Creating Alerts and Dashboard

Splunk® Configuration Guide

IBM Confidential

Note:

Before you use this information and the product it supports, read the information in "Notices" on page 11.

August 2024 edition

This edition applies to IBM Storage Defender Data Management Service and to all subsequent releases and modifications until otherwise indicated in new editions:

- IBM Storage Defender ordered through Passport Advantage® (product number 5900-AXW)
- IBM Storage Defender Data Management Service ordered through AAS (product number 5900-AY6)

Contents

About this publication

This publication provides overview, planning, installation, and user instructions for IBM Storage Defender Data Resiliency Service.

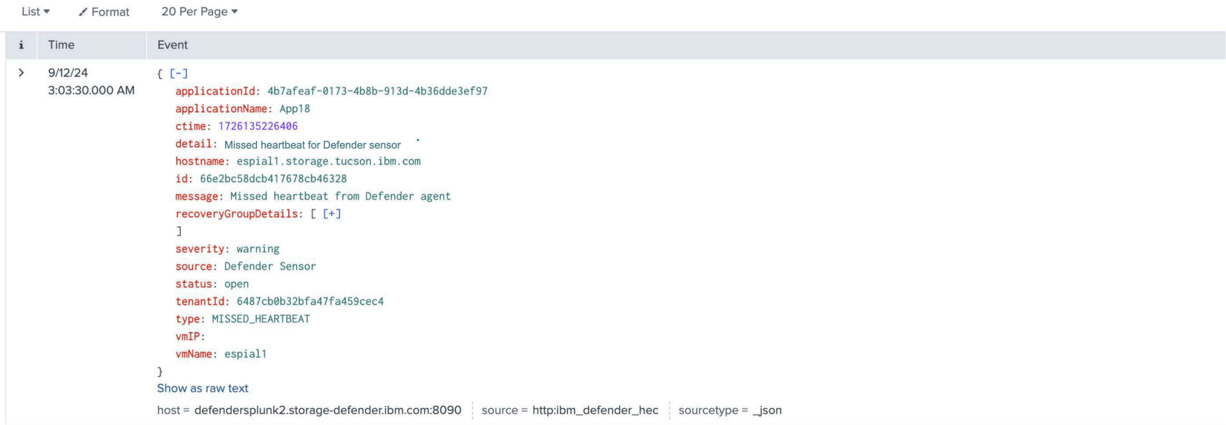
Chapter 1. Creating IBM Storage Defender alerts in Splunk®

Procedure

1. Log in with your Splunk® Enterprise account by using your admin credentials.
2. Click **Search and reporting** in the navigation bar under **Apps**.
3. Search for `index=ibm_defender type POTENTIAL_THREAT` in the search bar.

   ```
   index="ibm_defender" message="Potential threat detected"
   ```

   The following figure displays the alert details for the `MISSED_HEARTBEAT` type alert.

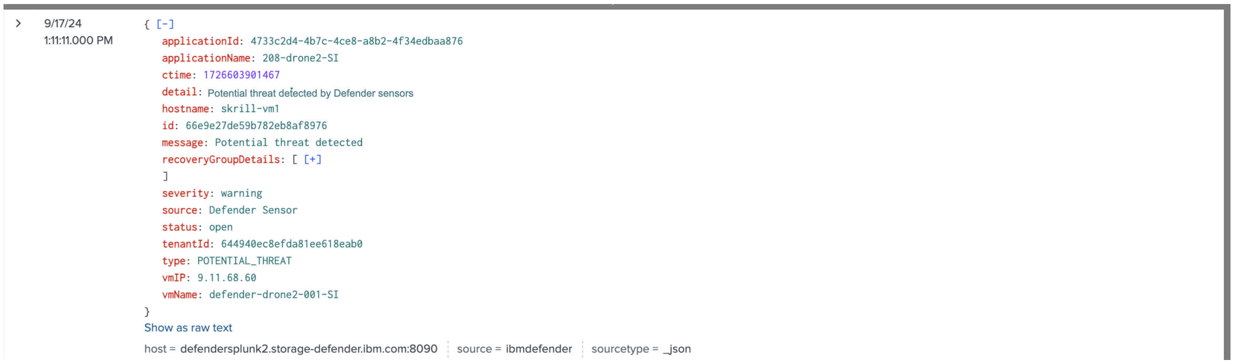
   9/12/24
   3:03:30.000 AM

   ```
   { [-]
     applicationId: 4b7afeaf-0173-4b8b-913d-4b36dde3ef97
     applicationName: App18
     ctime: 1726135226406
     detail: Missed heartbeat for Defender sensor
     hostname: espial1.storage.tucson.ibm.com
     id: 66e2bc58dcb417678cb46328
     message: Missed heartbeat from Defender agent
     recoveryGroupDetails: [ [+]
     ]
     severity: warning
     source: Defender Sensor
     status: open
     tenantId: 6487cb0b32bfa47fa459cec4
     type: MISSED_HEARTBEAT
     vmIP:
     vmName: espial1
   }
   ```

   host = defendersplunk2.storage-defender.ibm.com:8090 | source = http:ibm_defender_hec | sourcetype = _json

   Figure 1. Alert details for MISSED_HEARTBEAT

   The following figure displays the alert details for the `POTENTIAL_THREAT` type alert.

