

# Monitoring Cisco Cloud Services Platform 2100

Cisco: CSP-2100 PowerPack version 106

### Table of Contents

Introduction	
What is Cisco Cloud Services Platform 2100?	
What Does the Cisco: CSP-2100 PowerPack Monitor?	4
Installing the Cisco: CSP-2100 PowerPack	4
Configuration and Discovery	6
Prerequisites for Monitoring CSP-2100 Clusters	
Creating SNMP Credentials for CSP-2100 Clusters	7
Creating a Basic/Snippet Credential for CSP-2100 Clusters	9
Creating an SSH/Key Credential for CSP-2100 Clusters	
Discovering CSP-2100 Clusters	11
Viewing CSP-2100 Component Devices	13
Relationships Between Component Devices	15
Dashboards	16
Device Dashboards	
Cisco: CSP 2100 Cluster	
Cisco: CSP 2100 Node	18
Cisco: CSP 2100 Service	19

## Chapter

#### Introduction

#### Overview

This manual describes how to monitor Cisco Cloud Services Platform (CSP) 2100 clusters in SL1 using the Cisco: CSP-2100 PowerPack.

The following sections provide an overview of CSP-2100 devices and the Cisco: CSP-2100 PowerPack.

What is Cisco Cloud Services Platform 2100?	3
What Does the Cisco: CSP-2100 PowerPack Monitor?	4
Installing the Cisco: CSP-2100 PowerPack	4

**NOTE:** ScienceLogic provides this documentation for the convenience of ScienceLogic customers. Some of the configuration information contained herein pertains to third-party vendor software that is subject to change without notice to ScienceLogic. ScienceLogic makes every attempt to maintain accurate technical information and cannot be held responsible for defects or changes in third-party vendor software. There is no written or implied guarantee that information contained herein will work for all third-party variants. See the End User License Agreement (EULA) for more information.

#### What is Cisco Cloud Services Platform 2100?

Cisco Cloud Services Platform 2100 is a platform for virtualizing data center network functions. The hardware and software platform includes REST APIs, a command-line interface, and a web user interface for creating and managing virtual machines.

#### What Does the Cisco: CSP-2100 PowerPack Monitor?

To monitor CSP-2100 devices using SL1, you must install the *Cisco:* CSP-2100 PowerPack. This PowerPack enables you to discover, model, and collect data about CSP-2100 clusters, nodes, and services.

The Cisco: CSP-2100 PowerPack includes:

- Four example credentials (two SNMP credentials, a Basic/Snippet credential, and an SSH/Key credential) you can use to create the credentials that enable you to collect data from CSP-2100 devices
- Dynamic Applications to discover and monitor the CSP-2100 component devices
- Device Classes for each type of CSP-2100 component device SL1 monitors
- Event Policies and corresponding alerts that are triggered when CSP-2100 component devices meet certain status criteria
- Run Book Actions and Policies that align the correct device class to CSP-2100 component devices based on GUID and that merge CSP-2100 component devices with the appropriate physical components
- Device dashboards for each type of discovered CSP-2100 component device

#### Installing the Cisco: CSP-2100 PowerPack

Before completing the steps in this manual, you must import and install the latest version of the Cisco: CSP-2100 PowerPack.

TIP: By default, installing a new version of a PowerPack overwrites all content from a previous version of that PowerPack that has already been installed on the target system. You can use the Enable Selective PowerPack Field Protection setting in the Behavior Settings page (System > Settings > Behavior) to prevent new PowerPacks from overwriting local changes for some commonly customized fields. (For more information, see the System Administration manual.)

To download and install a PowerPack:

- 1. Download the PowerPack from the <u>ScienceLogic Support Site</u>.
- 2. Go to the **PowerPack Manager** page (System > Manage > PowerPacks).
- 3. In the **PowerPack Manager** page, click the **[Actions]** button, then select *Import PowerPack*.
- 4. The Import PowerPack dialog box appears:

Impor	rt PowerPack™		×
	Browse for file License: Import	Browse	

- 5. Click the [Browse] button and navigate to the PowerPack file.
- 6. When the **PowerPack Installer** modal appears, click the **[Install]** button to install the PowerPack.

