Forward-Looking Statements

This presentation may contain forward-looking statements regarding future events, plans or the expected financial performance of our company, including our expectations regarding our products, technology, strategy, customers, markets, acquisitions and investments. These statements reflect management's current expectations, estimates and assumptions based on the information currently available to us. These forward-looking statements are not guarantees of future performance and involve significant risks, uncertainties and other factors that may cause our actual results, performance or achievements to be materially different from results, performance or achievements expressed or implied by the forward-looking statements contained in this presentation.

For additional information about factors that could cause actual results to differ materially from those described in the forward-looking statements made in this presentation, please refer to our periodic reports and other filings with the SEC, including the risk factors identified in our most recent quarterly reports on Form 10-Q and annual reports on Form 10-K, copies of which may be obtained by visiting the Splunk Investor Relations website at www.investors.splunk.com or the SEC's website at www.sec.gov. The forward-looking statements made in this presentation are made as of the time and date of this presentation. If reviewed after the initial presentation, even if made available by us, on our website or otherwise, it may not contain current or accurate information. We disclaim any obligation to update or revise any forward-looking statement based on new information, future events or otherwise, except as required by applicable law.

In addition, any information about our roadmap outlines our general product direction and is subject to change at any time without notice. It is for informational purposes only and shall not be incorporated into any contract or other commitment. We undertake no obligation either to develop the features or functionalities described or to include any such feature or functionality in a future release.

Understanding the Monitoring Console

TRU1172B

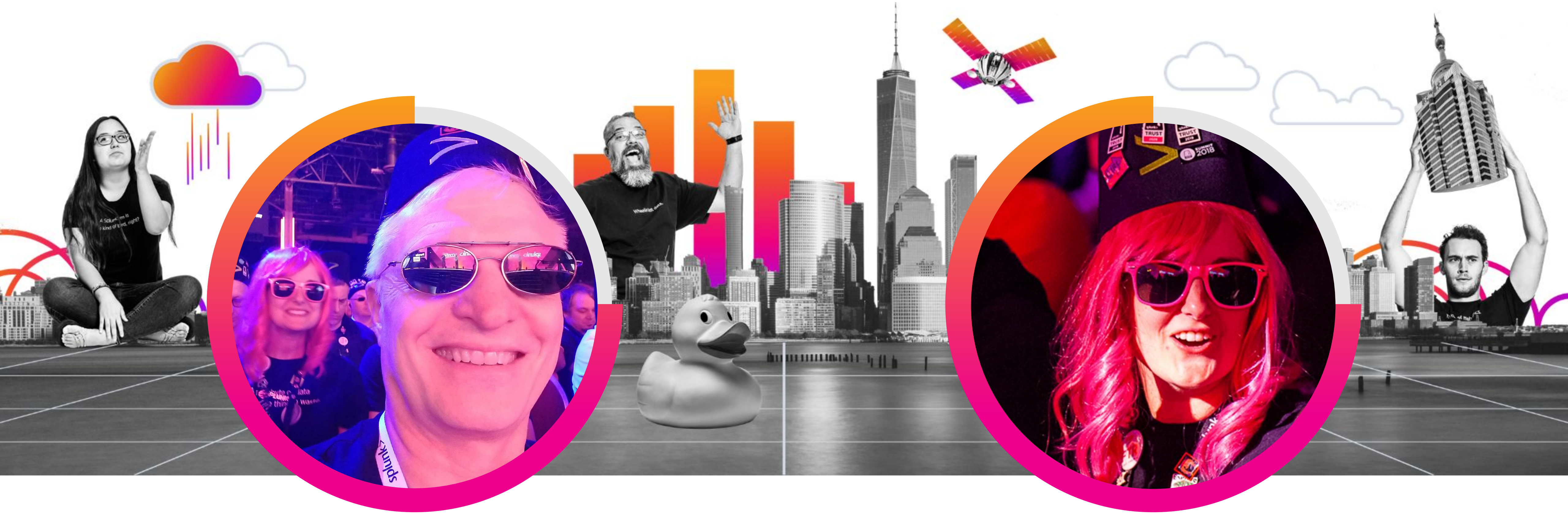
Clara Merriman

Senior Splunk Engineer | Splunk

Cary Petterborg

Splunk Architect | Stage 2 Security

splunk> .conf21



Cary Petterborg

Splunk Architect | Stage 2 Security

Clara Merriman

Senior Splunk Engineer | Splunk

Cary Petterborg

Splunk Architect | Stage 2 Security

Clara Merriman

Senior Splunk Engineer | Splunk

Agenda

What you will learn

The Monitoring Console is a complex and very useful tool that will make understanding your environment much easier.