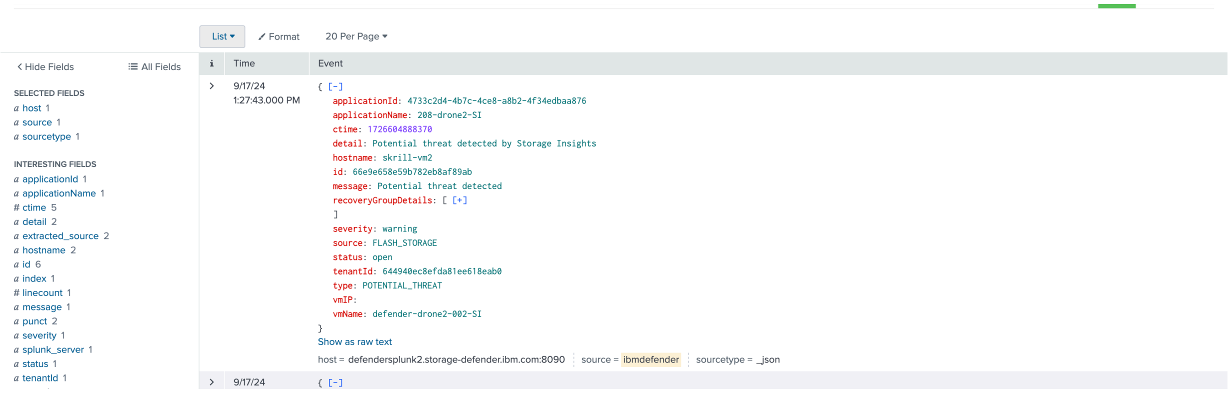
   9/17/24
   1:11:11.000 PM

   ```
   { [-]
     applicationId: 4733c2d4-4b7c-4ce8-a8b2-4f34edbaa876
     applicationName: 208-drone2-SI
     ctime: 1726603901467
     detail: Potential threat detected by Defender sensors
     hostname: skrill-vm1
     id: 66e9e27de59b782eb8af8976
     message: Potential threat detected
     recoveryGroupDetails: [ [+]
     ]
     severity: warning
     source: Defender Sensor
     status: open
     tenantId: 644940ec8efda81ee618eab0
     type: POTENTIAL_THREAT
     vmIP: 9.11.68.60
     vmName: defender-drone2-001-SI
   }
   ```

   host = defendersplunk2.storage-defender.ibm.com:8090 | source = ibmdefender | sourcetype = _json

   Figure 2. Alert details for POTENTIAL_THREAT

   The following figure displays the alert details for the `FLASH_STORAGE POTENTIAL_THREAT` type alert.



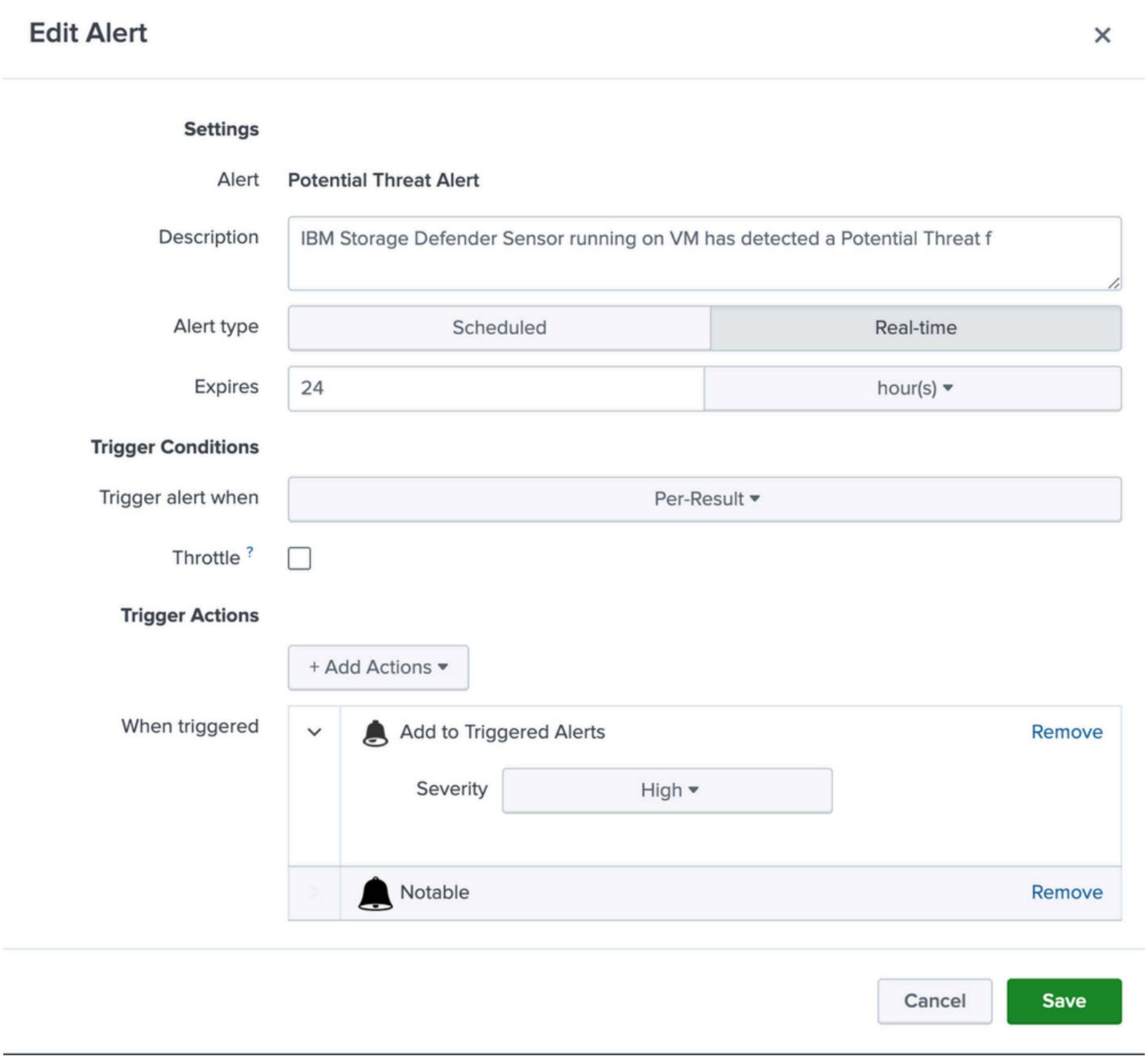
```
{ [-]
   applicationId: 4733c2d4-4b7c-4ce8-a8b2-4f34edbaa876
   applicationName: 208-drone2-SI
   ctime: 1726604888370
   detail: Potential threat detected by Storage Insights
   hostname: skrill-vm2
   id: 66e9e658e59b782eb8af89ab
   message: Potential threat detected
   recoveryGroupDetails: [ [+]
   ]
   severity: warning
   source: FLASH_STORAGE
   status: open
   tenantId: 644940ec8efda81ee618eab0
   type: POTENTIAL_THREAT
   vmIP:
   vmName: defender-drone2-002-SI
}
```

host = defendersplunk2.storage-defender.ibm.com:8090 | source = ibmdefender | sourcetype = _json

```
{ [-]
```

Figure 3. Alert details for FLASH_STORAGE POTENTIAL_THREAT

4. Click **Save As** and select **Alert**.
5. Provide details about the alert in the **Edit Alert** section. Enter the description in the **Description** field. Select the alert type and schedule in the respective fields.
   a) If Splunk® Enterprise Security app is installed, then in **Trigger Actions**, click **Add Actions**, and choose **Notable**. For example, **Add to Triggered Alerts**, and click **Save**. The step generates an alert in Splunk® Enterprise Security.
   b) You can choose other appropriate actions based on your setup.



