by clicking the **[Actions]** button (⋯) for that service and selecting *Duplicate*.

Creating Business, IT, or Device Services

To create a Business, IT, or Device Service:

1. On the **Business Services** page, click the **[Create Service]** button. The **New Service** page appears.



New Service

Select a Service Type

Business Service

See how your company provides business value to your customers

IT Service

Show how IT delivers value to the business

Device Service

Aggregate status of similar devices

Service Model

Create a service tree based upon how your organization defines your structure.

Service Name *

Retail Banking

What organization manages this service?

System

Service Description

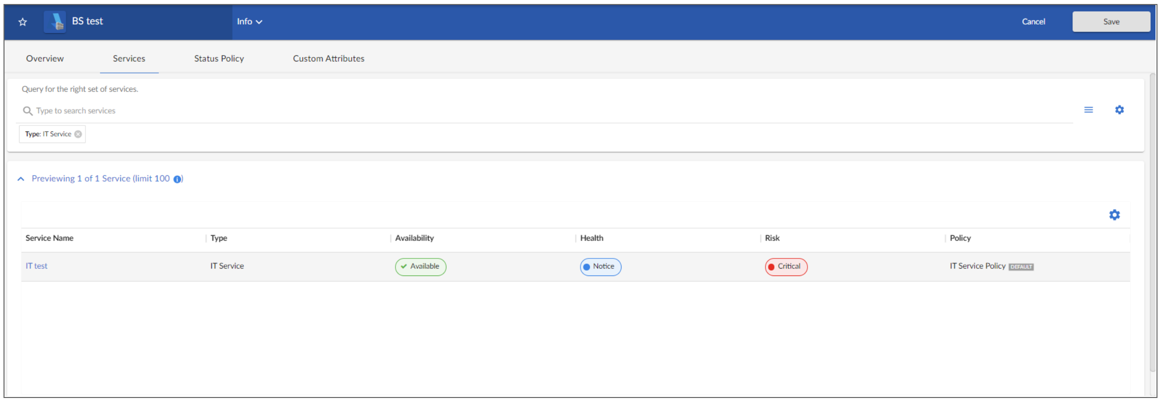
Monitors retail banking IT services, including online banking, teller systems, and the ATM network. Ensures that devices are responsive and performing as expected.

2. Select a service type. You should start by creating your device services, then your IT services, and then finally your business service. Your options include:
    - ***Device Service***. Monitors a set of related devices.
    - ***IT Service***. Monitors a service that IT provides to your organization. An IT service includes one or more device services.
    - ***Business Service***. Monitors a service that your organization provides to your customers. A business service includes one or more IT services.

3. Complete the remaining fields:
    - ***Service Name***. Type a unique name for this service.
    - ***What organization manages this service?***. Select the name of the organization that owns this service.
    - ***Service Description***. (Optional) Type a short description of this service and its purpose. You can use the text in this description to search for this service on the **Business Services** page. For example, if a collection of Device Services all have a description of "Shared Infrastructure", then an IT Service can search to include every Device Service in the same organization that has a description of "Shared Infrastructure". As you add more "Shared Infrastructure" device services, the IT Service will automatically expand to include them. This makes building service trees quick and self-maintaining, without resorting to rigid service names.

4. Click the **[Create Service]** button. If you selected *Device Service* in step 2, the **[Devices]** tab appears, with a list of available devices in the ***Preview*** section. If you selected *Business Service* or *IT Service* in step 2, the **[Services]** tab appears, with a list of available services in the ***Preview*** section.

5. In the ***Search*** field, type search criteria for the services or devices you want to monitor. A list of services or devices that match your search criteria appears in the **Preview** pane.



Query for the right set of services.

Type to search services

Type: IT Service

Previewing 1 of 1 Service (limit 100)

Service Name	Type	Availability	Health	Risk	Policy
IT test	IT Service	✓ Available	● Notice	● Critical	IT Service Policy DEFAULT

TIP: If you are looking for a very specific set of services or devices, click the gear icon (⚙) to the right of the ***Search*** field and select *Advanced*. In this mode you can create an advanced search using "AND" or "OR" for multiple search criteria. You must click **[Search]** before you can view the results of your search. For more information, see the "Performing an Advanced Search" topic in the ***Introduction to SL1*** manual.

TIP: If you want to search for devices that have specific custom attributes, use Advanced Search. Use the following format:

```
attribute has (id == custom attribute and value == value)
```

Note that search cannot process colons (:) in strings. The presence of a colon in service inclusion searches will stop the engine that calculates health, availability, and risk for that service.For more information, see the "Advanced Search" topic in the ***Introduction to SL1*** manual.

NOTE: The "ANY" search option is disabled on the **[Services]** or **[Devices]** tab.

TIP: The **Preview** pane indicates the maximum number of constituent services or devices that will be used for computing health, availability, and risk.

6. When you have the right combination of services or devices, click the **[Save]** button. The default policy for the type of service you selected is automatically added to the new service.
7. If you want to use a different business policy with the new service, see ***Selecting a Business Service Policy***.
8. If you want to create a *new* business policy to use with the new service, see ***Creating a Business Service Policy***.

9. Repeat this process until you have the right combination of device services and IT services in your business service (or business services, if needed).

Creating a Custom Service Model

If you require more flexibility in modeling your service beyond the standard three-tier business service/IT service/device service model, you can instead create a custom ***Service Model***, which is also called an "N-tier" service model.

For example, if you needed to monitor individual conference rooms within your organization from a high level, you could build the following service model to do so:

> Country > Region > State > City > Building > Floor > Conference Room

Custom service models enable you to build service hierarchies with a unique number of tiers that accurately reflect the service structures within your organization, using user-defined labels that can match the terminology used in your business.

NOTE: You cannot convert a three-tier business service model to a custom service model.

NOTE: SL1 PowerFlow users can use custom service models and the applications in the *ServiceNow Configuration Management Database (CMDB) Synchronization* PowerPack to sync business services between SL1 and ServiceNow.

Using this method, you can create, update, or delete services in ServiceNow and it will be reflected in SL1, or vice versa.

However, services that you want to sync between the two systems must either be built entirely in ServiceNow or entirely in SL1; you cannot merge services between the two.

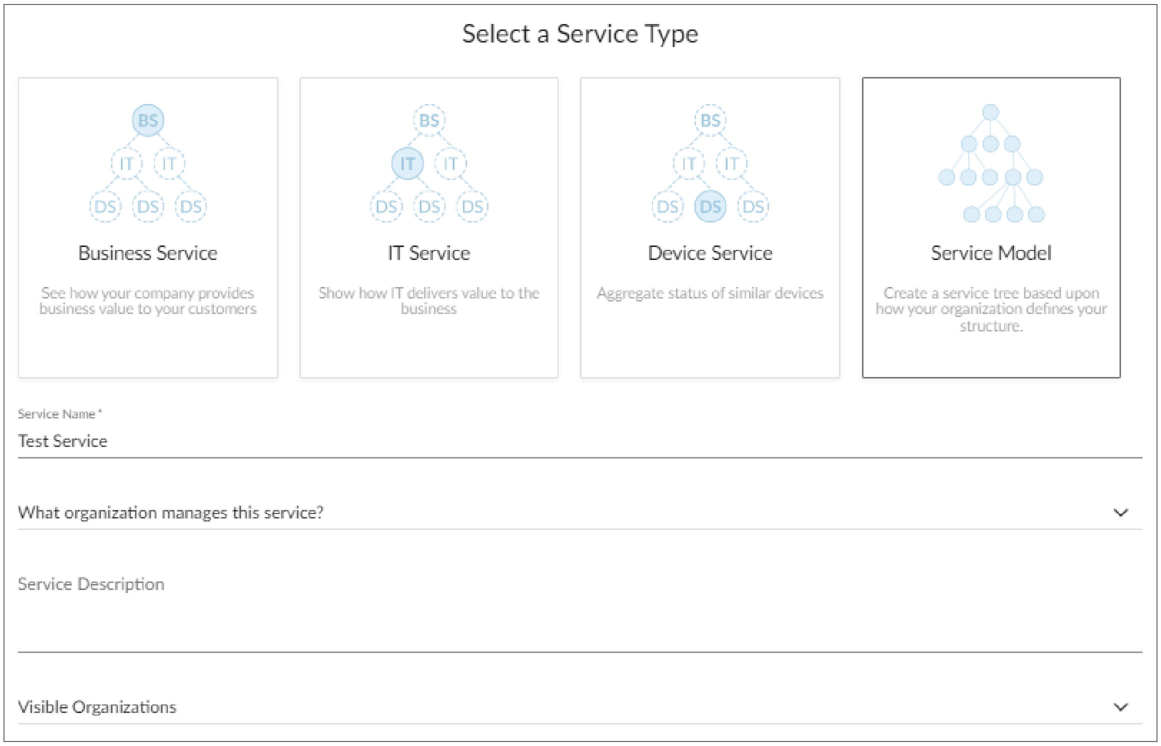
ScienceLogic recommends syncing services from ServiceNow into SL1 rather than building custom service models in SL1 and syncing them into ServiceNow.

For more information, see the section on "Syncing Business Services" in the ***ServiceNow CMDB SyncPack*** manual.

To create a custom service model:

1. On the **Business Services** page, click the **[Create Service]** button. The **New Service** page appears.
2. Select *Service Model*, and then complete the following fields:
    - ***Service Model Name***. Type a unique name for this service model.
    - ***What organization manages this service?***. Select the name of the organization that owns this service model.

- ***Service Description***. (Optional) Type a short description of this service model and its purpose. You can use the text in this description to search for this service on the **Business Services** page. For example, if multiple services all have a description of "Shared Infrastructure", then you could create another service search to include every service in the same organization that has a description of "Shared Infrastructure". As you add more "Shared Infrastructure" services, the other services that include those "Shared Infrastructure" services will automatically expand to include them. This makes building service trees quick and self-maintaining, without resorting to rigid service names.
- ***Visible Organizations***. (Optional) Select one or more organizations from which you can select devices to use in the service model. For example, if you selected *Acme* for this field, then any service that is aligned with Acme can access devices in the Acme organization.



Select a Service Type

Business Service

See how your company provides business value to your customers

IT Service

Show how IT delivers value to the business

Device Service

Aggregate status of similar devices

Service Model

Create a service tree based upon how your organization defines your structure.

Service Name *

Test Service

What organization manages this service?

Service Description

Visible Organizations

> **NOTE:** The ***Visible Organizations*** field allows the selected organizations to view the service and enables these organizations to query the service. For instance, if you want an IT service to have a device service as a child service, the device service will either need to be within the same organization as the IT service, or the device service will need to be included in the visible organizations that are aligned with the IT service.

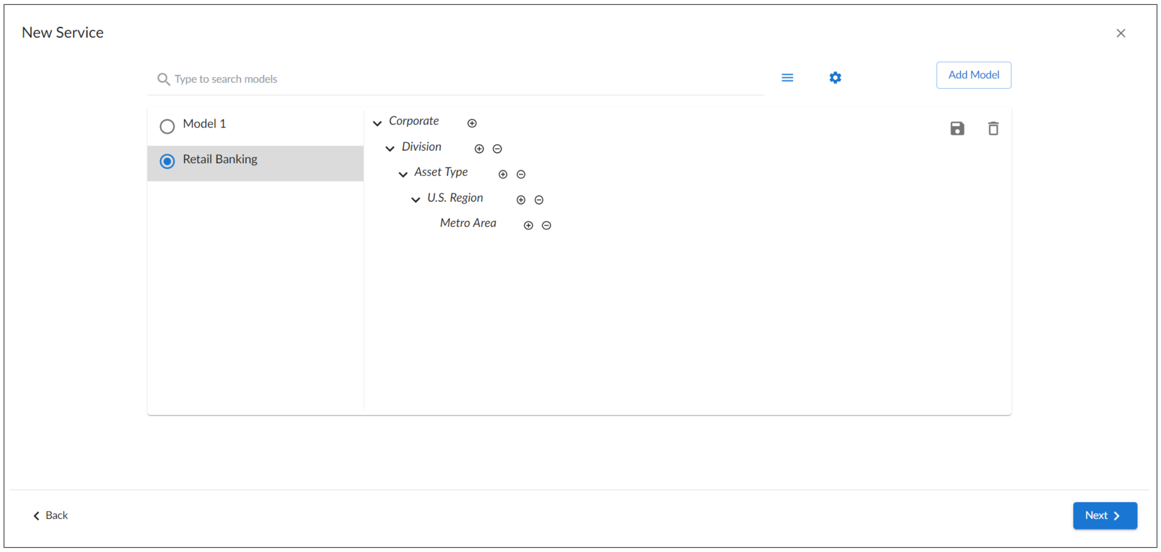
3. **[Next]**. The service creation page of the **New Service** wizard appears:
4. Click **[Next]**. The model selection page of the **New Service** wizard appears.

5. On the model selection page, do one of the following:

   - Click the **[Add Model]** button to design a new service model. If you do this, proceed to step 6.
   - Use the search bar if necessary to search for an existing model to which you want to make customizations or changes. If you do this, skip ahead to step 7.
   - Use the search bar if necessary to search for an existing model to which you *do not* want to make any customizations or changes. Select that model's radio button and then click **[Next]**. If you do this, skip ahead to step 9.

TIP: If you are looking for a very specific set of models, click the gear icon (⚙) to the right of the ***Search*** field and select *Advanced*. In this mode you can create an advanced search using "AND" or "OR" for multiple search criteria. For more information, see the "Performing and Advanced Search" topic in the ***Introduction to SL1*** manual.

6. On the **New Model** modal, type a name for the service model in the ***Model Name*** field and then click **[Create]**. The newly created service model is added to the model selection page.
7. On the model selection page, select the new service model you just created or an existing model to which you want to make customizations or changes, and then customize the model as needed:

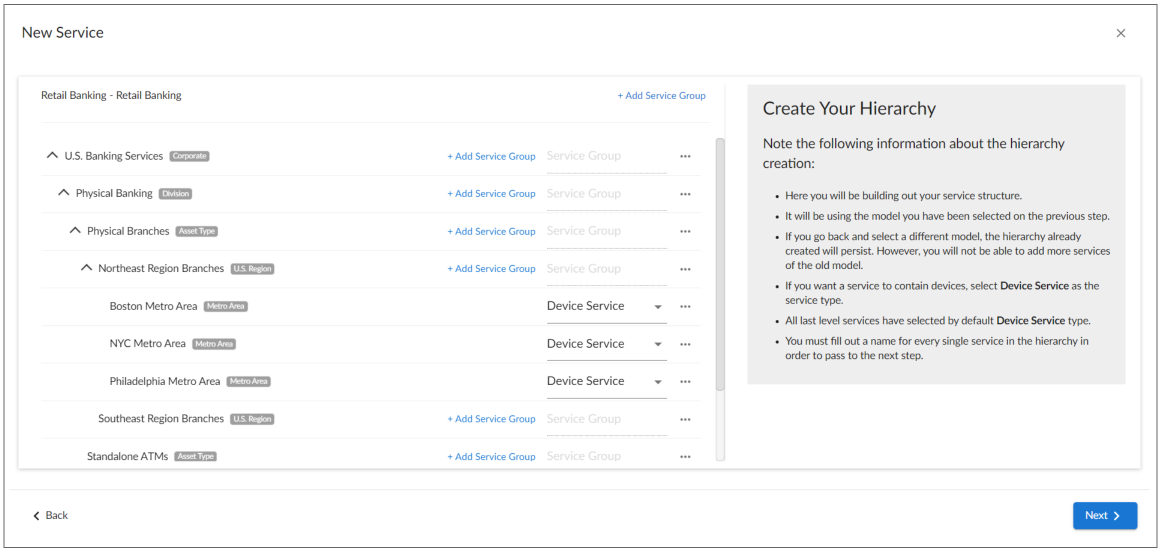


You can customize the service model to fit your business needs in the following ways:

- Click the model name, then type a new model name to replace the existing name.
- Use the plus (⊕) and minus (⊖) icons to build the tiers of your service model. For each tier, click the tier label and then type a new tier label to replace the existing label.
- Click the save icon (💾) to save your custom service model.
- Click the delete icon (🗑) to delete your custom service model.

8. When you are finished customizing the service model, click **[Next]**. The hierarchy creation page of the **New Service** wizard appears.

9. On the hierarchy creation page, use the model you selected to build out the full hierarchy structure of your service:



New Service

Retail Banking - Retail Banking

U.S. Banking Services Corporate — Service Group

Physical Banking Division — Service Group

Physical Branches Asset Type — Service Group

Northeast Region Branches U.S. Region — Service Group

Boston Metro Area Metro Area — Device Service

NYC Metro Area Metro Area — Device Service

Philadelphia Metro Area Metro Area — Device Service

Southeast Region Branches U.S. Region — Service Group

Standalone ATMs Asset Type — Service Group

Create Your Hierarchy

Note the following information about the hierarchy creation:

- Here you will be building out your service structure.
- It will be using the model you have been selected on the previous step.
- If you go back and select a different model, the hierarchy already created will persist. However, you will not be able to add more services of the old model.
- If you want a service to contain devices, select **Device Service** as the service type.
- All last level services have selected by default **Device Service** type.
- You must fill out a name for every single service in the hierarchy in order to pass to the next step.

You can customize the service hierarchy to fit your business needs in the following ways:

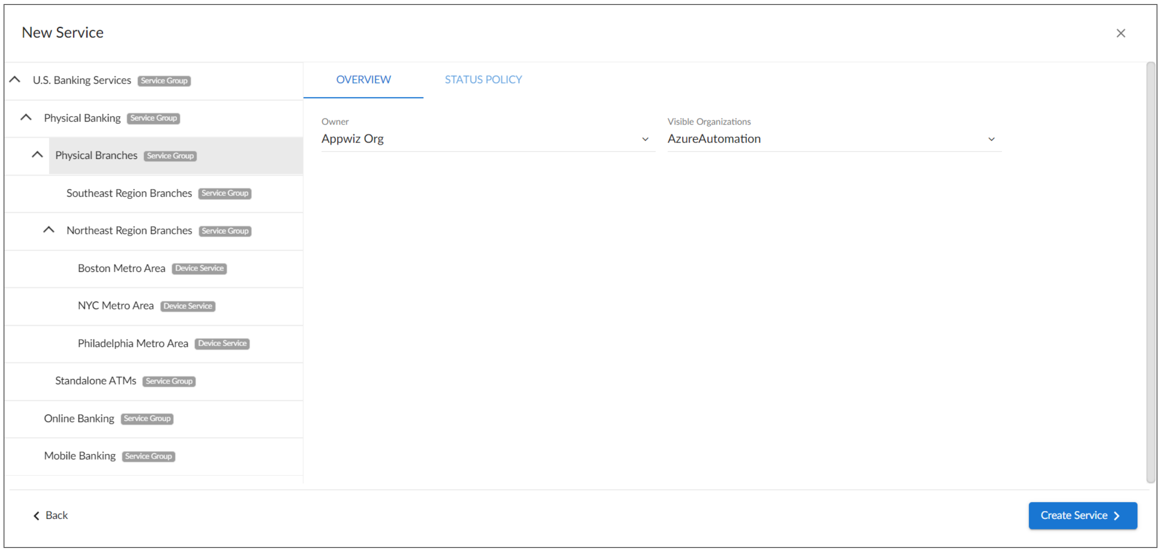
- Click the name of each tier in your service model, then for each tier, type a new label that is specific to the service you want to monitor. For example, your service model might have a tier labeled "U.S. Region"; you might click that tier and type "Northeast" if your service includes assets in the Northeast.

NOTE: You must fill out a name for every service in the hierarchy before you can proceed to step 10.

- Click the expand (⌄) and contract (⌃) icons to expand and contract parts of the service hierarchy tree.
- Click a hierarchy row to drag and drop that row (and any rows that fall below it on the service hierarchy) into a different location in the service hierarchy. If you are able to drop the row in a particular location, the row will turn solid blue. If you are unable to drop the row in a particular location, the row will be white with a red border.
- Click **[+Add Service Group]** at the top of the service hierarchy to add a copy of the entire service model structure to the hierarchy. For example, if your service model includes five tiers and you click **[+Add Service Group]** at the top of the service hierarchy, SL1 will add an additional set of all five tiers to the hierarchy.
- Click **[+Add Service Group]** for a particular row to add to a new set of sub-tier rows in the hierarchy under the existing row. For example, if you have a service model tier labeled "Physical Banking" and the next level of the service model under that is a tier labeled "Branch Locations" and under that are several other tiers, then when you click **[+Add Service Group]** on the "Physical Banking" row, SL1 will add a new "Branch Locations" tier along with all of its sub-tiers under the "Physical Banking" row.

- Click the Actions button (···) for a particular row and then select *Delete* to delete that row from the hierarchy.
- If you want the next-to-last-level service row within the hierarchy to have device services below it, click the Actions button (···) for that row and then select *Add Device Services*. The **Add Device Services** modal appears. On that modal, search for and select any existing device services that you want to add below the selected service row, and then click **[Add Services]**.
- If you want the last-level service row within the hierarchy to contain devices, select *Device Service* from the service type drop-down at the end of the row. If you do not want the row to contain devices, select *Service*. All last-level services are set to *Device Service* by default. All service rows that are not last-level rows have a service type of *Service Group*.

10. When you are finished customizing your service hierarchy, click **[Next]**. The **[Overview]** tab for the new service appears:


New Service
×
U.S. Banking Services Service Group
Physical Banking Service Group
Physical Branches Service Group
Southeast Region Branches Service Group
Northeast Region Branches Service Group
Boston Metro Area Device Service
NYC Metro Area Device Service
Philadelphia Metro Area Device Service
Standalone ATMs Service Group
Online Banking Service Group
Mobile Banking Service Group
OVERVIEW
STATUS POLICY
Back
Create Service

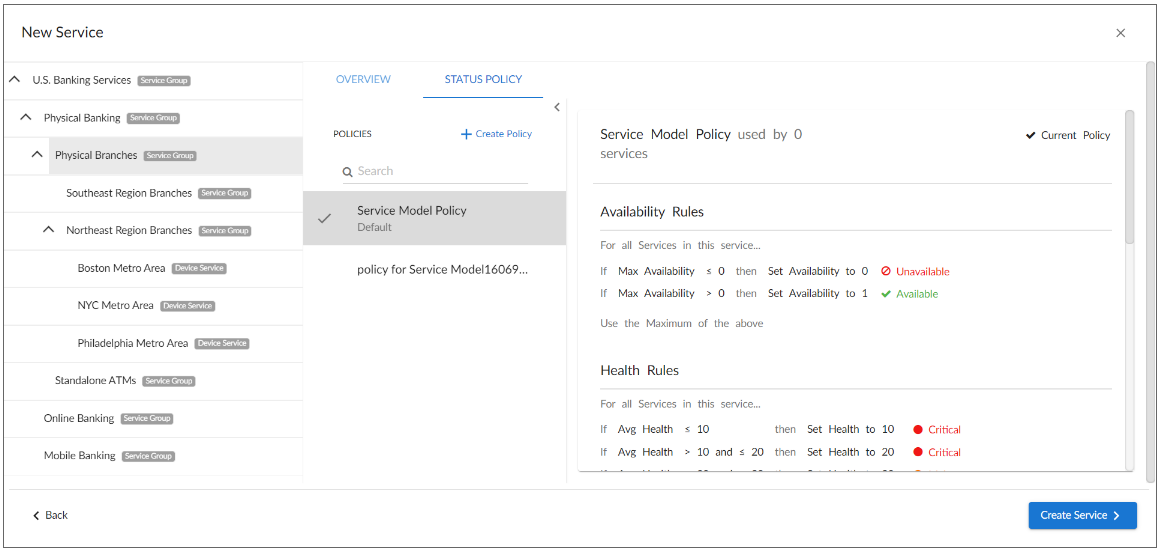
Owner
Appwiz Org

Visible Organizations
AzureAutomation

11. On the **[Overview]** tab, you can update the managing organization and visible organizations for the individual levels within your service model hierarchy if they differ from the managing organization and visible organizations you selected for the entire model in step 3. To do so, click the hierarchy level on the left side of the page, and then complete the following fields:

- ***Owner***. Select the name of the organization that owns the selected service level.
- ***Visible Organizations***. Select one or more organizations from which you can select devices to use in the selected service level.

12. Click the **[Status Policy]** tab:



New Service

×
U.S. Banking Services Service Group
Physical Banking Service Group
Physical Branches Service Group
Southeast Region Branches Service Group
Northeast Region Branches Service Group
Boston Metro Area Device Service
NYC Metro Area Device Service
Philadelphia Metro Area Device Service
Standalone ATMs Service Group
Online Banking Service Group
Mobile Banking Service Group
OVERVIEW
STATUS POLICY
POLICIES
+ Create Policy
Search
Service Model Policy
Default
policy for Service Model16069...
✓ Current Policy
Back
Create Service

Service Model Policy used by 0 services

Availability Rules

For all Services in this service...

If Max Availability ≤ 0 then Set Availability to 0 ⊘ Unavailable

If Max Availability > 0 then Set Availability to 1 ✓ Available

Use the Maximum of the above

Health Rules

For all Services in this service...

If Avg Health ≤ 10 then Set Health to 10 ● Critical

If Avg Health > 10 and ≤ 20 then Set Health to 20 ● Critical

13. On the **[Status Policy]** tab, click on each row within your service hierarchy and then do one of the following for each:

    - To apply an existing policy to the selected service level, search for and select the policy that you want to apply. When you select a policy from the list, the details of that policy appear in the right panel. If a status policy is already applied to a service level, "Current Policy" appears in the top right corner of the right panel; otherwise, a **[Use Policy]** button appears. To apply a different status policy, click the **[Use Policy]** button.
    - To create a new policy, click the **[Create Policy]** button. In the **Create Policy** modal, type a ***Policy Name***, and then click **[Create Policy]**. The policy is added to the list. To apply it to the selected service level, select the policy from the list and then click the **[Use Policy]** button in the top right corner of the right panel.

14. Click **[Create Service]**. A confirmation message displays, indicating that your service model and its hierarchy have been created successfully.

NOTE: After you have created the service model, you cannot use the **New Service** wizard to edit the model.

15. Click **[Close]**.
16. If you want to use a different service policy with the new service, see *Selecting a Business Service Policy*.
17. If you want to create a *new* service policy to use with the new service, see *Creating a Business Service Policy*.

Selecting a Service Policy

Each service type requires a ***policy*** that determines what it monitors. A business service policy contains a set of rules and conditions that define the Availability, Health, and Risk values for the service, depending on your business needs. Each service requires that one policy be associated with a service at a time.

NOTE: The *Business Services PowerPack* contains a set of business service policies you can use for your services.

When you create a business service of any type, SL1 automatically uses the *default* policy for that particular type of business service. You can remove the default policy after you create a new policy. The default policies cannot be edited.

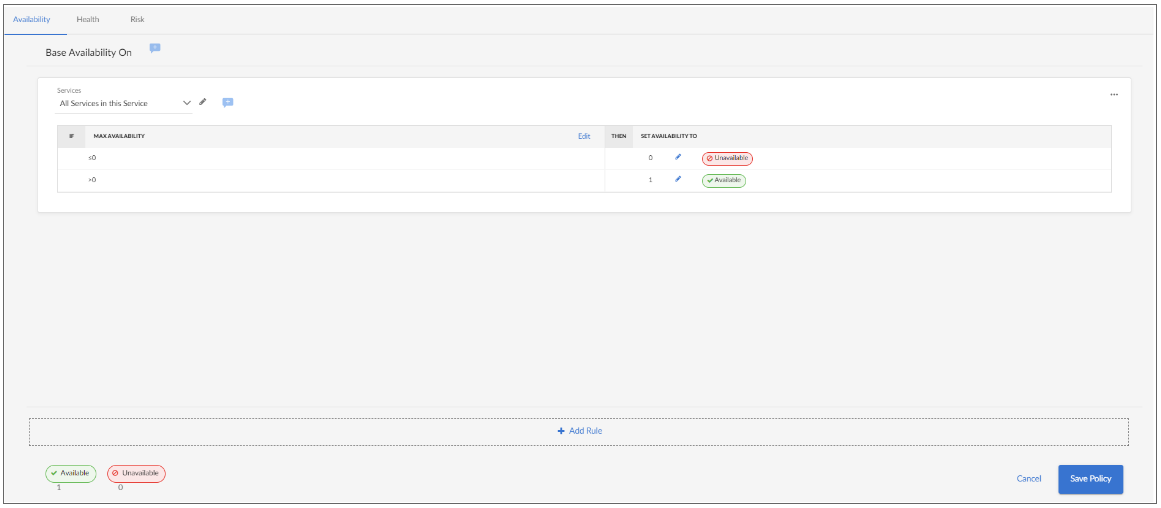
TIP: If a policy contains errors, an error icon (⚠) appears next to the policy name. To view details about what makes the policy invalid, select the policy and hover over the error icon next to the policy name in the right-hand section. A pop-up window lists the problems with the policy. Note that most Status Policies will display the icon during the time between a save and the next HAR aggregation cycle. For best results, wait for the next HAR cycle before investigating whether there is a true error.

To select an existing business service policy:

1. On the **Business Services** page, select the service that needs a policy. The **[Overview]** tab for the service appears.
2. Click the **[Status Policy]** tab.
3. In the **Policies** section on the left, select the policy you want to use.

TIP: You can type basic search criteria in the ***Search*** field to locate a specific policy in the list.

4. To view the details of a selected policy, click the **[Actions]** button (⋯) for that policy and select *Edit* (or *View* for the default policy). The **Policy Editor** page appears:



IF	MAX AVAILABILITY	Edit	THEN	SET AVAILABILITY TO
	≤0		0	⊘ Unavailable
	>0		1	✓ Available

5. Click the **[Cancel]** button when you are done viewing the details for that policy.

TIP: You can *copy* an existing service policy on the **Business Services** page by clicking the **[Actions]** button (⋯) for that policy and selecting *Duplicate*.

6. To add a policy to the service, select the policy in the **Policies** section and click the **[Use Policy]** button in the right-hand section. A check mark icon (☑) appears next to that policy in the **Policies** section, and the words "Current Policy" replace the **[Use Policy]** button in the right-hand section.
7. To make a copy of a policy, click the **[Actions]** button (⋯) for that policy and select *Duplicate*.
8. To *delete* a policy you no longer want to use, click the **[Actions]** button (⋯) for that policy, select *Delete*, and then click **[Delete Policy]**. If that policy is used by any other services, those services are assigned the default policy type. You cannot delete a default policy.

Creating a Service Policy

When you create a business service of any type, SL1 automatically uses the *default* policy for that particular type of business service. You can create a new policy to replace the default policy. When you create a new policy, the new policy uses the values from the default policy for that type of service as a starting point.

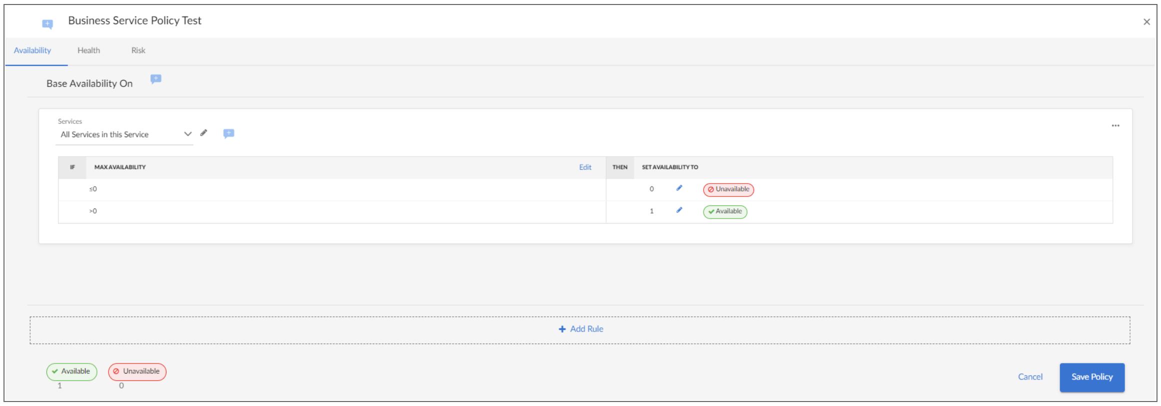
A policy includes a set of ***rules***, and each rule can include one to three ***conditions***. If you have multiple rules and conditions, *all* rules and conditions on a tab must be met to generate the Availability, Health, or Risk value. In other words, if a rule had three conditions, you would set up the conditions for that rule as an IF, AND, AND, THEN statement.