**NOTE:** If you exit the **PowerPack Installer** modal without installing the imported PowerPack, the imported PowerPack will not appear in the **PowerPack Manager** page. However, the imported PowerPack will appear in the **Imported PowerPacks** modal. This page appears when you click the **[Actions]** menu and select *Install PowerPack*.

## Chapter

## 2

## **Configuration and Discovery**

#### Overview

The following sections describe how to configure and discover Cisco Cloud Services Platform (CSP) 2100 clusters for monitoring by SL1 using the Cisco: CSP-2100 PowerPack:

Prerequisites for Monitoring CSP-2100 Clusters	6
Creating SNMP Credentials for CSP-2100 Clusters	7
Creating a Basic/Snippet Credential for CSP-2100 Clusters	9
Creating an SSH/Key Credential for CSP-2100 Clusters	10
Discovering CSP-2100 Clusters	11
Viewing CSP-2100 Component Devices	13
Relationships Between Component Devices	15

#### Prerequisites for Monitoring CSP-2100 Clusters

To configure the SL1 system to monitor CSP-2100 clusters using the Cisco: CSP-2100 PowerPack, you must have the following information about the clusters that you want to monitor:

- Username and password of a user with REST API read access and a role of operator-group or admin-group
- SNMP community string with read privileges and the port set to 161

NOTE: For more information about these requirements, see <u>http://www.cisco.com/c/en/us/td/docs/switches/datacenter/csp 2100/config guide/b Cisco</u> <u>CSP 2100 Config Guide.html</u>.

Additionally, you must establish a Net-SNMP public community string with the port set to 1610. To do so:

- 1. Log in to the command line of the CSP-2100 device as an administrative user.
- 2. Run the following commands:

netsnmp agent port 1610 netsnmp community public

#### Creating SNMP Credentials for CSP-2100 Clusters

Before you can discover and monitor CSP-2100 clusters in SL1, you must first create two SNMP credentials (one for port 161 and another for port 1610) in SL1. These credentials, along with a *Basic/Snippet credential* and *SSH/Key credential* that you must also create, enable SL1 to collect data from the clusters. Two example SNMP credentials that you can edit for your own use are included in the *Cisco*: CSP-2100 PowerPack.

**NOTE**: For more information about the configuration required for the two SNMP credentials, see the *Prerequisites* section.

To configure the port 161 SNMP credential for CSP-2100:

- 1. Go to the **Credential Management** page (System > Manage > Credentials).
- 2. Locate the Cisco: CSP SNMP Port 161 Example credential, then click its wrench icon (<sup>2</sup>). The Edit SNMP Credential modal page appears.

3. Make entries in the following fields:

Credential Editor [91]		×
Edit SNMP Credential #91		New Reset
Basic Settings Profile	Name	SNMP Version
Cisco: CSP SNMP Port 161 Example	)	[SNMP V2] V
Port 161	Timeout(ms) (1500	Retries
SNMP Community (Read-C admin SNMP V3 Settings		IP Community (Read/Write)
Security Name	Security P	assphrase
Authentication Protocol	Security Level No Authentication / No Encryption	SNMP v3 Engine ID
Context Name	Privacy Protocol DES	Privacy Protocol Pass Phrase
	Save Save As	

- Profile Name. Enter a new name for the credential.
- SNMP Community (Read Only). Enter the port 161 community string for the CSP-2100 cluster.
- 4. Use the default values for the other fields on this page.
- 5. Click the **[Save As]** button.
- 6. When the confirmation message appears, click **[OK]**.