Edit Alert

Settings

Alert: Potential Threat Alert

Description: IBM Storage Defender Sensor running on VM has detected a Potential Threat f

Alert type: Scheduled | Real-time

Expires: 24 hour(s)

Trigger Conditions

Trigger alert when: Per-Result

Throttle: □

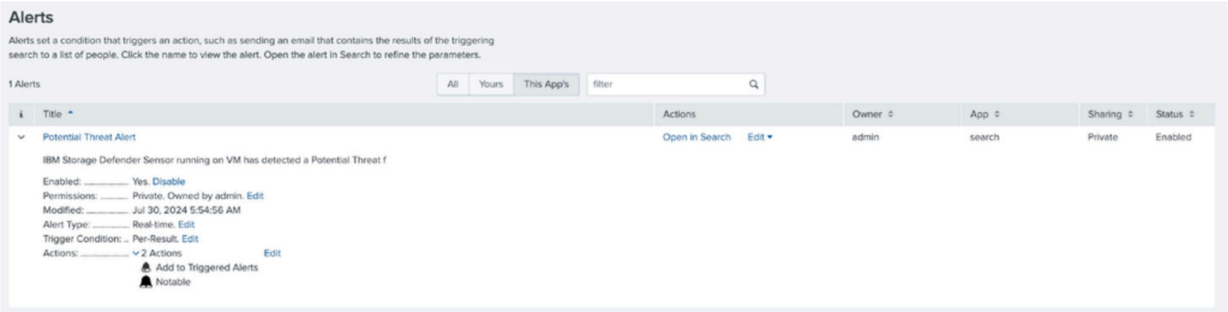
Trigger Actions

When triggered:

- Add to Triggered Alerts — Severity: High
- Notable

Figure 4. Editing alerts

6. Verify the alerts that you have created in the **Alert** section.



Alerts

Alerts set a condition that triggers an action, such as sending an email that contains the results of the triggering search to a list of people. Click the name to view the alert. Open the alert in Search to refine the parameters.

1 Alerts

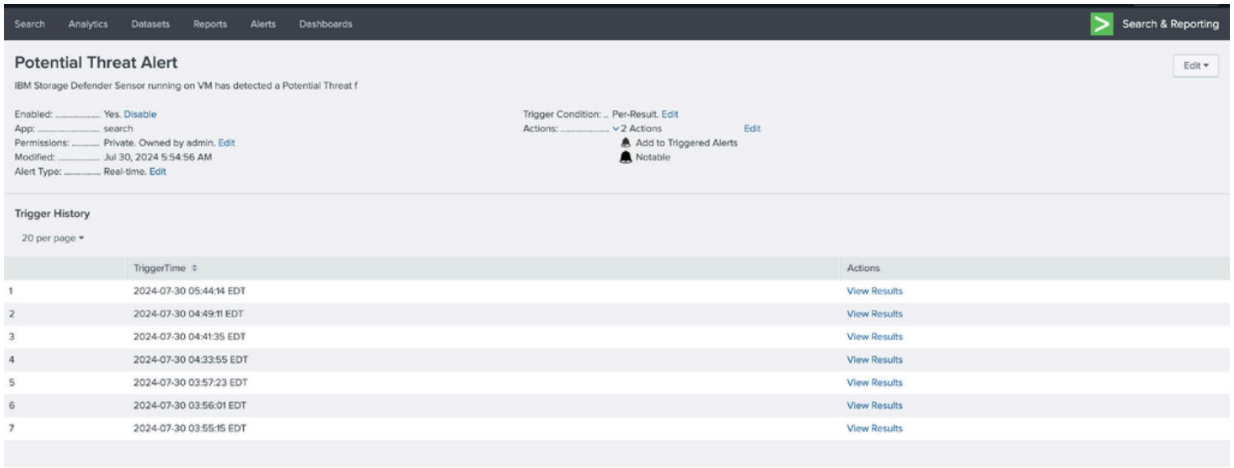
i	Title	Actions	Owner	App	Sharing	Status
⌄	Potential Threat Alert	Open in Search Edit ▾	admin	search	Private	Enabled

IBM Storage Defender Sensor running on VM has detected a Potential Threat f

Enabled: .... Yes. Disable
Permissions: .... Private. Owned by admin. Edit
Modified: .... Jul 30, 2024 5:54:56 AM
Alert Type: .... Real-time. Edit
Trigger Condition: .. Per-Result. Edit
Actions: .... ⌄2 Actions Edit
Add to Triggered Alerts
Notable

Figure 5. Verifying alerts

The following figure displays a sample of alerts' trigger history.



Potential Threat Alert

IBM Storage Defender Sensor running on VM has detected a Potential Threat f

Enabled: Yes. Disable
App: search
Permissions: Private. Owned by admin. Edit
Modified: Jul 30, 2024 5:54:56 AM
Alert Type: Real-time. Edit

Trigger Condition: Per-Result. Edit
Actions: 2 Actions Edit
Add to Triggered Alerts
Notable