NOTE: Before you configure your service policy, it is important to understand why each severity is set as a range. For example, Critical for Risk is 81-100. The range allows one rule to be more causal or important than another. For example, suppose a Device Service for Linux servers has two risk rules: one for memory utilization and one for swap utilization. A server that has exhausted memory but still has free swap space to expand into will stay running but will slow down. A server that has exhausted swap space is likely to fail. Therefore, while both statuses can be bad, the lack of free swap space is worse than having low memory. When building Risk rules, we could set 95% memory utilization as Critical with a score of 85, but set Swap at 95% utilization to Critical with a score of 95. This will indicate that swap space is more causal then memory, and that as soon as you fix the swap space issue, you will need to check into the problems with memory.

To create a policy:

1. On the **Business Services** page, select the service for which you want to create a policy. The **Service Investigator** page appears.
2. Click the **[Status Policy]** tab, and then click **Create Policy** in the ***Policies*** section. A **Create Policy** window appears.
3. Type a policy name and click **[Create Policy]**. The new policy is added to the ***Policies*** section on the **[Status Policy]** tab.

4. Click the **[Actions]** button (•••) for the new policy and select *Edit*, or click the **[Edit Policy]** button. The **Service Policy Editor** page appears, with a default rule already configured on each tab for Availability, Health, and Risk:



Base Availability On

Services: All Services in this Service

IF	MAX AVAILABILITY	THEN	SET AVAILABILITY TO
	≤0	0	⊘ Unavailable
	>0	1	✓ Available

✓ Available 1 ⊘ Unavailable 0

5. On the **[Availability]**, **[Health]**, and **[Risk]** tabs, edit the rules and conditions for each of the three values that make up this policy. Each tab uses the same layout.

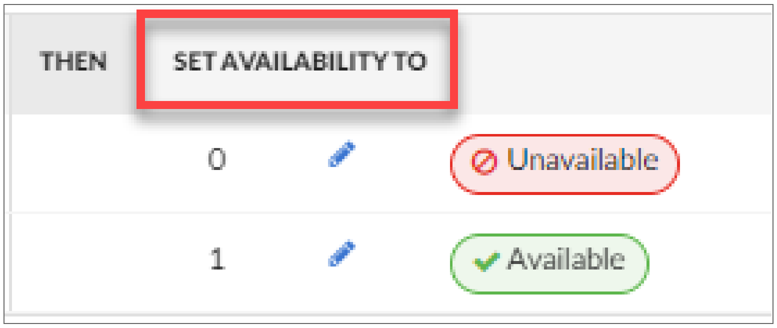
NOTE: Availability is not populated for component devices. Therefore, Availability will have a null value for any Device Service that includes component devices. The null value is displayed as a hyphen. However, a potential alternative is to change the rule from Availability to Count and query devices that are enabled to collect data (isActive = true). The reason for this is because Count is the number of devices that matches the filter query, and querying on isActive matches all devices that are currently collecting data.

6. In the **Services** or **Devices** drop-down list, select one of the following options to filter the services for this policy, as needed:

    - *All Services in this Service* or *All Devices in this Service*. This default setting uses all services or devices that are included in the service.
    - *Queried Services* or *Queried Devices*. This setting uses only the devices or services you specify in the ***Search*** field that appears when you select this option. This setting lets you filter the list of devices or services for this policy.
    - *Edit* . Click the **Edit** icon (✎) to specify a query to find specific devices. To filter health, availability, or risk based on a specific message text mask, click the ⚙ icon to allow for an advanced search. Search using the following format:

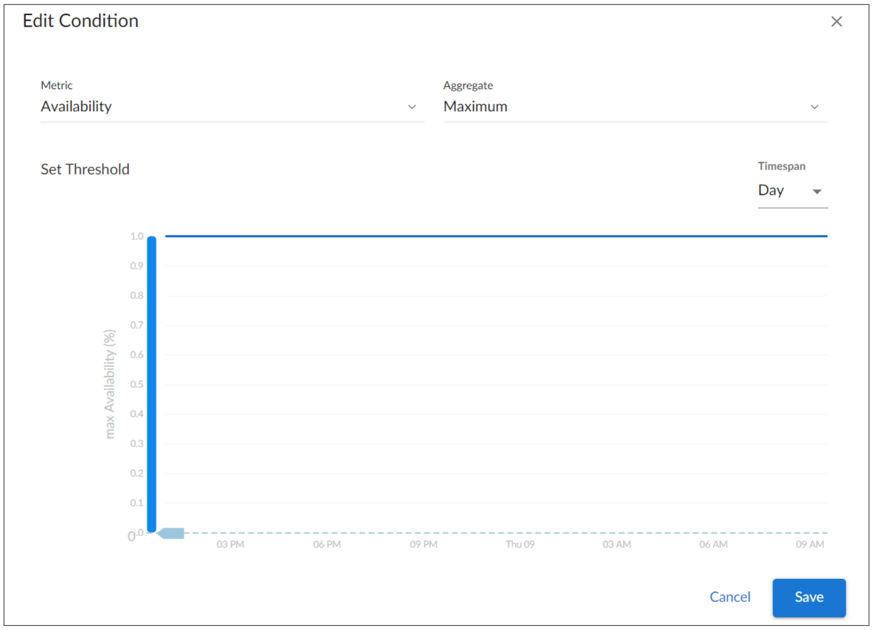
      ```
      event has (message contains 'text mask' )
      ```

7. To update an Availability, Health, or Risk value for a rule, edit the value in the **SET <*VALUE*> TO** column:



THEN	SET AVAILABILITY TO		
	0	✎	⊘ Unavailable
	1	✎	✓ Available

8. To edit the default conditions for an existing rule, click the **[Edit]** button for that rule. The **Edit Condition** window appears:



Edit Condition

Metric: Availability

Aggregate: Maximum

Set Threshold

Timespan: Day

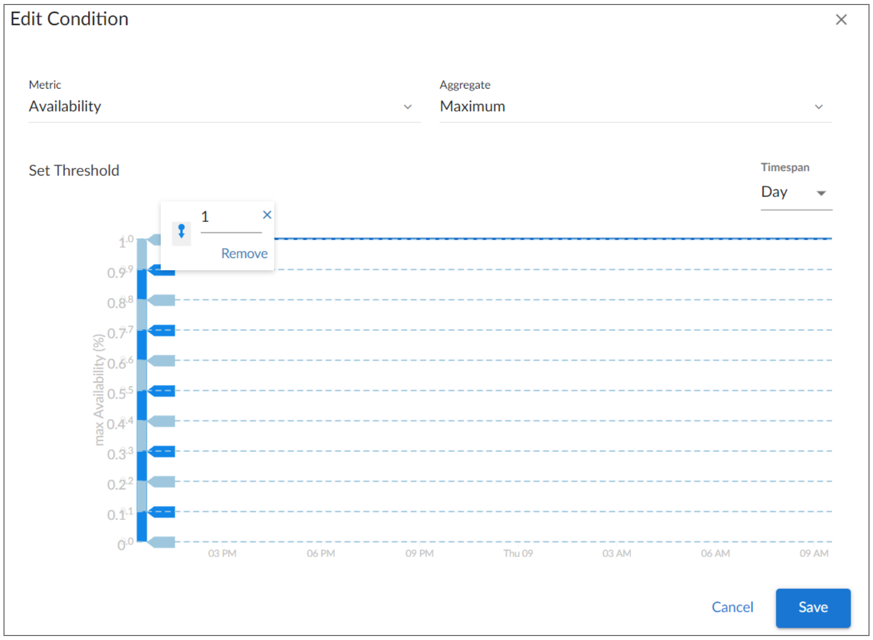
9. Complete the following fields:

   - ***Metric***. Select the metric you want to monitor for this condition:
     - If this is a business service or an IT service, your options include *Availability*, *Health*, and *Risk* for the services you want to monitor.
     - If this is a device service, select a device metric, such as Vitals like *Availability* and *Latency*, performance metrics, metrics collected by the SL1 Agent, or Dynamic Application metrics.
   - ***Aggregate***. Select an aggregation method for the data for this condition. Your options include *Average*, *Minimum*, *Maximum*, *Count*, and *Sum*. For example, suppose you have a web server farm consisting of three web servers. You have created a rule for web response time and are building for Health.
     - *Minimum* will drive health based on the fastest responding web server.
     - *Maximum* will drive health based on the slowest responding web server.
     - *Average* will drive health based on the average between slowest and fastest. This may give false positives. For example, assume that 5 seconds is the ideal target response time. If web server 1 gives a .1-second response time, web server 2 gives a 5-second response time, and web server 3 gives a 10-second response time, then the average will be 5 seconds, masking the fact that one of the response times is grossly unacceptable.
     - *Count* determines how many devices are currently being included in the Device Service. (The devices must be available as seen on the Device page). This is useful if we need at least 2 out of our 3 web servers to be active at any one time.
     - *Sum* is the result of adding up the value of the metric from all devices currently included in the Device Service. This is useful when you need to know how many devices are available across all the devices in the Device Service.
   - ***Day***. Select a time frame for the data in the graph in the ***Set Threshold*** section, below. You can use this graph to select reasonable thresholds for your condition. Your options include *Day*, *Week*, and *Month*.

10. In the ***Set Threshold*** section, click and drag the slider to specify a threshold for this condition. A small **Threshold** window appears, where you can specify the following threshold details:

    - The upper threshold icon (↕) lets you set the highest acceptable number for that condition, including any numbers less than that number. For example, x <= 80.
    - The lower threshold icon (↕) lets you set the lowest acceptable number for that condition, including any numbers greater than that number. For example, x >= 60.
    - The equals icon (●) in conjunction with a number lets you set a specific number only for this condition. For example, x = 75.
    - You can specify a range of values by clicking to add a second slider to the ***Set Threshold*** graph. For example, 40 < x < 60.
    - You can type a number in the ***Threshold*** window instead of using the slider.

- If needed, you can add a threshold that extends past the existing Y-axis of the table. The scale of the table automatically adjust to the new value.
- The different ranges for your conditions display in alternating shades of dark blue and light blue:



Edit Condition

Metric
Availability

Aggregate
Maximum

Set Threshold

Timespan
Day

1

TIP: If the line below the number in the ***Threshold*** window is red, then your current threshold is invalid. Click the icons or adjust the slider to make sure the line is not red under the threshold value.

11. To save the conditions and threshold settings and close the **Edit Condition** window, click the **[Save]** button.
12. To add more conditions to a rule, click **Edit** on the **Service Policy Editor** page and follow the instructions in steps 8-11.

TIP: To *remove* a condition from a rule, click the **[Actions]** button (⋯) for that condition and select *Delete*. To *copy* a condition, click the **[Options]** button (⋯) for that condition and select *Duplicate*.

13. If you have more than one rule, select the type of aggregation you want to use in the **Use <type> of rules** field. You can choose to use the minimum, maximum, or average value for the rules.

NOTE: The Availability value calculates only the minimum and maximum values for rules.

14. Edit any additional conditions or rules on the remaining tabs for this policy, and then click the **[Save Policy]** button.

Deleting a Service Policy

On the **Policies** page (Business Services > Policies), you can search for and delete one or more service policies.

To delete a single service policy from the **Policies** page, click the **[Actions]** button for the service policy you want to delete, and then select *Delete*.

To delete multiple service policies from the **Policies** page, select the check boxes of the policies you want to delete, and then click **[Delete Policies]** at the bottom of the page.

NOTE: You can select every visible service policy by selecting one check box and then clicking **[Select All Visible]**, or you can deselect every check box by clicking **[Deselect All]**.

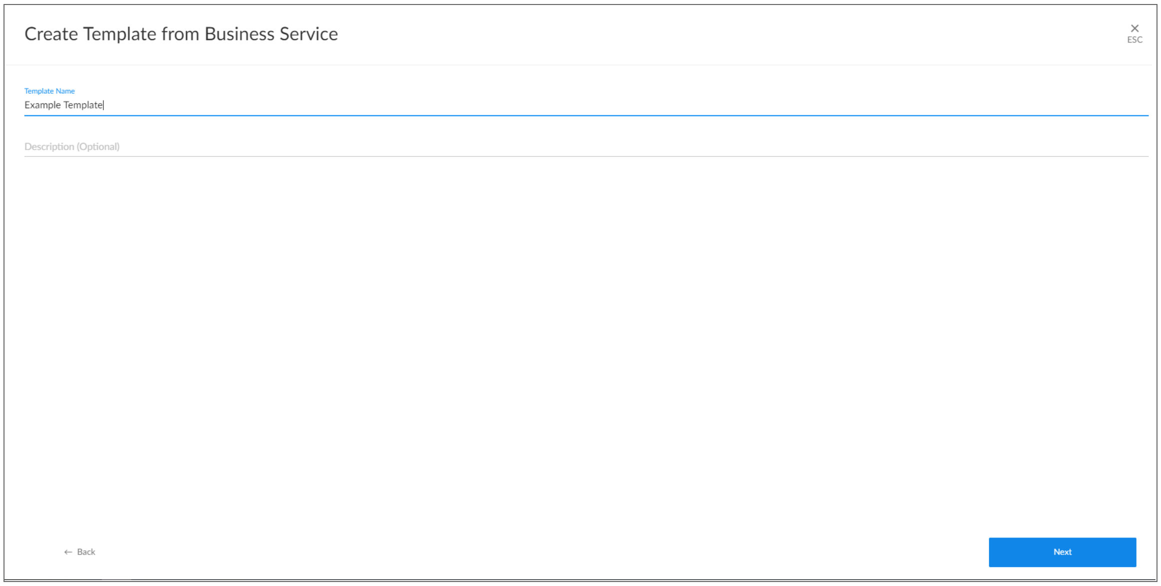
Creating a Service Template

You can create a ***service template*** from an existing service to simplify the process of replicating an entire service or service hierarchy on another SL1 system. For example, if you want to create the same service hierarchy, but only change the owner of the service hierarchy, creating a service template from an existing service streamlines this process.

To create a service template:

1. On the **Business Services** page, click the **[Actions]** button (⋯) for the service you want to use as the basis for your template and select ***Create Template***. The **Create Template From Service** window appears. This window contains important information about what you can and cannot do with a service template.

2. After reading the information that appears on the **Create Template From Service** window, click **[Next]**. The next **Create Template From Service** window appears:

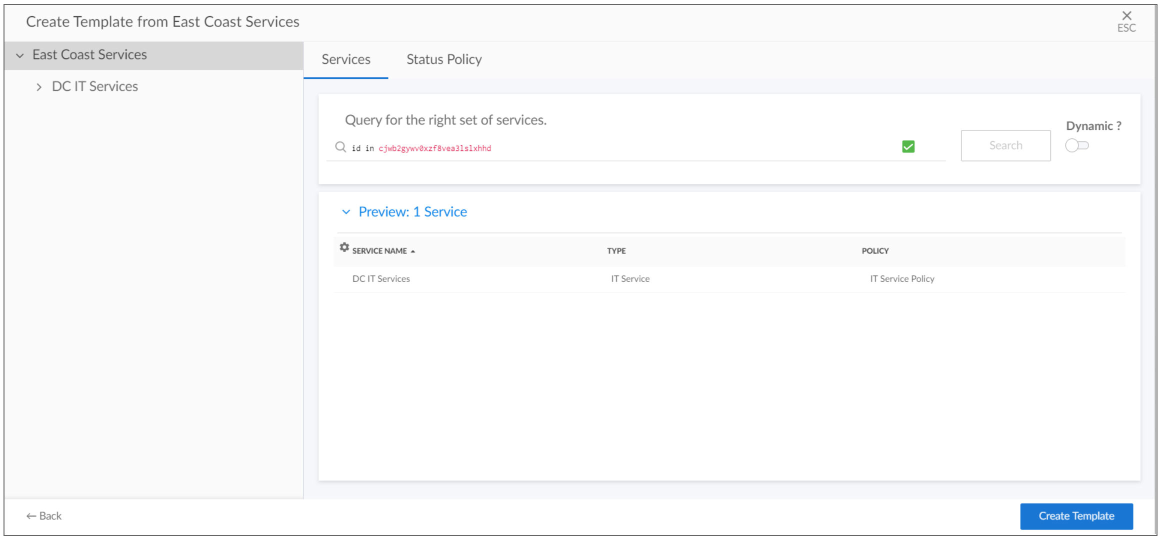


Create Template from Business Service

Template Name
Example Template

Description (Optional)

3. Type a name for the template in the ***Template Name*** field, and type a description of the template in the ***Description*** field, if needed. Click **[Next]**. The next **Create Template From Service** window appears:



Create Template from East Coast Services

Query for the right set of services.

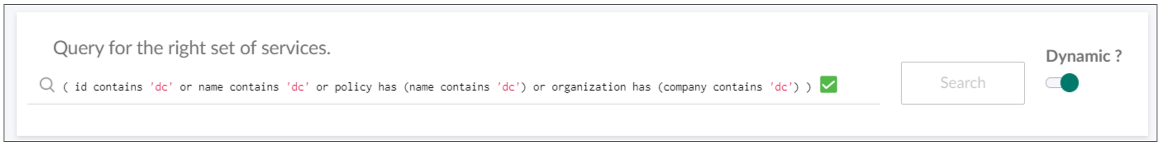
```
id in cjwb2gywv0xzf8vea3lslxhhd
```

Preview: 1 Service

SERVICE NAME	TYPE	POLICY
DC IT Services	IT Service	IT Service Policy

4. The left side of the window displays the tree for the service hierarchy that is being made into a template. You can select each service in the tree to see information related to that service on the right side of the window. For example, if you select a device service, the **Devices** tab displays the search query used for the devices included in that service. If you select a business service or an IT service, the **Services** tab displays the search query for that service. Note the following about the **Dynamic?** slider.

- If **Dynamic?** is disabled, the template inherits the result of the services inclusion search. This is useful is you want to lock the service tree at the time of template creation. For example, a Managed Service Provider (MSP) might do this to allow end customers to create services from the template but not to modify them. Another use case is if you want to use searches for tags to lock in a set of services that matched the rules at template creation time. By default, **Dynamic?** is disabled.
- If **Dynamic?** is enabled, the original rule is maintained in the template, so every service tree created from the template will be dynamic based on the services that match the rules.

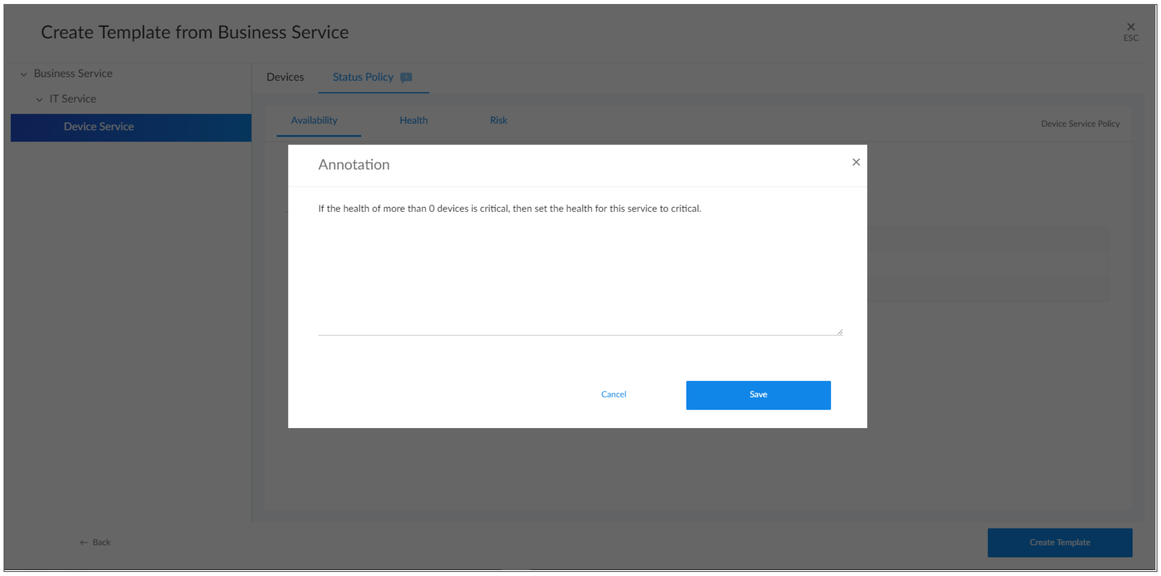


Query for the right set of services.

```
( id contains 'dc' or name contains 'dc' or policy has (name contains 'dc') or organization has (company contains 'dc') )
```

> **TIP:** The search uses the Advanced Search mode that lets you use "AND" or "OR" for multiple search criteria. For more information, see the "Performing an Advanced Search" topic in the ***Introduction to SL1*** manual.

5. Click the **Status Policy** tab to view the status policy definition for Availability, Health and Risk for that service.
6. On the **Status Policy** tab for a device service, you can add annotations for the policies in the template. When a new user uses the template on another system, your annotations can help that user understand the purpose of this status policy.



If the health of more than 0 devices is critical, then set the health for this service to critical.

7. To leave an annotation for a status policy or rule, click the annotation icon (💬) next to the rule or tab. Type your annotation text in the **Annotation** window and click **[Save]**. The annotation icon now displays as solid blue, while empty annotation icons contain a plus sign.

8. Click **[Create Template]**. A confirmation window appears stating that you created the template. Click **[Close]**. The template appears on the **Service Templates** page (Business Services > Templates).

NOTE: To delete one or more service templates, select the check boxes of the templates you want to delete from the **Service Templates** page and then click **[Delete Templates]**. You can also select every visible template by selecting one check box and then clicking **[Select All Visible]**, or you can deselect every check box by clicking **[Deselect All]**. Alternatively, you can delete a single service template by clicking the **Actions** button (···) for that template and then selecting *Delete*.

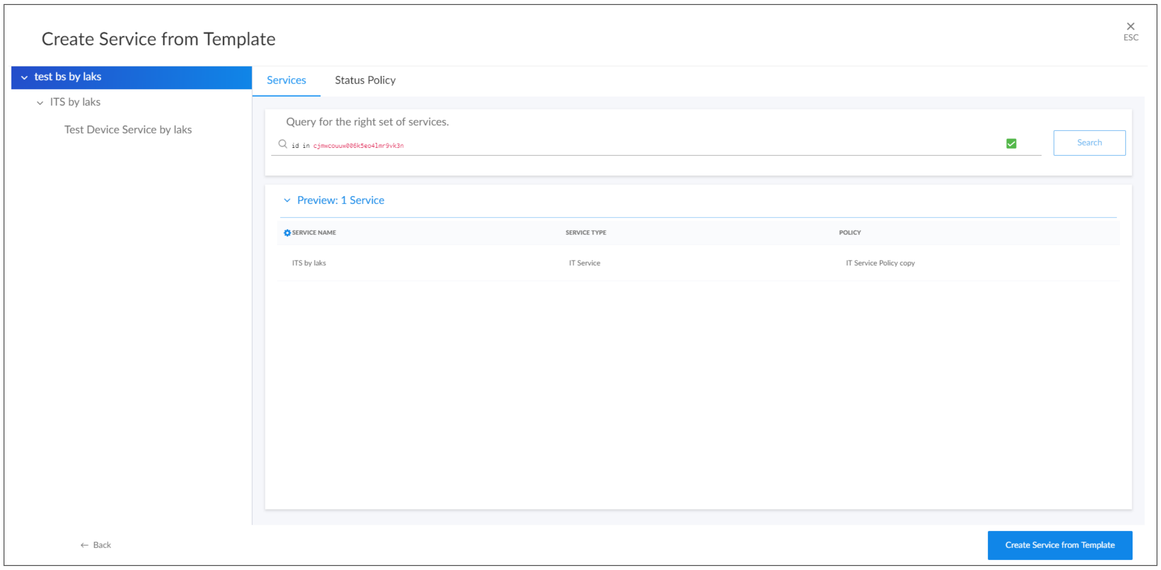
Creating a Service From a Template

To create a service from a template:

1. Go to the **Service Templates** page (Business Services > Templates) and click the **[Actions]** button (···) for the template you want to use and select *Create Service*. The **Create Service from Template** window appears.

TIP: You can also go to the **Business Services** page, click the down arrow on the **[Create Service]** button, and select *Create Service from Template*.

2. Select an organization from the ***What organization manages this service?*** drop-down list and click **[Next]**. The next **Create Service from Template** window appears:

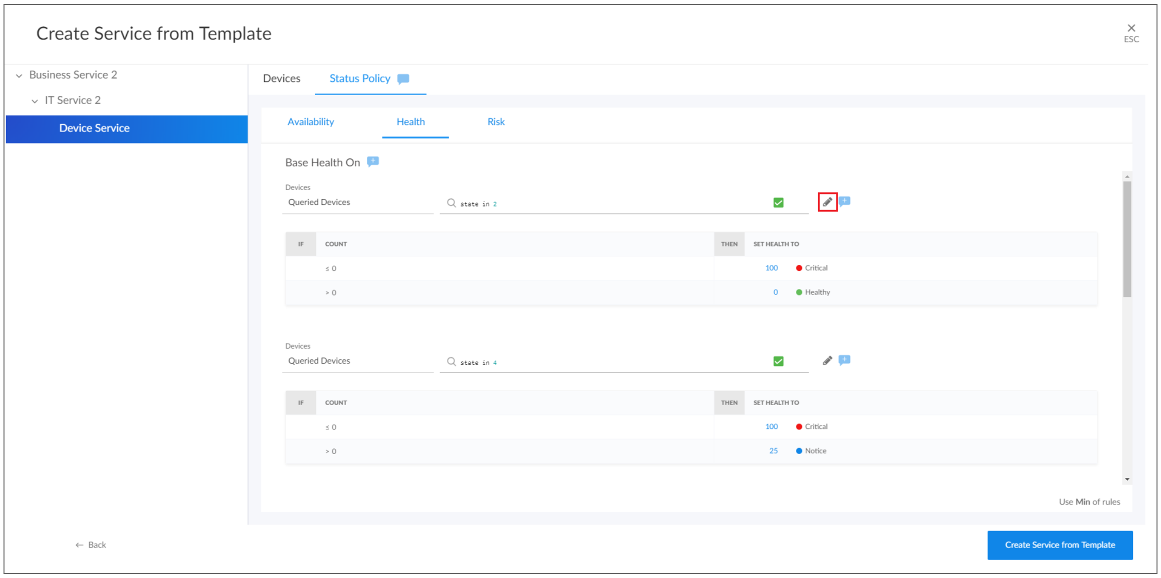

Create Service from Template
ESC
test bs by laks
ITS by laks
Test Device Service by laks
Services
Status Policy
Search
Preview: 1 Service
Back
Create Service from Template

Query for the right set of services.

```
id in cjmwcouuw006k5eo4lmr9vk3n
```

SERVICE NAME	SERVICE TYPE	POLICY
ITS by laks	IT Service	IT Service Policy copy

3. To edit the names of the services in the hierarchy at the left, click the service name and update the name. Updating the service names is recommended if you are creating the new service on the same system from which the template was created.
4. Any annotations for a device service that were added when the template was created will be present, and you can edit them and add new annotations.
5. You can edit the rules for Availability, Health, and Risk for a device service in the template.



Base Health On

Devices: Queried Devices — state in 2

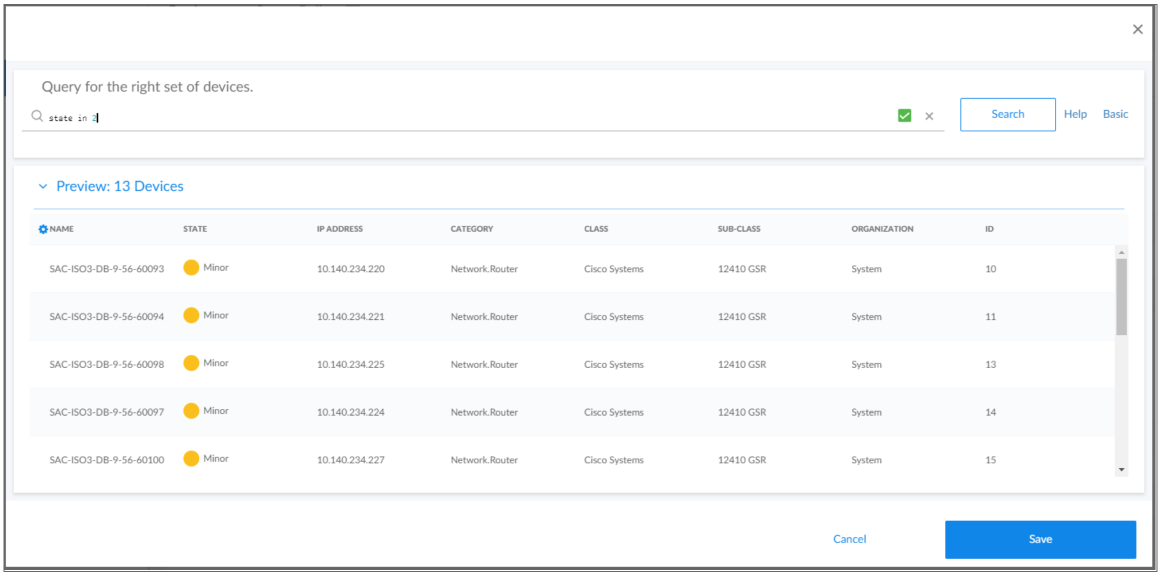
IF	COUNT	THEN	SET HEALTH TO
	≤ 0		100 ● Critical
	> 0		0 ● Healthy

Devices: Queried Devices — state in 4

IF	COUNT	THEN	SET HEALTH TO
	≤ 0		100 ● Critical
	> 0		25 ● Notice

Use **Min** of rules

6. To edit a rule, click the gray pencil icon (✎) next to the rule, and an edit window appears where you can update the rule:



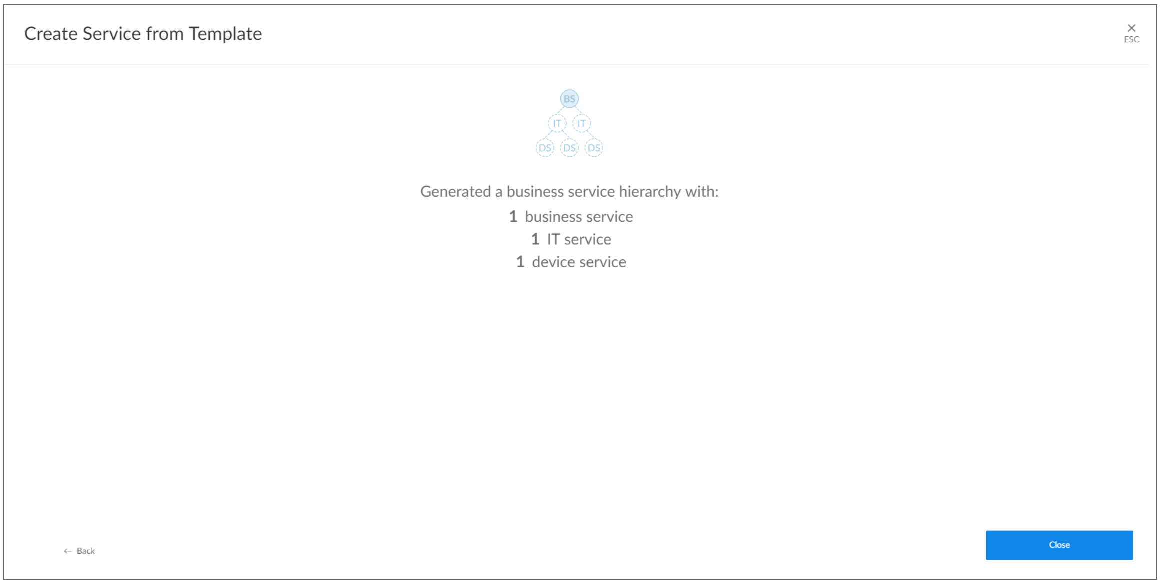
Query for the right set of devices.

state in 2

Preview: 13 Devices

NAME	STATE	IP ADDRESS	CATEGORY	CLASS	SUB-CLASS	ORGANIZATION	ID
SAC-ISO3-DB-9-56-60093	● Minor	10.140.234.220	Network.Router	Cisco Systems	12410 GSR	System	10
SAC-ISO3-DB-9-56-60094	● Minor	10.140.234.221	Network.Router	Cisco Systems	12410 GSR	System	11
SAC-ISO3-DB-9-56-60098	● Minor	10.140.234.225	Network.Router	Cisco Systems	12410 GSR	System	13
SAC-ISO3-DB-9-56-60097	● Minor	10.140.234.224	Network.Router	Cisco Systems	12410 GSR	System	14
SAC-ISO3-DB-9-56-60100	● Minor	10.140.234.227	Network.Router	Cisco Systems	12410 GSR	System	15

7. Click the **[Save]** button to close the edit window.
8. Click the **[Create Service from Template]** button to save your service. A confirmation window appears:



Create Service from Template

Generated a business service hierarchy with:
1 business service
1 IT service
1 device service

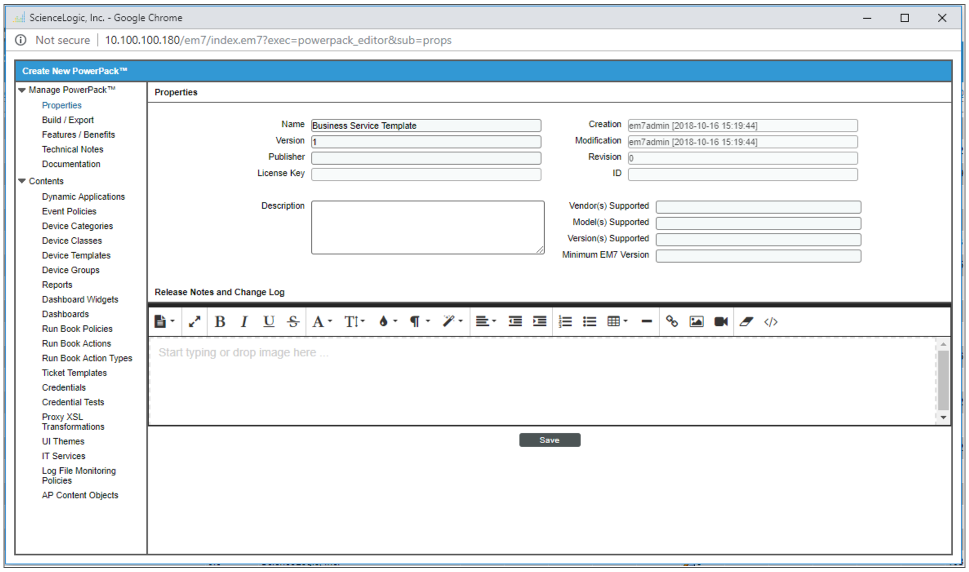
9. Click the **[Close]** button. The new services appear on the **Business Services** page.