1) What Should Be Monitored?
   Health of Searching & Indexing, Resource usage, etc.

2) How to Monitor?
   Navigating the UI

3) Where to Run Monitoring?
   Search head, License Master, or ??

4) Set Up Monitoring
   Quick setup guide

5) Troubleshooting Ideas
   Expanding the MC

What's Important?

splunk> .conf21

Content to Monitor

Search

- Scheduler
- Search activity
- Replication
- KV Store

Indexing

- License usage
- Inputs
- SmartStore
- Volumes

Resources

- Memory
- Disk
- CPU

Forwarders

- Status
- Event counts

Instances

- Status

Content to Monitor

Search

- Scheduler
- Search activity
- Replication
- KV Store

Indexing

- License usage
- Inputs
- SmartStore
- Volumes

Resources

- Memory
- Disk
- CPU

Forwarders

- Status
- Event counts

Instances

- Status

Content to Monitor

Search

- Scheduler
- Search activity
- Replication
- KV Store

Indexing

- License usage
- Inputs
- SmartStore
- Volumes

Resources

- Memory
- Disk
- CPU

Forwarders

- Status
- Event counts

Instances

- Status

Content to Monitor

Search

- Scheduler
- Search activity
- Replication
- KV Store

Indexing

- License usage
- Inputs
- SmartStore
- Volumes

Resources

- Memory
- Disk
- CPU

Forwarders

- Status
- Event counts

Instances

- Status

Content to Monitor

Search

- Scheduler
- Search activity
- Replication
- KV Store

Indexing

- License usage
- Inputs
- SmartStore
- Volumes

Resources

- Memory
- Disk
- CPU

Forwarders

- Status
- Event counts

Instances

- Status

Monitor? But How?

splunk> .conf21

Options for Monitoring

Third Party

- Not Splunk supported
- Requires integration

Splunk Alerts

- Splunk supported
- Used for Monitoring
- Create alerts for each use case

Splunk Observability

- Splunk supported
- Developed for Observability
- Create alerts for each use case

Monitoring Console

- Splunk supported
- Developed for Monitoring
- Out of the box dashboards, healthchecks, and alerts.

Options for Monitoring

Third Party

- Not Splunk supported
- Requires integration

Splunk Alerts

- Splunk supported
- Used for Monitoring
- Create alerts for each use case

Splunk Observability

- Splunk supported
- Developed for Observability
- Create alerts for each use case

Monitoring Console

- Splunk supported
- Developed for Monitoring
- Out of the box dashboards, healthchecks, and alerts.

Options for Monitoring

Third Party

- Not Splunk supported
- Requires integration

Splunk Alerts

- Splunk supported
- Used for Monitoring
- Create alerts for each use case

Splunk Observability

- Splunk supported
- Developed for Observability
- Create alerts for each use case

Monitoring Console

- Splunk supported
- Developed for Monitoring
- Out of the box dashboards, healthchecks, and alerts.

Options for Monitoring

Third Party

- Not Splunk supported
- Requires integration

Splunk Alerts

- Splunk supported
- Used for Monitoring
- Create alerts for each use case

Splunk Observability

- Splunk supported
- Developed for Observability
- Create alerts for each use case

Monitoring Console

- Splunk supported
- Developed for Monitoring
- Out of the box dashboards, healthchecks, and alerts.

Wherefore art Thou, MC?

Where do I put it?

splunk> .conf21

Where Makes Sense?

So many locations

When in doubt, a Standalone SH will work.