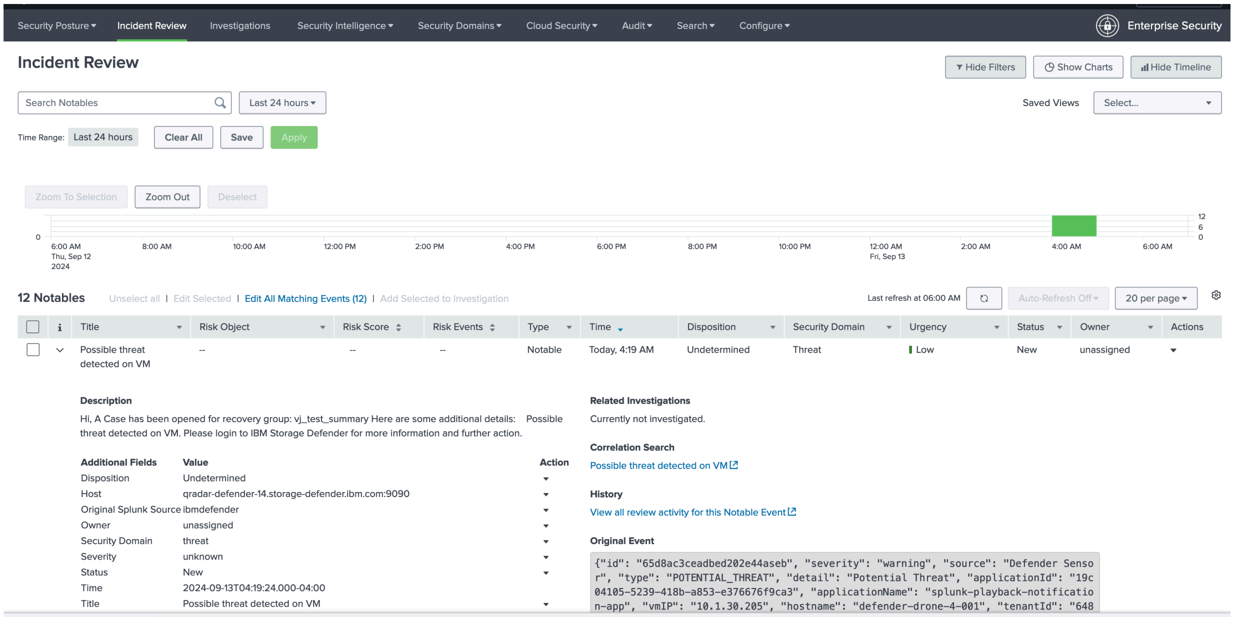
Trigger History

20 per page ▾

	TriggerTime	Actions
1	2024-07-30 05:44:14 EDT	View Results
2	2024-07-30 04:49:11 EDT	View Results
3	2024-07-30 04:41:35 EDT	View Results
4	2024-07-30 04:33:55 EDT	View Results
5	2024-07-30 03:57:23 EDT	View Results
6	2024-07-30 03:56:01 EDT	View Results
7	2024-07-30 03:55:15 EDT	View Results

Figure 6. Viewing trigger history of alerts

7. If you are using Splunk® Enterprise Security, you can check the **Incident Review** dashboard. Go to **Enterprise Security** > **Incident Review**. You can view the notable events and incidents that are generated.



Incident Review

Time Range: Last 24 hours

12 Notables

Last refresh at 06:00 AM

☐	i	Title	Risk Object	Risk Score	Risk Events	Type	Time	Disposition	Security Domain	Urgency	Status	Owner	Actions
☐	⌄	Possible threat detected on VM	--	--	--	Notable	Today, 4:19 AM	Undetermined	Threat	Low	New	unassigned	▾

Description

Hi, A Case has been opened for recovery group: vj_test_summary Here are some additional details: Possible threat detected on VM. Please login to IBM Storage Defender for more information and further action.

Additional Fields	Value	Action
Disposition	Undetermined	▾
Host	qradar-defender-14.storage-defender.ibm.com:9090	▾
Original Splunk Source	ibmdefender	▾
Owner	unassigned	▾
Security Domain	threat	▾
Severity	unknown	▾
Status	New	▾
Time	2024-09-13T04:19:24.000-04:00	
Title	Possible threat detected on VM	▾

Related Investigations

Currently not investigated.

Correlation Search

Possible threat detected on VM

History

View all review activity for this Notable Event

Original Event

```
{"id": "65d8ac3ceadbed202e44aseb", "severity": "warning", "source": "Defender Senso
r", "type": "POTENTIAL_THREAT", "detail": "Potential Threat", "applicationId": "19c
04105-5239-418b-a853-e376676f9ca3", "applicationName": "splunk-playback-notificatio
n-app", "vmIP": "10.1.30.205", "hostname": "defender-drone-4-001", "tenantId": "648
```

Figure 7. Viewing incidents and events

The following table describes the custom properties of IBM Storage Defender events.

Table 1. Custom properties of IBM Storage Defender events

Property name	Description
`applicationId`	The ID of the recovery group for which the IBM Storage Defender event is triggered.
`applicationName`	The name of the recovery group for which the IBM Storage Defender event is triggered.
`hostname`	The hostname of the virtual machine for which an IBM Storage Defender event is generated.
`status`	The case status of the IBM Storage Defender event.

Table 1. Custom properties of IBM Storage Defender events (continued)

Property name	Description
`type`	The type of the IBM Storage Defender event.
`vmIP`	The IP address of the virtual machine for which the IBM Storage Defender event is generated.
`vmName`	The name of the virtual machine for which the IBM Storage Defender event is generated.

For more information, see Recovery group.

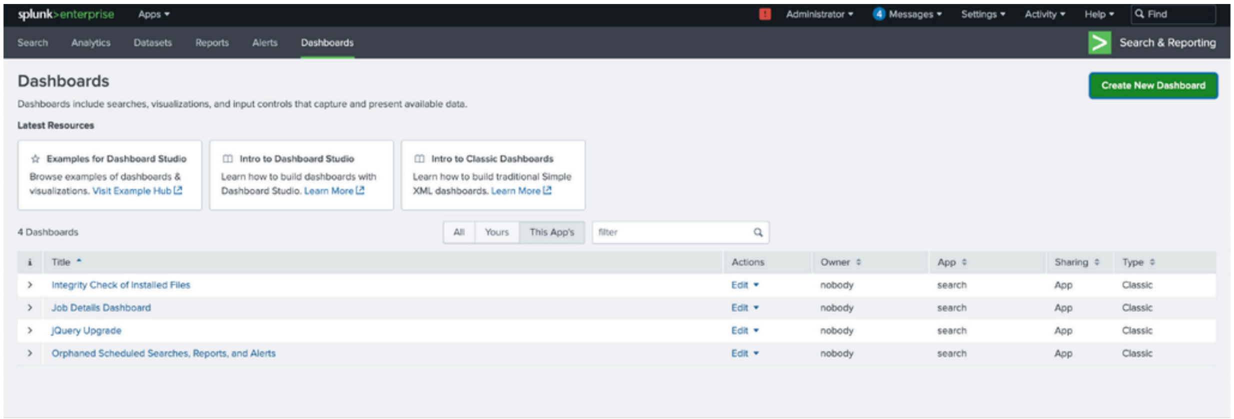
Chapter 2. Creating a dashboard in Splunk®

The following steps are optional and are meant to be a guide for you to add dashboards in Splunk® for IBM Storage Defender events, if needed.