Exporting a Service Template

If you want to use a business service template on another SL1 system, you can package that template into a PowerPack and export it to the other system.

To package and export a service template:

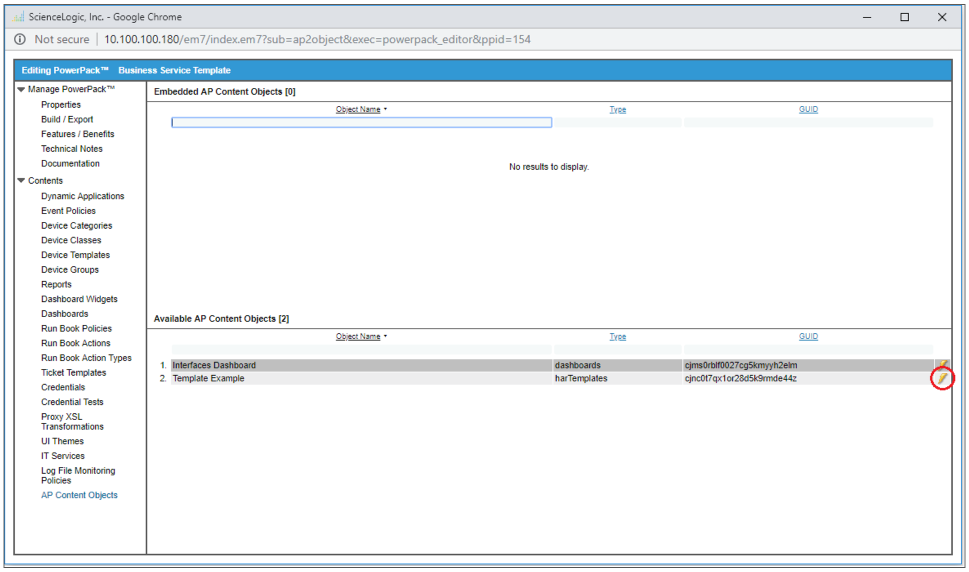
1. Go to **The PowerPack Manager** page (System > Manage > PowerPacks).
2. Click the **[Actions]** button and select *Create a New PowerPack*.
3. On the **PowerPack Properties** page, type a name for the PowerPack in the ***Name*** field and click **[Save]**.



Properties

Name: Business Service Template
Version: 1
Publisher:
License Key:
Description:
Creation: em7admin [2018-10-16 15:19:44]
Modification: em7admin [2018-10-16 15:19:44]
Revision: 0
ID:
Vendor(s) Supported:
Model(s) Supported:
Version(s) Supported:
Minimum EM7 Version:

4. Select *AP Content Objects* from the left-nav on the **PowerPack Properties** page. Your template appears in the **Available AP Content Objects** pane:



Embedded AP Content Objects [0]

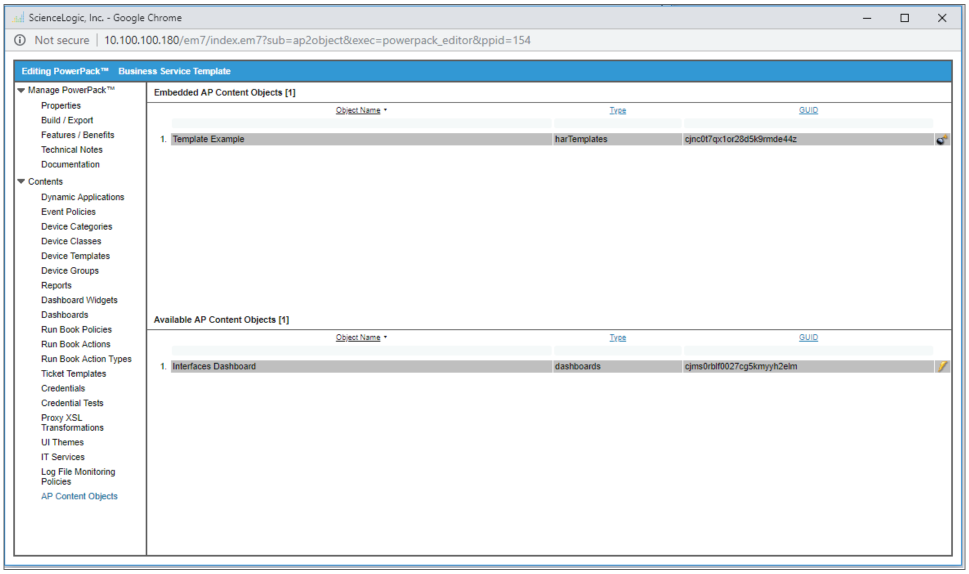
Object Name	Type	GUID

No results to display.

Available AP Content Objects [2]

	Object Name	Type	GUID
1.	Interfaces Dashboard	dashboards	cjms0rblf0027cg5kmyyh2elm
2.	Template Example	harTemplates	cjnc0t7qx1or28d5k9rmde44z

5. Click the lightning bolt icon (⚡) next to the template to add it to the PowerPack. The template moves up to the **Embedded AP Content Objects** pane:



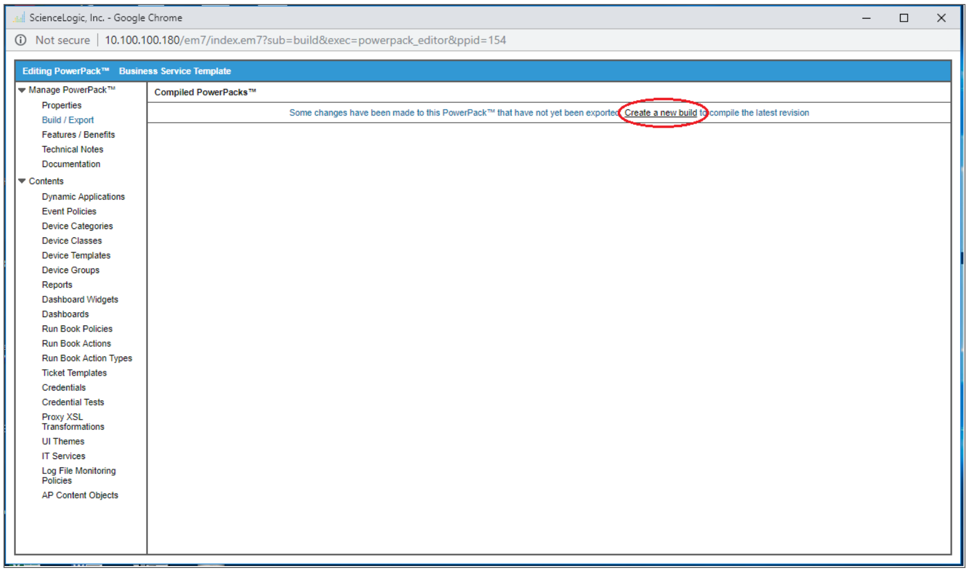
Embedded AP Content Objects [1]

	Object Name	Type	GUID
1.	Template Example	harTemplates	cjnc0t7qx1or28d5k9rmde44z

Available AP Content Objects [1]

	Object Name	Type	GUID
1.	Interfaces Dashboard	dashboards	cjms0rblf0027cg5kmyyh2elm

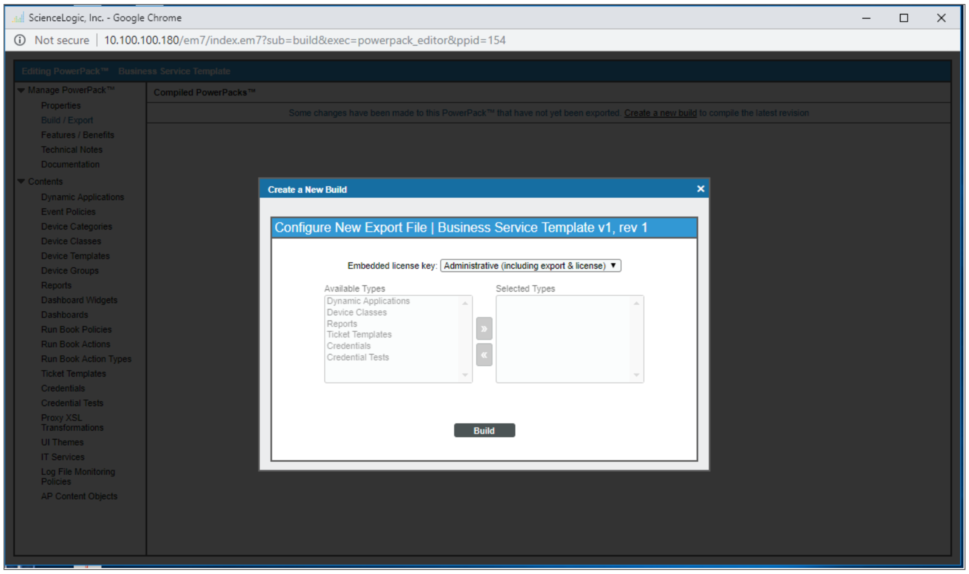
6. Select *Build/Export* from the left-nav to open the **Compiled PowerPacks** window, and then click the *Create a new build* link:



Compiled PowerPacks™

Some changes have been made to this PowerPack™ that have not yet been exported. Create a new build to compile the latest revision

7. In the **Configure New Export File** window, select *Administrative (including export & license)* from the ***Embedded license key*** drop-down list. Click **[Build]**.



ScienceLogic, Inc. - Google Chrome

Not secure | 10.100.100.180/em7/index.em7?sub=build&exec=powerpack_editor&ppid=154

Editing PowerPack™ Business Service Template

Compiled PowerPacks™

Some changes have been made to this PowerPack™ that have not yet been exported. Create a new build to compile the latest revision

Create a New Build

Configure New Export File | Business Service Template v1, rev 1

Embedded license key: Administrative (including export & license)

8. When the PowerPack finishes building, you can download the build with the download icon (💾) and use that file to upload the template to a new SL1 system.

Installing a Template from a PowerPack

1. On the SL1 system where you want to install the template, import the PowerPack on the **PowerPack Manager** page (System > Manage > PowerPacks).
2. After you have imported the PowerPack, click the **[Actions]** button and select *Install PowerPack*.
3. Locate the PowerPack you created in the **Imported PowerPacks** window and click its lightning bolt icon (⚡).
4. When the **Install PowerPack** window appears, click the **[Install]** button.
5. After you install the PowerPack, you can access the template on the Service Templates (Business Services > Templates).

Default Service Policy Settings

The following sections describe how the three default service policies calculate Availability, Health, and Risk:

Device Service Default Policy

Availability: Maximum available: if one device is available, then all are available

Health: Based upon the worst device severity, then uses the following settings:

- Critical = 0-20
- Major = 21-40
- Minor = 41-60
- Notice = 61-80
- Healthy = 81-100

Risk: Based upon the worst device severity, then uses the following percentages:

- Healthy= 0-20%
- Notice = 21-40%
- Minor = 41-60%
- Major = 61-80%
- Critical = 81-100%

IT Service Default Policy

Availability: Maximum available: If one service is available, then all are available

Health: Average Health value of all services

Risk: Maximum Risk value of any service

Business Service Default Policy

Availability: Maximum available: If one service is available, then all are available

Health: Average Health value of all services

Risk: Maximum Risk value of any service

Custom Service Model Default Policy

Availability: Maximum available: If one service is available, then all are available

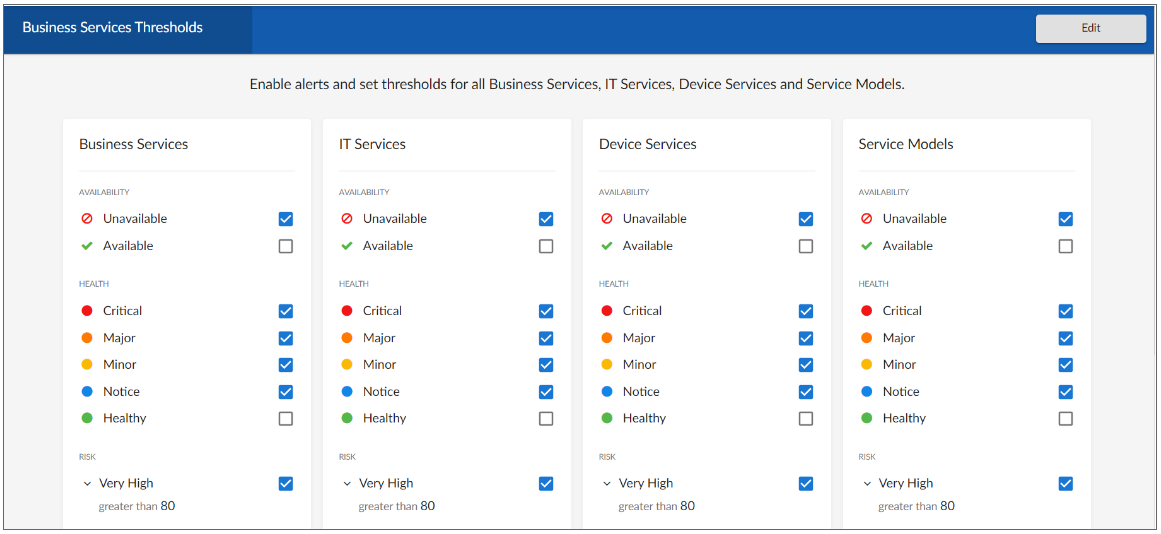
Health: Average Health value of all services

Risk: Maximum Risk value of any service

> NOTE: Unlike IT services and business services, which use "0" as the lowest possible Health and Risk values in their default service policies, custom service models use "10" as the lowest Health and Risk values in their default service policies.

Managing Service Thresholds

When SL1 evaluates the state of a service, it reviews the Health, Availability, and Risk values produced by your business services, IT services, devices services, and service models. SL1 then compares those values against the alert thresholds that are defined on the **Business Service Thresholds** page (Business Services > Thresholds).



Enable alerts and set thresholds for all Business Services, IT Services, Device Services and Service Models.

	Business Services	IT Services	Device Services	Service Models
AVAILABILITY				
Unavailable	☑	☑	☑	☑
Available	☐	☐	☐	☐
HEALTH				
Critical	☑	☑	☑	☑
Major	☑	☑	☑	☑
Minor	☑	☑	☑	☑
Notice	☑	☑	☑	☑
Healthy	☐	☐	☐	☐
RISK				
Very High greater than 80	☑	☑	☑	☑

If any of the thresholds on the **Business Service Thresholds** page are crossed, SL1 generates an alert message. For an event to be produced, you need to create or install an event policy that watches for that alert message and produces an event when it sees that alert message.

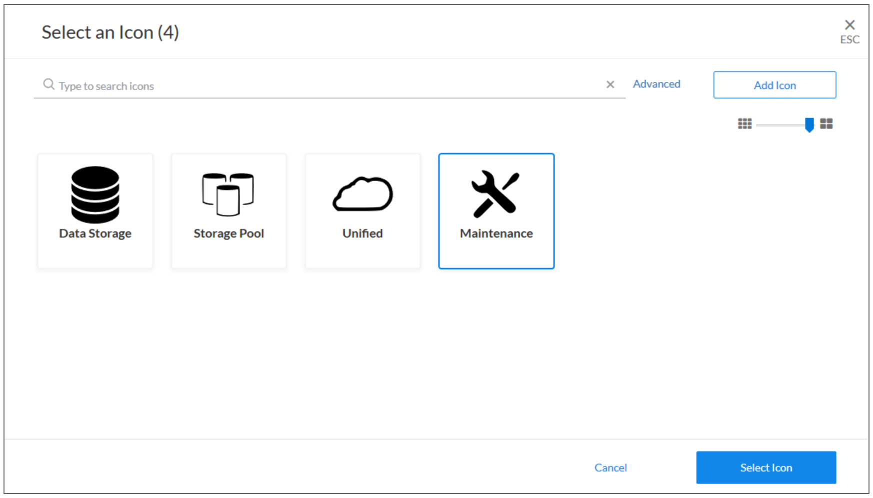
By monitoring the events tied to your business services, you can act quickly if one of your services is unavailable, unhealthy, or potentially at risk.

> TIP: To update the thresholds on this tab, click the **[Edit]** button, select which thresholds should generate an alert message, and then click **[Save]**.

Assigning an Icon to a Service

To assign an icon to a service:

1. On the **Business Services** page, locate the service to which you want to add an icon.
2. Click the **[Actions]** button (⋯) for that service and select *Assign Icon*. The **Select an Icon** window appears:

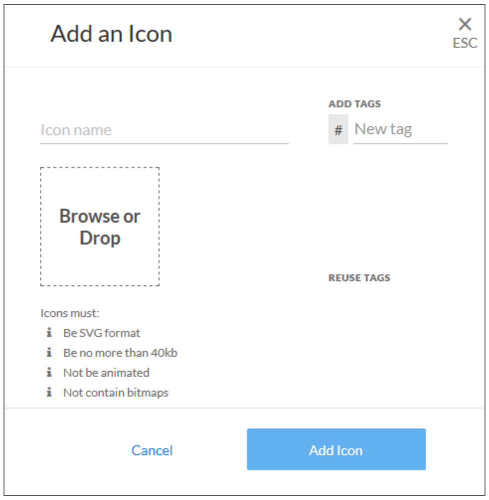


3. To use an existing icon, select that icon from the list of icons and click the **[Select Icon]** button.

TIP: If an icon includes a tag, you can search for that icon by typing some or all of the tag text in the ***Search*** field.

4. To upload an icon from your local drive, make sure that the image file meets the following criteria:
   - The image file should be in .SVG format.
   - The file should not be larger than 40 KB.
   - The file should not be animated.
   - The file should not contain bitmaps

5. To start the upload process, click the **[Add Icon]** button. The **Add an Icon** window appears:



Add an Icon

Icon name

ADD TAGS

# New tag

Browse or Drop

REUSE TAGS

Icons must:

- Be SVG format
- Be no more than 40kb
- Not be animated
- Not contain bitmaps

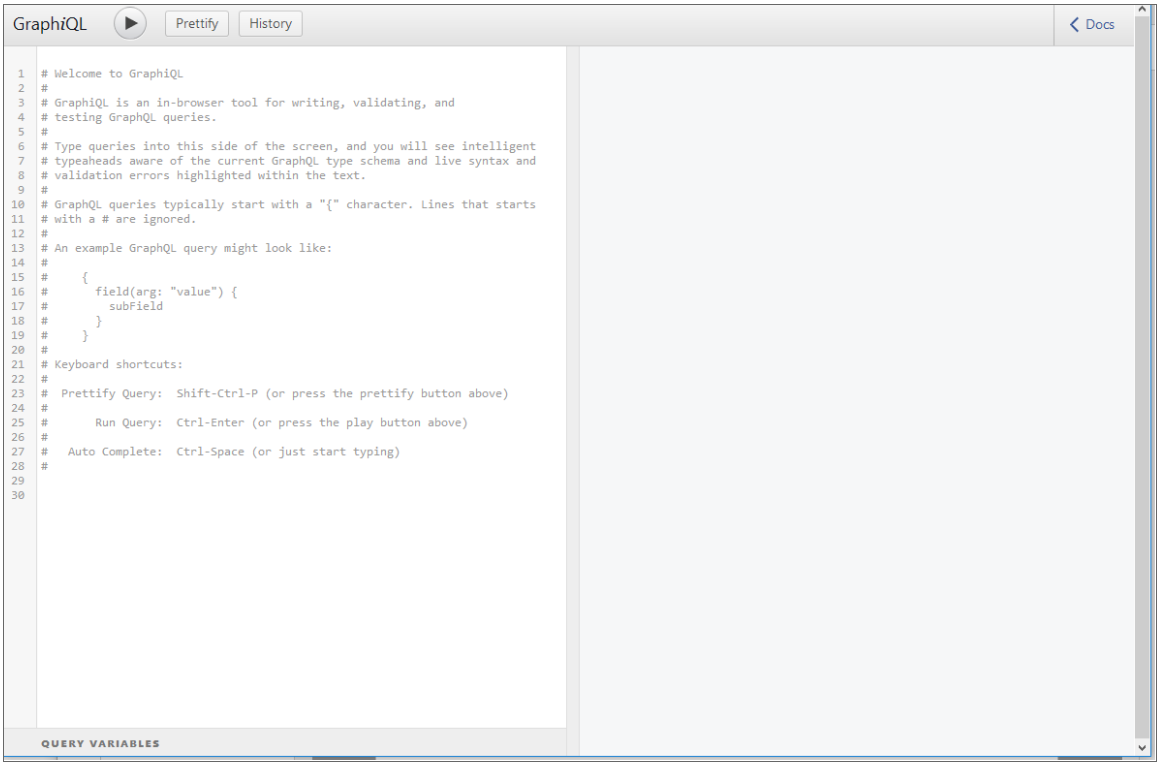
6. In the ***Icon name*** field, type a name for the icon you want to upload.
7. In the ***Add Tags*** field, type a short descriptor for the icon, without spaces. You can use this tag for searching later.
8. You can click the ***Browse or Drop*** area to browse for and select the icon, or you can drag and drop the icon file onto the **Add an Icon** window.
9. Click the **[Add Icon]** button. The icon is added to the **Select an Icon** window.
10. Click the **[Select Icon]** button to add the icon to the service.

Exporting Service Data with the ScienceLogic API

By navigating to the GraphiQL interface, you can export business service data with the ScienceLogic API. GraphiQL is a user interface for interactively exploring the capabilities of, and executing queries against, a GraphQL API.

To access the GraphiQL interface:

1. In a browser, type the URL or IP address for SL1.
2. Type **/gql** at the end of the URL or IP address. For example, you could type **https://sl1.sciencelogic.com/gql**. The GraphiQL interface appears:



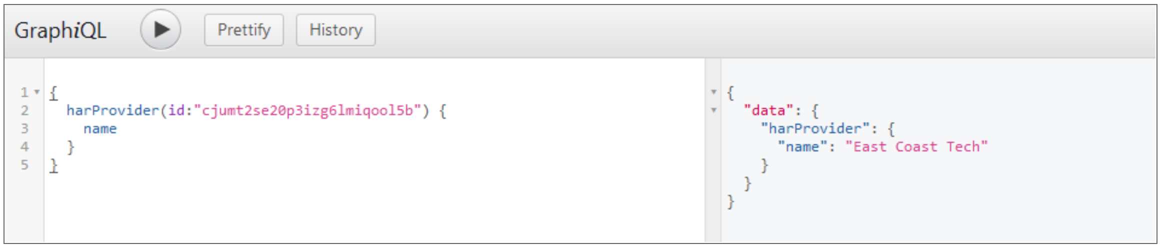
```
# Welcome to GraphiQL
#
# GraphiQL is an in-browser tool for writing, validating, and
# testing GraphQL queries.
#
# Type queries into this side of the screen, and you will see intelligent
# typeaheads aware of the current GraphQL type schema and live syntax and
# validation errors highlighted within the text.
#
# GraphQL queries typically start with a "{" character. Lines that starts
# with a # are ignored.
#
# An example GraphQL query might look like:
#
#     {
#       field(arg: "value") {
#         subField
#       }
#     }
#
# Keyboard shortcuts:
#
#  Prettify Query:  Shift-Ctrl-P (or press the prettify button above)
#
#       Run Query:  Ctrl-Enter (or press the play button above)
#
#   Auto Complete:  Ctrl-Space (or just start typing)
#
```

3. In SL1, make a note of the URL that displays for the service you want to export. For example, if you have a service named "East Coast Tech," and its URL in SL1 is **http://sl1.sciencelogic.com/inventory/services/cjumt2se20p3izg6lmiqool5b/overview**. Make a note of the unique value between **/services** and **/overview**. In this example, the value you need is ***cjumt2se20p3izg6lmiqool5b***.
4. In the GraphiQL interface, create a *harProvider* query for the service you want to export, using the following format:

```
query {harProvider (id:"<Service_URI>") { name} }
```

where `<Service_URI>` is the value found in the URL for the Service you want to export.

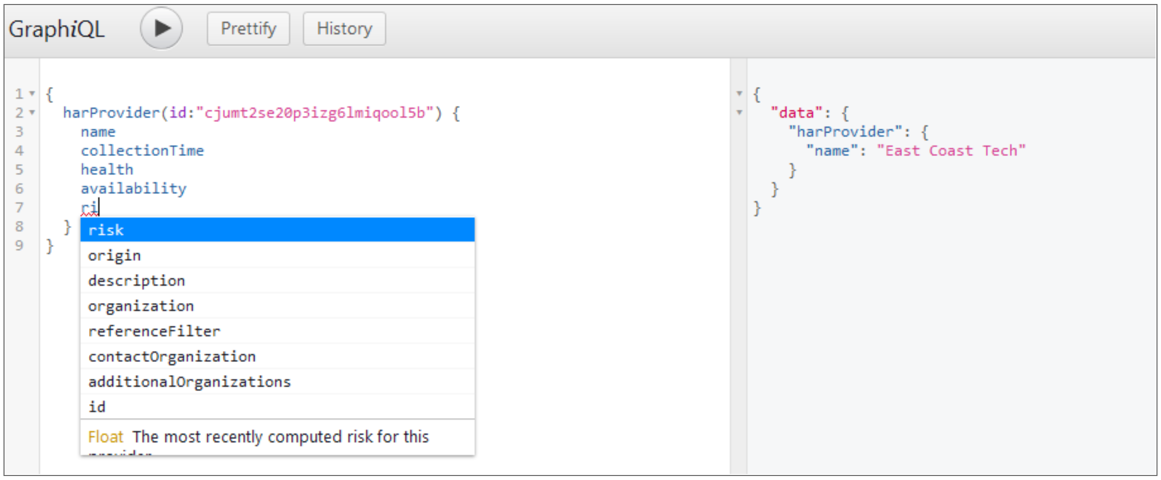
5. Click the **[Execute Query]** (Play) button to tell GraphiQL to send the query to the GraphQL server and get the results. Using the example service from step 3, the query and its data appear in the following format:



```
{
  harProvider(id:"cjumt2se20p3izg6lmiqool5b") {
    name
  }
}
```

```
{
  "data": {
    "harProvider": {
      "name": "East Coast Tech"
    }
  }
}
```

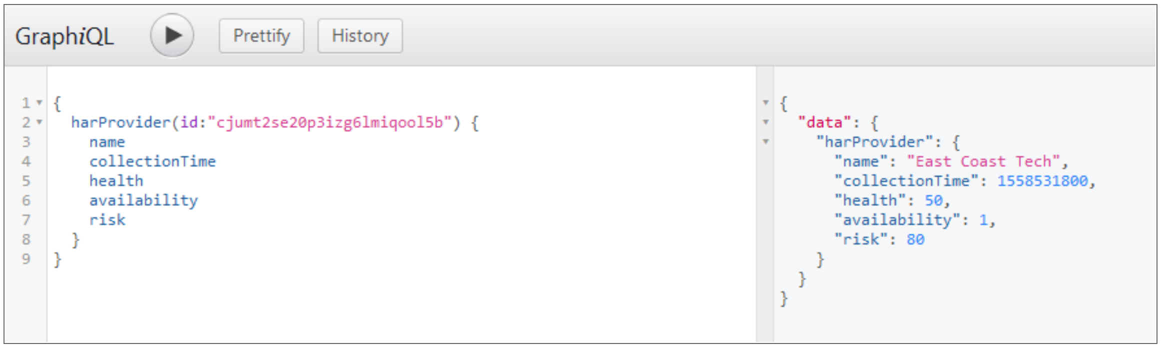
6. To export additional data, use the filter-while-you-type capabilities of the GraphiQL interface to gather other information, such as the collection timestamp, health, availability, and risk:



```
{
  harProvider(id:"cjumt2se20p3izg6lmiqool5b") {
    name
    collectionTime
    health
    availability
    ri
  }
}
```

```
{
  "data": {
    "harProvider": {
      "name": "East Coast Tech"
    }
  }
}
```

7. After you finish updating your query, click the **[Execute Query]** button.



```
{
  harProvider(id:"cjumt2se20p3izg6lmiqool5b") {
    name
    collectionTime
    health
    availability
    risk
  }
}
```

```
{
  "data": {
    "harProvider": {
      "name": "East Coast Tech",
      "collectionTime": 1558531800,
      "health": 50,
      "availability": 1,
      "risk": 80
    }
  }
}
```

8. To return to the SL1 user interface, replace the "gql" and any text after it in the URL with "ap2", such as **https://sl1.sciencelogic.com/ap2**.

TIP: For more information about GraphQL and the GraphiQL user interface, see the ***ScienceLogic GraphQL API Quick Start Guide***.

Chapter

2

Using the Default Service Investigator

Overview

This chapter describes how to use the **Service Investigator** page for a particular business, IT, device service, or custom service model.

NOTE: The **Service Investigator** page has two different user interfaces and viewing options depending on the SL1 version you are running:

- *Default Service Investigator*. The default view of the **Service Investigator** page in SL1 version 12.2.0 and earlier.
- *Enhanced Service Investigator*. The enhanced view of the Service Investigator page. This page is disabled by default and requires a minimum SL1 version of 12.2.0 or later, and a minimum of AP2 Biscotti version 8.0.20.

For instructions on how to download and install AP2 Biscotti version 8.0.20, see the ***AP2 Biscotti Release Notes***.

For instructions on how to enable to disable the enhanced **Service Investigator** page, see the section on ***Enabling or Disabling the Enhanced Service Investigator Page and its Elements***.

For more information on how you can use the features on the **Service Investigator** page to help you avoid business service impact and lower Mean Time to Repair (MTTR), watch the video at https://sciencelogic.com/product/resources/avoid-business-service-impact.

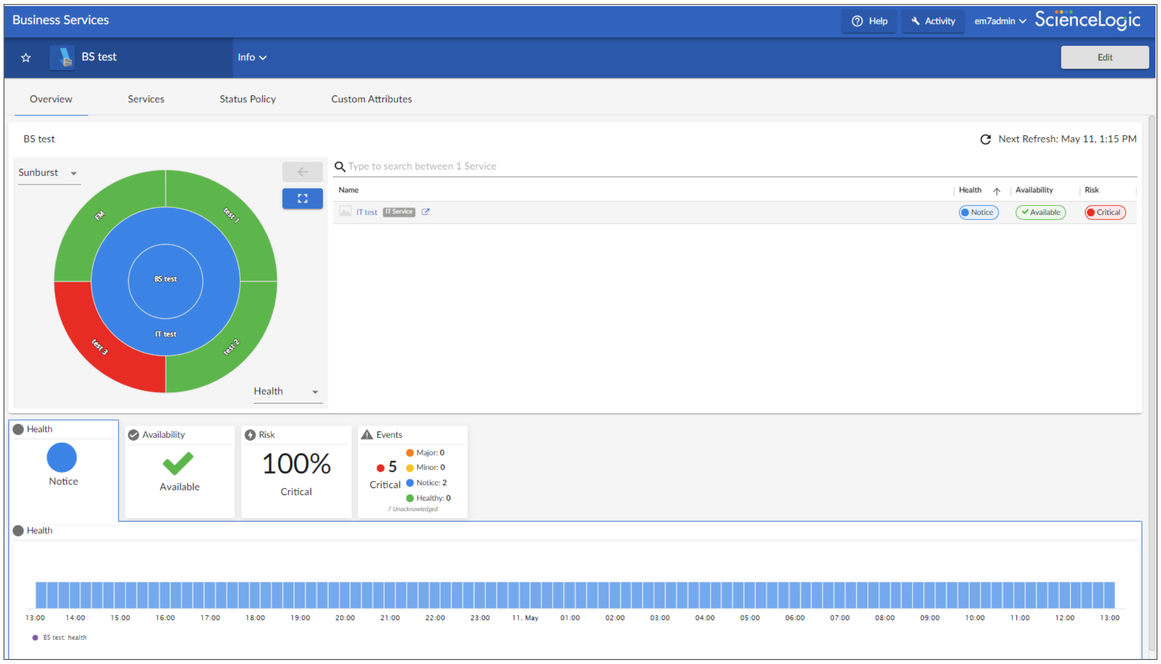
Use the following menu options to navigate the SL1 user interface:

- To view a pop-out list of menu options, click the menu icon (☰).
- To view a page containing all of the menu options, click the Advanced menu icon (•••).