To configure the port 1610 SNMP credential for CSP-2100:

- 1. Go to the **Credential Management** page (System > Manage > Credentials).
- 2. Locate the Cisco: CSP SNMP Port 1610 Example credential, then click its wrench icon (*P*). The Edit SNMP Credential modal page appears.

3. Make entries in the following fields:

Credential Editor [92]		×
Edit SNMP Credential #92		New Reset
Basic Settings	News	ON MEN Andrea
Cisco: CSP SNMP Port 1610 Exampl	Name	SNMP Version
Port [1610	Timeout(ms) [1500	Retries
SNMP V1/V2 Settings SNMP Community (Read-C admin	Only) St	IMP Community (Read/Write)
SNMP V3 Settings Security Name	Security	Passphrase
Authentication Protocol	Security Level	SNMP v3 Engine ID
Context Name	Privacy Protocol	Privacy Protocol Pass Phrase
	Save Save As	

- Profile Name. Enter a new name for the credential.
- SNMP Community (Read Only). Enter the port 1610 community string for the CSP-2100 cluster.
- 4. Use the default values for the other fields on this page.
- 5. Click the [Save As] button.
- 6. When the confirmation message appears, click [OK].

#### Creating a Basic/Snippet Credential for CSP-2100 Clusters

Some Dynamic Applications in the Cisco: CSP-2100 PowerPack collect data from CSP-2100 clusters using REST API. These Dynamic Applications require a Basic/Snippet credential to enable SL1 to communicate with the cluster. An example Basic/Snippet credential that you can edit for your own use is included in the Cisco: CSP-2100 PowerPack.

**NOTE**: For more information about the configuration required for the Basic/Snippet credential, see the *Prerequisites* section.

To create a Basic/Snippet credential to monitor CSP-2100:

1. Go to the **Credential Management** page (System > Manage > Credentials).

- 2. Locate the Cisco: CSP Example credential, and then click its wrench icon (*P*). The Edit Basic/Snippet Credential modal page appears.
- 3. Enter values in the following fields:

Credential Editor [90]				×
Edit Basic/Snippet Credential #90			New	Reset
Basic Settings				
	Credential Name			
Cisco: CSP Example				
Hostname/IP	Port	ті	meout(ms)	
http://%D	80	30000		
User	name	1	Password	
admin		] [		
	Save Save As			

- Credential Name. Enter a new name for the credential.
- Username. Enter the username for a user with REST API read access to the CSP-2100 cluster and a role of operator-group or admin-group.
- Password. Enter the password for the REST API user.
- 4. Use the default values for the other fields on this page.
- 5. Click the **[Save As]** button.
- 6. When the confirmation message appears, click [OK].

#### Creating an SSH/Key Credential for CSP-2100 Clusters

Some Dynamic Applications in the Cisco: CSP-2100 PowerPack collect data from CSP-2100 clusters from the command line interface instead of the API. These Dynamic Applications require an SSH/Key credential to enable SL1 to communicate with the cluster. An example SSH/Key credential that you can edit for your own use is included in the Cisco: CSP-2100 PowerPack.

**NOTE:** This functionality utilizes MD5 password encryption. As such, it is not currently available for use in Federal Information Processing Standard (FIPS)-compliant installations of SL1. If you attempt to discover CSP-2100 cluster data using an SSH/Key credential in FIPS-compliant installations of SL1, the cluster component device will not be created and an exception error message appears in the system log.