About this task

Procedure

1. Click the **Dashboard** tab, then click **Create New Dashboard**.



Dashboards

Dashboards include searches, visualizations, and input controls that capture and present available data.

Latest Resources

☆ Examples for Dashboard Studio
Browse examples of dashboards & visualizations. Visit Example Hub

Intro to Dashboard Studio
Learn how to build dashboards with Dashboard Studio. Learn More

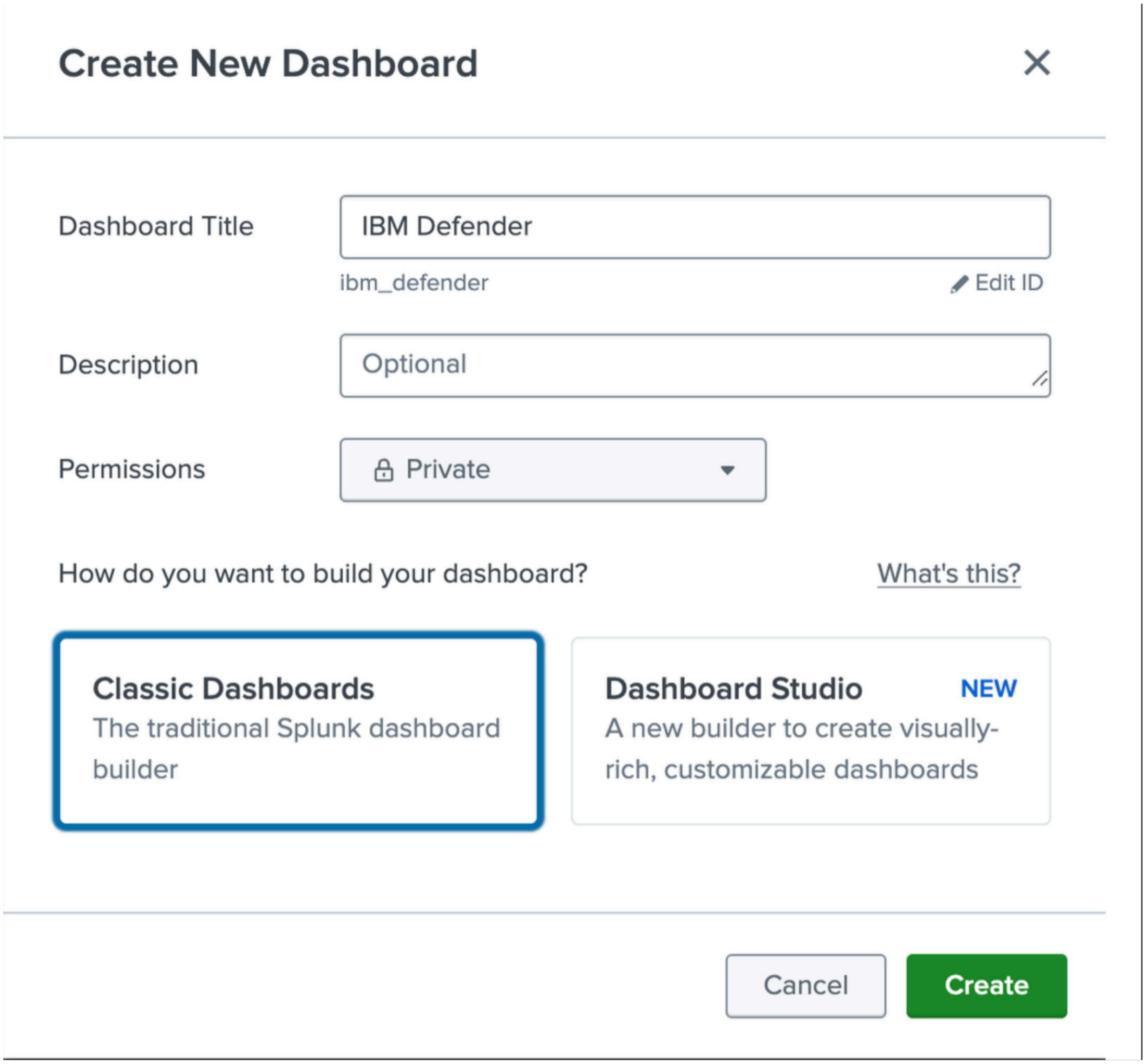
Intro to Classic Dashboards
Learn how to build traditional Simple XML dashboards. Learn More

4 Dashboards

i	Title ▴	Actions	Owner ⇕	App ⇕	Sharing ⇕	Type ⇕
>	Integrity Check of Installed Files	Edit ▾	nobody	search	App	Classic
>	Job Details Dashboard	Edit ▾	nobody	search	App	Classic
>	JQuery Upgrade	Edit ▾	nobody	search	App	Classic
>	Orphaned Scheduled Searches, Reports, and Alerts	Edit ▾	nobody	search	App	Classic

Figure 8. Creating a dashboard

2. Provide the details, and select **Classic Dashboard**.



Create New Dashboard

Dashboard Title: IBM Defender

ibm_defender

Description: Optional

Permissions: Private

How do you want to build your dashboard?

Classic Dashboards
The traditional Splunk dashboard builder

Dashboard Studio NEW
A new builder to create visually-rich, customizable dashboards