This chapter covers the following topics:

Viewing the Default Service Investigator

To view the **Service Investigator** page, select a service from the list on the **Business Services** page (💼).



Name	Health	Availability	Risk
IT test IT Service	Notice	✓ Available	Critical

Starting in SL1 version 12.2.0, you can view Zebrium suggestions and alerts in the **Timeline** widget and the **Log Insights** tab of the **Service Investigator** page. For SL1 12.2.0, you will need to set up the connection between Zebrium and SL1. For more information, see *Configuring the Zebrium Connector for SL1*.

The Tabs on the Default Service Investigator Page

The **Service Investigator** page contains the following tabs:

- *Overview*
- *Services/Devices*
- *Status Policy*
- *Custom Attributes*

Each of these tabs is described in the following sections.

The Overview Tab

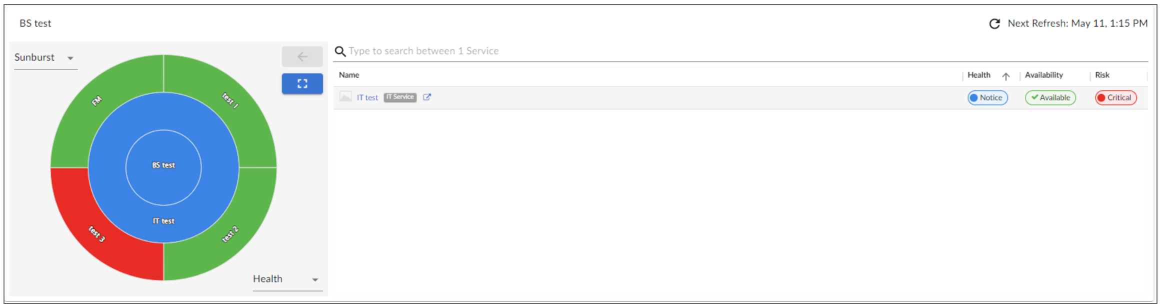
The **[Overview]** tab provides a single-page view of your services. This tab enables users to determine the ***behavioral correlation*** between a service's health, availability, and risk values and the events, anomalies, or other causes that might be impacting those values. This behavioral correlation feature provides users with a "big picture" view of the service and enables them to determine the root cause of any problems the service might be experiencing and then troubleshoot those problems.

The **[Overview]** tab consists of the following widgets:

- *Sunburst* or *Map* dashboard widget
- *Health, Availability, and Risk* widgets
- *Changes widget*
- *Events widget*
- *Anomalies widget*

Each of these widgets is described in the following sections.

Sunburst Widget



Next Refresh: May 11, 1:15 PM

Type to search between 1 Service

Name	Health	Availability	Risk
IT test IT Service	Notice	✓ Available	Critical

The top dashboard widget of the **[Overview]** tab displays either a *Sunburst* chart view or a *Map* view of your services. Use the drop-down menu in the top left corner of the widget to select which view you want to appear.

When you select the *Sunburst* view:

- The left pane includes a sunburst chart that displays the current Health, Availability, and Risk values for the service, as well as for any constituent IT services or device services that belong to that top-level service. For device services, the sunburst includes the device name and Health values for any devices that belong to the service. Additionally, this pane indicates the maximum number of constituent services or devices that will be used for computing health, availability, and risk.
- The right panel includes a list of constituent services or devices. Each service in this panel includes icons that represent that service's Availability, Health, and Risk metrics; devices include icons that represent each device's Health value. The right panel also includes a search bar at the top of the panel that enables you to search for specific constituent services or devices.

In the sunburst chart, the center circle represents the selected service. The selected service drives the context for the page title and **Info** drawer, as well as all the other panels and widgets on the **[Overview]** tab. This means that the right panel, widgets, and other elements on the page will all reflect the metrics for the service in the center circle of the sunburst.

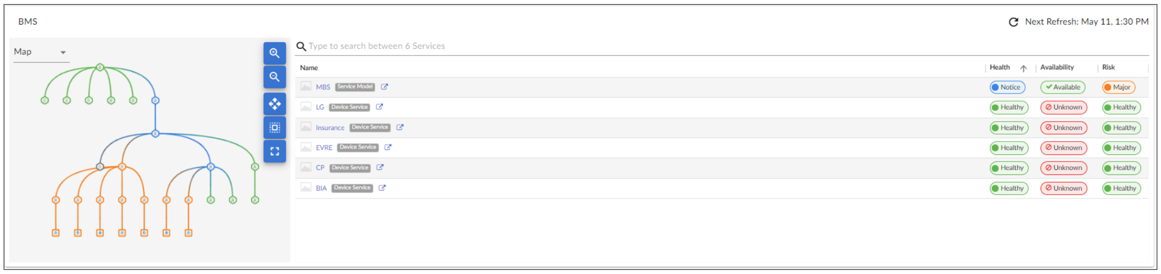
You can navigate through services on the widget in the following ways:

- In the left panel, you can click any of the constituent IT services or device services in the sunburst to select that service. To return to the parent IT service or business service, click the center circle or click the **[Back]** button.
- In the right panel, you can click the service name of any of the constituent IT services or device services to select that service. To return to the parent IT service or business service, click the breadcrumb links that appear in the top-left corner of the widget.

By default, the sunburst displays the Health value for the selected service and its constituent services or devices. To view the current Availability or Risk value for the selected service, click the drop-down button in the lower-right corner of the left pane and select *Availability* or *Risk*.

To collapse the sunburst widget, click the up arrow icon (^) in the top-right corner of the widget. To reopen it, click the down arrow icon (⌄).

Map Widget


BMS
Next Refresh: May 11, 1:30 PM
Map
Type to search between 6 Services

Name	Health	Availability	Risk
MBS Service Model	Notice	✓ Available	Major
LG Device Service	Healthy	Unknown	Healthy
Insurance Device Service	Healthy	Unknown	Healthy
EVRE Device Service	Healthy	Unknown	Healthy
CP Device Service	Healthy	Unknown	Healthy
BIA Device Service	Healthy	Unknown	Healthy

The top dashboard widget of the **[Overview]** tab displays either a *Sunburst* chart view or a *Map* view of your services. Use the drop-down menu in the top left corner of the widget to select which view you want to appear.

When you select the *Map* view:

- The left pane includes a map of the service and any constituent services and devices that belong to that top-level service.
- The right panel includes a list of constituent services or devices. Each service in this panel includes icons that represent that service's Availability, Health, and Risk metrics; devices include icons that represent each device's Health value. The right panel also includes a search bar at the top of the panel that enables you to search for specific constituent services or devices.

In the map view, you can click on the top-level service or any of its constituent services or devices. The selected service drives the context for the page title and **Info** drawer, as well as all the other panels and widgets on the **[Overview]** tab. This means that the right panel, widgets, and other elements on the page will all reflect the metrics for the service that you have clicked in the map view.

In the map view, use the following buttons to manipulate the map in the left pane:

🔍: Zoom in on the map.

🔍: Zoom out on the map.

✥: Fit all elements of a map into the viewing pane.

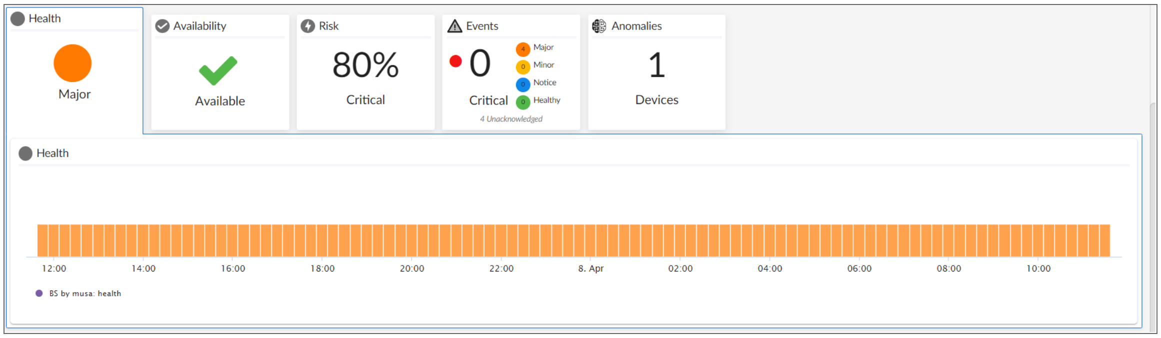
⊡: Center all selected elements of a map in the viewing pane.

The viewing pane displays the following two types of graphical elements:

1. ***Nodes*** that represent Devices, Topology Elements, and Business Services defined in SL1. The shape of the node represents its type: *Services*, such as business services, IT services, or device services, are represented by hexagons, while devices are represented by squares. The color of the outline specifies the current state of the node.
2. ***Edges*** are lines that represent the relationships and hierarchies between nodes.

> **TIP:** When you hover over a node, a pop-up **Properties** pane appears with the metadata for that node. Click the **[Go to service]** or **[Go to device]** link at the top of the pane to open the **Investigator** page for that service or device in a new browser window.

Health, Availability, and Risk Widgets



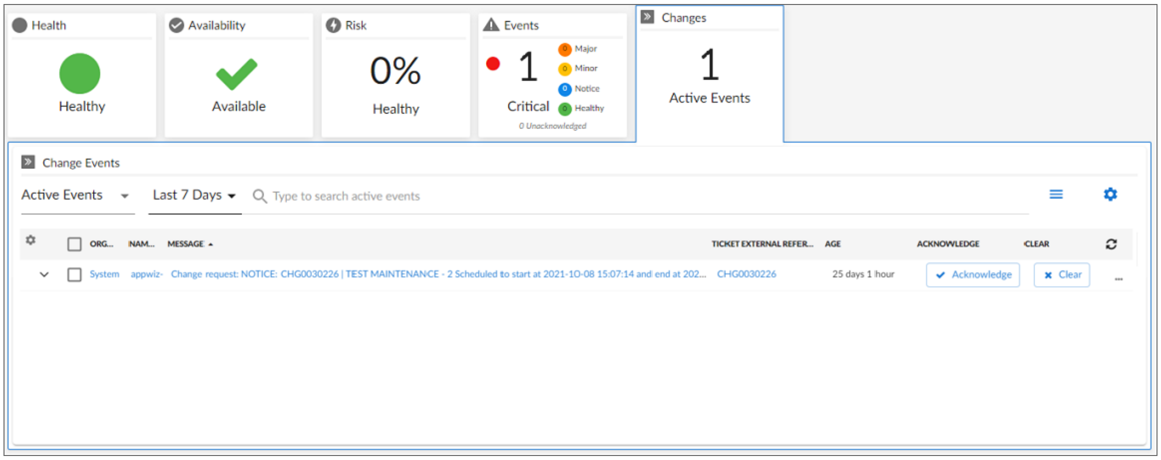
The **Health**, **Availability**, and **Risk** widgets display a time series chart with the historical values of those metrics for the selected service from each polling cycle over the previous 24 hours.

From these widgets, you can do the following:

- Hover your mouse over the chart to view the value for each polling cycle from the previous 24 hours.
- Click and drag your mouse over a series of bars in the chart to zoom in on that specific timespan. To return to the 24-hour view, click **[Reset zoom]**.
- Click a specific polling cycle to view the historic Health, Availability, and Risk values for that polling cycle.

> TIP: If the ***RCA Options*** field is enabled, you can also view Root Cause Analysis information for the service to help you troubleshoot the root cause of a particular Health, Availability, or Risk value for a specific polling cycle. To view Root Cause Analysis information, click one of the polling cycles in the time series chart.

Changes Widget



	ORG...	NAM...	MESSAGE	TICKET EXTERNAL REFER...	AGE	ACKNOWLEDGE	CLEAR
□	System	appwiz-	Change request: NOTICE: CHG0030226 | TEST MAINTENANCE - 2 Scheduled to start at 2021-10-08 15:07:14 and end at 202...	CHG0030226	25 days 1 hour	✓ Acknowledge	✖ Clear

The **Changes** widget is available to customers who have purchased Configuration and Change Management as part of their SL1 Standard or Premium subscription. This widget displays a list of events that are created when PowerFlow pulls change data from ServiceNow or Restorepoint, including both active and cleared change events.

The **Changes** widget tile displays the number of active change events that are impacting the service. Events on the widget will automatically clear after 30 minutes.

From the **Changes** widget, you can do the following:

- Use the drop-down menu to choose which type of change events display in the widget: *Active Events* or *Cleared Events*.
- Filter and search for events by their date; either by 5, 7, 14, 30 days, or more than 30 days.
- Use the ***Search*** field to search for specific change events.

- For active events that are aligned to devices, click the down-arrow icon (⌄) next to the event to open the Event Drawer panel, which displays the following panes:

  - ***Vitals***. A widget displaying the past 24 hours of CPU and memory usage for the device related to the event. You can zoom in on a shorter time frame by clicking and dragging, and you can go back to the original timespan by clicking the **[Reset zoom]** button.

  - ***Tools***. A set of network diagnostic tools or user-initiated actions that you can run on the device associated with the event. Click the search bar to search for a tool or action to run, or click one of the default tools or actions that are available based on the device type and your user permissions.

  - ***Logs***. A list of the log entries from the device's log file, sorted from newest to oldest by default.

- View the **Organizational Summary** page for the organization aligned with an active event by clicking the link in the ***Organization*** column.
- View the **Service Investigator** or **Device Investigator** page for the service or device aligned with an active event by clicking the link in the ***Name*** column.
- View the **Event Investigator** page for an active event by clicking the link in the ***Message*** column.
- For ServiceNow integrations, view the ServiceNow ticket associated with an active event by clicking the link in the ***Ticket External Reference*** column.
- For ServiceNow integrations, view the ServiceNow ticket associated with a cleared event by clicking the link in the ***External Ticket*** column.
- Acknowledge an active event by clicking the **[Acknowledge]** button. When you acknowledge an event, you let other users know that you are aware of that event, and you are working on a response.
- Clear an active event by clicking the **[Clear]** button. When you clear an event, you let other users know that the event has been addressed.
- Create a ticket from an active event.
- View the event policy for an active event.
- Select multiple active events for action using the check boxes next to the events.

Configuring and Enabling the Changes Widget

To use the **Changes** widget, you must first configure and enable the widget. To do so, perform the following steps:

1. Ensure that you are running SL1 version 11.2.0 or later and have *Business Services Base Pack* PowerPack version 2.2.0 or later installed in SL1. For more information, see the chapter on "Installing a PowerPack" in the ***PowerPacks*** manual.
2. Ensure that you are running SL1 PowerFlow Platform version 2.2.2 or greater and one or more of the following PowerPacks, depending on your integration:
   - ***For a ServiceNow integration***:

     - *ServiceNow CMDB* SyncPack version 3.2.0 or later installed in PowerFlow. For more information, see the ***ServiceNow CMDB Synchronization PowerPack*** manual.

    - *ServiceNow Change Management* SyncPack version 3.2.1 or later installed in PowerFlow. For more information, see the ***ServiceNow Change Management Synchronization PowerPack*** manual.

- ***For a Restorepoint integration***:

    - *Restorepoint* SyncPack version 1.2.0 or later installed in PowerFlow.
    - *Restorepoint* PowerPack version 102 or later installed in SL1.
    - *Restorepoint Automation* PowerPack version 102 or later installed in SL1. For more information, see the ***Restorepoint Integrations*** manual.

3. In SL1, ***create a SOAP/XML credential*** to connect with PowerFlow and make note of its credential ID.
4. ***For a ServiceNow integration***:
    a. In PowerFlow, ***sync SL1 devices with ServiceNow*** and make note of the ***Configuration*** field value in the Sync Devices from SL1 to ServiceNow application.
    b. In SL1, open the "ServiceNow: Send Change Request Event to PowerFlow" Run Book Action (which is included in the *Business Services Base Pack* PowerPack v2.1 and greater) and ***edit the input parameters*** to include the credential ID from step 3 and the ***Configuration*** field value from step 4.
5. ***For a Restorepoint integration***, follow the steps in "Sync Devices with Restorepoint" section in the ***Device Management*** manual.
6. Finally, do one of the following:
    - Permanently enable the **Changes** widget by ***editing the NextUI configuration file*** on your SL1 system.
    - Temporarily enable the **Changes** widget by ***running a GraphQL mutation*** on your SL1 system.

Creating a SOAP/XML Credential for PowerFlow

To create a SOAP/XML credential to connect SL1 with PowerFlow:

1. Follow the steps in the section on "Creating a SOAP/XML Credential for PowerFlow" in the ***Monitoring SL1 PowerFlow*** manual.
2. After saving the credential, make note of the credential ID. This number can be found at the top of the **Edit SOAP/XML Credential** modal or in the ***ID*** column on the **Credentials** page (Manage > Credentials) or **Credential Management** page (System > Manage > Credentials).

Syncing SL1 devices with ServiceNow

To sync SL1 devices with ServiceNow:

1. Follow the steps in the section on "Running a Device Sync" in the ***ServiceNow CMDB Synchronization*** PowerPack manual.
2. In the **Configuration** pane of the "Sync Devices from SL1 to ServiceNow" application, make note of the value in the ***Configuration*** field.

Editing the Run Book Action

To edit the input parameters in the "ServiceNow: Send Change Request Event to PowerFlow" Run Book Action:

1. Go to the **PowerPack Manager** page (System > Manage > PowerPacks).
2. Locate the *Business Services Base Pack* PowerPack and click its wrench icon (🔧). The **Editing PowerPack** modal appears.
3. In the **Editing PowerPack** modal, click ***Run Book Actions*** in the left Navbar. The **Embedded Run Book Actions** page appears in the modal.
4. Click the wrench icon (🔧) for the "ServiceNow: Send Change Request Event to PowerFlow" Run Book Action. The **Policy Editor** modal appears.
5. In the **Policy Editor** modal, make the following edits to the ***Input Parameters*** field:
   - Replace `<sl1 credential id for powerflow>` with the credential ID of the ***SOAP/XML credential you created for PowerFlow***.
   - Replace `<pf config id>` with the ***Configuration*** field value from the ***"Sync Devices from SL1 to ServiceNow" application in PowerFlow***.
6. Click **[Save]**, then exit the **Policy Editor** modal.
7. Exit the **Editing PowerPack** modal.

Syncing SL1 Devices with Restorepoint

To sync SL1 devices with Restorepoint:

1. Follow the steps in the section on "Running a Device Sync" in the ***Restorepoint Integrations*** manual.
2. In PowerFlow, open the **Configuration** pane for the "Restorepoint: Sync Devices" application and select *Enable* for the ***restorepoint_config*** field to allow device change detection.
3. Make a note of the ***restorepoint_id*** value on the **Configuration** pane for the "Restorepoint: Sync Devices" application.
4. In SL1, make sure that the same ***restorepoint_id*** value was added to the **Values** column on the **[Attributes]** tab on the **Device Investigator** page for the devices synced from Restorepoint.

Permanently Enabling the Widget

To permanently enable the **Changes** widgetusing the NextUI configuration file, run the following steps on all appliances, including the Administration Portal, the Data Collector, the Database Server, the Data Engine, and the All-In-One Appliance.

To permanently enable the **Changes** widget:

1. Start an SSH session into one of the SL1 appliances.
2. Using vi or another text editor, edit the `/opt/em7/nextui/nextui.conf` file. To do so, enter the following at the shell prompt:

```
sudo vi /opt/em7/nextui/nextui.conf
```

3. Add the following line at the bottom of the NextUI configuration file:

```
BUSINESS_SERVICES_CHANGE_EVENTS_TAB=enabled
```

4. Save your changes, and then restart the NextUI service by running the following command:

```
sudo systemctl restart nextui
```

5. Repeat steps 1-4 for the remaining SL1 appliances.

Temporarily Enabling the Widget

To temporarily enable the **Changes** widget using GraphQL:

1. To access the GraphiQL interface, type the URL or IP address for SL1 in a browser, add **/gql** to the end of the URL or IP address, and press **[Enter]**. The GraphiQL interface appears.
2. In the main query pane, type the following mutation:

```
mutation updateChangeEventsTab {
       updateFeatureToggle(
               id: "system:BUSINESS_SERVICES_CHANGE_EVENTS_TAB"
               value: "enabled"
       ) {
               id
               value
       }
}
```

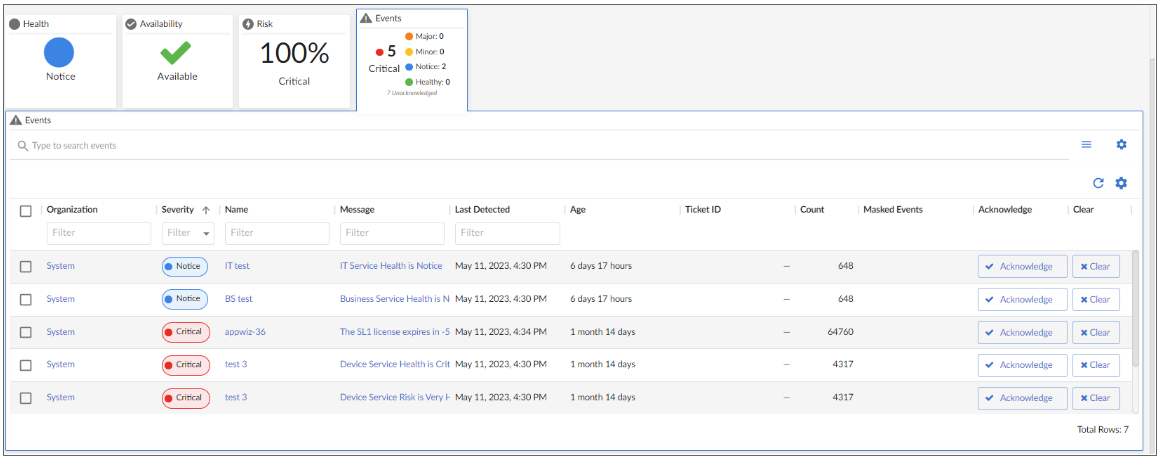
> TIP: Click the **[Prettify]** button to format the mutation and to add syntax highlighting to make the mutation easier to read. Note that the *Prettify* process removes the `query` syntax if only one query is present in the main query pane.

3. Click the **[Execute Query]** (Play) button. The mutation executes, and the results appear in the pane on the right side.

> NOTE: If the **Changes** widget does not appear in SL1 after executing the mutation, refresh the page using the **[F5]** key or by clicking the refresh button in your web browser.

> NOTE: For more information about GraphQL, see the GraphQL documentation. For more information about the GraphiQL user interface, see the GraphiQL user interface documentation.

Events Widget



□	Organization	Severity ↑	Name	Message	Last Detected	Age	Ticket ID	Count	Masked Events	Acknowledge	Clear
	Filter	Filter	Filter	Filter	Filter						
□	System	Notice	IT test	IT Service Health is Notice	May 11, 2023, 4:30 PM	6 days 17 hours	–	648		✓ Acknowledge	✖ Clear
□	System	Notice	BS test	Business Service Health is N	May 11, 2023, 4:30 PM	6 days 17 hours	–	648		✓ Acknowledge	✖ Clear
□	System	Critical	appwiz-36	The SL1 license expires in -5	May 11, 2023, 4:34 PM	1 month 14 days	–	64760		✓ Acknowledge	✖ Clear
□	System	Critical	test 3	Device Service Health is Crit	May 11, 2023, 4:30 PM	1 month 14 days	–	4317		✓ Acknowledge	✖ Clear
□	System	Critical	test 3	Device Service Risk is Very H	May 11, 2023, 4:30 PM	1 month 14 days	–	4317		✓ Acknowledge	✖ Clear

Total Rows: 7

The **Events** widget displays a list of events for the selected service. This widget has much of the same functionality as the **Events** page.

NOTE: The **Events** widget tile displays the number of events of each severity type, after masking, that are currently impacting the service. When opened, the **Events** widget lists all events impacting the service, including masked events. Therefore, the number of events that appear in the widget tile might be smaller than the number of events that appear in the opened widget.

From the **Events** widget, you can do the following:

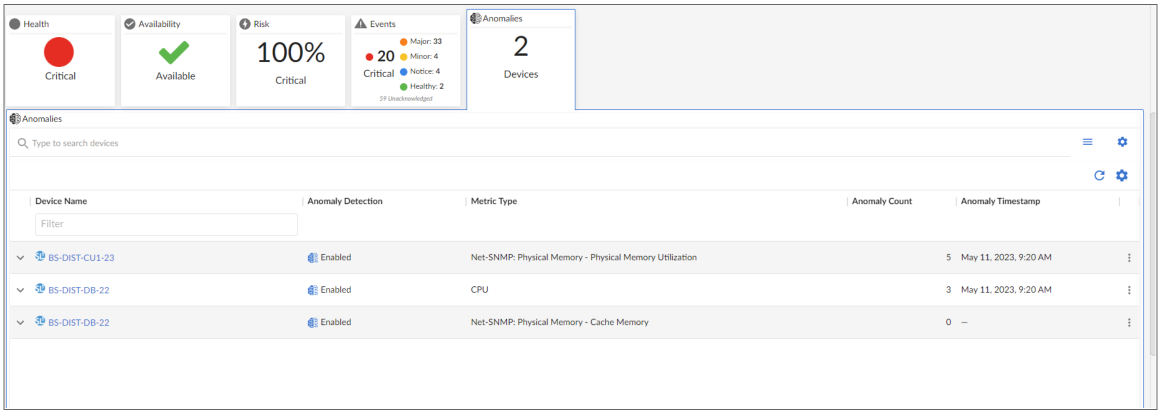
- Use the search field to search for specific events.
- For events that are aligned to devices, click the down-arrow icon (⌄) next to the event to open the Event Drawer panel, which displays the following panes:
  - ***Vitals***. A widget displaying the past 24 hours of CPU and memory usage for the device related to the event. You can zoom in on a shorter time frame by clicking and dragging, and you can go back to the original timespan by clicking the **[Reset zoom]** button.
  - ***Tools***. A set of network diagnostic tools or user-initiated actions that you can run on the device associated with the event. Click the search bar to search for a tool or action to run, or click one of the default tools or actions that are available based on the device type and your user permissions.
  - ***Logs***. A list of the log entries from the device's log file, sorted from newest to oldest by default.
- View the **Organizational Summary** page for the organization aligned with the event by clicking the link in the ***Organization*** column.
- View the **Service Investigator** or **Device Investigator** page for the service or device aligned with the event by clicking the link in the ***Name*** column.

- View the **Event Investigator** page for the event by clicking the link in the ***Message*** column.
- View or edit event notes by clicking the **Note** icon ( ) in the ***Event Note*** column or by clicking the **[Actions]** button (···) and selecting *Edit Event Note*. Event notes contain event definitions, probable causes, and resolutions for the event, along with a text field where you can add more information about the event or the service or device you are monitoring.
- View more information about masked events by clicking the magnifying glass icon ( ) or the **Masked** link in the ***Masked Events*** column. Masked events are related events that occur in quick succession on a single device or service that are rolled up and posted together under one event description, with only the highest severity event displayed.
- Acknowledge the event by clicking the **[Acknowledge]** button. When you acknowledge an event, you let other users know that you are aware of that event, and you are working on a response.
- Clear the event by clicking the **[Clear]** button. When you clear an event, you let other users know that the event has been addressed.
- Create a ticket from the event.
- View the event policy.
- View a log of automations that have occurred for the event by clicking the **[Actions]** icon (···) and selecting *View Automation Actions*.
- Select multiple events for action using the check boxes next to the events.

NOTE: For more information about events, see the ***Events*** manual.

Anomalies Widget

If one or more devices within a business, IT, or device service has anomaly detection enabled, the **Anomalies** widget will appear on the **[Overview]** tab of the **Service Investigator**. The **Anomalies** widget displays a list of all the devices within the selected service that have anomaly detection enabled.



Device Name	Anomaly Detection	Metric Type	Anomaly Count	Anomaly Timestamp
BS-DIST-CU1-23	Enabled	Net-SNMP: Physical Memory - Physical Memory Utilization	5	May 11, 2023, 9:20 AM
BS-DIST-DB-22	Enabled	CPU	3	May 11, 2023, 9:20 AM
BS-DIST-DB-22	Enabled	Net-SNMP: Physical Memory - Cache Memory	0	–

NOTE: The **Anomalies** widget appears only if you have at least one device in the selected service that has anomaly detection enabled. For more information about enabling anomaly detection, see the ***Machine Learning and Anomaly Detection*** manual.

NOTE: Machine learning and anomaly detection are available only in SL1 Premium solutions. To upgrade, contact ScienceLogic Customer Support.

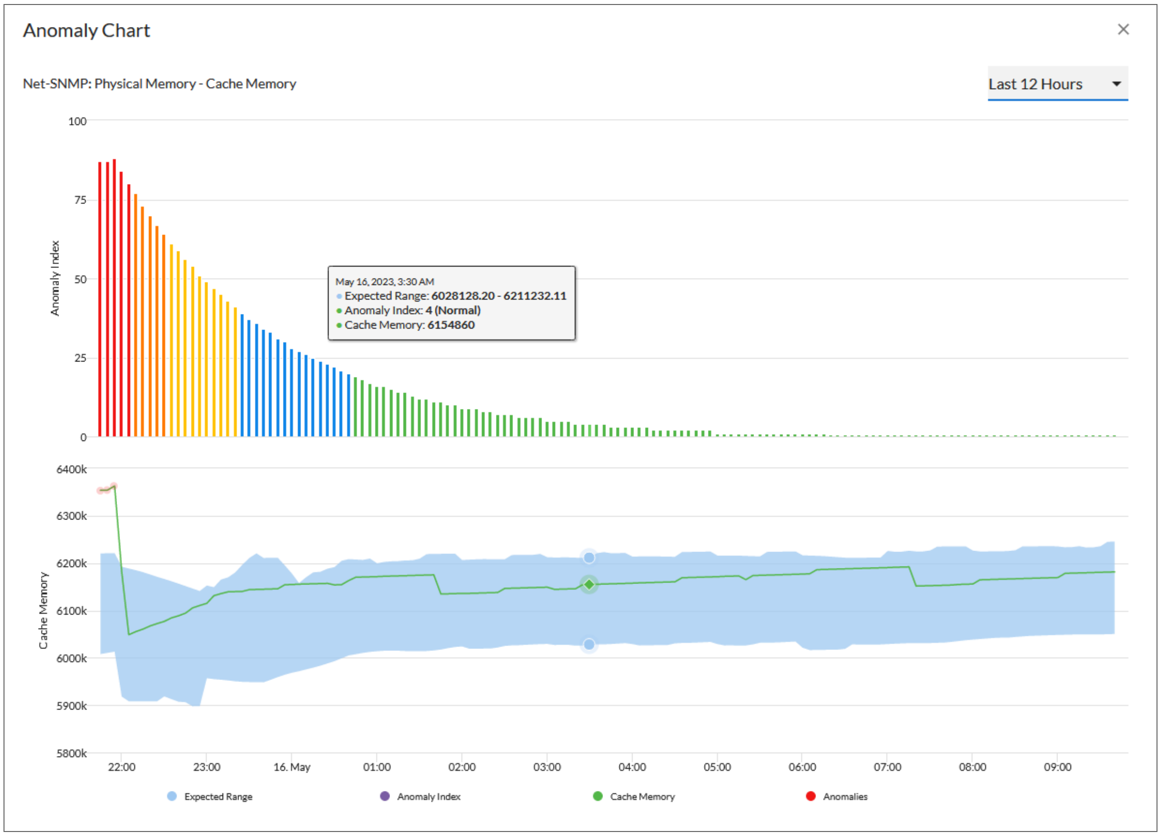
TIP: You can filter the items on this inventory page by typing filter text or selecting filter options in one or more of the filters found above the columns on the page. For more information, see "Filtering Inventory Pages" in the ***Introduction to SL1*** manual.

On the **[Anomalies]** widget of the **Device Investigator**, you can view a list of devices that are enabled for anomaly detection. Each device has a set of graphs that tracks the anomaly detection data for that device.