- meet SH hardware requirements

Do not host the MC on a SH used for another purpose

- ties up resources
- searches may be incomplete

Do not host the MC on a DS with more than 50 clients

- interfere with each other

Instance Type	Distributed Mode?	Indexer Clustering?	Search Head Clustering
LM/DS	No	N/A	N/A
Manager Node	Yes	Yes	N/A
Standalone SH	N/A	N/A	N/A
Deployer	Yes	No	Yes

MC Setup

The ***WHERE*** and the ***HOW***

splunk> .conf21

Set Up

Checklist

- For each monitored instance:
  - Unique `serverName` in server.conf
  - Unique `host` in inputs.conf
  - Enable platform instrumentation, except forwarders
  - Forward internal logs
- `admin_all_objects` capability is required for users setting up the Monitoring Console

Set Up

By environment type

Distributed Mode

- Set SHC and IDXC labels
  - Both found in server.conf
  - IDXC: While setting up the Manager node

    ```
    [clustering]
    cluster_label =
    ```
  - SHC: While setting up the Deployer

    ```
    [shclustering]
    shcluster_label =
    ```
- Add search peers
- Set distributed mode

Standalone Mode

- Set standalone mode

OPTIONS FOR BOTH:

- Configure Forwarder monitoring
- Enable platform alerts
- Customize Health Checks
- Customize Overview dashboard

Set Up

By Environment Type

Distributed Mode

- Set SHC and IDXC labels
  - Both found in server.conf
  - IDXC: While setting up the Manager node

    ```
    [clustering]
    cluster_label =
    ```
  - SHC: While setting up the Deployer

    ```
    [shclustering]
    shcluster_label =
    ```
- Add search peers
- Set distributed mode

Standalone Mode

- Set standalone mode

OPTIONS FOR BOTH:

- Configure Forwarder monitoring
- Enable platform alerts
- Customize Health Checks
- Customize Overview dashboard

Set Up

By Environment Type

Distributed Mode

- Set SHC and IDXC labels
  - Both found in server.conf
  - IDXC: While setting up the Manager node

```
[clustering]
cluster_label =
```

  - SHC: While setting up the Deployer

```
[shclustering]
shcluster_label =
```

- Add search peers
- Set distributed mode

Standalone Mode

- Set standalone mode

OPTIONS FOR BOTH:

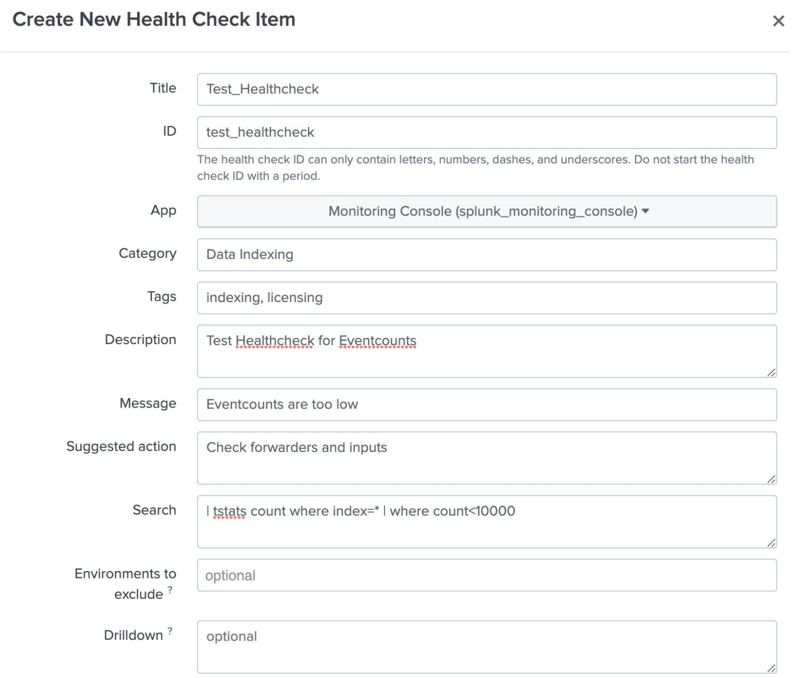
- Configure Forwarder monitoring
- Enable platform alerts
- Customize Health Checks
- Customize Overview dashboard