Figure 9. Providing required details

3. Click **Add Panel**, then select **Statistics Table**.

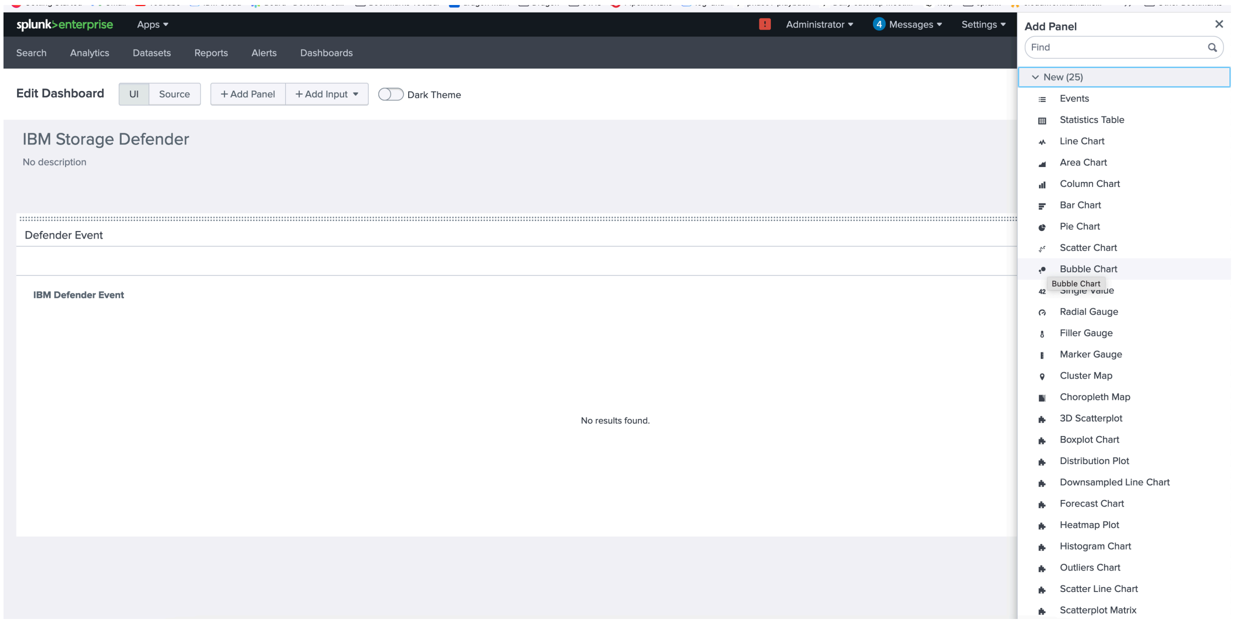
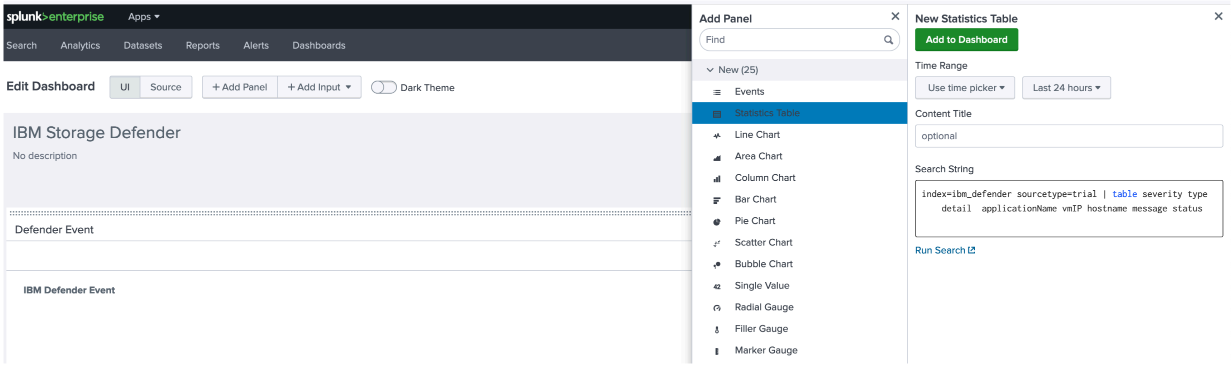


Figure 10. Adding panel and table

4. Provide content title and search string. A sample search string is shown as follows:

```
index=ibm_defender | table severity type
     detail applicationName vmIP hostname message status
```



Time Range: Use time picker ▾ Last 24 hours ▾

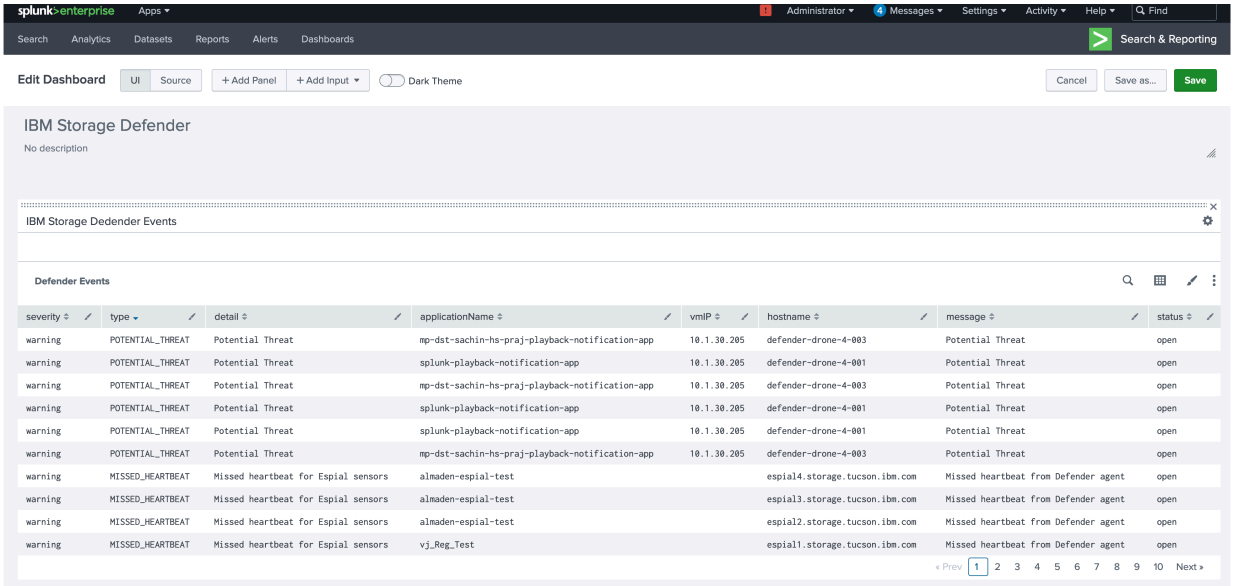
Content Title: optional

Search String:

```
index=ibm_defender sourcetype=trial | table severity type
    detail  applicationName vmIP hostname message status
```