You can view these graphs by clicking the **Expand** icon (⌄) next to the device or the metric for the device. The **Anomaly Chart** modal appears, displaying the "Anomaly Index" chart above the chart for the specified metric you are monitoring.

The "Anomaly Index" chart displays a graph of values from 0 to 100 that represent how far the real data for a metric diverges from its normal patterns. The lines in the chart are color-coded by the level of event that gets triggered as the data diverges further and further. You can define the thresholds for the Anomaly Index, and whether those values generate alerts, on the **Machine Learning Thresholds** page (Machine Learning > Thresholds). For more information, see ***Enabling Alerts and Thresholds for the Anomaly Index***.

In the second graph, the blue shape represents the expected value range for the selected device metric over the given time period, the green line indicates the actual values that SL1 collected over that time period, and the small red dots at top left represent the anomalies where the actual value fell outside of the expected range.



Anomaly Chart

Net-SNMP: Physical Memory - Cache Memory

Last 12 Hours

May 16, 2023, 3:30 AM
- Expected Range: **6028128.20 - 6211232.11**
- Anomaly Index: **4 (Normal)**
- Cache Memory: **6154860**

TIP: You can hover over a value in one of the charts to see a pop-up box with the **Expected Range** and the metric value. The **Anomaly Index** value also displays in the pop-up box, with the severity in parentheses: Normal, Low, Medium, High, or Very High.

The second graph displays the following data:

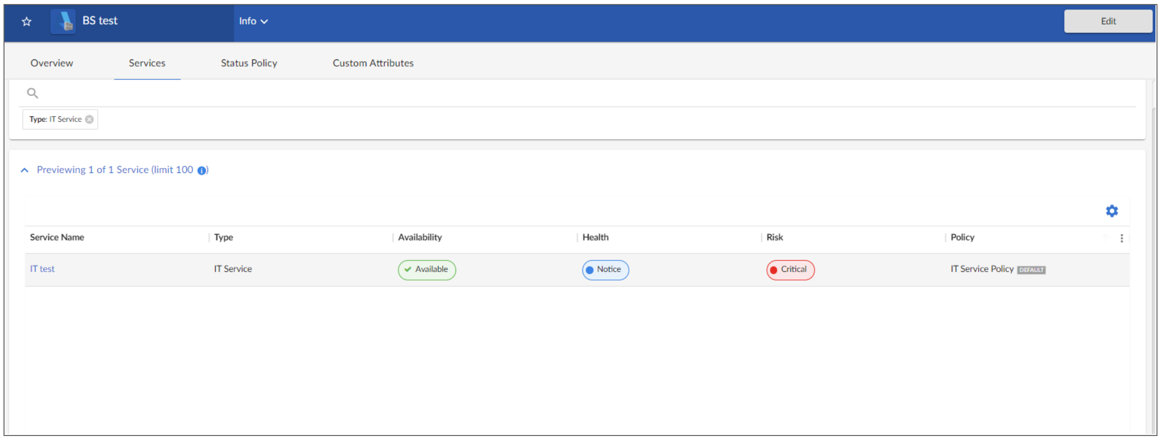
- A blue band representing the range of probable values that SL1 expected for the device metric.
- A green line representing the actual value for the device metric.
- A red dot indicating anomalies where the actual value appears outside of the expected value range.

TIP: You can use the time span filter on the **Anomalies** widget to adjust the time span of anomalies that appears in the graph. The default filter is *Last 24 hours*, but you can select a time span ranging from *Last Hour* up to *Last 2 Years*. You can also zoom in on a shorter time frame by clicking and dragging your mouse over the part of the chart representing that time frame, and you can return to the original time span by clicking the **[Reset zoom]** button.

The Services/Devices Tab

For business services and IT services, the **[Services]** tab displays the services currently being used in the service; for device services, the **[Devices]** tab displays devices included in the service.

You can edit the query at the top of the tab to control which services or devices appear on the page when you click **[Search]**.



Type: IT Service

Previewing 1 of 1 Service (limit 100)

Service Name	Type	Availability	Health	Risk	Policy
IT test	IT Service	✓ Available	● Notice	● Critical	IT Service Policy DEFAULT

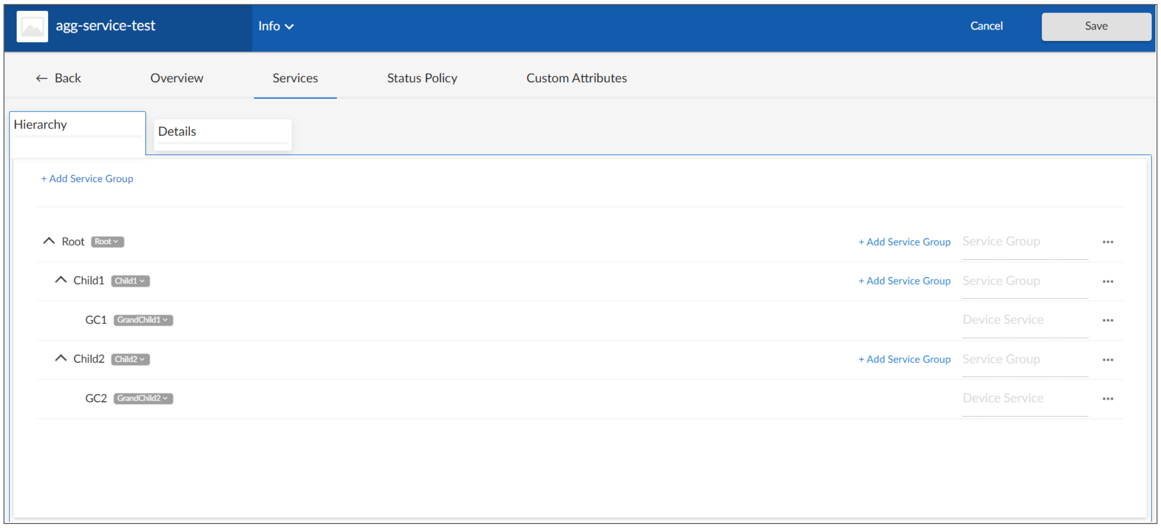
NOTE: The "ANY" search option is disabled on the **[Services]** or **[Devices]** tab.

NOTE: For more information about the **[Services]** or **[Devices]** tab for business services, IT services, and device services, see the section on ***Creating Business, IT, or Device Services***.

For Custom Service Models, the **[Services]** tab displays two tabs:

- ***Hierarchy***. Enables you to edit your service hierarchy by adding, moving, or deleting service groups.
- ***Details***. Includes two sub-tabs:
  - *Overview*. Enables you to update the managing organization and visible organizations for the individual levels within your service model hierarchy.
  - *Status Policy*. Enables you to create a new status policy or apply an existing status policy for the individual levels within your service model hierarchy.

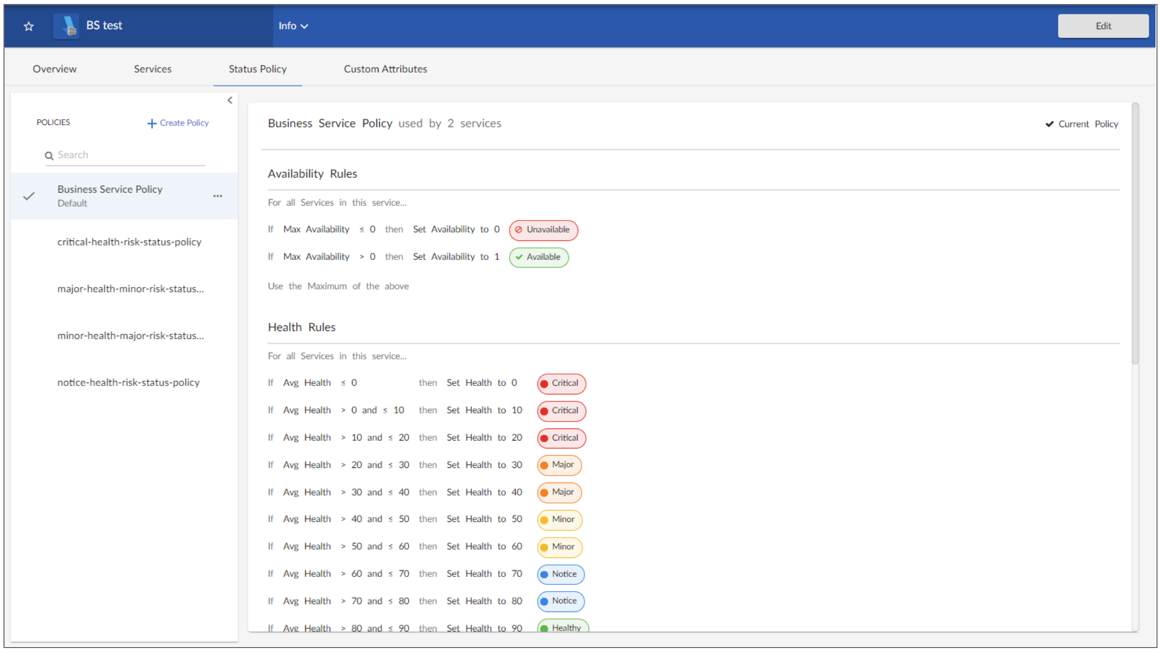
To make changes on either of these tabs, click **[Edit]**, make your updates, and then click **[Save]**.



> **NOTE:** For more information about the **[Services]** tab for service models, see the section on ***Creating a Custom Service Model***.

The Status Policy Tab

The **[Status Policy]** tab displays a list of all the policies of that service type that are currently in the system and that can be chosen to associate with the service being viewed.



Business Service Policy used by 2 services

Availability Rules

For all Services in this service...

If Max Availability ≤ 0 then Set Availability to 0 Unavailable

If Max Availability > 0 then Set Availability to 1 Available

Use the Maximum of the above

Health Rules

For all Services in this service...

If Avg Health ≤ 0 then Set Health to 0 Critical

If Avg Health > 0 and ≤ 10 then Set Health to 10 Critical

If Avg Health > 10 and ≤ 20 then Set Health to 20 Critical

If Avg Health > 20 and ≤ 30 then Set Health to 30 Major

If Avg Health > 30 and ≤ 40 then Set Health to 40 Major

If Avg Health > 40 and ≤ 50 then Set Health to 50 Minor

If Avg Health > 50 and ≤ 60 then Set Health to 60 Minor

If Avg Health > 60 and ≤ 70 then Set Health to 70 Notice

If Avg Health > 70 and ≤ 80 then Set Health to 80 Notice

If Avg Health > 80 and ≤ 90 then Set Health to 90 Healthy

On this tab, you can change the policy used by a service, and you can also create a new service policy. A **Default** label appears next to the default policies.

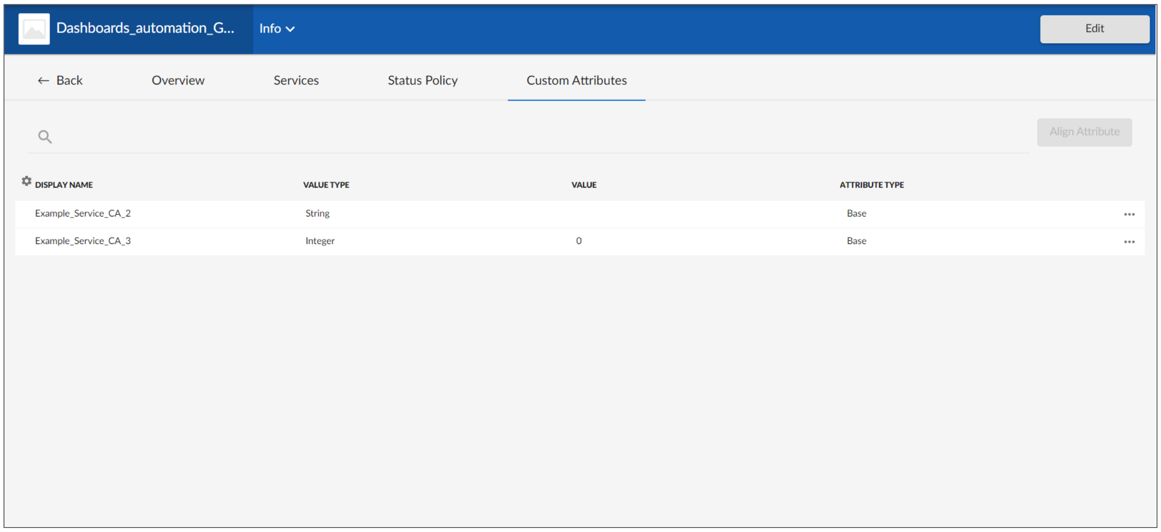
> NOTE: For more information about selecting or changing a service policy, see the section on *Selecting a Service Policy*. For more information about creating a new service policy, see the section on *Creating a Service Policy*.

Depending on the thresholds you configured on the **Business Services Thresholds** page (Business Services > Thresholds), SL1 generates an alert message if a threshold is crossed.

> NOTE: For more information about thresholds, see the section on *Managing Service Thresholds*.

The Custom Attributes Tab

The **[Custom Attributes]** tab displays a list of all of the custom attributes that are aligned with your service. On this tab, you can align additional custom attributes to the service, edit the values for the custom attributes, and unalign custom attributes from the service.



DISPLAY NAME	VALUE TYPE	VALUE	ATTRIBUTE TYPE	
Example_Service_CA_2	String		Base	•••
Example_Service_CA_3	Integer	0	Base	•••

Custom Attributes are customized name-value pairs. You can use custom attributes to add custom fields to services. In SL1, you can create and update custom attributes via the API, in configuration Dynamic Applications, and on the **Custom Attributes** page (Manage > Custom Attributes).

You can use custom attributes when importing services from an integrated system to handle incoming properties that are not defined in SL1.

There are two categories of custom attributes:

- **Base Custom Attributes**. Base custom attributes for services are aligned to all services. Therefore, all base custom attributes in your SL1 system that have a ***Resource Type*** of *Service* will appear on the **[Custom Attributes]** tab for all services. You can edit the value of a base custom attribute for a particular service, but you cannot unalign a base custom attribute from a service.
- **Extended Custom Attributes**. Extended custom attributes that have a ***Resource Type*** of *Service* can be aligned individually to one or more services. For example, you could align an extended custom attribute only to those services to which the custom field applies. You can also edit an extended attribute value for a particular service or unalign an extended custom attribute from a service.

From the **[Custom Attributes]** tab, you can click the **[Edit]** button to do the following:

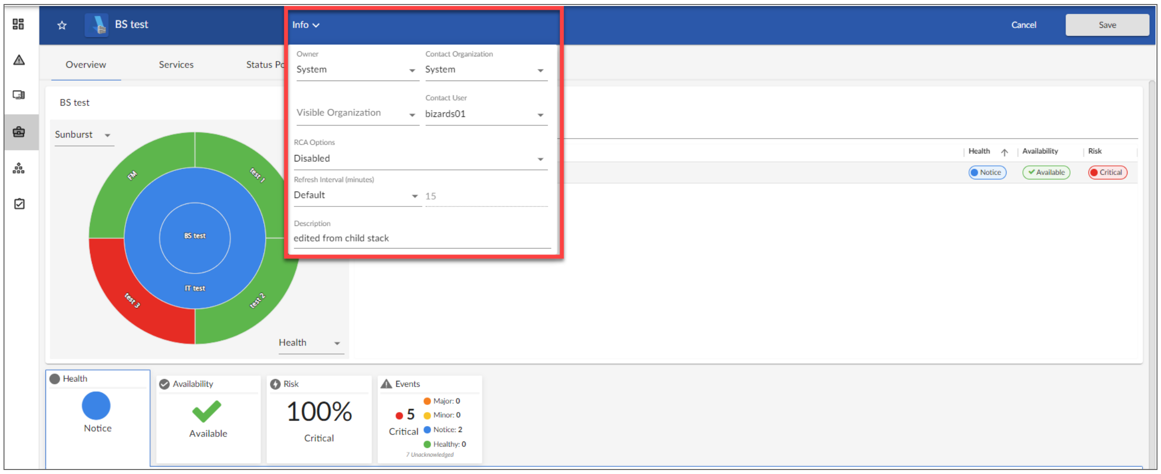
- Click **[Align Attribute]** to align an extended custom attribute to the service and define its value.
- Click the **Actions** button (···) and then select *Edit Attribute* to edit an attribute value.
- Click the **Actions** button (···) and then select *Unalign Attribute* to unalign an extended custom attribute.

NOTE: Custom attributes cannot be used in dashboards for business services.

NOTE: For more information about custom attributes, see the "Custom Attributes" chapter in the ***Device Management*** manual.

The Info Drawer on the Default Service Investigator Page

The **Info** drawer at the top of the **Service Investigator** page displays the following:


Owner: System
Contact Organization: System
Visible Organization
Contact User: bizards01
RCA Options: Disabled
Refresh Interval (minutes): Default 15
Description: edited from child stack

- ***Owner***. The organization that owns the service.
- ***Contact Organization***. The organization that should be contacted with any questions about the service.

- ***Visible Organizations***. A list of organizations from which you can select devices to use in Device Services or IT Services. For example, if you selected Acme for this field, then any service that is aligned with Acme can access devices in the Acme organization. This implies the devices can be included in IT Services. There are two uses for Visible Organizations:
    1. *Device Services*. Allow the inclusion of devices from the owning organization, as well as the visible organizations.
    2. *IT Services*. Allow the inclusion of Device Services from the owning organization, as well as the visible organizations.
- ***Contact User***. The user who should be contacted with any questions about the service.
- ***RCA Options***. Allows you to enable or disable the Root Cause Analysis feature, an advanced feature for troubleshooting. For more information, see ***Using the Root Cause Analysis Feature***.
- ***Refresh Interval (minutes)***. Allows users with edit permissions to edit the Har Provider's Poll Frequency time. The value allows a minimum of 1 minute and a maximum of 24 hours (in minutes). Default minute value is 15 minutes.
- ***Description***. A description of the service. You can use this field as a metadata tagging field that can be exploited in the search by a parent service. For example, if a collection of Device Services all have a description of "Shared Infrastructure", then an IT Service can search to include every Device Service in the same organization that has a description of "Shared Infrastructure". As you add more "Shared Infrastructure" device services, the IT Service will automatically expand to include them. This makes building service trees quick and self-maintaining, without resorting to rigid service names.
- ***Include devices from visible organizations***. Allows you to include devices from other organizations in a Device Service. Turn the toggle on (blue) to include other organizations' devices; turn it off (gray) to exclude other organizations' devices. This option appears only on the **Service Investigator** page for Device Services.

NOTE: Click the **[Edit]** button to edit the content on all three tabs and to edit the fields on the **Info** drawer. You can also edit the service name and the icon associated with the service. Click **[Save]** to save your changes.

Using the Root Cause Analysis Feature

SL1 users can use the ***Root Cause Analysis*** feature to determine what is causing a service to be unhealthy, troubleshoot that service, and refine their policies.

NOTE: When you enable Root Cause Analysis on a business service or IT service, it will also implicitly enable Root Cause Analysis on any child IT services or device services.

NOTE: Root Cause Analysis is a beta feature.

Enabling Root Cause Analysis

To enable Root Cause Analysis:

1. Click on the **Business Services** icon ( ) to go to the **Business Services** page.
2. Click the ***Name*** of an existing service. The **Service Investigator** page for that service displays.
3. On the **Service Investigator** page, click **[Edit]**.
4. Click the ***Info*** drawer and select one of the following options from the ***RCA Options*** drop-down:

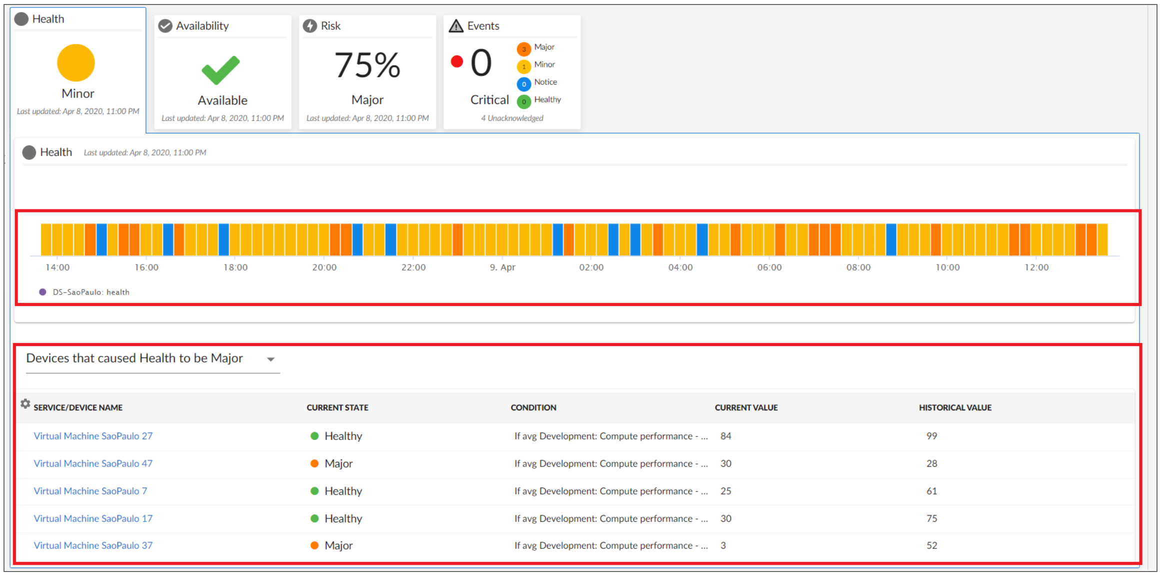
    - *Disabled*. The Root Cause Analysis feature is disabled.
    - *Enabled (contributors only)*. The Root Cause Analysis feature is continuously enabled only for contributing rules and devices. When you select this option, a full analysis will be generated and saved in the time series chart, but it will exclude results from non-contributing rules and devices.
    - *Enabled (next run only)*. The Root Cause Analysis feature is enabled only for the next data collection.
    - *Enabled*. The Root Cause Analysis feature is continuously enabled for all rules and devices. When you select this option, a full analysis will be generated and saved in the time series chart, and it will include results from non-contributing rules and devices.

NOTE: You might experience performance slowdown if Root Cause Analysis is continuously enabled.

5. Click **[Save]**.

Viewing Root Cause Analysis

You can view the Root Cause Analysis for a service's Health, Availability, or Risk metrics by clicking one of the time stamps in the time series chart for that metric. When you do so, a pane appears that explains which child devices or services contributed in the calculation for the resulting Health, Availability, or Risk for the selected time period:



SERVICE/DEVICE NAME	CURRENT STATE	CONDITION	CURRENT VALUE	HISTORICAL VALUE
Virtual Machine SaoPaulo 27	● Healthy	If avg Development: Compute performance - ...	84	99
Virtual Machine SaoPaulo 47	● Major	If avg Development: Compute performance - ...	30	28
Virtual Machine SaoPaulo 7	● Healthy	If avg Development: Compute performance - ...	25	61
Virtual Machine SaoPaulo 17	● Healthy	If avg Development: Compute performance - ...	30	75
Virtual Machine SaoPaulo 37	● Major	If avg Development: Compute performance - ...	3	52

The following columns appear on the Root Cause Analysis pane:

- ***Service/Device Name***. The name of the service or device that contributed to the Health, Availability, or Risk status for the selected time period.
- ***Current State***. The current Health, Availability, or Risk status for the service or device.
- ***Condition***. The equation that is used to determine the Health, Availability, or Risk status for the service or device.
- ***Current Value***. The current Health, Availability, or Risk value for the service or device, as determined by the value of the equation used in the ***Condition*** column.
- ***Historical Value***. The Health, Availability, or Risk value for the service or device for the selected time period, as determined by the value of the equation used in the ***Condition*** column.

TIP: You can click on any of the column heading labels to sort the Root Cause Analysis pane by the values in that column.

Chapter

2

Using the Enhanced Service Investigator

Overview

This chapter describes how to use the enhanced **Service Investigator** page for a particular business, IT, device service, or custom service model.

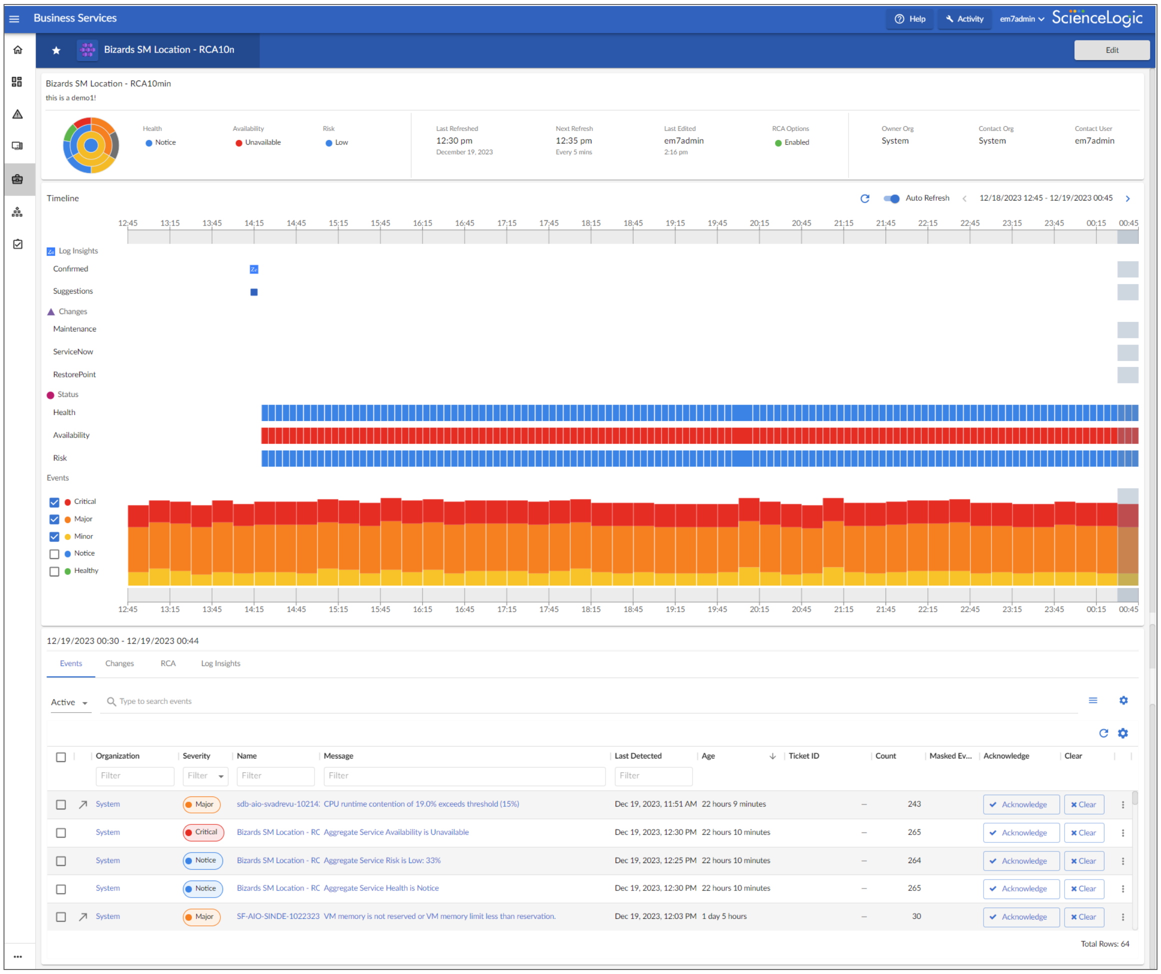
> NOTE: The **Service Investigator** page has two different user interfaces and viewing options depending on the SL1 version you are running:
>
> - *Default Service Investigator*. The default view of the **Service Investigator** page in SL1 version 12.2.0 and earlier.
> - *Enhanced Service Investigator*. The enhanced view of the **Service Investigator** page. This page is disabled by default and requires a minimum SL1 version of 12.2.0 or later, and a minimum of AP2 Biscotti version 8.0.20.
>
> For instructions on how to download and install AP2 Biscotti version 8.0.20, see the ***AP2 Biscotti Release Notes***.
>
> For instructions on how to enable to disable the enhanced **Service Investigator** page, see the section on ***Enabling or Disabling the Enhanced Service Investigator Page and its Elements***.

Use the following menu options to navigate the SL1 user interface:

- To view a pop-out list of menu options, click the menu icon (☰).
- To view a page containing all of the menu options, click the Advanced menu icon (•••).

This chapter covers the following topics:

Viewing the Enhanced Service Investigator



Bizards SM Location - RCA10min
this is a demo1!

Health	Availability	Risk	Last Refreshed	Next Refresh	Last Edited	RCA Options	Owner Org	Contact Org	Contact User
● Notice	● Unavailable	● Low	12:30 pm December 19, 2023	12:35 pm Every 5 mins	em7admin 2:16 pm	● Enabled	System	System	em7admin

12/19/2023 00:30 - 12/19/2023 00:44

□	Organization	Severity	Name	Message	Last Detected	Age	Ticket ID	Count	Masked Ev...	Acknowledge	Clear
□	System	Major	sdb-aio-svadrevu-10214:	CPU runtime contention of 19.0% exceeds threshold (15%)	Dec 19, 2023, 11:51 AM	22 hours 9 minutes	–	243		✓ Acknowledge	✖ Clear
□	System	Critical	Bizards SM Location - RC	Aggregate Service Availability is Unavailable	Dec 19, 2023, 12:30 PM	22 hours 10 minutes	–	265		✓ Acknowledge	✖ Clear
□	System	Notice	Bizards SM Location - RC	Aggregate Service Risk is Low: 33%	Dec 19, 2023, 12:25 PM	22 hours 10 minutes	–	264		✓ Acknowledge	✖ Clear
□	System	Notice	Bizards SM Location - RC	Aggregate Service Health is Notice	Dec 19, 2023, 12:30 PM	22 hours 10 minutes	–	265		✓ Acknowledge	✖ Clear
□	System	Major	SF-AIO-SINDE-1022323	VM memory is not reserved or VM memory limit less than reservation.	Dec 19, 2023, 12:03 PM	1 day 5 hours	–	30		✓ Acknowledge	✖ Clear

Total Rows: 64

NOTE: You must be running SL1 version 12.2.0 or later to view the enhanced **Service Investigator** page. However, this page is disabled by default in SL1 12.2.0. To enable or disable the enhanced **Service Investigator** page, follow the instructions in the section on ***Enabling or Disabling the Service Investigator Page***.

The Sections on the Enhanced Service Investigator Page

The **Service Investigator** page contains the following sections:

- *Overview*. A summary panel at the top of the page that displays organization and system information such as ***Contact Organization***, ***Visible Organization***, and ***Owner***. This information bar also displays a preview of a sunburst chart, which you can click to see a more detailed breakdown of the **Health**, **Availability**, and **Risk** statuses of your devices.
- *Timeline*. A panel that displays swim lanes and bar graphs to show **Historical**, **Change**, **Health**, **Availability**, **Risk**, and **Zebrium** events. Swim lanes are visual flowcharts that show a process from start to finish for an event.
- *Events* . An interactive pane that displays the ***Events***, ***Changes***, **RCA** (Root Cause Analysis), and ***Log Insights*** related to the service you have selected.

Each of these sections are described in the following sections.

The Overview Panel

The overview panel on the enhanced **Service Investigator** page displays the following information:

- ***Last Refreshed***. Displays the date and timestamp of the most recent system refresh.
- ***Next Refresh***. Displays the timestamp of the next system refresh and its frequency.
- ***Last Edited***. Displays the timestamp of the most recent change made to this service and the username of the last user to edit this service.
- ***RCA Options***. Indicates whether Root Cause Analysis is enabled or disabled for the service.
- ***Owner Org***. The organization that owns the service.
- ***Contact Org***. The organization that should be contacted with any questions about the service.
- ***Contact User***. The user who should be contacted with any questions about the service.