Health Checks

Environmental physicals

Create

Monitoring Console > Settings > Health Check Items



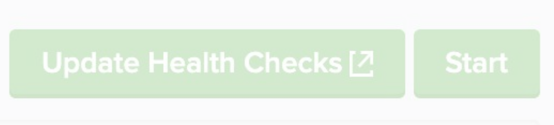
Create New Health Check Item ×

Title	Test_Healthcheck
ID	test_healthcheck The health check ID can only contain letters, numbers, dashes, and underscores. Do not start the health check ID with a period.
App	Monitoring Console (splunk_monitoring_console) ▾
Category	Data Indexing
Tags	indexing, licensing
Description	Test Healthcheck for Eventcounts
Message	Eventcounts are too low
Suggested action	Check forwarders and inputs
Search	| tstats count where index=* | where count<10000
Environments to exclude ?	optional
Drilldown ?	optional

Update

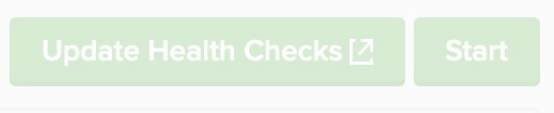
Monitoring Console > Settings > Health Check Items

Monitoring Console > Health Check > Update Health Checks



Use

Monitoring Console > Health Check > Start

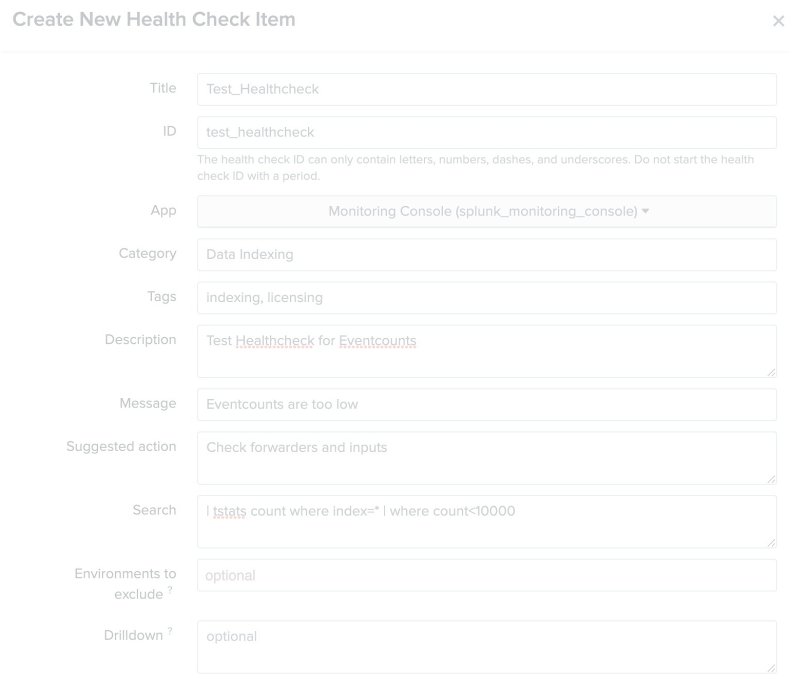


Health Checks

Environmental physicals

Create

Monitoring Console > Settings > Health Check Items

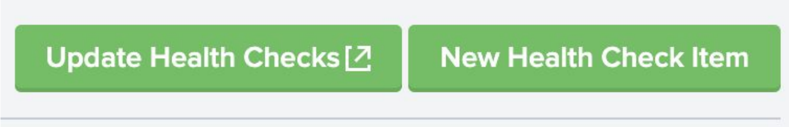


Create New Health Check Item

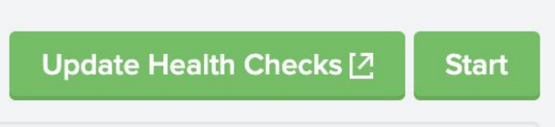
Title	Test_Healthcheck
ID	test_healthcheck The health check ID can only contain letters, numbers, dashes, and underscores. Do not start the health check ID with a period.
App	Monitoring Console (splunk_monitoring_console) ▾
Category	Data Indexing
Tags	indexing, licensing
Description	Test Healthcheck for Eventcounts
Message	Eventcounts are too low
Suggested action	Check forwarders and inputs
Search	| tstats count where index=* | where count<10000
Environments to exclude ?	optional
Drilldown ?	optional