To create an SSH/Key credential to monitor CSP-2100:

1. Go to the **Credential Management** page (System > Manage > Credentials).

- 2. Locate the Cisco: CSP 2100 CLI Example credential, and then click its wrench icon (*P*). The Edit SSH/Key Credential modal page appears.
- 3. Enter values in the following fields:

Credential Editor [130]				×
Edit SSH/Key Credential #130			New	Reset
Basic Settings Cisco: CSP 2100 CLI Example	Credential Name			)
Hostname/IP [10.2.8.31] 22	Port	Timeout(n ) [5000	ns)	)
Username em7admin		Passwor	ď	)
Priva	ate Key (PEM Format)			
				4
	Save 📘 Save As			

- Credential Name. Type a new name for the credential.
- Hostname/IP. Type the IP address or hostname of the CSP 2100 cluster you want to monitor.
- Port. Type the SSH port number for the CSP-2100 cluster you want to monitor.
- Timeout(ms). Keep the default setting.
- **Username**. Type the username for a user with administrator access to the CSP-2100 cluster command line interface.
- Password. Type the user's password.
- Private Key (PEM Format). Keep this field blank.
- 4. Click the [Save As] button.
- 5. When the confirmation message appears, click [OK].

#### Discovering CSP-2100 Clusters

When you discover your CSP-2100 cluster with SL1, SL1 auto-aligns a series of Dynamic Applications to discover, configure, and monitor the CSP-2100 cluster and all of its associated component devices.

To discover your CSP-2100 cluster, perform the following steps:

- 1. Go to the **Discovery Control Panel** page (System > Manage > Classic Discovery).
- 2. Click the [Create] button. The Discovery Session Editor page appears:

Discovery Session Editor   Create New		New	Reset
Identification Information			
Name Descri	ption		
IP and Credentials IP Address/Hostname Discovery List Upload File Browse for file SNMP Credentials SNMP Cisco SNMPV2 - Example	Detection and Scanning Initial Scan Level         System Default (recommended)       ▼         System Default (recommended)       ▼         Port Scan All IPs         System Default (recommended)       ▼         Port Scan All IPs         System Default (recommended)       ▼         Port Scan All IPs         System Default (recommended)       ▼         Port Scan Timeout       ▼         System Default (recommended)       ▼         Port Scan Timeout       ▼         Optection Method & Port       ₽	Basic Settings Discover Model Non-SNMP Devices DHCP Collection Server PID: em7_ao (System) Add Devices to Device Grou	Duplication Protection v v v v p(s) v
Cisco SNMPV2 - Example Cisco SNMPV3 - Example EM7 Default V2 EM7 Default V3 Internal IPSLA Example LifeSize: Endpoint SNMP netapp_rmode_snmp Neurotections Cher Credentials Cher Credentials	[Default Method] UDP: 161 SNMP TCP: 1 - topmux TCP: 2 - compressnet TCP: 5 - rie TCP: 7 - echo TCP: 9 - discard TCP: 13 - daytime TCP: 13 - daytime TCP: 14 - systat TCP: 19 - chargen TCP: 19 - chargen TCP: 19 - chargen TCP: 19 - chargen	Please create a device group first	•
Cisco CCI ample Cale Cisco: ACI 2 Cisco: ACI 2 Cisco: ACI 2 Cisco: ACI Sample Credential 1 Cisco: ACI Sample Credential 2 Cloudkick - Example EMC - Example	Interface Inventory Timeout (ms) 600000 Maximum Allowed Interfaces 10000 Bypass Interface Inventory ©	Apply Device Template	• • 2
	Save	Log Al	

- 3. Supply values in the following fields:
  - IP Address/Hostname Discovery List. Enter the IP address of each CSP-2100 node you want to discover.
  - **SNMP Credentials**. Select the two SNMP credentials that you created (one for port 161 and the other for port 1610) for each of the CSP-2100 nodes you want to discover.
  - Other Credentials. Select the Basic/Snippet credential and the SSH/Key credential for each of the CSP-2100 nodes you want to discover.
  - Discover Non-SNMP. Select this checkbox.

**NOTE**: You must include a minimum of three credentials (one SNMP credential and two Basic/Snippet credentials) for each CSP-2100 node with unique credential information.