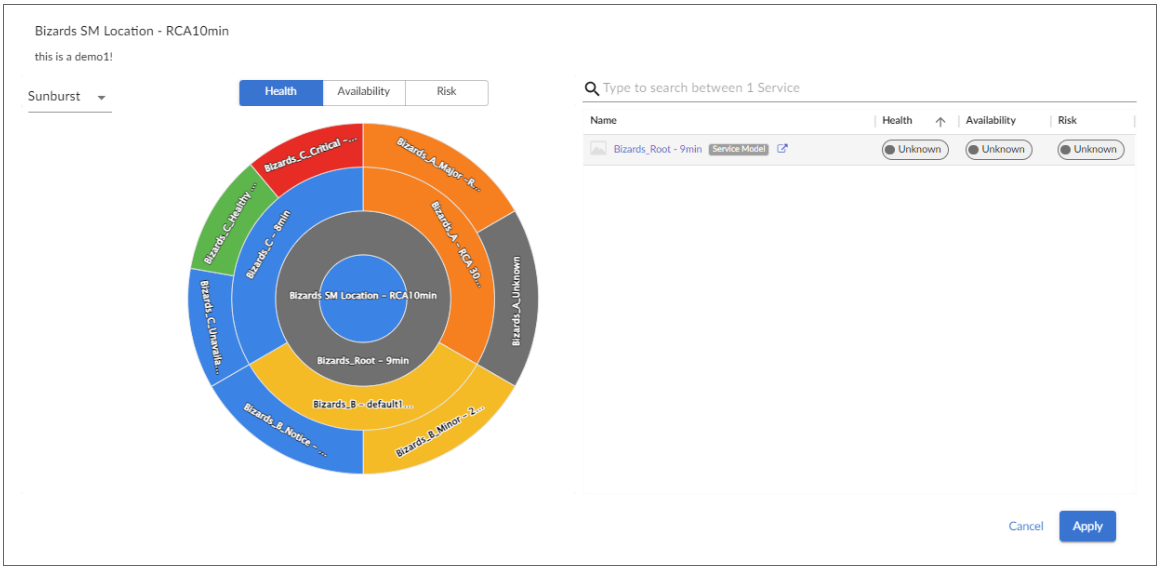
You can click the sunburst chart to see a more detailed breakdown of the ***Health***, ***Availability***, and ***Risk*** statuses of your services. Doing so will open a larger modal that provides different ways to view and filter the statuses of your devices on this particular service.

This diagram window consists of the following viewing options for your services:

- *Sunburst*
- *Map*

Each of these viewing options is described in the following sections.

Sunburst View



Bizards SM Location - RCA10min

this is a demo1!

Name	Health	Availability	Risk
Bizards_Root - 9min Service Model	Unknown	Unknown	Unknown

The overview summary panel displays either a *Sunburst* chart view or a *Map* view of your services. Use the drop-down menu in the top left corner of the window to select which view you want to use.

When you select the *Sunburst* view:

- The sunburst chart displays the current ***Health***, ***Availability***, and ***Risk*** values for the services, as well as for any constituent services or device services that belong to that top-level service. For device services, the sunburst chart includes the device name and health values for any devices that belong to the service. Additionally, this chart indicates the maximum number of constituent services or devices that will be used for computing health, availability, and risk.
- The right panel includes a list of constituent services or devices. Each service in this panel includes icons that represent that service's ***Health***, ***Availability***, and ***Risk*** metrics; devices include icons that represent each device's health value. The right panel also includes a search bar at the top of the panel that enables you to search for specific constituent services or devices.

In the sunburst chart view, the center circle represents the selected service. The selected service drives the context for the page title and **Info** drawer, as well as all the other panels and widgets in the **Overview** section. This means that the right panel and other elements on the page will all reflect the metrics for the service in the center circle of the sunburst.

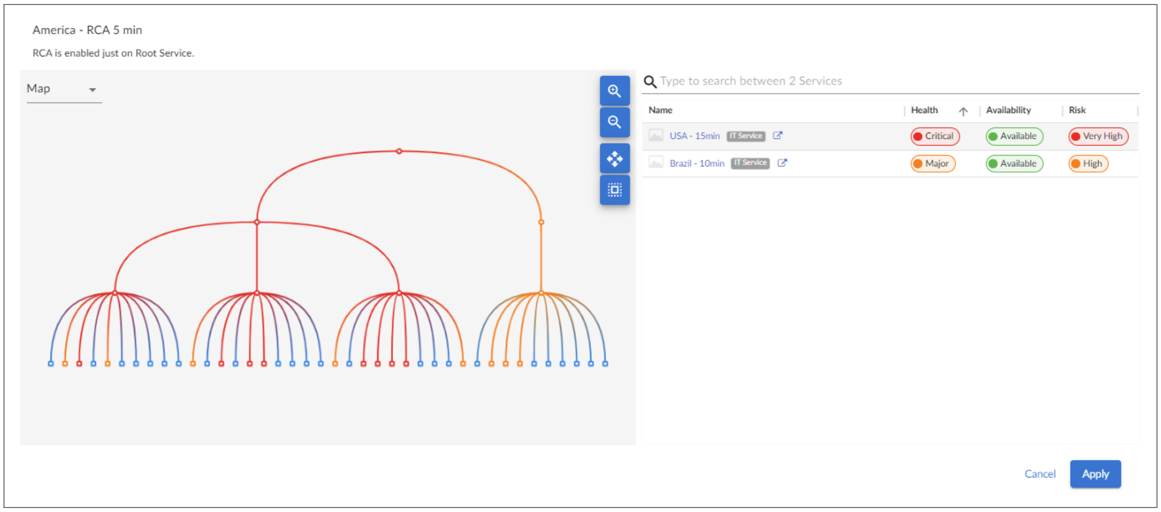
You can navigate through services on the widget in the following ways:

- On the sunburst chart, you can click any constituent IT services or device services in the sunburst to select that service. To return to the parent IT service or business service, click the center circle or click the breadcrumb links that appear in the top-left corner of the window.

- In the right panel, you can click the service name of any of the constituent IT services or device services to select that service. To return to the parent IT service or business service, click the breadcrumb links that appear in the top-left corner of the window.

By default, the sunburst displays the health value for the selected service and its constituent services or devices. To view the current availability or risk value for the selected service, click either the **[Availability]** or **[Risk]** tab above the sunburst chart.

Map View



America - RCA 5 min

RCA is enabled just on Root Service.

Name	Health	Availability	Risk
USA - 15min IT Service	● Critical	● Available	● Very High
Brazil - 10min IT Service	● Major	● Available	● High

The overview summary panel displays either a *Sunburst* chart view or a *Map* view of your services. Use the drop-down menu in the top left corner of the window to select which view you want to use.

When you select the *Map* view:

- The map view displays a map of the service and any constituent services and devices that belong to that top-level service.
- The right panel includes a list of constituent services or devices. Each service in this panel includes icons that represent that service's ***Health***, ***Availability***, and ***Risk*** metrics; devices include icons that represent each device's health value. The right panel also includes a search bar at the top of the panel that enables you to search for specific constituent services or devices.

In the map view, you can click on the top-level service or any of its constituent services or devices. The selected service drives the context for the page title and Info drawer, as well as all the other panels and widgets on the overview summary pane. This means that the right panel, and other elements on the page will all reflect the metrics for the service that you have clicked in the map view.

In the map view, use the following buttons to manipulate the map in the left pane:

🔍: Zoom in on the map.

🔍: Zoom out on the map.

✥: Fit all elements of a map into the viewing pane.

⊡: Center all selected elements of a map in the viewing pane.

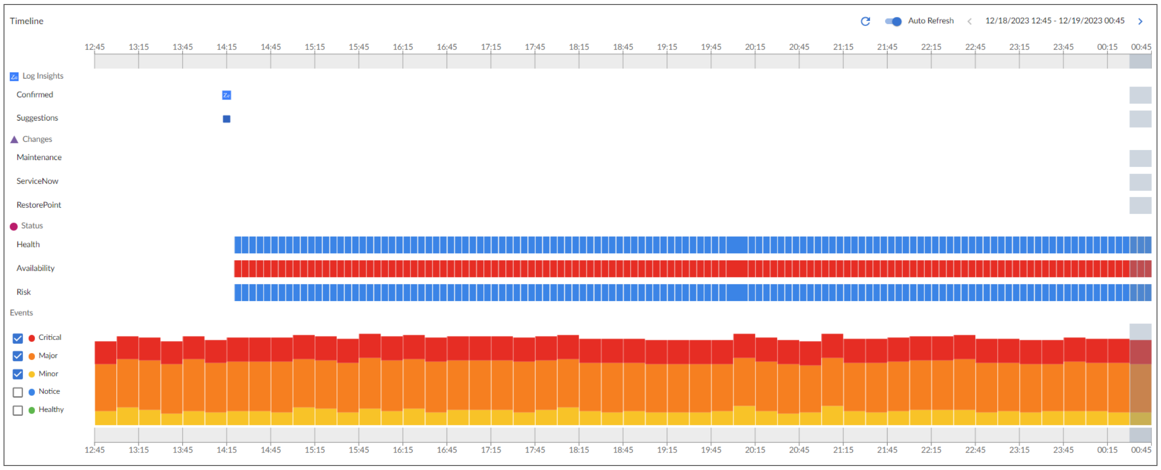
The viewing pane displays the following two types of graphical elements:

1. ***Nodes*** that represent devices, topology elements, and business services defined in SL1. The shape of the node represents its type: *Services*, such as business services, IT services, or device services, are represented by hexagons, while devices are represented by squares. The color of the outline specifies the current state of the node.
2. ***Edges*** are lines that represent the relationships and hierarchies between nodes.

TIP: When you hover over a node, a pop-up **Properties** pane appears with the metadata for that node. Click the **[Go to service]** or **[Go to device]** link at the top of the pane to open the **Investigator** page for that service or device in a new browser window.

The Timeline Panel

The **Timeline** panel displays a graphic that combines swim lanes and bar graphs to show the health, availability, and risk of your events, including Zebrium events. Swim lanes are visual flowcharts that show a process from start to finish for an event. This panel is interactive and allows you to select any time range on the graph to display the **Changes**, **Health**, **Availability**, and **Risk** information to your device or service in that selected time range.



The **Timeline** panel consists of the following tabs:

- *Log Insights*
- *Changes*
- *Status*
- *Events*

Log Insights Tab

You can view Zebrium suggestions and alerts in the **[Log Insights]** tab of the **Timeline** panel on the enhanced **Service Investigator** page. To use this feature, you will need to set up the connection between Zebrium and SL1. For more information, see *Configuring the Zebrium Connector for SL1*.

The **[Log Insights]** tab contains two fields:

- *Confirmed*
- *Suggestions*

Confirmed Alerts

Confirmed alerts in the **[Log Insights]** tab of the **Timeline** panel represent log events that Zebrium has collected for your service or device. In Zebrium, they appear as categorized events under *Accepted/Custom*. These logs typically contain metadata such as title, description, and so forth and use machine learning to analyze and collect event logs that show abnormalities.

Suggested Alerts

Suggested alerts in the **[Log Insights]** tab of the **Timeline** panel contains metadata such as tile, description, and so forth; a root cause report, which is a set of correlated log lines that help to explain a problem; and a suggested alert rule consisting of one or two log event types that form the signature for this type of alert.

As logs are ingested, the machine learning from Zebrium analyzes your system or device logs for event patterns such as abnormally correlated rare and error events from across all log streams. When it detects one of these "abnormal" clusters, it will generate a suggested alert, which allows you to choose if you want these events to be recorded as event logs in the future.

You can choose to either accept or reject a suggested alert.

- If you accept a suggested alert, you can edit the metadata and alert rule. You can also decide on the action to take if the same kind of alert occurs again, such as sending a notification to Slack, email, or another communications platform.
- If you reject a suggested alert, the same kind of alert will not be recorded in the future and it will not offer you the options to either "accept" or "reject" it.

Changes Tab

The **[Changes]** tab on the **Timeline** panel is available to customers who have purchased Configuration and Change Management as part of their SL1 Standard or Premium subscription. This tab displays a list of events that are created when PowerFlow pulls change data from ServiceNow or Restorepoint, including both active and cleared change events.

This **[Changes]** tab contains the following fields:

- *Maintenance*
- *ServiceNow*
- *Restorepoint*

Maintenance

The ***Maintenance*** field indicates whether a device is in maintenance mode. Devices in maintenance have start and end times, which are determined by a start event and an end event for each change data. The device's ***Collection State*** field will change from *Active* to *Maintenance*, and then back to *Active* once maintenance reaches its end time.

You can see a device's collection state in the ***Collection State*** column on the **Events** page. To see a list of all devices in maintenance mode and their start times, end times, and duration, go to the **Schedules** tab of the **Device Investigator** page.

NOTE: For more information, see the "Viewing the Schedule Manager" topic in the ***Device Management*** manual.

ServiceNow

The ***ServiceNow*** field shows a visual representation of all SL1 events that are synced with ServiceNow incidents in a specific time range.

NOTE: You can permanently enable or disable ***ServiceNow*** swim lane diagrams on the **Timeline** panel through the nextui.conf file, or temporarily enable or disable them through GraphQL mutations. To do so, follow the instructions outlined in the ***Enabling or Disabling the Service Investigator Page*** section.

NOTE: For more information on how to monitor a ServiceNow instance with SL1 events, see the "What Does the ServiceNow Base Pack PowerPack Monitor" chapter in the ***Using the ServiceNow Base Pack PowerPack*** manual.

Restorepoint

The ***Restorepoint*** field shows a visual representation of all SL1 events on devices that are synced between SL1 and Restorepoint. The events are created when PowerFlow pulls change data from Restorepoint.

NOTE: You can permanently enable or disable ***Restorepoint*** swim lane diagrams on the **Timeline** panel through the nextui.conf file, or temporarily enable or disable them through GraphQL mutations. To do so, follow the instructions outlined in the ***Enabling or Disabling the Service Investigator Page*** section.

NOTE: For more information, see the ***Restorepoint SyncPack*** manual.

Status Tab

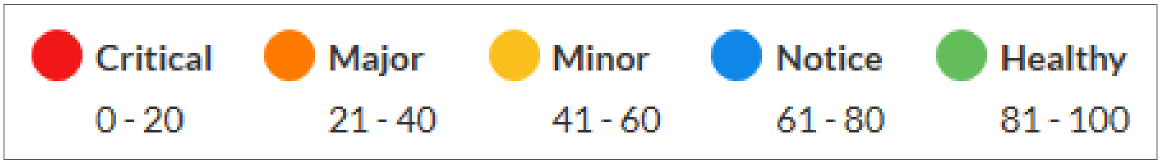
The **[Status]** tab shows the health, availability, and risk status for your service or device. You can select any time range on the graph in the **Timeline** panel to open a pop-over modal that displays the ***Health***, ***Availability***, and ***Risk*** information specific to your device or service.

- *Health*
- *Availability*
- *Risk*

Health

The ***Health*** field displays device or service health over a period of time.

This field indicates the current status of a device service—for example, the rate of processing or throughput for the devices in the service. In the case of SL1 Database Servers, the "Rows Behind" value can provide a good measure of how effectively the Database Server is processing data from Data Collectors. ***Health*** is represented by a color-coded "severity" icon that corresponds to a numerical value between 0 and 100. For example, the ***Health*** value could indicate when a device is intermittently unavailable because of a power problem, thereby falling below the required level of performance. ***Health*** uses the following icons:

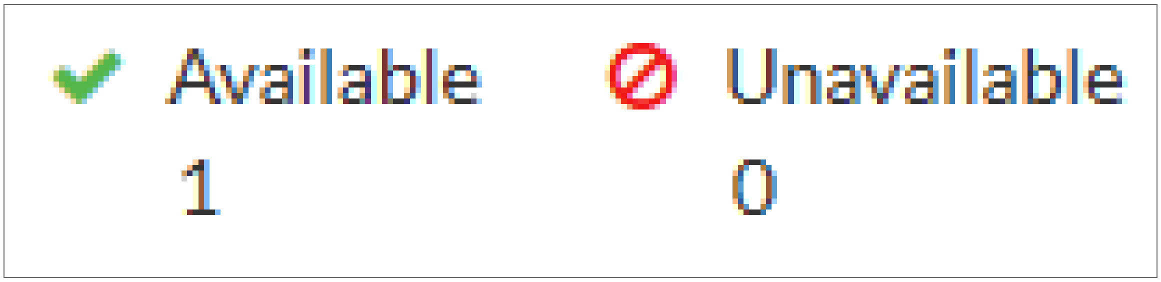


🔴 Critical	🟠 Major	🟡 Minor	🔵 Notice	🟢 Healthy
0 - 20	21 - 40	41 - 60	61 - 80	81 - 100

Availability

The ***Availability*** field shows the availability status of your device or service over a period of time.

The availability of a device service is derived from the availability rules. This may or may not be linked to device availability. A service or device is considered unavailable if SL1 is not able to collect data from the device or service, or if a device is usable or not usable. A value of *0* means a device or service is unavailable, and a value of *1* means a device is available. Availability uses the following icons:

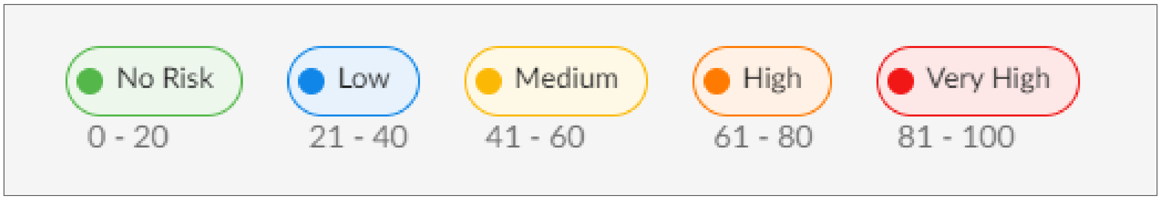


Risk

The ***Risk*** field in the **[Log Insights]** tab of the **Timeline** panel displays the risk status of your device or service over a period of time.

This field measures the risk status of your device or service using a percentage value between 0 and 100 that indicates how close a service is to being in an undesirable state. Use risk for data that is known to cause issues if left unchecked, such as critical events, swap usage, or low database logging space. The safest possible risk value is 0%, while the worst risk value is 100%.

These values are computed in this order because SL1 uses ***Availability*** values to compute ***Health***, and then uses both ***Availability*** and ***Health*** values to compute ***Risk***.



Events Tab

The **[Events]** tab contains five fields that displays various data points regarding events from your devices or services, depending on the tab you have selected.

The Events Pane

The **Events** pane contains the following tabs:

- *Events*
- *Changes*
- *RCA*
- *Log Insights*
- *Metric Anomalies*

Events Tab

The **[Events]** tab displays a list of events for the selected service or device. This tab has much of the same functionality as the **Events** page.

> NOTE: The **[Events]** tab in the **Events** pane at the bottom of the **Service Investigator** page displays the number of events of each severity type, after masking, that are currently impacting the service. When opened, the **[Events]** tab lists all events impacting the service, including masked events.

You can perform the following action from the **[Events]** tab:

- Use the drop-down menu to choose which type of change events display in the widget: *Active* or *Cleared*.

  > NOTE: If you select *Active*, SL1 will display all events that are older than 24 hours. If you select *Cleared*, SL1 will display all events that were created within the last 24 hours.

- Use the search field to search for specific events.
- For events that are aligned to devices, click the arrow icon (↗) next to the event to open the **Device Summary** window, which displays the following panes:
  - ***Tools***. A set of network diagnostic tools or user-initiated actions that you can run on the device associated with the event. Click the search bar to search for a tool or action to run, or click one of the default tools or actions that are available based on the device type and your user permissions.
  - ***Vitals***. A widget displaying the past 24 hours of CPU and memory usage for the device related to the event. You can zoom in on a shorter time frame by clicking and dragging, and you can go back to the original timespan by clicking the **[Reset zoom]** button.
  - ***Logs***. A list of the log entries from the device's log file, sorted from newest to oldest by default.
- View the **Organizational Summary** page for the organization aligned with the event by clicking the link in the ***Organization*** column.
- View the **Service Investigator** or **Device Investigator** page for the service or device aligned with the event by clicking the link in the ***Name*** column.
- View the **Event Investigator** page for the event by clicking the link in the ***Message*** column.
- View or edit event notes by clicking the **Note** icon (⊞) in the ***Event Note*** column or by clicking the **[Actions]** button (···) and selecting *Edit Event Note*. Event notes contain event definitions, probable causes, and resolutions for the event, along with a text field where you can add more information about the event or the service or device you are monitoring.
- View more information about masked events by clicking the magnifying glass icon (🔍) or the **Masked** link in the ***Masked Events*** column. Masked events are related events that occur in quick succession on a single

device or service that are rolled up and posted together under one event description, with only the highest severity event displayed.

- Acknowledge the event by clicking the **[Acknowledge]** button. When you acknowledge an event, you let other users know that you are aware of that event, and you are working on a response.
- Clear an event by clicking the **[Clear]** button. When you clear an event, you let other users know that the event has been addressed.
- Create a ticket from the event.
- View the event policy.
- View a log of automations that have occurred for the event by clicking the **[Actions]** icon (⋯) and selecting *View Automation Actions*.
- Select multiple events for action using the check boxes next to the events.

NOTE: For more information about events, see the ***Events*** manual.

Changes Tab

The **[Changes]** tab displays the number of active change events that are impacting the service. Events on this tab will automatically clear after 30 minutes.

NOTE: The **[Changes]** tab is available if you have purchased Configuration and Change Management as a part of your SL1 Standard or Premium subscription. This tab displays a list of events that are created when PowerFlow pulls change data from ServiceNow or Restorepoint, including both active and cleared change events. For more information on how to configure, enable, or disable the **[Changes]** tab on the **Events** pane, see the section on ***Enabling and Disabling the Service Investigator and its Elements***.

You can perform the following actions on the **[Changes]** tab:

- Use the drop-down menu to choose which type of change events display in the widget: *Active* or *Cleared*.

  NOTE: If you select *Active*, SL1 will display all events that are older than 24 hours. If you select *Cleared*, SL1 will display all events that were created within the last 24 hours.

- Filter and search for events by their date; either by 5, 7, 14, 30 days, or more than 30 days.
- Use the ***Search*** field to search for specific change events.
- For active events that are aligned to devices, click the arrow icon (↗) next to the event to open the **Device Summary** window, which displays the following panes:

- ○ ***Tools***. A set of network diagnostic tools or user-initiated actions that you can run on the device associated with the event. Click the search bar to search for a tool or action to run, or click one of the default tools or actions that are available based on the device type and your user permissions.
- ○ ***Vitals***. A widget displaying the past 24 hours of CPU and memory usage for the device related to the event. You can zoom in on a shorter time frame by clicking and dragging, and you can go back to the original timespan by clicking the **[Reset zoom]** button.
- ○ ***Logs***. A list of the log entries from the device's log file, sorted from newest to oldest by default.

- View the **Organizational Summary** page for the organization aligned with an active event by clicking the link in the ***Organization*** column.
- View the **Service Investigator** or **Device Investigator** page for the service or device aligned with an active event by clicking the link in the ***Name*** column.
- View the **Event Investigator** page for an active event by clicking the link in the ***Message*** column or the ***Event ID*** column.
- For ServiceNow integrations, view the ServiceNow ticket associated with an active event by clicking the link in the ***Ticket ID*** column.
- For ServiceNow integrations, view the ServiceNow ticket associated with a cleared event by clicking the link in the ***External Ticket*** column.
- Acknowledge an active event by clicking the **[Acknowledge]** button. When you acknowledge an event, you let other users know that you are aware of that event, and you are working on a response.
- Clear an active event by clicking the **[Clear]** button. When you clear an event, you let other users know that the event has been addressed.
- Create a ticket from an active event.
- Align an event to an existing ticket.
- View the event policy for an active event.
- Select multiple active events for action using the check boxes next to the events.

RCA Tab

The **[RCA]** tab displays the Root Cause Analysis of a device or service and shows what is causing either one to be unhealthy based on the **Status Policy**.

NOTE: For more information about enabling Root Cause Analysis for a service, see the section on *Using the Root Cause Analysis Feature*.

The following columns appear on the **[RCA]** tab:

- ***Service/Device Name***. The name of the service or device that contributed to the health, availability, or risk status for the selected time period.
- ***Current State***. The current Health, Availability, or Risk status for the service or device.

- ***Condition***. The equation that is used to determine the Health, Availability, or Risk status for the service or device.
- ***Current Value***. The current Health, Availability, or Risk value for the service or device, as determined by the value of the equation used in the ***Condition*** column.
- ***Historical Value***. The historical Health, Availability, or Risk value for the service or device for the selected time period, as determined by the value of the equation used in the ***Condition*** column.
- ***Timestamp***. The date and time the root cause analysis was collected from the service or device.

TIP: You can click on any of the column heading labels to sort the **[RCA]** tab by the values in that column.

Log Insights Tab

The **[Log Insights]** tab displays a list of Zebrium events.

You can view Zebrium suggestions and alerts in the **[Log Insights]** tab of the **Events** pane on the enhanced **Service Investigator** page. To use this feature, you will need to set up the connection between Zebrium and SL1. For more information, see *Configuring the Zebrium Connector for SL1*.

You can perform the following actions on the **[Log Insights]** tab:

- Use the drop-down menu to choose which type of change events display in the tab: *Active Events* or *Cleared Events*.

> **NOTE:** If you select *Active*, SL1 will display all events that are older than 24 hours. If you select *Cleared*, SL1 will display all events that were created within the last 24 hours.

- Filter and search for Zebrium events by their date: either by 5, 7, 14, 30, or more than 30 days.
- Use the ***Search*** field to search for specific change events.
- For active events that are aligned to devices, click the arrow icon (↗) next to the event to open the **Device Summary** window, which displays the following panes:
  - ***Tools***. A set of network diagnostic tools or user-initiated actions that you can run on the device associated with the event. Click the search bar to search for a tool or action to run, or click one of the default tools or actions that are available based on the device type and your user permissions.
  - ***Vitals***. A widget displaying the past 24 hours of CPU and memory usage for the device related to the event. You can zoom in on a shorter time frame by clicking and dragging, and you can go back to the original timespan by clicking the **[Reset zoom]** button.
  - ***Logs***. A list of the log entries from the device's log file, sorted from newest to oldest by default.

- View the **Organizational Summary** page for the organization aligned with an active Zebrium event by clicking the link in the ***Organization*** column.
- View the **Service Investigator** or **Device Investigator** page for the service or device aligned with an active Zebrium event by clicking the link in the ***Name*** column.
- View the **Event Investigator** page for an active Zebrium event by clicking the link in the ***Message*** column.
- For ServiceNow integrations, view the ServiceNow ticket associated with an active event by clicking the link in the ***Ticket External Reference*** column.
- For ServiceNow integrations, view the ServiceNow ticket associated with a cleared event by clicking the link in the ***External Ticket*** column.
- Acknowledge an active event by clicking the **[Acknowledge]** button. When you acknowledge a Zebrium event, you let other users know that you are aware of that event, and you are working on a response.
- Clear an active Zebrium event by clicking the **[Clear]** button. When you clear a Zebrium event, you let other users know that the event has been addressed.
- Create a ticket from an active Zebrium event.
- View the event policy for an active Zebrium event.
- Select multiple active Zebrium events for action using the check boxes next to the events.

Metric Anomalies Tab

The **[Metric Anomalies]** tab displays a list all devices within the selected services that have anomaly detection enabled. If one or more devices within a business, IT, or device service has anomaly detection enabled, the **[Metric Anomalies]** tab will appear in the **Events** pane of the **Service Investigator** page.

NOTE: The **[Metric Anomalies]** tab appears only if you have at least one device in the selected service that has anomaly detection enabled. For more information about enabling anomaly detection, see the ***Machine Learning and Anomaly Detection*** manual.

NOTE: Machine learning and anomaly detection are available only in SL1 Premium solutions. To upgrade, contact ScienceLogic Customer Support.

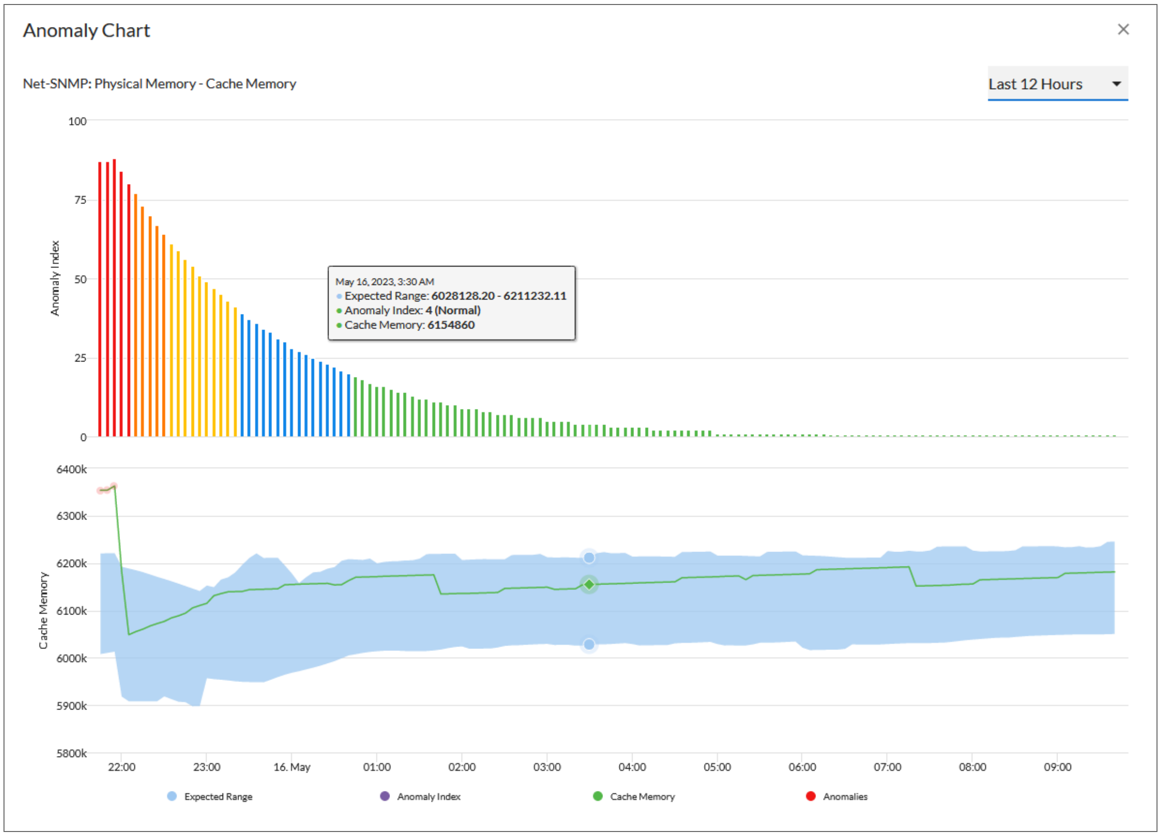
TIP: You can filter the items on this inventory page by typing filter text or selecting filter options in one or more of the filters found above the columns on the page. For more information, see "Filtering Inventory Pages" in the ***Introduction to SL1*** manual.

On the **[Metric Anomalies]** tab of the **Device Investigator**, you can view a list of devices that are enabled for anomaly detection. Each device has a set of graphs that tracks the anomaly detection data for that device.

You can view these graphs by clicking the **Expand** icon (⌄) next to the device or the metric for the device. The **Anomaly Chart** modal appears, displaying the "Anomaly Index" chart above the chart for the specified metric you are monitoring.

The "Anomaly Index" chart displays a graph of values from 0 to 100 that represent how far the real data for a metric diverges from its normal patterns. The lines in the chart are color-coded by the level of event that gets triggered as the data diverges further and further. You can define the thresholds for the Anomaly Index, and whether those values generate alerts, on the **Machine Learning Thresholds** page (Machine Learning > Thresholds). For more information, see ***Enabling Alerts and Thresholds for the Anomaly Index***.

In the second graph, the blue shape represents the expected value range for the selected device metric over the given time period, the green line indicates the actual values that SL1 collected over that time period, and the small red dots at top left represent the anomalies where the actual value fell outside of the expected range.



Anomaly Chart

Net-SNMP: Physical Memory - Cache Memory

Last 12 Hours

May 16, 2023, 3:30 AM
● Expected Range: **6028128.20 - 6211232.11**
● Anomaly Index: **4 (Normal)**
● Cache Memory: **6154860**

TIP: You can hover over a value in one of the charts to see a pop-up box with the **Expected Range** and the metric value. The **Anomaly Index** value also displays in the pop-up box, with the severity in parentheses: Normal, Low, Medium, High, or Very High.

The second graph displays the following data:

- A blue band representing the range of probable values that SL1 expected for the device metric.
- A green line representing the actual value for the device metric.
- A red dot indicating anomalies where the actual value appears outside of the expected value range.

TIP: You can use the time span filter on the **Metric Anomalies** tab to adjust the time span of anomalies that appears in the graph. The default filter is *Last 24 hours*, but you can select a time span ranging from *Last Hour* up to *Last 2 Years*. You can also zoom in on a shorter time frame by clicking and dragging your mouse over the part of the chart representing that time frame, and you can return to the original time span by clicking the **[Reset zoom]** button.

Using the Root Cause Analysis Feature

SL1 users can use the ***Root Cause Analysis*** feature to determine what is causing a service to be unhealthy, troubleshoot that service, and refine their policies.

NOTE: When you enable Root Cause Analysis on a business service or IT service, it will also implicitly enable Root Cause Analysis on any child IT services or device services.