Update

Monitoring Console > Settings > Health Check Items

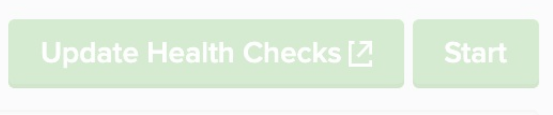


Monitoring Console > Health Check > Update Health Checks



Use

Monitoring Console > Health Check > Start

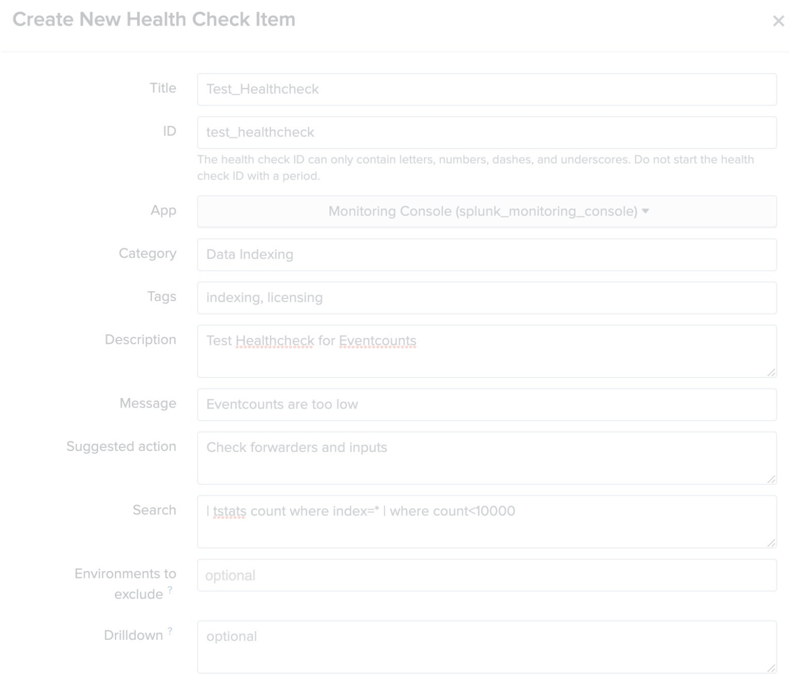


Health Checks

Environmental physicals

Create

Monitoring Console > Settings > Health Check Items

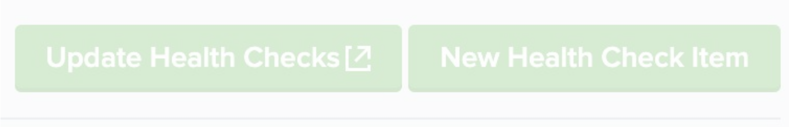


Create New Health Check Item

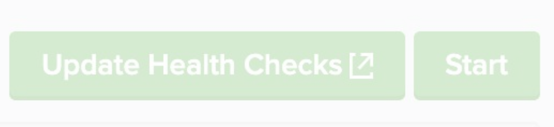
Title	Test_Healthcheck
ID	test_healthcheck The health check ID can only contain letters, numbers, dashes, and underscores. Do not start the health check ID with a period.
App	Monitoring Console (splunk_monitoring_console) ▾
Category	Data Indexing
Tags	indexing, licensing
Description	Test Healthcheck for Eventcounts
Message	Eventcounts are too low
Suggested action	Check forwarders and inputs
Search	| tstats count where index=* | where count<10000
Environments to exclude ?	optional
Drilldown ?	optional

Update

Monitoring Console > Settings > Health Check Items

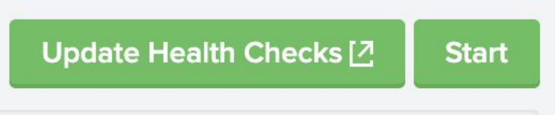


Monitoring Console > Health Check > Update Health Checks



Use

Monitoring Console > Health Check > Start



Platform Alerts

Monitoring made easy

- Monitoring Console > Settings > Alerts Setup
  - edit threshold
  - go to saved search
  - disable
- Settings > Searches, reports, and alerts
  - edit/run search
- If creating new alert via UI in MC app, thresholds are uneditable