Figure 11. Adding content tile and search string

5. Click **Add to Dashboard**, then click **Save**.



IBM Storage Defender

No description

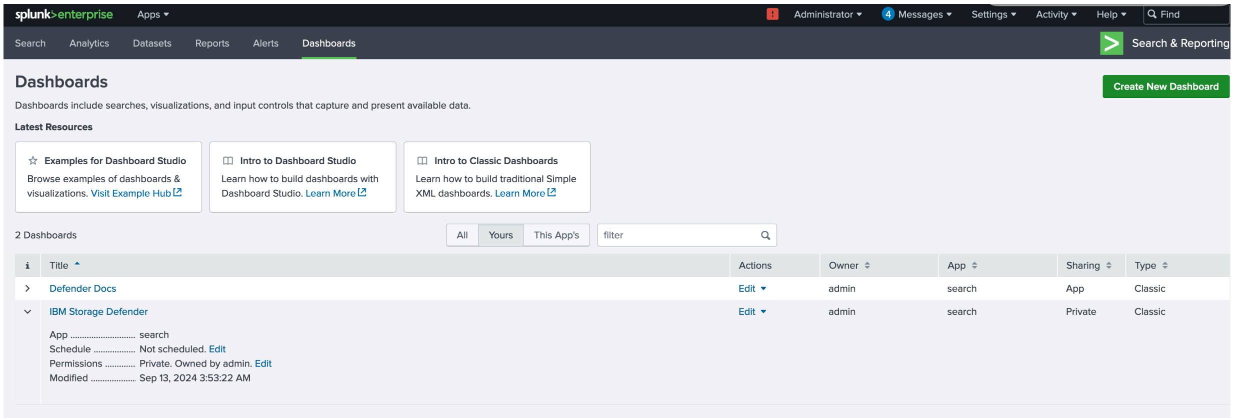
IBM Storage Dedender Events

Defender Events

severity	type	detail	applicationName	vmIP	hostname	message	status
warning	POTENTIAL_THREAT	Potential Threat	mp-dst-sachin-hs-praj-playback-notification-app	10.1.30.205	defender-drone-4-003	Potential Threat	open
warning	POTENTIAL_THREAT	Potential Threat	splunk-playback-notification-app	10.1.30.205	defender-drone-4-001	Potential Threat	open
warning	POTENTIAL_THREAT	Potential Threat	mp-dst-sachin-hs-praj-playback-notification-app	10.1.30.205	defender-drone-4-003	Potential Threat	open
warning	POTENTIAL_THREAT	Potential Threat	splunk-playback-notification-app	10.1.30.205	defender-drone-4-001	Potential Threat	open
warning	POTENTIAL_THREAT	Potential Threat	splunk-playback-notification-app	10.1.30.205	defender-drone-4-001	Potential Threat	open
warning	POTENTIAL_THREAT	Potential Threat	mp-dst-sachin-hs-praj-playback-notification-app	10.1.30.205	defender-drone-4-003	Potential Threat	open
warning	MISSED_HEARTBEAT	Missed heartbeat for Espial sensors	almaden-espial-test		espial4.storage.tucson.ibm.com	Missed heartbeat from Defender agent	open
warning	MISSED_HEARTBEAT	Missed heartbeat for Espial sensors	almaden-espial-test		espial3.storage.tucson.ibm.com	Missed heartbeat from Defender agent	open
warning	MISSED_HEARTBEAT	Missed heartbeat for Espial sensors	almaden-espial-test		espial2.storage.tucson.ibm.com	Missed heartbeat from Defender agent	open
warning	MISSED_HEARTBEAT	Missed heartbeat for Espial sensors	vj_Reg_Test		espial1.storage.tucson.ibm.com	Missed heartbeat from Defender agent	open

Figure 12. Saving dashboard

6. Go to the **Dashboard** tab, and selecting IBM Storage Defender to view the dashboard you created.



Dashboards

Dashboards include searches, visualizations, and input controls that capture and present available data.

Latest Resources

Examples for Dashboard Studio
Browse examples of dashboards & visualizations. Visit Example Hub

Intro to Dashboard Studio
Learn how to build dashboards with Dashboard Studio. Learn More

Intro to Classic Dashboards
Learn how to build traditional Simple XML dashboards. Learn More

2 Dashboards

i	Title	Actions	Owner	App	Sharing	Type
>	Defender Docs	Edit ▾	admin	search	App	Classic
⌄	IBM Storage Defender	Edit ▾	admin	search	Private	Classic

App .... search
Schedule .... Not scheduled. Edit
Permissions .... Private. Owned by admin. Edit
Modified .... Sep 13, 2024 3:53:22 AM

Figure 13. Viewing dashboard

Related information

Splunk | Steps to create an alert in splunk

Modify notable event urgency

Notices

This information was developed for products and services offered in the US. This material might be available from IBM® in other languages. However, you may be required to own a copy of the product or product version in that language in order to access it.

IBM may not offer the products, services, or features discussed in this document in other countries. Consult your local IBM representative for information on the products and services currently available in your area. Any reference to an IBM product, program, or service is not intended to state or imply that only that IBM product, program, or service may be used. Any functionally equivalent product, program, or service that does not infringe any IBM intellectual property right may be used instead. However, it is the user's responsibility to evaluate and verify the operation of any non-IBM product, program, or service.

IBM may have patents or pending patent applications covering subject matter described in this document. The furnishing of this document does not grant you any license to these patents. You can send license inquiries, in writing, to:

IBM Director of Licensing
IBM Corporation
North Castle Drive, MD-NC119
Armonk, NY 10504-1785
US

For license inquiries regarding double-byte character set (DBCS) information, contact the IBM Intellectual Property Department in your country or send inquiries, in writing, to:

Intellectual Property Licensing
Legal and Intellectual Property Law
IBM Japan Ltd.
19-21, Nihonbashi-Hakozakicho, Chuo-ku
Tokyo 103-8510, Japan

INTERNATIONAL BUSINESS MACHINES CORPORATION PROVIDES THIS PUBLICATION "AS IS" WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESS OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF NON-INFRINGEMENT, MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE. Some jurisdictions do not allow disclaimer of express or implied warranties in certain transactions, therefore, this statement may not apply to you.

This information could include technical inaccuracies or typographical errors. Changes are periodically made to the information herein; these changes will be incorporated in new editions of the publication. IBM may make improvements and/or changes in the product(s) and/or the program(s) described in this publication at any time without notice.

Any references in this information to non-IBM websites are provided for convenience only and do not in any manner serve as an endorsement of those websites. The materials at those websites are not part of the materials for this IBM product and use of those websites is at your own risk.