Enabling Root Cause Analysis

To enable Root Cause Analysis:

1. Click on the **Business Services** icon (💼) to go to the **Business Services** page.
2. Click the ***Name*** of an existing service. The enhanced **Service Investigator** page for that service displays.
3. On the enhanced **Service Investigator** page, click **[Edit]**.
4. Select one of the following options from the ***RCA Options*** drop-down field:

    - *Disabled*. The Root Cause Analysis feature is disabled.
    - *Enabled (contributors only)*. The Root Cause Analysis feature is continuously enabled only for contributing rules and devices. When you select this option, a full analysis will be generated and saved in the time series chart, but it will exclude results from non-contributing rules and devices.
    - *Enabled (next run only)*. The Root Cause Analysis feature is enabled only for the next data collection.
    - *Enabled*. The Root Cause Analysis feature is continuously enabled for all rules and devices. When you select this option, a full analysis will be generated and saved in the time series chart, and it will include results from non-contributing rules and devices.

NOTE: You might experience performance slowdown if Root Cause Analysis is continuously enabled.

5. Click **[Save]**.

TIP: You can click on any of the column heading labels to sort the Root Cause Analysis pane by the values in that column.

Enabling or Disabling the Enhanced Service Investigator Page and its Elements

You can permanently enable or disable the new **Service Investigator** page through the NextUI configuration file (nextui.conf) or temporarily enable or disable it through GraphQL mutations.

You can also ***enable the [Changes] tab***, either permanently or temporarily, thought the same methods.

Enabling the Enhanced Service Investigator Page

Permanently Enabling the Enhanced Service Investigator Page

To ***permanently*** enable the enhanced **Service Investigator** page and the ServiceNow or Restorepoint swim lane diagrams on the new **Timeline** widget:

1. Use SSH to access the SL1 appliance.
2. Using vi or another text editor, edit the `/opt/em7/nextui/nextui.conf` file. To do so, enter the following at the shell prompt:

   ```
   sudo vi /opt/em7/nextui/nextui.conf
   ```

3. Add the following line at the bottom of the `nextui.conf` file:

   ```
   _AP2_BUSINESS_SERVICES_INVESTIGATOR=enabled
   AP2_BUSINESS_SERVICES_SERVICENOW=enabled
   AP2_BUSINESS_SERVICES_RESTOREPOINT=enabled
   ```

4. Save your changes, and then restart the NextUI service by running the following command:

   ```
   sudo systemctl restart nextui
   ```

Temporarily Enabling the Enhanced Service Investigator Page

Alternatively, you can ***temporarily*** enable these new features via GraphQL. To do so:

1. Access the GraphiQL interface by typing the URL or IP address for SL1 in a browser, add **/gql** to the end of the URL or IP address, and press **[Enter]**.
2. To temporarily enable the enhanced **Service Investigator** page, type the following mutation in the main query pane:

```
mutation investigatorPage {
  updateFeatureToggle(id: "system:_AP2_BUSINESS_SERVICES_INVESTIGATOR",
```

```
value: "enabled") {
    id
    value
  }
}
```

3. To temporarily enable the ServiceNow swim lane diagrams on the new **Timeline** widget, type the following mutation:

```
mutation updateServiceNowSwimLane {
  updateFeatureToggle(id: "system:_AP2_BUSINESS_SERVICES_SERVICENOW",
value: "enabled") {
    id
    value
  }
}
```

4. To temporarily enable the Restorepoint swim lane diagrams on the new **Timeline** widget, type the following mutation:

```
mutation updateRestorepointSwimLane {
  updateFeatureToggle(id: "system:_AP2_BUSINESS_SERVICES_RESTOREPOINT",
value: "enabled") {
    id
    value
  }
}
```

> **NOTE:** After you have enabled or disabled the enhanced **Service Investigator** page via GraphQL mutations, refresh the page or sign out and sign back into your account. If the NextUI service restarts, all GraphQL feature toggles will also need to restart. To make these changes permanent, modify the `nextui.conf` file as described in the instructions at the beginning of this section.

Disabling The Enhanced Service Investigator Page

Permanently Disabling the Enhanced Service Investigator Page

To ***permanently*** disable the enhanced **Service Investigator** page and the ServiceNow or Restorepoint swim lane diagrams on the new **Timeline** widget:

1. Use SSH to access the SL1 appliance.
2. Using vi or another text editor, edit the `/opt/em7/nextui/nextui.conf` file. To do so, enter the following at the shell prompt:

   ```
   sudo vi /opt/em7/nextui/nextui.conf
   ```

3. Add the following line at the bottom of the `nextui.conf` file:

   ```
   _AP2_BUSINESS_SERVICES_INVESTIGATOR=disabled
   AP2_BUSINESS_SERVICES_SERVICENOW=disabled
   AP2_BUSINESS_SERVICES_RESTOREPOINT=disabled
   ```

4. Save your changes, and then restart the NextUI service by running the following command:

   ```
   sudo systemctl restart nextui
   ```

Temporarily Disabling the Enhanced Service Investigator Page

Alternatively, you can ***temporarily*** disable these new features via GraphQL. To do so:

1. Access the GraphiQL interface by typing the URL or IP address for SL1 in a browser, add /gql to the end of the URL or IP address, and press Enter.
2. To temporarily disable the enhanced **Service Investigator** page, type the following mutation in the main query pane:

```
mutation investigatorPage {
  updateFeatureToggle(id: "system:_AP2_BUSINESS_SERVICES_INVESTIGATOR",
value: "disabled") {
    id
    value
  }
}
```

3. To temporarily disable the ServiceNow swim lane diagrams on the new **Timeline** widget, type the following mutation:

```
mutation updateServiceNowSwimLane {
  updateFeatureToggle(id: "system:_AP2_BUSINESS_SERVICES_SERVICENOW",
value: "disabled") {
    id
    value
  }
}
```

4. To temporarily disable the Restorepoint swim lane diagrams on the new **Timeline** widget, type the following mutation:

```
mutation updateRestorepointSwimLane {
  updateFeatureToggle(id: "system:_AP2_BUSINESS_SERVICES_RESTOREPOINT",
value: "disabled") {
    id
    value
  }
}
```

NOTE: After you have enabled or disabled the enhanced **Service Investigator** page via GraphQL mutations, refresh the page or sign out and sign back into your account. If the NexUI service restarts, all GraphQL feature toggles will also need to restart. To make these changes permanent, modify the `nextui.conf` file as described in the instructions at the beginning of this section.

Configuring and Enabling the Changes Tab

To use the **Changes** tab on the **Events** pane, you must first configure and enable the tab. To do so:

1. Ensure that you are running SL1 version 12.1.0 or later and have *Business Services Base Pack* PowerPack version 2.2.0 or later installed in SL1. For more information, see the chapter on "Installing a PowerPack" in the ***PowerPacks*** manual.
2. Ensure that you are running SL1 PowerFlow Platform version 2.2.2 or greater and one or more of the following PowerPacks, depending on your integration:
   - ***For a ServiceNow integration***:
     - *ServiceNow CMDB*SyncPack version 3.2.0 or later installed in PowerFlow. For more information, see the ***ServiceNow CMDB Synchronization PowerPack*** manual.
     - *ServiceNow Change Management*SyncPack version 3.2.1 or later installed in PowerFlow. For more information, see the ***ServiceNow Change Management Synchronization PowerPack*** manual.
   - ***For a Restorepoint integration***:
     - *Restorepoint* SyncPack version 1.2.0 or later installed in PowerFlow.
     - *Restorepoint* PowerPack version 102 or later installed in SL1.
     - *Restorepoint Automation* PowerPack version 102 or later installed in SL1. For more information, see the ***Restorepoint Integrations*** manual.

3. In SL1, ***create a SOAP/XML credential*** to connect with PowerFlow and make note of its credential ID.

4. ***For a ServiceNow integration***:

   a. In PowerFlow, ***sync SL1 devices with ServiceNow*** and make note of the ***Configuration*** field value in the Sync Devices from SL1 to ServiceNow application.

   b. In SL1, open the "ServiceNow: Send Change Request Event to PowerFlow" Run Book Action (which is included in the *Business Services Base Pack* PowerPack v2.1 and greater) and ***edit the input parameters*** to include the credential ID from step 3 and the ***Configuration*** field value from step 4.

5. ***For a Restorepoint integration***, follow the steps in "Sync Devices with Restorepoint" section in the ***Device Management*** manual.

6. Do one of the following:

   - Permanently enable the **Changes** tab by ***editing the NextUI configuration file*** on your SL1 system.
   - Temporarily enable the **Changes** tab by ***running a GraphQL mutation*** on your SL1 system.

Creating a SOAP/XML Credential for PowerFlow

To create a SOAP/XML credential to connect SL1 with PowerFlow:

1. Follow the steps in the section on "Creating a SOAP/XML Credential for PowerFlow" in the ***Monitoring SL1 PowerFlow*** manual.
2. After saving the credential, make note of the credential ID. This number can be found at the top of the **Edit SOAP/XML Credential** modal or in the ***ID*** column on the **Credentials** page (Manage > Credentials) or **Credential Management** page (System > Manage > Credentials).

Syncing SL1 Devices with ServiceNow

To sync SL1 devices with ServiceNow:

1. Follow the steps in the section on "Running a Device Sync" in the ***ServiceNow CMDB Synchronization*** PowerPack manual.
2. In the **Configuration** pane of the "Sync Devices from SL1 to ServiceNow" application, make note of the value in the ***Configuration*** field.

Editing the Run Book Action

To edit the input parameters in the "ServiceNow: Send Change Request Event to PowerFlow" Run Book Action:

1. Go to the **PowerPack Manager** page (System > Manage > PowerPacks).
2. Locate the *Business Services Base Pack* PowerPack and click its wrench icon (🔧). The **Editing PowerPack** modal appears.
3. In the **Editing PowerPack** modal, click ***Run Book Actions*** in the left Navbar. The **Embedded Run Book Actions** page appears in the modal.

4. Click the wrench icon (🔧) for the "ServiceNow: Send Change Request Event to PowerFlow" Run Book Action. The **Policy Editor** modal appears.
5. In the **Policy Editor** modal, make the following edits to the ***Input Parameters*** field:

   - Replace `<sl1 credential id for powerflow>` with the credential ID of the *SOAP/XML credential you created for PowerFlow*.
   - Replace `<pf config id>` with the ***Configuration*** field value from the *"Sync Devices from SL1 to ServiceNow" application in PowerFlow*.

6. Click **[Save]**, then exit the **Policy Editor** modal.
7. Exit the **Editing PowerPack** modal.

Syncing SL1 Devices with Restorepoint

To sync SL1 devices with Restorepoint:

1. Follow the steps in the section on "Running a Device Sync" in the ***Restorepoint Integrations*** manual.
2. In PowerFlow, open the **Configuration** pane for the "Restorepoint: Sync Devices" application and select *Enable* for the ***restorepoint_config*** field to allow device change detection.
3. Make a note of the ***restorepoint_id*** value on the **Configuration** pane for the "Restorepoint: Sync Devices" application.
4. In SL1, make sure that the same ***restorepoint_id*** value was added to the **Values** column on the **[Attributes]** tab on the **Device Investigator** page for the devices synced from Restorepoint.

Permanently Enabling the Changes Tab

To permanently enable the **Changes** tab using the NextUI configuration file, run the following steps on all appliances, including the Administration Portal, the Database Server, the Data Engine, and the All-In-One Appliance.

To permanently enable the **Changes** tab:

1. Start an SSH session into one of the SL1 appliances.
2. Using vi or another text editor, edit the `/opt/em7/nextui/nextui.conf` file. To do so, enter the following at the shell prompt:

   ```
   sudo vi /opt/em7/nextui/nextui.conf
   ```

3. Add the following line at the bottom of the NextUI configuration file:

   ```
   BUSINESS_SERVICES_CHANGE_EVENTS_TAB=enabled
   ```

4. Save your changes, and then restart the NextUI service by running the following command:

```
sudo systemctl restart nextui
```

5. Repeat steps 1-4 for the remaining SL1 appliances.

Temporarily Enabling the Changes Tab

To temporarily enable the **Changes** tab using GraphQL:

1. To access the GraphiQL interface, type the URL or IP address for SL1 in a browser, add **/gql** to the end of the URL or IP address, and press **[Enter]**. The GraphiQL interface appears.
2. In the main query pane, type the following mutation:

```
mutation updateChangeEventsTab {
       updateFeatureToggle(
               id: "system:BUSINESS_SERVICES_CHANGE_EVENTS_TAB"
               value: "enabled"
       ) {
               id
               value
       }
}
```

> **TIP:** Click the **[Prettify]** button to format the mutation and to add syntax highlighting to make the mutation easier to read. Note that the *Prettify* process removes the `query` syntax if only one query is present in the main query pane.

3. Click the **[Execute Query]** (Play) button. The mutation executes, and the results appear in the pane on the right side.

> **NOTE:** If the **Changes** tab does not appear in SL1 after executing the mutation, refresh the page using the **[F5]** key or by clicking the refresh button in your web browser.

> **NOTE:** For more information about GraphQL, see the GraphQL documentation. For more information about the GraphiQL user interface, see the GraphiQL user interface documentation.

Chapter

3

Resolving Service Issues with Behavioral Correlation

Overview

This chapter describes how to identify and diagnose service issues using Behavioral Correlation in SL1.

Use the following menu options to navigate the SL1 user interface:

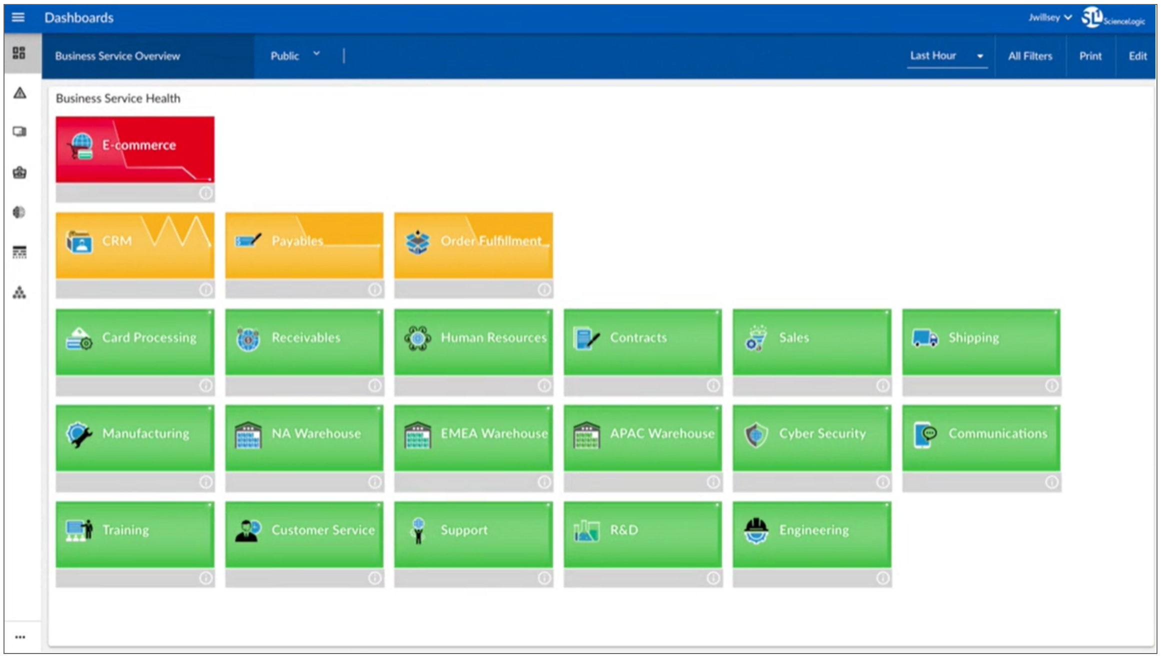
- To view a pop-out list of menu options, click the menu icon (☰).
- To view a page containing all of the menu options, click the Advanced menu icon (⋯).

This chapter covers the following topics:

Understanding Behavioral Correlation in Business Services

SL1 offers an elevated enterprise visibility experience that allows you to monitor and view the health of your services, from an individual device to a larger Business Service view. SL1 has the ability to show a service's behavior and its interactions; in other words, it enables you to analyze a service's ***Behavioral Correlation***. This Behavioral Correlation analysis enables you to implement changes with the hopes of reducing complexity and noise.

To determine a business service's health, you might first look at the **Business Service Overview** dashboard, where the health of a Business Services's components is displayed:



Using the color-coded health widgets in SL1, you can determine which areas of your enterprise are considered healthy and which are not.

Analyzing a Service's Behavioral Correlation

You can determine the Behavioral Correlation for a Business Service by further analyzing the health data of specific areas.

To analyze the health of a specific area:

1. On the **Business Service Overview** dashboard, click the widget of the Business Service area that you want to further analyze. The **[Overview]** tab of the **Service Investigator** displays.

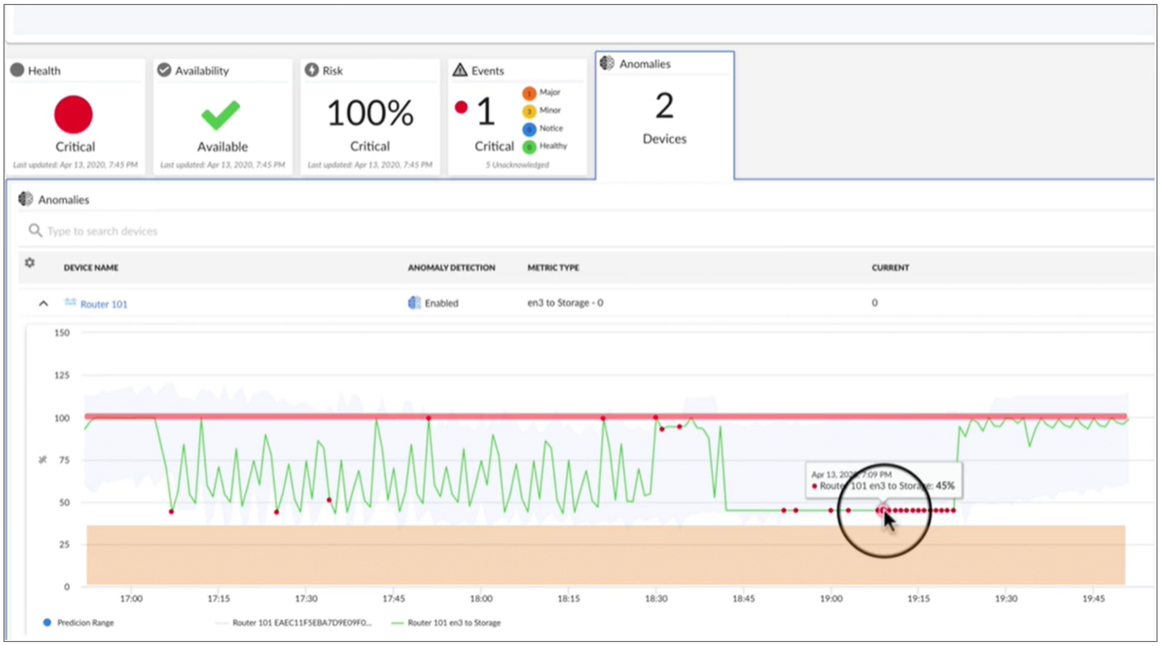
2. Identify problem areas by reviewing the relevant widgets on the **Overview** page. The widgets on this page allow you to sift through any problem sources and pinpoint their various severities. See ***Business Services Investigator*** for more information on widgets and their functionality.

3. By clicking into a widget's source data, you can view the Health, Availability, Risk, Events, Changes, and Anomaly data for a specific area. The machine learning capability of SL1 lets you view and recognize patterns for yourservice's problem source areas.

The majority of service-based issues are displayed in the **[Anomalies]** or **[Events]** tabs of the **Service Investigator** page. SL1's machine learning capability focuses on the services' raw data, as opposed to outdated or static data systems, to capture anomalous patterns.

You can begin using Behavioral Correlation analysis to identify and diagnose service issues by focusing on two key areas:

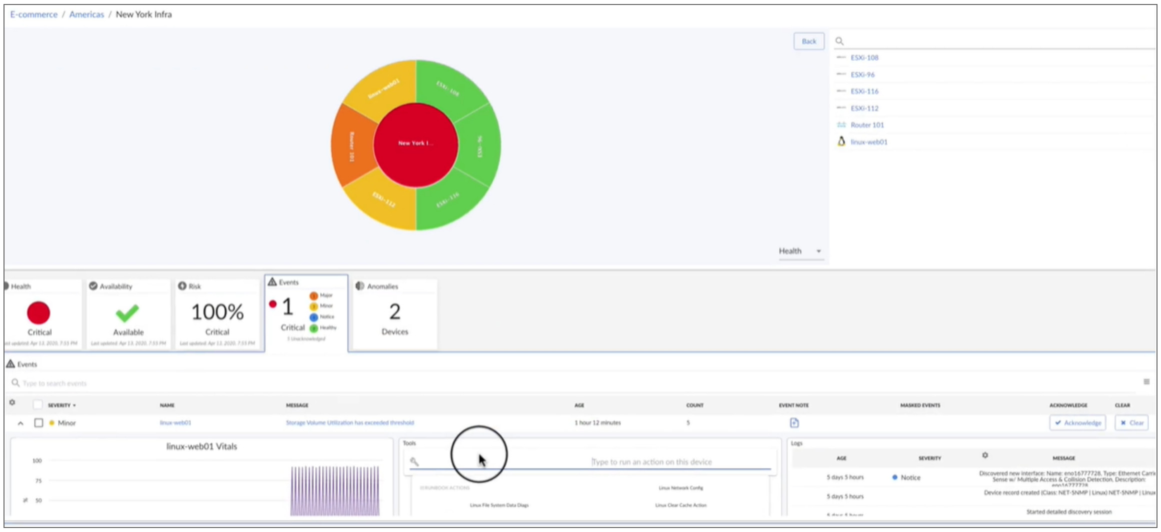
- **The Anomalies widget's time graph**. You can hover over any part of the time graph with your mouse to see the exact historical values for each polling cycle. Also, you can zoom in on a shorter time frame by clicking and dragging your mouse over the part of the interactive chart for a time frame, and you can return to the original time span by clicking the **[Reset zoom]** button. The historical values for each cycle can offer major insight into problem areas within your enterprise.



DEVICE NAME	ANOMALY DETECTION	METRIC TYPE	CURRENT
Router 101	Enabled	en3 to Storage - 0	0

To learn more about how to use the graph to identify detected anomalies, see the ***Anomalies Widget*** section.

- **The Event Drawer panel**. On the **[Events]**widget, you can click on a specific event to open the Event Drawer panel, which contains widgets that allow you to view and perform SL1's recommended actions and remediations.
  For events that are aligned to devices, click the down-arrow icon (﹀) next to the event to open the Event Drawer panel, which displays the following panes:
  - ***Vitals***. A widget displaying the event health for the past 24 hours of CPU and its memory usage for the device related to the event.
  - ***Tools***. A set of network diagnostic tools or user-initiated actions that you can run on the device associated with the problem event. Click the search bar to search for a tool or action to run, or click one of the default tools or actions that are available based on the device type and your user permissions.
  - ***Logs***. You can review a list of the log entries from the device's log file and determine errors recorded by SL1's logging feature.



SEVERITY	NAME	MESSAGE	AGE	COUNT	EVENT NOTE	MASKED EVENTS	ACKNOWLEDGE	CLEAR
Minor	linux-web01	Storage Volume Utilization has exceeded threshold	1 hour 12 minutes	5			✓ Acknowledge	✖ Clear

AGE	SEVERITY	MESSAGE
5 days 5 hours	Notice	Discovered new interface: Name: eno16777728, Type: Ethernet Carri Sense w/ Multiple Access & Collision Detection, Description: eno16777728
5 days 5 hours		Device record created (Class: NET-SNMP | Linux) NET-SNMP | Linux
		Started detailed discovery session

To learn more about how to view and perform SL1's recommended actions and remediations, see the ***Events Widget*** section.

Appendix

A

Troubleshooting Business Services

Overview

This chapter covers some of the issues you might encounter while working with services and policies on the **Business Services** page, and how to resolve those issues.

Use the following menu options to navigate the SL1 user interface:

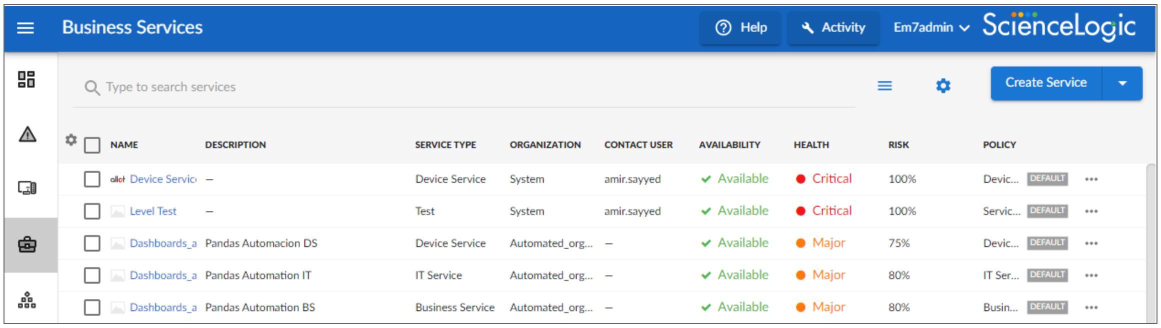
- To view a pop-out list of menu options, click the menu icon (☰).
- To view a page containing all of the menu options, click the Advanced menu icon (⋯).

This chapter covers the following topics:

Business Services Have Empty Values

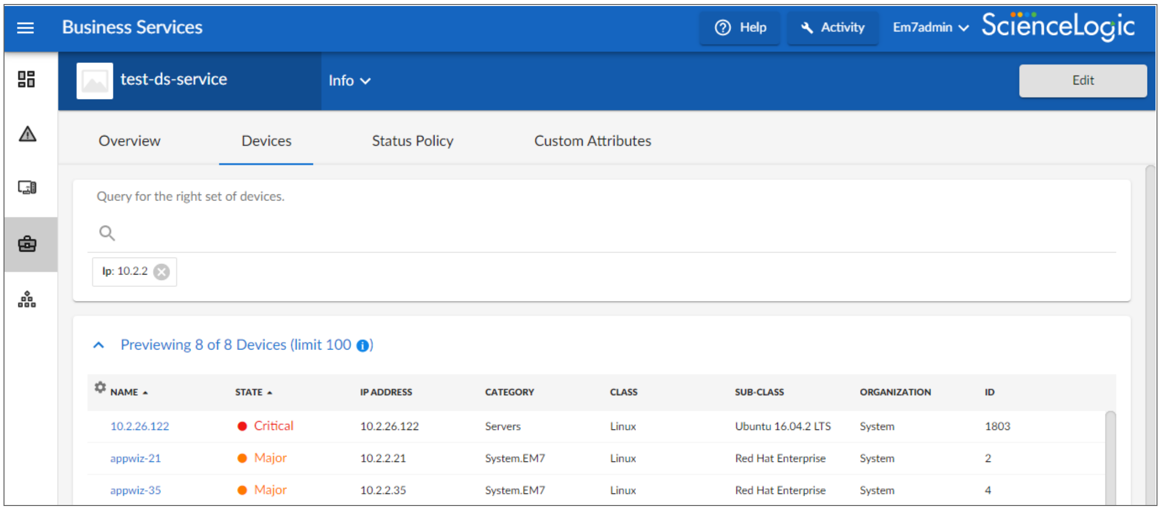
All Business Services Have Empty Values

If all of your business services show empty values, as shown in the figure below, ensure that you have given your admin processes adequate time to complete. To populate these values, both the "Business Services: Service Management Engine" and "Business Services: Service Topology Engine" processes must run once. With default settings, it could take up to 30 minutes to see your first results.



NAME	DESCRIPTION	SERVICE TYPE	ORGANIZATION	CONTACT USER	AVAILABILITY	HEALTH	RISK	POLICY
Device Servic	–	Device Service	System	amir.sayyed	✓ Available	● Critical	100%	Devic... DEFAULT
Level Test	–	Test	System	amir.sayyed	✓ Available	● Critical	100%	Servic... DEFAULT
Dashboards_a	Pandas Automacion DS	Device Service	Automated_org...	–	✓ Available	● Major	75%	Devic... DEFAULT
Dashboards_a	Pandas Automation IT	IT Service	Automated_org...	–	✓ Available	● Major	80%	IT Ser... DEFAULT
Dashboards_a	Pandas Automation BS	Business Service	Automated_org...	–	✓ Available	● Major	80%	Busin... DEFAULT

In SL1 platform version 10.1.0 and later, services are not evaluated if they have an empty filter. For more information on using a filter, see the section on ***Creating a Service***. The figure below shows the results of using a filter to find all devices for which the IP address contains "10".



Query for the right set of devices.

Ip: 10.2.2

Previewing 8 of 8 Devices (limit 100)

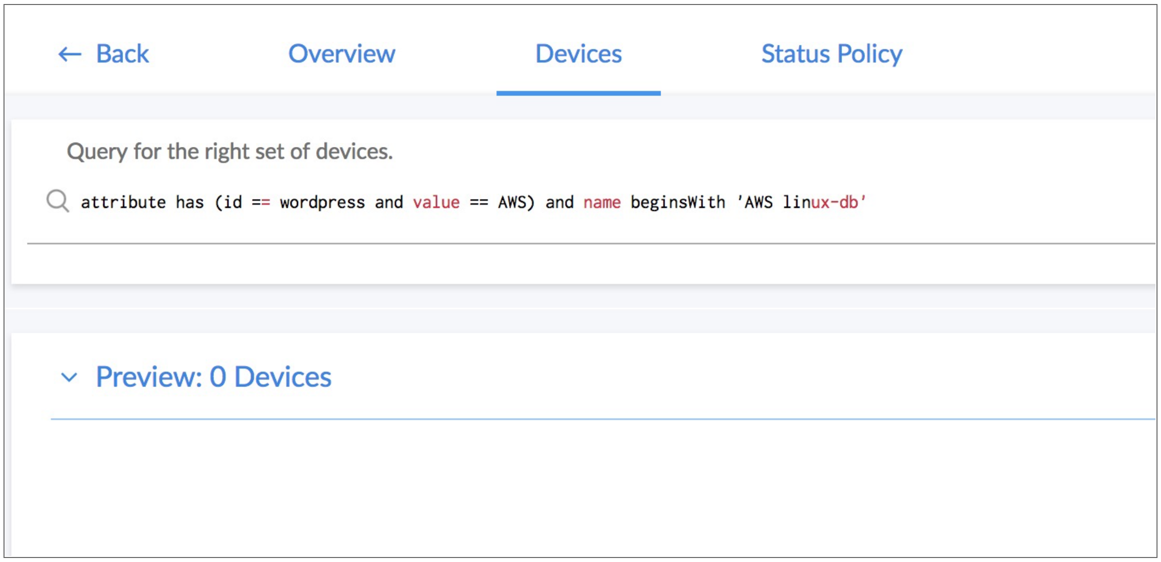
NAME	STATE	IP ADDRESS	CATEGORY	CLASS	SUB-CLASS	ORGANIZATION	ID
10.2.26.122	● Critical	10.2.26.122	Servers	Linux	Ubuntu 16.04.2 LTS	System	1803
appwiz-21	● Major	10.2.2.21	System.EM7	Linux	Red Hat Enterprise	System	2
appwiz-35	● Major	10.2.2.35	System.EM7	Linux	Red Hat Enterprise	System	4

Some Business Services Have Empty Values

If only some of your business services are missing values, troubleshoot using the following procedure.

To troubleshoot a business services missing values:

1. Ensure that your business service has some constituents:
   a. Go to the **Business Services** page (💼).
   b. Click on the service that is missing values.
   c. Click on the **[Devices]** or **[Services]** tab and review the devices or services listed. Modify your query as needed.

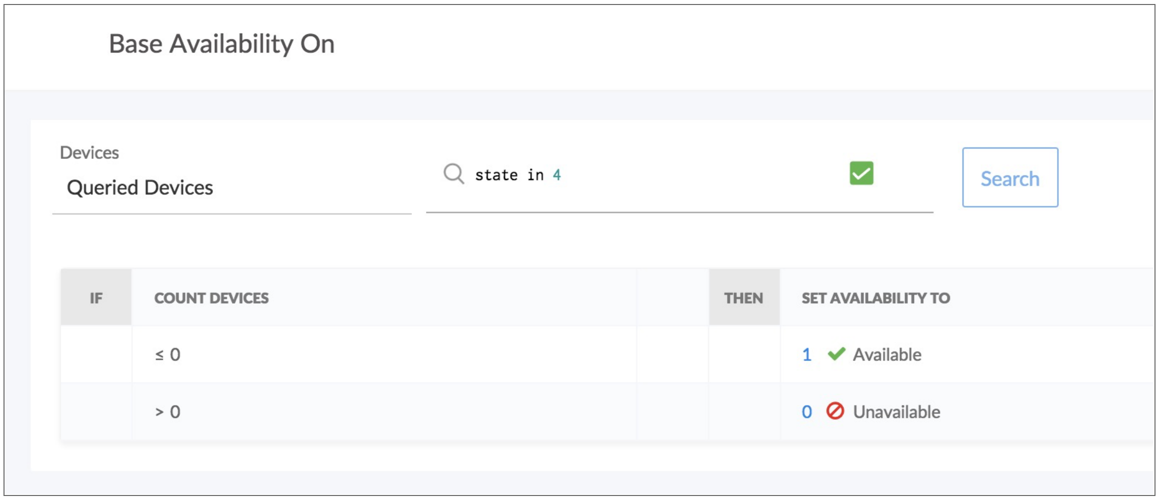


Query for the right set of devices.

```
attribute has (id == wordpress and value == AWS) and name beginsWith 'AWS linux-db'
```

2. Ensure that your service filter results in some constituents. Click on the **[Status Policy]** tab and modify your service filter as needed.
   - Rule filters select a subset of the devices or services defined by the service filter. For example, if a device service filter results in five devices, the rule filter will select some subset of those five devices. A rule filter might exclude all devices or services for a given business service, resulting in no metric values.