If adding new alerts:

Changes need to be made in:

- local/dmc_alerts.conf
- local/savedsearches.conf
- Threshold may not be reflected in the UI, unless updated there as well

Platform Alerts

Monitoring Made Easy

- Monitoring Console > Settings > Alerts Setup
  - edit threshold
  - go to saved search
  - disable
- Settings > Searches, reports, and alerts
  - edit/run search
- If creating new alert via UI in MC app, thresholds are uneditable

If adding new alerts:

Changes need to be made in:

- local/dmc_alerts.conf
- local/savedsearches.conf
- Threshold may not be reflected in the UI, unless updated there as well

Platform Alerts

Monitoring Made Easy

- Monitoring Console > Settings > Alerts Setup
  - edit threshold
  - go to saved search
  - disable
- Settings > Searches, reports, and alerts
  - edit/run search
- If creating new alert via UI in MC app, thresholds are uneditable

If adding new alerts, changes must be made in:

- local/dmc_alerts.conf
- local/savedsearches.conf
- Threshold may not be reflected in the UI, unless updated there as well

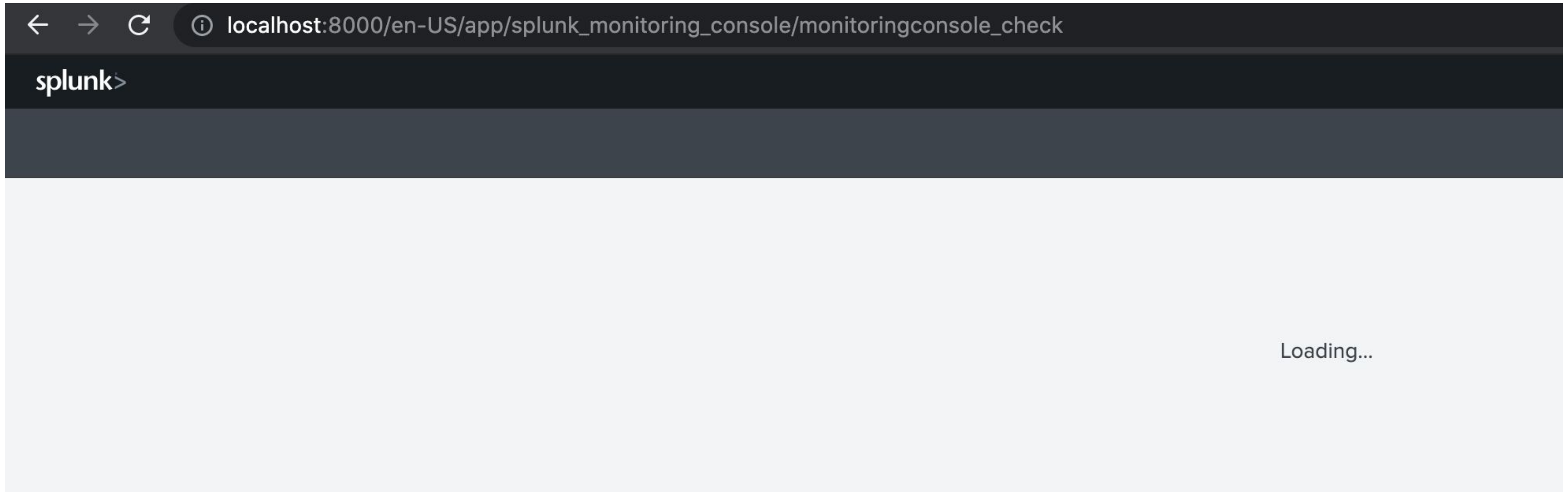
What About Issues?

splunk> .conf21

Health Check Issues

Just load already!

- Monitoring Console > Health Check stuck on Loading…
  - empty checklist.conf, use btool
  - Pre v7.3.6/v8.0.4, UF license in use



localhost:8000/en-US/app/splunk_monitoring_console/monitoringconsole_check

Loading...

Health Check Issues

Where’s my inventory?!