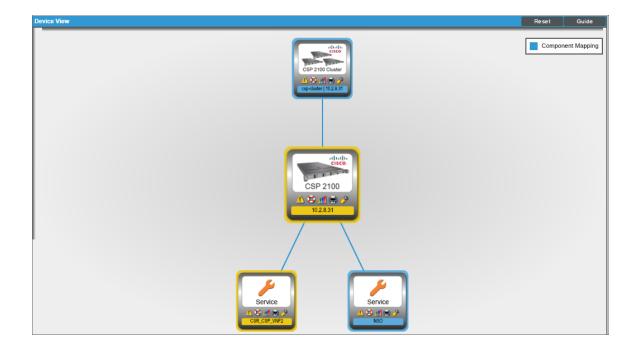
- **NOTE:** If you are running a Federal Information Processing Standard (FIPS)-compliant installations of the ScienceLogic platform, then you should not select an SSH/Key credential in the **Other Credentials** field.
- 4. Optionally, supply values in the other fields in this page. For a description of the fields in this page, see the **Discovery & Credentials** manual.
- 5. Click the **[Save]** button.
- 6. The **Discovery Control Panel** page will refresh. Click the lightning bolt icon (*F*) for the discovery session you created.
- 7. In the pop-up window that appears, click the **[OK]** button. The **Discovery Session** page displays the progress of the discovery session.

#### Viewing CSP-2100 Component Devices

When SL1 discovers your CSP-2100 cluster, SL1 creates component devices that represent each component in the cluster.

In addition to the **Device Manager** page, you can view all associated component devices in the following places in the user interface:

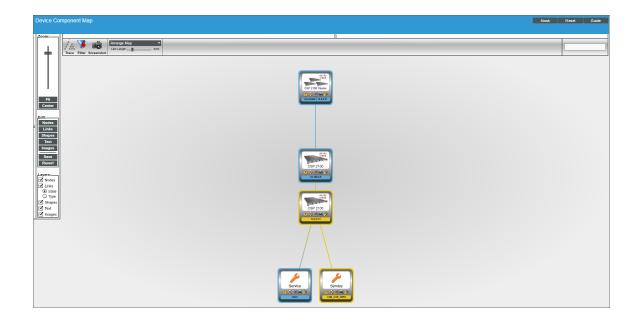
• The **Device View** modal page (click the bar-graph icon [411]) for a device, then click the **Topology** tab) displays a map of the selected device and all of the devices with which it has parent-child relationships. Double-clicking any of the devices listed reloads the page to make the selected device the primary device:



• The **Device Components** page (Registry > Devices > Device Components) displays a list of all root devices and component devices discovered by SL1, in an indented view, so you can easily view the hierarchy and relationships between child devices, parent devices, and root devices. To view the component devices associated with your CSP-2100 cluster, find the root device and click its plus icon (+):

		Device Name •	IP Address	Device Category	Device Class   Sub-class		Organization	Current State	Collection Group	Collection State	
8 a	ncsp-	cluster   10.2.8.31	۰. ۳	Servers	Cisco Systems   CSP2100 Cluster	197	System	1 Notice	CUG	Active	🖶 🔀 🗞 /
		Device Name •	IP Address	Device Categor	Device Class   Sub-class		Organization	Current State >=Health: ▼	Collection Group	Collection State	
1.	Pa	10.198.6.5	<b>.</b> .	Servers	Cisco Systems   CSP Node	199	System	🔥 Notice	CUG	Active	H 🕇 🗞 🗷
2. –	<u> 9</u> 1	10.2.8.31	<b>W</b> 10.2.8.31	Services	Cisco Systems   CSP2100	194	System	<u> 1</u> Minor	CUG	Active	<b>H</b> 🎝 🗞 🛛
		Device Name •	IP Addre	ss <u>Cate</u>	iory Device Class   Sub-class		Organization	Current State >=Health ▼	Collection Group	Collection State	)
	1.			Servers	Cisco Systems   CSP Service	196	System	A Minor	CUG	Active	11 <b>1</b> 2 10 <u>18</u>
	2.	<i>₽</i> <u>m</u> NSO		Servers	Cisco Systems   CSP Service	195	System	🔥 Notice	CUG	Active	🖶 🖏 🖏 🛲