- ***Example.*** The following rule filter will select only the devices that have a state of "4", meaning "Critical". If no devices have a state of "4", the resulting list of devices will be empty; therefore, it will be impossible to get device metric values back. In this example, we are counting the devices, so the count will be zero. Values are produced based on the condition table. If the metric had been a normal device metric, such as latency, the result would have been null, because gathering the average latency on zero devices results in null.



Base Availability On

Devices: Queried Devices

`state in 4` ☑

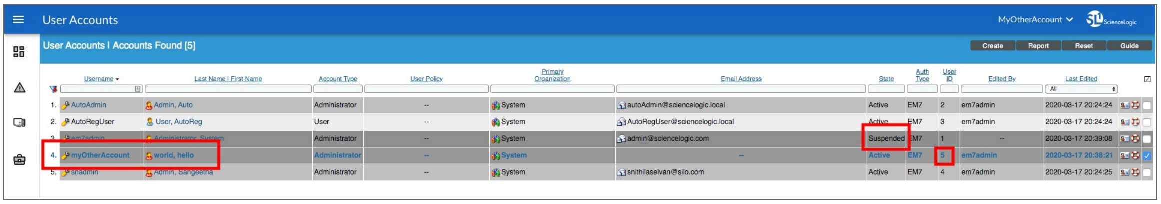
IF	COUNT DEVICES	THEN	SET AVAILABILITY TO
	≤ 0		1 ✓ Available
	> 0		0 ⊘ Unavailable

Services Missing Up-to-Date Values

If you have disabled the default administrator account ("em7admin"), you will need to identify another account to use for running business services and run a database query to change the account used for internal communication in SL1.

To change the internal account:

1. Go to the **User Accounts** page (Registry > Accounts > User Accounts).
2. Identify the account you want SL1 to use for internal communication. In this example, notice that the "em7admin" account is suspended. We want to use the account with ID "5" instead.



User Accounts | Accounts Found [5]

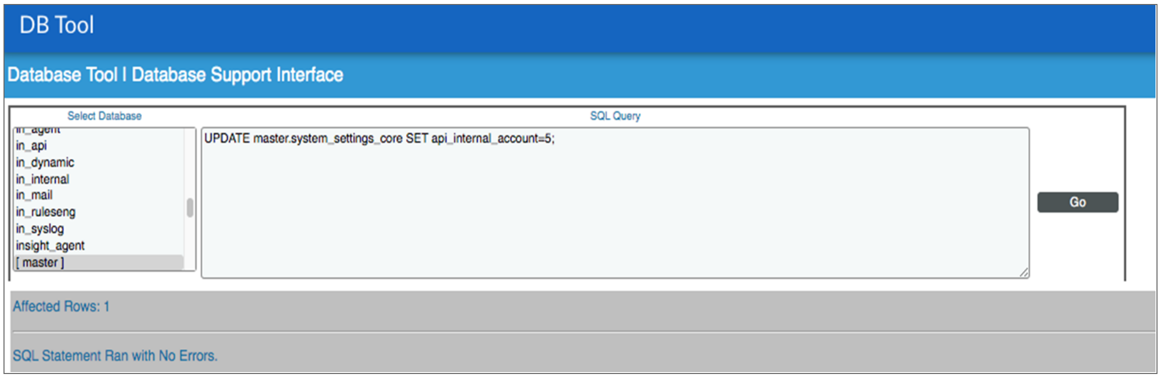
	Username	Last Name I First Name	Account Type	User Policy	Primary Organization	Email Address	State	Auth Type	User ID	Edited By	Last Edited	☑
1.	AutoAdmin	Admin, Auto	Administrator	--	System	autoAdmin@sciencelogic.local	Active	EM7	2	em7admin	2020-03-17 20:24:24	□
2.	AutoRegUser	User, AutoReg	User	--	System	AutoRegUser@sciencelogic.local	Active	EM7	3	em7admin	2020-03-17 20:24:24	□
3.	em7admin	Administrator, System	Administrator	--	System	admin@sciencelogic.com	Suspended	EM7	1	--	2020-03-17 20:39:08	□
4.	myOtherAccount	world, hello	Administrator	--	System	--	Active	EM7	5	em7admin	2020-03-17 20:38:21	☑
5.	snadmin	Admin, Sangeetha	Administrator	--	System	snithilaselvan@silo.com	Active	EM7	4	em7admin	2020-03-17 20:24:25	□

3. Update the internal account.
   a. Go to the **Database Tool** page (System > Tools > DB Tool).
   b. Select "master" as the database.

c. Enter the following SQL Query and then click **[Go]**:

```
UPDATE
   master.system_settings_core
SET
   api_internal_account =<account_id>
```

Where `<account_id>` is the ID number of the account you want to use. In the example, we use "5".



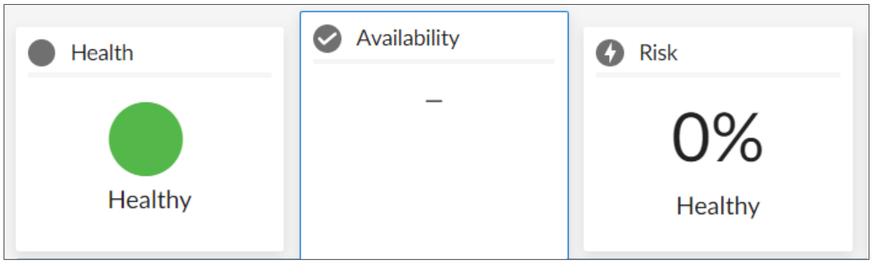
```
UPDATE master.system_settings_core SET api_internal_account=5;
```

Affected Rows: 1

SQL Statement Ran with No Errors.

Some Services Fail to Generate Health, Availability, or Risk Values

In this situation, some services in SL1 do not generate any values for Health, Availability, or Risk. For example, a dash might appear instead of a value in one of the widgets on the **Service Investigator** page:



To address this issue, review the following settings and suggestions:

Step 1: Turn up the log level to trace:

1. Either go to the console of the SL1 server or use SSH to access the SL1 appliance.
2. Log in as user **em7admin**.
3. Open the file */usr/local/silo/nextui/nextui.env* with vi or another text editor:

```
sudo vi /usr/local/silo/nextui/nextui.env
```

4. Change the log setting to the following: **NEXT_UI_LOG_LEVEL=all:trace**
5. Restart SL1 and GraphQL with the following command:

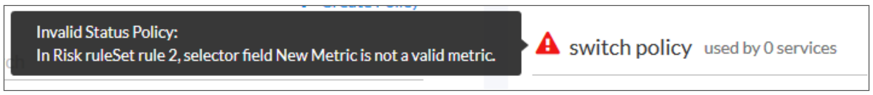
```
sudo systemctl restart nextui
```

6. Tail the log with the following command:

```
sudo journalctl -u nextui -f
```

Step 2: Ensure that your service policy is valid:

1. In SL1, navigate to your service on the **Business Services** page.
2. Review the policy used by that service for any validation errors, as in the following example:

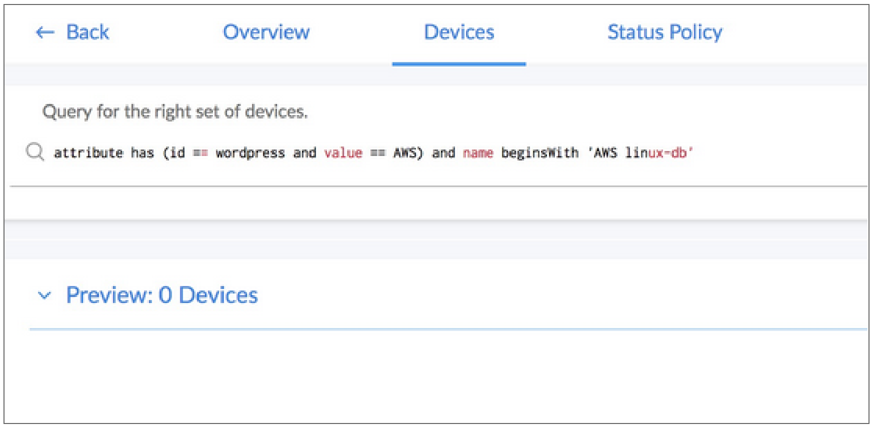


Invalid Status Policy:
In Risk ruleSet rule 2, selector field New Metric is not a valid metric.

3. Address any errors in the service policy.

Step 3: Ensure that your *service* contains at least one service or device:

1. Navigate to the **Business Services** page.
2. Navigate to the **[Devices]** or **[Services]** tab for the service or services that are not displaying values.



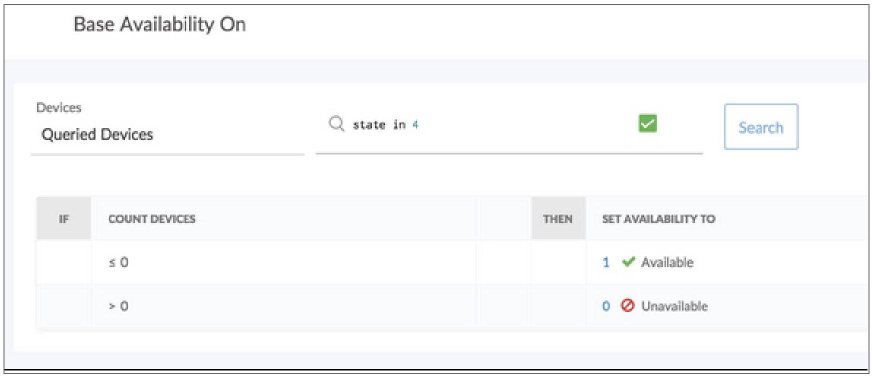
Query for the right set of devices.

```
attribute has (id == wordpress and value == AWS) and name beginsWith 'AWS linux-db'
```

3. Ensure that at least one device or service appears in the **Preview** section. If not, create a new filter to search for devices or services.

Step 4: Ensure that your service policy *rules* contain at least one service or device:

1. Rule filters select a subset of the devices or services defined by the service filter. If a device service filter results in five devices, the rule filter selects some subset of those five devices. You might create rule filters that exclude all devices or services in the service, resulting in no metric values.
2. The following rule filter only selects the devices with a state of 4, or Critical. If no devices have a state of 4, the resulting list of devices for that filter will be empty, and you cannot get any device metric values:



Base Availability On

Devices: Queried Devices

state in 4 ✓

IF	COUNT DEVICES	THEN	SET AVAILABILITY TO
	≤ 0		1 ✓ Available
	> 0		0 ⊘ Unavailable

3. In this case, we are counting devices, so the count is zero and produces a value based in the condition table.
4. If the metric had been a normal device metric like latency, the result would have been "null," because getting the average latency from zero devices results in null.

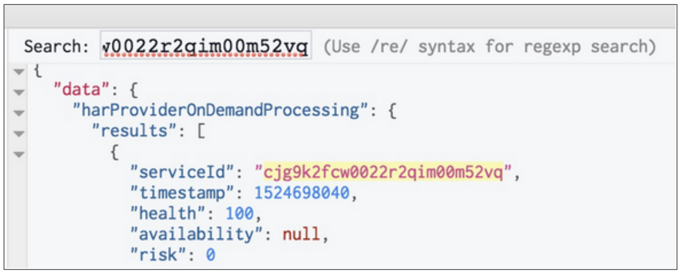
Step 5: Generate audit data by running onDemandProcessing with the GraphiQL interface:

1. In a browser, type the URL or IP address for the new user interface, and then type **/gql** at the end of the URL or IP address. The GraphiQL interface appears.
2. On the left side of the GraphiQL editor, type the following query:

```
                    query onDemand {
  harProviderOnDemandProcessing(ids: []) {
    results { serviceId timestamp health availability risk }
    auditHistory { serviceId ruleSetId ruleId timestamp sequence
message }
  }
}
```

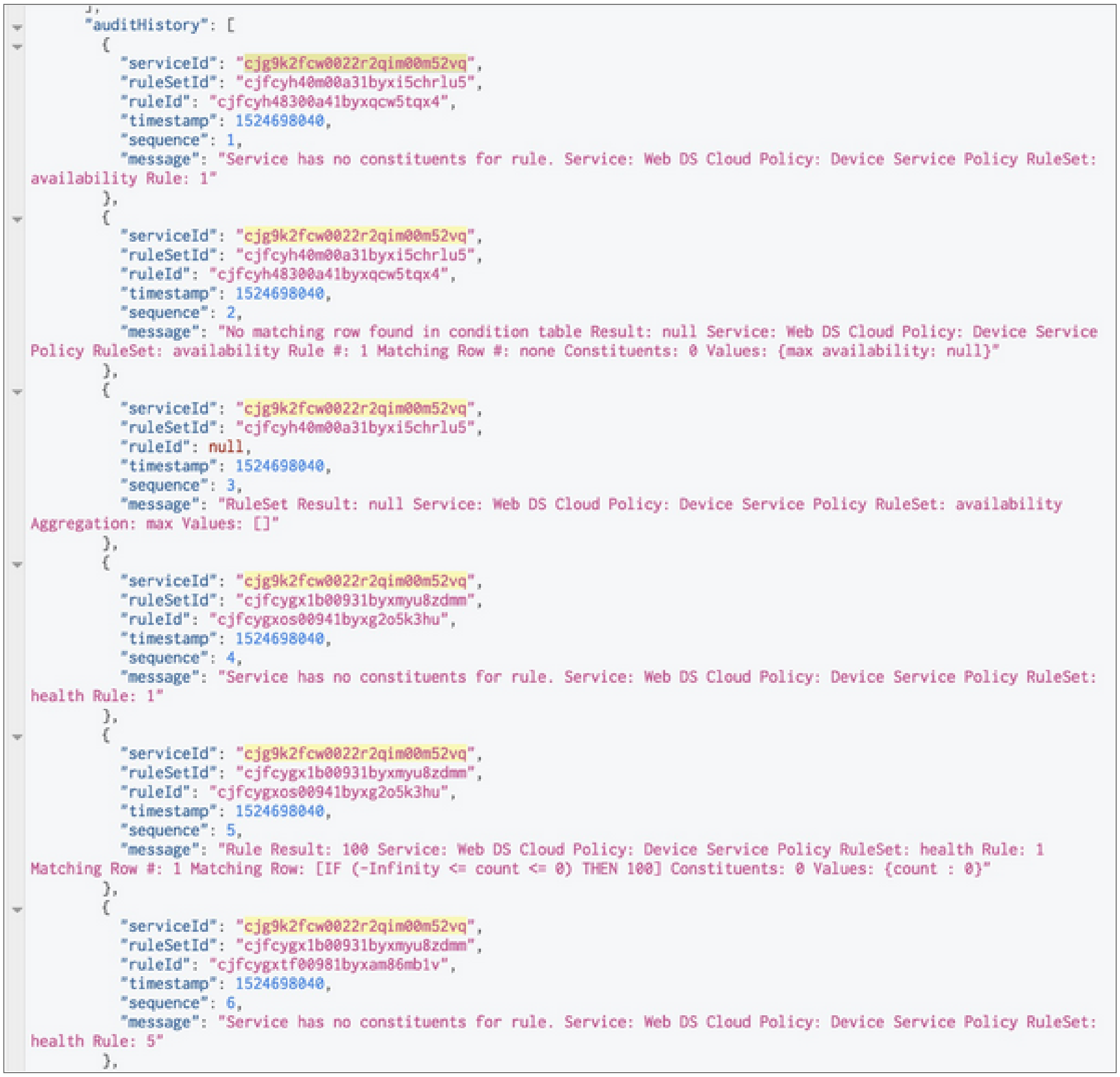
3. Click the **[Execute Query]** (Play) button to tell GraphiQL to send the query to the GraphQL server and get the results:

4. Review the resulting audit information on the right side of the GraphiQL editor:
5. If you know the service ID you are looking for, search for it by clicking inside the right pane and entering **Ctrl+f**. The GraphiQL interface highlights the services that match the ID you searched for:



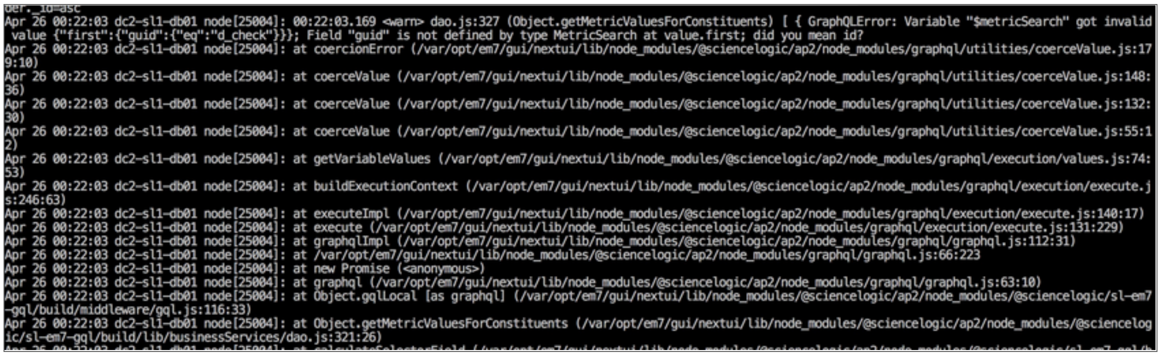
```
Search: v0022r2qim00m52vq (Use /re/ syntax for regexp search)
{
  "data": {
    "harProviderOnDemandProcessing": {
      "results": [
        {
          "serviceId": "cjg9k2fcw0022r2qim00m52vq",
          "timestamp": 1524698040,
          "health": 100,
          "availability": null,
          "risk": 0
```

6. Scroll down to see the audit information for this service (look for the highlighted information):



```
        ],
        "auditHistory": [
          {
            "serviceId": "cjg9k2fcw0022r2qim00m52vq",
            "ruleSetId": "cjfcyh40m00a31byxi5chrlu5",
            "ruleId": "cjfcyh48300a41byxqcw5tqx4",
            "timestamp": 1524698040,
            "sequence": 1,
            "message": "Service has no constituents for rule. Service: Web DS Cloud Policy: Device Service Policy RuleSet: 
availability Rule: 1"
          },
          {
            "serviceId": "cjg9k2fcw0022r2qim00m52vq",
            "ruleSetId": "cjfcyh40m00a31byxi5chrlu5",
            "ruleId": "cjfcyh48300a41byxqcw5tqx4",
            "timestamp": 1524698040,
            "sequence": 2,
            "message": "No matching row found in condition table Result: null Service: Web DS Cloud Policy: Device Service 
Policy RuleSet: availability Rule #: 1 Matching Row #: none Constituents: 0 Values: {max availability: null}"
          },
          {
            "serviceId": "cjg9k2fcw0022r2qim00m52vq",
            "ruleSetId": "cjfcyh40m00a31byxi5chrlu5",
            "ruleId": null,
            "timestamp": 1524698040,
            "sequence": 3,
            "message": "RuleSet Result: null Service: Web DS Cloud Policy: Device Service Policy RuleSet: availability 
Aggregation: max Values: []"
          },
          {
            "serviceId": "cjg9k2fcw0022r2qim00m52vq",
            "ruleSetId": "cjfcygx1b00931byxmyu8zdmm",
            "ruleId": "cjfcygxos00941byxg2o5k3hu",
            "timestamp": 1524698040,
            "sequence": 4,
            "message": "Service has no constituents for rule. Service: Web DS Cloud Policy: Device Service Policy RuleSet: 
health Rule: 1"
          },
          {
            "serviceId": "cjg9k2fcw0022r2qim00m52vq",
            "ruleSetId": "cjfcygx1b00931byxmyu8zdmm",
            "ruleId": "cjfcygxos00941byxg2o5k3hu",
            "timestamp": 1524698040,
            "sequence": 5,
            "message": "Rule Result: 100 Service: Web DS Cloud Policy: Device Service Policy RuleSet: health Rule: 1 
Matching Row #: 1 Matching Row: [IF (-Infinity <= count <= 0) THEN 100] Constituents: 0 Values: {count : 0}"
          },
          {
            "serviceId": "cjg9k2fcw0022r2qim00m52vq",
            "ruleSetId": "cjfcygx1b00931byxmyu8zdmm",
            "ruleId": "cjfcygxtf00981byxam86mb1v",
            "timestamp": 1524698040,
            "sequence": 6,
            "message": "Service has no constituents for rule. Service: Web DS Cloud Policy: Device Service Policy RuleSet: 
health Rule: 5"
          },
```

7. After running onDemandProcessing with the GraphiQL interface and updating the log settings on the server to do *all:trace*, you can now see trace-level log messages in the terminal where you ran `sudo journalctl -u nextui -f`.
8. Review the log messages for errors and warnings:



```
der._id=asc
Apr 26 00:22:03 dc2-sl1-db01 node[25004]: 00:22:03.169 <warn> dao.js:327 (Object.getMetricValuesForConstituents) [ { GraphQLError: Variable "$metricSearch" got invalid
 value {"first":{"guid":{"eq":"d_check"}}}; Field "guid" is not defined by type MetricSearch at value.first; did you mean id?
Apr 26 00:22:03 dc2-sl1-db01 node[25004]: at coercionError (/var/opt/em7/gui/nextui/lib/node_modules/@sciencelogic/ap2/node_modules/graphql/utilities/coerceValue.js:17
9:10)
Apr 26 00:22:03 dc2-sl1-db01 node[25004]: at coerceValue (/var/opt/em7/gui/nextui/lib/node_modules/@sciencelogic/ap2/node_modules/graphql/utilities/coerceValue.js:148:
36)
Apr 26 00:22:03 dc2-sl1-db01 node[25004]: at coerceValue (/var/opt/em7/gui/nextui/lib/node_modules/@sciencelogic/ap2/node_modules/graphql/utilities/coerceValue.js:132:
30)
Apr 26 00:22:03 dc2-sl1-db01 node[25004]: at coerceValue (/var/opt/em7/gui/nextui/lib/node_modules/@sciencelogic/ap2/node_modules/graphql/utilities/coerceValue.js:55:1
2)
Apr 26 00:22:03 dc2-sl1-db01 node[25004]: at getVariableValues (/var/opt/em7/gui/nextui/lib/node_modules/@sciencelogic/ap2/node_modules/graphql/execution/values.js:74:
53)
Apr 26 00:22:03 dc2-sl1-db01 node[25004]: at buildExecutionContext (/var/opt/em7/gui/nextui/lib/node_modules/@sciencelogic/ap2/node_modules/graphql/execution/execute.j
s:246:63)
Apr 26 00:22:03 dc2-sl1-db01 node[25004]: at executeImpl (/var/opt/em7/gui/nextui/lib/node_modules/@sciencelogic/ap2/node_modules/graphql/execution/execute.js:140:17)
Apr 26 00:22:03 dc2-sl1-db01 node[25004]: at execute (/var/opt/em7/gui/nextui/lib/node_modules/@sciencelogic/ap2/node_modules/graphql/execution/execute.js:131:229)
Apr 26 00:22:03 dc2-sl1-db01 node[25004]: at graphqlImpl (/var/opt/em7/gui/nextui/lib/node_modules/@sciencelogic/ap2/node_modules/graphql/graphql.js:112:31)
Apr 26 00:22:03 dc2-sl1-db01 node[25004]: at /var/opt/em7/gui/nextui/lib/node_modules/@sciencelogic/ap2/node_modules/graphql/graphql.js:66:223
Apr 26 00:22:03 dc2-sl1-db01 node[25004]: at new Promise (<anonymous>)
Apr 26 00:22:03 dc2-sl1-db01 node[25004]: at graphql (/var/opt/em7/gui/nextui/lib/node_modules/@sciencelogic/ap2/node_modules/graphql/graphql.js:63:10)
Apr 26 00:22:03 dc2-sl1-db01 node[25004]: at Object.gqlLocal [as graphql] (/var/opt/em7/gui/nextui/lib/node_modules/@sciencelogic/ap2/node_modules/@sciencelogic/sl-em7
-gql/build/middleware/gql.js:116:33)
Apr 26 00:22:03 dc2-sl1-db01 node[25004]: at Object.getMetricValuesForConstituents (/var/opt/em7/gui/nextui/lib/node_modules/@sciencelogic/ap2/node_modules/@sciencelog
ic/sl-em7-gql/build/lib/businessServices/dao.js:321:26)
```

All Services Fail to Generate Health, Availability, and Risk Values

In this situation, *all* of your services in SL1 fail to generate any values for Health, Availability, or Risk.

To address this issue, review the following settings and suggestions.

Step 1: Confirm that the Business Services processes exist:

1. Go to the **Process Manager** page (System > Settings > Admin Processes) and start typing "Business" in the **Process Name** filter.
2. Ensure that the "Business Services: Service Management Engine" and "Business Services: Service Topology Engine" processes appear and are enabled.

Step 2: Follow the steps in ***Generate audit data using the GraphiQL user interface***, above. If the process times out, then the processing has taken more than two minutes to complete, and no computed results are stored.

Step 3: Look for logs from the Python process:

1. The Python process calls the onDemandProcessing GraphQL query. If Python is having trouble connecting to GraphQL, it could be an authentication problem or some other code-related issue.
2. Look in */var/log/em7* for newly created logs, and `ls -lrt` to see if any new error logs were created with "business" in the file name.
3. Also check the ***silo.log*** for messages related to the business_service_management process by using the following command:

```
grep service /var/log/em7/silo.log
```

Device Services Fail to Load After an Upgrade

If you have upgraded your appliance from an earlier version of SL1 and your device services are not loading on Business Service pages, you might have outdated device class filters in your user preferences.

To clear the older device class filters:

1. Open the GraphiQL interface on your appliance by appending "/gql" to your appliance name (or IP address) in a browser window.
2. Enter the following in the left side of the GQL interface and execute the mutation by pressing the **[Execute Query]** button:

```
mutation deletePreference{
  deletePreference(preferenceId:
"services.detaildevices.table.sort.order") {
    id
    preferenceValue
  }
}
```

502, 503, or 504 Errors: Health, Availability, and Risk Values are All the Same or are Inaccurate

Step 1: Check the number of services you have configured. If you are seeing 503 errors in the nextui log or within the SL1user interface, use the following procedure to check the number of services you have configured on your ScienceLogic SL1 system.

To determine the number of services you have:

1. Open the GraphiQL editor on your system:

```
http://<SL1_IP_address>/gql
```

2. Enter the following query:

   ```
   query harProviders {
     harProviders {
       pageInfo {
         matchCount
       }
     }
   }
   ```

3. Click **[Execute Query]** (Play) to see the number of services. In this example, the results shows that 10 services are configured.

   ```
   "data": {
     harProviders {
       pageInfo {
         matchCount: 10
       }
     }
   }
   ```

Step 2: (503 Errors) Confirm that the nginx configuration has an appropriate limit set. In some cases, the `limit_conn` value might be set to 20. Increase the value to 200.

To address this issue:

1. Either go to the console of the SL1 server or use SSH to access the SL1 appliance.
2. Log in as user **em7admin**.
3. Confirm that the nginx config file has the `limit_conn perip` value set to 200 instead of 20:
   `sudo vi /etc/nginx/conf.d/em7_limits.conf`
4. If needed, update the line to say:
   `limit_conn perip 200;`
5. Run the following command:
   `sudo systemctl restart nginx`

Step 3: (503 Errors) Check to see if the nginx server is rate-limiting you.

1. Either go to the console of the SL1 server or use SSH to access the SL1 appliance.
2. Log in as user **em7admin**.
3. Enter the following command:
   `sudo grep excess /var/log/em7/ngx.log`

4. If you see any results from the above command, then the nginx proxy is rate-limiting requests to your database. In that case, you should increase the rate limit to 100 requests per second. Edit the **em7_limits.conf** file:
   ```
   sudo vi /etc/nginx/conf.d/em7_limits.conf
   ```
5. Change the following line to **100r/s** from the default 5 r/s.
   ```
   limit_req_zone $binary_remote_addr zone-addr_req:10m rate=100r/s;
   ```
6. Restart your SL1 system.
   ```
   sudo systemctl restart nextui
   ```

Step 4: (502 Errors) Check node memory usage.

1. Either go to the console of the SL1 server or use SSH to access the SL1 appliance.
2. Log in as user **em7admin**.
3. Enter the following command:
   ```
   sudo journalctl -u nextui|grep "JavaScript heap out of memory"
   ```
4. If you see any results form the above command, the node.js process is running out of memory. In that case, you should increase the space limit allocated. Edit the **nextui.service** to increase memory to 4096 or 8192 MB, depending on how much memory you have at your disposal.
   ```
   ExecStart=/usr/bin/node --max-old-space-size=4096
   /usr/local/silo/nextui/index.js
   ```
5. Restart your SL1 system.
   ```
   sudo systemctl restart nextui
   ```

Step 5: (504 Errors) Check Nginx timeout.

1. Either go to the console of the SL1 server or use SSH to access the SL1 appliance.
2. Log in as user **em7admin**.
3. Edit the `nextui.fragment` file:
   ```
   sudo vi /opt/em7/share/config/nginx.d/nextui.fragment
   ```
4. Change the `proxy_read_timeout` under "location /gql" to **900** as follows:
   ```
   proxy_read_timeout 900;
   ```
5. Restart your SL1 system.
   ```
   sudo systemctl restart nextui
   ```

Advanced Troubleshooting

Customization for Environments with More Than 2,500 Services

If you have an environment that has more than 2,500 services, you might need to modify some default settings in SL1, as described in this section.

Update Settings and Increase Default Values

To update your settings and increase your default values:

1. Either go to the console of the SL1 server or use SSH to access the SL1 appliance.
2. Log in as user **em7admin**.
3. Increase the maximum service count variable. (The default value is 2500.)
   a. At the command line, enter
      ```
      sudo vi /opt/em7/nextui/nextui.env
      ```
   b. Add the following line (or modify it, if it already exists), where "new_service_limit" is the maximum number of services you need in your environment:
      ```
      BUSINESS_SERVICES_MAX_SERVICES=new_service_limit
      ```
4. Increase the Node.js memory limit.
   a. At the command line, enter
      ```
      sudo vi /etc/systemd/system/multi-user.target.wants/nextui.service
      ```
   b. Change the ExecStart line to the following, where the size is either 4096 or 8192, depending on how much memory you have available:
      ```
      ExecStart=/usr/bin/node --max-old-space-size=size
      /usr/local/silo/nextui/index.js
      ```
5. Restart `nextui` by entering the following at the command line:
   ```
   sudo systemctl restart nextui
   ```

Modify NGINX Rate Limit

If you have a large number of services in your environment and are seeing 503 errors, you might need to increase your NGINX rate limit.

To increase your NGINX rate limit:

1. Either go to the console of the SL1 server or use SSH to access the SL1 appliance.
2. Log in as user **em7admin**.
3. At the command line, enter the following:
   ```
   sudo grep excess /var/log/em7/ngx.log
   ```
4. If you see any results from this command, consider increasing your NGINX rate limit to 100 requests per second.
   a. Enter the following at the command line to edit the limit file:
      ```
      sudo vi /etc/nginx/conf.d/em7_limits.conf
      ```
   b. Change the *value* in the following line to "300r/s" from the default value of "100r/s":
      ```
      limit_req_zone $binary_remote_addr zone=addr_req:10m rate=value
      ```

      WARNING: If this value is set too high, the database will begin seeing errors for too many connections.
5. Restart NGINX.
   ```
   sudo systemctl restart nginx
   ```

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™ 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™ has attempted to provide accurate information on this Site, information on this Site may contain inadvertent technical inaccuracies or typographical errors, and ScienceLogic™ assumes no responsibility for the accuracy of the information. Information may be changed or updated without notice. ScienceLogic™ 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™
- EM7™ and em7™
- Simplify IT™
- Dynamic Application™
- Relational Infrastructure Management™

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. For more information, see https://sciencelogic.com/company/legal.

ScienceLogic

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

International: +1-703-354-1010