- assets.csv
  - All MC searches run from this
  - Settings > Distributed Search > Search Peers
  - May need to update/apply changes in Monitoring Console > Settings > General Setup
- dmc_forwarder_assets.csv
  - Monitoring Console > Settings > Forwarder Monitoring Setup > Rebuild forwarder assets
  - Limited to 50,000 forwarders in the UI

Health Check Issues

Where's my inventory?!

- assets.csv
  - All MC searches run from this
  - Settings > Distributed Search > Search Peers
  - May need to update/apply changes in Monitoring Console > Settings > General Setup
- dmc_forwarder_assets.csv
  - Monitoring Console > Settings > Forwarder Monitoring Setup > Rebuild forwarder assets
  - Limited to 50,000 forwarders in the UI

Key Takeaways

splunk> .conf21

What to Remember

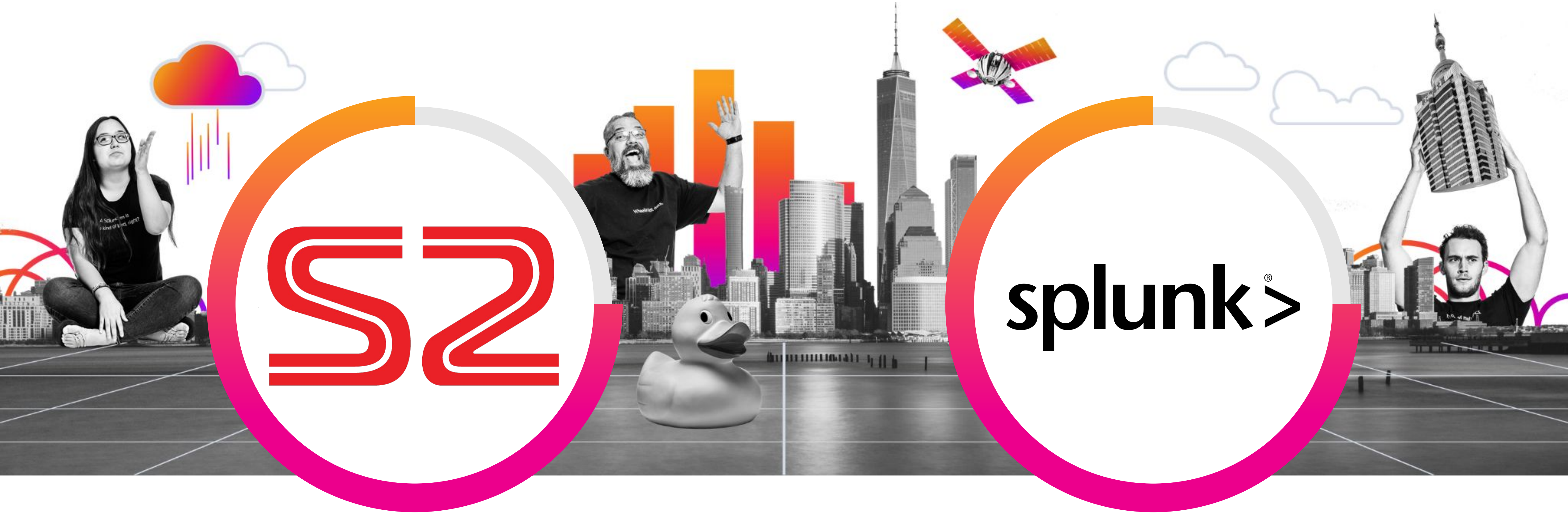
- Monitoring the critical aspects of the entire environment is crucial
- Using the Monitoring Console paired with Splunk Alerts and Splunk Observability gives an all around picture and flexibility
- Proper setup of the Monitoring Console is vital
- Health Checks and Platform Alerts are customizable

Resources

splunk> .conf21

Resources/ Links/ Additional Help

- Where to set up a DMC
- Setup Checklist
- Single Instance Setup
- Deployment Setup
- Health Checks
- Platform Alerts
- Health Check Not Running
- New Indexers Not Updating



Cary Petterborg

Splunk Architect | Stage 2 Security

Clara Merriman

Senior Splunk Engineer | Splunk

Thank You

Please provide feedback via the

SESSION SURVEY