The Component Map page (Classic Maps > Device Maps > Components) allows you to view devices by root node and view the relationships between root nodes, parent components, and child components in a map. This makes it easy to visualize and manage root nodes and their components. SL1 automatically updates the Component Map as new component devices are discovered. The platform also updates each map with the latest status and event information. To view the map for your CSP-2100 cluster, go to the Component Map page and select the map from the list in the left NavBar. To learn more about the Component Map page, see the Views manual.



#### Relationships Between Component Devices

In addition to parent/child relationships between component devices, SL1 also creates relationships between CSP-2100 nodes and Cisco UCS Standalone servers.

## Chapter



### **Dashboards**

#### Overview

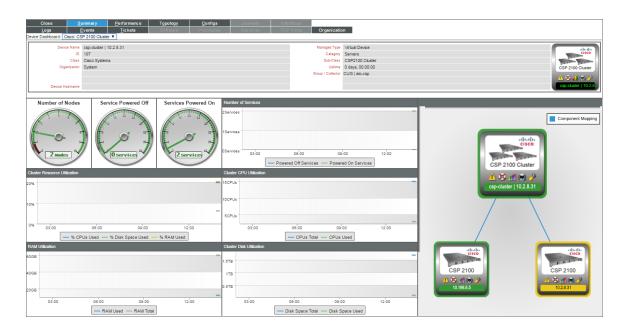
The following sections describe the device dashboards that are included in the Cisco: CSP-2100 PowerPack.

Device Dashboards	
Cisco: CSP 2100 Cluster	
Cisco: CSP 2100 Node	
Cisco: CSP 2100 Service	

#### Device Dashboards

The Cisco: CSP-2100 PowerPack includes device dashboards that provide summary information for Cisco Cloud Services Platform (CSP) 2100 component devices. Each of the device dashboards in the Cisco: CSP-2100 PowerPack are set as the default device dashboard for the equivalent device class.

#### Cisco: CSP 2100 Cluster



The Cisco: CSP 2100 Cluster device dashboard displays the following information:

- Gauges that indicate:
  - The number of nodes in the cluster
  - The number of services in the cluster that are currently powered off
  - The number of services in the cluster that are currently powered on
- The number of services over a specified period of time
- Cluster resource utilization over a specified period of time
- Cluster CPU utilization over a specified period of time
- RAM utilization over a specified period of time
- Cluster disk utilization over a specified period of time
- A topology map displaying the component device and its parent-child relationships

#### Cisco: CSP 2100 Node

Close         Summary         Performance         Topology         Cont           Logs         Events         Tickets         Software         Proce           Device Dashboard:         Cistor: CSP 2100 Node V         V         Proce         Proce	lgs Journalis Interfaces csets Services TCP Ports Organization	
Device Name         102.8.31           IP Address         102.8.31           Casa         Class 5/stems           Ogaracian         System           Calaction Mode         Active           Description         Class Coldud Services Flatform-2100           Rot Detwice ap-chalter (102.8.31         Description	Manago Tyse Physical Device Crargory Methon: Services Suc-Class C5P2100 Uptime 6409, 022812 Collector Time 2017;02-13141000 Oroup / Collector (Old (alc-stop Pavent Device spic-batter   10.2.8.31	
Services Powered On Services Powered Off	ts App: 59, Snppet: 51 threw exception: invakid iteral for int () with base 10 'enp13030'0' ('NukeError: Interface state changed to operationally down: 1, Name: Cisco Cloud Services Platform; previous so Interface state changed to operationally down: 7, Name: Cisco Cloud Services Platform; previous so Interface state changed to operationally down: 7, Name: Cisco Cloud Services Platform; previous so	tate was up (1) tate was up (1)
CSP 2100 Node Vitals	Top 5 Physical Interface by BW Utilization	Node Resource Utilization
	enp130s0f2 enp130s0f0 enp130s0f1	20%
	enp950 4	10%
	4	-
04'00 09'00 09'00 10'00 12'00 14'0 	4	-
	4 0 0kbps 10kbps 20kbps 30kbps 40kbps 50kbps 80kbps 70	Me 0% 03'00 00'00 00'00 12'00
No Matching Data	4 0 Okbps 10kbps 20kbps 30kbps 40kbps 50kbps 60kbps 70 Bandwidth Usage In	AR 0% 00'00 00'00 00'00 12'00 - % CPUS Used - % Disk Space Used - % RAM Used