IBM may use or distribute any of the information you supply in any way it believes appropriate without incurring any obligation to you.

Licensees of this program who wish to have information about it for the purpose of enabling: (i) the exchange of information between independently created programs and other programs (including this one) and (ii) the mutual use of the information which has been exchanged, should contact:

IBM Director of Licensing
IBM Corporation
North Castle Drive, MD-NC119
Armonk, NY 10504-1785
US

Such information may be available, subject to appropriate terms and conditions, including in some cases, payment of a fee.

The licensed program described in this document and all licensed material available for it are provided by IBM under terms of the IBM Customer Agreement, IBM International Program License Agreement or any equivalent agreement between us.

The performance data discussed herein is presented as derived under specific operating conditions. Actual results may vary.

Information concerning non-IBM products was obtained from the suppliers of those products, their published announcements or other publicly available sources. IBM has not tested those products and cannot confirm the accuracy of performance, compatibility or any other claims related to non-IBM products. Questions on the capabilities of non-IBM products should be addressed to the suppliers of those products.

This information contains examples of data and reports used in daily business operations. To illustrate them as completely as possible, the examples include the names of individuals, companies, brands, and products. All of these names are fictitious and any similarity to the names and addresses used by an actual business enterprise is entirely coincidental.

COPYRIGHT LICENSE:

This information contains sample application programs in source language, which illustrate programming techniques on various operating platforms. You may copy, modify, and distribute these sample programs in any form without payment to IBM, for the purposes of developing, using, marketing or distributing application programs conforming to the application programming interface for the operating platform for which the sample programs are written. These examples have not been thoroughly tested under all conditions. IBM, therefore, cannot guarantee or imply reliability, serviceability, or function of these programs. The sample programs are provided "AS IS", without warranty of any kind. IBM shall not be liable for any damages arising out of your use of the sample programs.

Each copy or any portion of these sample programs or any derivative work must include a copyright notice as follows: © (your company name) (year). Portions of this code are derived from IBM Corp. Sample Programs. © Copyright IBM Corp. _enter the year or years_.

Trademarks

IBM, the IBM logo, and ibm.com® are trademarks or registered trademarks of International Business Machines Corp., registered in many jurisdictions worldwide. Other product and service names might be trademarks of IBM or other companies. A current list of IBM trademarks is available on the Web at "Copyright and trademark information" at www.ibm.com/legal/copytrade.shtml.

Splunk, Splunk>, and Turn Data Into Doing are trademarks or registered trademarks of Splunk Inc. in the United States and other countries. All other brand names, product names, or trademarks belong to their respective owners. © 2023 Splunk Inc. All rights reserved.

Adobe is a registered trademark of Adobe Systems Incorporated in the United States, and/or other countries.

Linear Tape-Open, LTO, and Ultrium are trademarks of HP, IBM Corp. and Quantum in the U.S. and other countries.

Intel and Itanium are trademarks or registered trademarks of Intel Corporation or its subsidiaries in the United States and other countries.

The registered trademark Linux® is used pursuant to a sublicense from the Linux Foundation, the exclusive licensee of Linus Torvalds, owner of the mark on a worldwide basis.

Microsoft, Windows, and Windows NT are trademarks of Microsoft Corporation in the United States, other countries, or both.

Java™ and all Java-based trademarks and logos are trademarks or registered trademarks of Oracle and/or its affiliates.

Red Hat®, OpenShift®, Ansible®, and Ceph® are trademarks or registered trademarks of Red Hat, Inc. or its subsidiaries in the United States and other countries.

UNIX is a registered trademark of The Open Group in the United States and other countries.

VMware, VMware vCenter Server, and VMware vSphere are registered trademarks or trademarks of VMware, Inc. or its subsidiaries in the United States and/or other jurisdictions.

Terms and conditions for product documentation

Permissions for the use of these publications are granted subject to the following terms and conditions.

Applicability

These terms and conditions are in addition to any terms of use for the IBM website.

Personal use

You may reproduce these publications for your personal, noncommercial use provided that all proprietary notices are preserved. You may not distribute, display or make derivative work of these publications, or any portion thereof, without the express consent of IBM.

Commercial use

You may reproduce, distribute and display these publications solely within your enterprise provided that all proprietary notices are preserved. You may not make derivative works of these publications, or reproduce, distribute or display these publications or any portion thereof outside your enterprise, without the express consent of IBM.

Rights

Except as expressly granted in this permission, no other permissions, licenses or rights are granted, either express or implied, to the publications or any information, data, software or other intellectual property contained therein.

IBM reserves the right to withdraw the permissions granted herein whenever, in its discretion, the use of the publications is detrimental to its interest or, as determined by IBM, the above instructions are not being properly followed.

You may not download, export or re-export this information except in full compliance with all applicable laws and regulations, including all United States export laws and regulations.

IBM MAKES NO GUARANTEE ABOUT THE CONTENT OF THESE PUBLICATIONS. THE PUBLICATIONS ARE PROVIDED "AS-IS" AND WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESSED OR IMPLIED, INCLUDING BUT NOT LIMITED TO IMPLIED WARRANTIES OF MERCHANTABILITY, NON-INFRINGEMENT, AND FITNESS FOR A PARTICULAR PURPOSE.

Privacy policy considerations

IBM Software products, including software as a service solutions, (“Software Offerings”) may use cookies or other technologies to collect product usage information, to help improve the end user experience, to tailor interactions with the end user, or for other purposes. In many cases no personally identifiable information is collected by the Software Offerings. Some of our Software Offerings can help enable you to collect personally identifiable information. If this Software Offering uses cookies to collect personally identifiable information, specific information about this offering’s use of cookies is set forth below.

This Software Offering does not use cookies or other technologies to collect personally identifiable information.

If the configurations deployed for this Software Offering provide you as customer the ability to collect personally identifiable information from end users via cookies and other technologies, you should seek your own legal advice about any laws applicable to such data collection, including any requirements for notice and consent.

For more information about the use of various technologies, including cookies, for these purposes, see IBM’s Privacy Policy at http://www.ibm.com/privacy and IBM’s Online Privacy Statement at http://www.ibm.com/privacy/details in the section entitled “Cookies, Web Beacons and Other Technologies,” and the “IBM Software Products and Software-as-a-Service Privacy Statement” at http://www.ibm.com/software/info/product-privacy.

Product Number:	5900-AXW5900-AY6

IBM Confidential