The Cisco: CSP 2100 Node device dashboard displays the following information:

- Gauges that indicate:
  - The number of services in the node that are currently powered on
  - The number of services in the node that are currently powered off
- A list of tickets and events relating to the node
- Node vitals over a specified period of time
- The top 5 physical interfaces in the node based on bandwidth utilization
- Node resource utilization over a specified period of time
- The top 5 services in the node based on memory utilization
- The top 5 services in the node based on CPU load
- The top 5 services in the node based on disk space utilization

#### Cisco: CSP 2100 Service

Close         Summary         Performance         Topology         Config           Logs         Events         Tickets         Software         Process           Devke Dashboard:         Claco: CSP 2100 Service V         Software         Process	a Journals Interfaces es Services TCP Ports Organization	
Device Name (DSR_CSR_VNF2 0 198 Class / Obeo Systems Oganization System Rect Device is gas dualer   10.2.8.31 Parent Device   10.2.8.31 Device Histikame	Massed Tyse, Component Device Creacyon, Servers & Sub-Chass, CSP Service Uptime, 0 (days, 00.00.00 Group / Collector, CUIG   ab-stp	
Power Status (1-On, 0-Off)	ICkets and Events Gloca: CSP Memory Usage 82.05% Has Exceeded Threshold 50% 2. Topology change: Root DID changed from 194 to 197	
Service Resource Consumption	Service Resource Memory Consumption	Service Resource Disk Consumption
<u> </u>	.808	268
0% 03:00 08:00 08:00 12:00  CPU Load — % Memory Used — % Disk Space Used  Top Service Interfaces by Packets (Total over Last Hour)	03/00 06/00 09/00 12/00  Memory Used — Allocated Memory  Top Service Interfaces by Dropped Packets (Total Last Hour)	03:00 00:00 09:00 12:00  Disk Space Used — Allocated Disk  Top Service Interfaces by Errors (Total Last Hour)
vnet1	vnet1	vnet1 Jenv
2 0Pits 0.01Pits 0.02Pits 0.01Pits 0.04Pits 0.04Pits 0.04Pits 0.00Pits 0.077 Packets Out Packets In	2 0Pxts 0.01Pxts 0.02Pxts 0.02Pxts 0.04Pxts 0.04Pxts 0.04Pxts 0.07 Toropped Packets Out Dropped Packets In	2 0 0.01 0.02 0.03 0.04 0.05 0.06 0.0 Errors Dut Errors In

The Cisco: CSP 2100 Service device dashboard displays the following information:

- The service's power status (i.e., on or off) over a specified period of time
- A list of tickets and events relating to the service
- Service resource consumption over a specified period of time
- Service resource memory consumption over a specified period of time
- Service resource disk consumption over a specified period of time
- The top service interfaces based on packets in and out over the previous hour
- The top service interfaces based on dropped packets in and out over the previous hour
- The top service interfaces based on errors in and out over the previous hour

#### © 2003 - 2021, ScienceLogic, Inc.

#### All rights reserved.

#### LIMITATION OF LIABILITY AND GENERAL DISCLAIMER

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

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

#### Copyrights and Trademarks

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

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

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

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

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

#### Other

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

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



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

International: +1-703-354-1010