

Red Hat Insights 紹介

森若 和雄 <kmoriwak@redhat.com>
Red Hat K.K. Solution Architect
2021-07

概要

- Red Hat Insightsとは
- Red Hat Insightsの仕組み
- Red Hat Insightsが特に有益なシーン
- Red Hat Insightsの使い方
- 機密情報の隠匿
- まとめ

Red Hat Insightsとは

プロアクティブなシステム分析サービスです
重大な問題や設定の齟齬を検出

- 統計情報
- ハードウェア情報
- パッケージ情報
- 特定の設定やログ
- サードパーティ製品

主な機能

- Advisor: 問題の発見と説明、対策方法を含むレポートを生成
- Drift: システム同士の比較、あらかじめ保存したBaselineとの比較
- Vulnerability: 脆弱性情報や(あれば)回避方法
- Patch: errata情報

Filter by tags: All systems

Recommendations

Recommendations Systems

Description Filter by description

1-7 of 7 1 of 1

Status Enabled Clear filters

Description	Added	Total risk	Systems	Ansible
> Database performance decreases when Transparent Huge Pages is enabled	1 year ago	Moderate	34	✓
▼ Network connections will hang when insufficient memory is allocated for the TCP packet fragmentation	7 months ago	Important	25	✓

Recommendation is disabled for 1 system. [View systems](#)

Due to a known bug in kernel, network connections hang when insufficient memory is allocated for the TCP packet fragmentation. This is a regression introduced by the fix for CVE-2019-11478.

[Knowledgebase article](#)

Total risk

Important

The likelihood that this will be a problem is Important. The impact of the problem would be Important if it occurred.

Advisor

可用性、パフォーマンス、安定性、セキュリティのリスクを分析

Comparison

- Dashboard
- Advisor >
- Vulnerability
- Compliance >
- Policies
- Drift** >
 - Comparison**
 - Baselines
- Subscription Watch >
- Patch
- Inventory
- Remediations
- Documentation

Filter by fact View: Different ▾ Add systems or baselines 1 - 2 of 2 < >

State Different

Fact ↓	State ↑	rhel8 STANDARD × <small>★ 18 Feb 2020, 23:38 UTC</small>	rhel8aws × <small>☆ 27 Mar 2020, 20:55 UTC</small>	rhel8kvm × <small>☆ 31 Mar 2020, 20:38 UTC</small>
os_release	!	8.1	8.0	8.2
installed_packages <ul style="list-style-type: none"> zlib yum xkeyboard-config xfsprogs which vim-minimal util-linux unbound-libs tzdata 	!			
zlib	!	1.2.11-10.el8.x86_64	1.2.11-10.el8.x86_64	1.2.11-13.el8.x86_64
yum	!	4.2.7-7.el8_1.noarch	4.0.9.2-5.el8.noarch	4.2.17-3.el8.noarch
xkeyboard-config	!	2.24-3.el8.noarch	2.24-3.el8.noarch	2.28-1.el8.noarch
xfsprogs	!	5.0.0-1.el8.x86_64	4.19.0-2.el8.x86_64	5.0.0-2.el8.x86_64
which	!	2.21-10.el8.x86_64	2.21-10.el8.x86_64	2.21-12.el8.x86_64
vim-minimal	!	8.0.1763-13.el8.x86_64	8.0.1763-10.el8.x86_64	8.0.1763-13.el8.x86_64
util-linux	!	2.32.1-17.el8.x86_64	2.32.1-8.el8.x86_64	2.32.1-17.el8.x86_64
unbound-libs	!	1.7.3-8.el8.x86_64	1.7.3-8.el8.x86_64	1.7.3-10.el8.x86_64
tzdata	!	2019c-1.el8.noarch	2019a-1.el8.noarch	2019c-1.el8.noarch

Vulnerability

CVEs Systems

Dashboard

Advisor

Vulnerability

Compliance

Policies

Drift

Subscription Watch

Patch

Inventory

Remediations

Documentation

Find a CVE... Filters 1 - 25 of 2591 1 of 104

	CVE ID	Publish date	Impact	CVSS base score	Systems exposed	Business risk	Status
>	CVE-2019-17666	17 Oct 2019	Important	6.3	226	Low	On-hold
>	CVE-2018-3646	14 Aug 2018	Important	5.6	226	High	In-review
▼	CVE-2019-11487	21 Apr 2019	Important	7.8	211	Medium	Resolved via mitigation

Description

The Linux kernel before 5.1-rc5 allows page->_refcount reference count overflow, with resultant use-after-free issues, if about 140 GiB of RAM exists. This is related to fs/fuse/dev.c, fs/pipe.c, fs/splice.c, include/linux/mm.h, include/linux/pipe_fs_i.h, kernel/trace/trace.c, mm/gup.c, and mm/hugetlb.c. It can occur with FUSE requests.

>	CVE-2019-18634	29 Jan 2020	Important	7.8	197	Not defined	Not reviewed
---	--------------------------------	-------------	-----------	-----	-----	-------------	--------------

Patch

[Applicable advisories](#) [Systems](#)
 Search advisories

1 - 25 of 4517 < >

	Name ↑	Publish date ↓	Type ↑	Applicable systems ↑	Synopsis ↑
>	RHSA-2020:0984	26 Mar 2020	Security	59	Important: ipmitool security update
>	RHSA-2020:0981	26 Mar 2020	Security	1	Important: ipmitool security update
▼	RHSA-2020:0980	26 Mar 2020	Security	8	Moderate: rh-postgresql10-postgresql security update

Description

PostgreSQL is an advanced object-relational database management system (DBMS). The following packages have been upgraded to a later upstream version: rh-postgresql10-postgresql (10.12). Security Fix(es): * PostgreSQL: stack-based buffer overflow via setting a password (CVE-2019-10164) * PostgreSQL: ALTER ... DEPENDS ON EXTENSION is missing authorization checks (CVE-2020-1720) For more details about the security issue(s), including the impact, a CVSS score, acknowledgments, and other related information, refer to the CVE page(s) listed in the References section.

[View packages and errata at access.redhat.com](#)

Patch

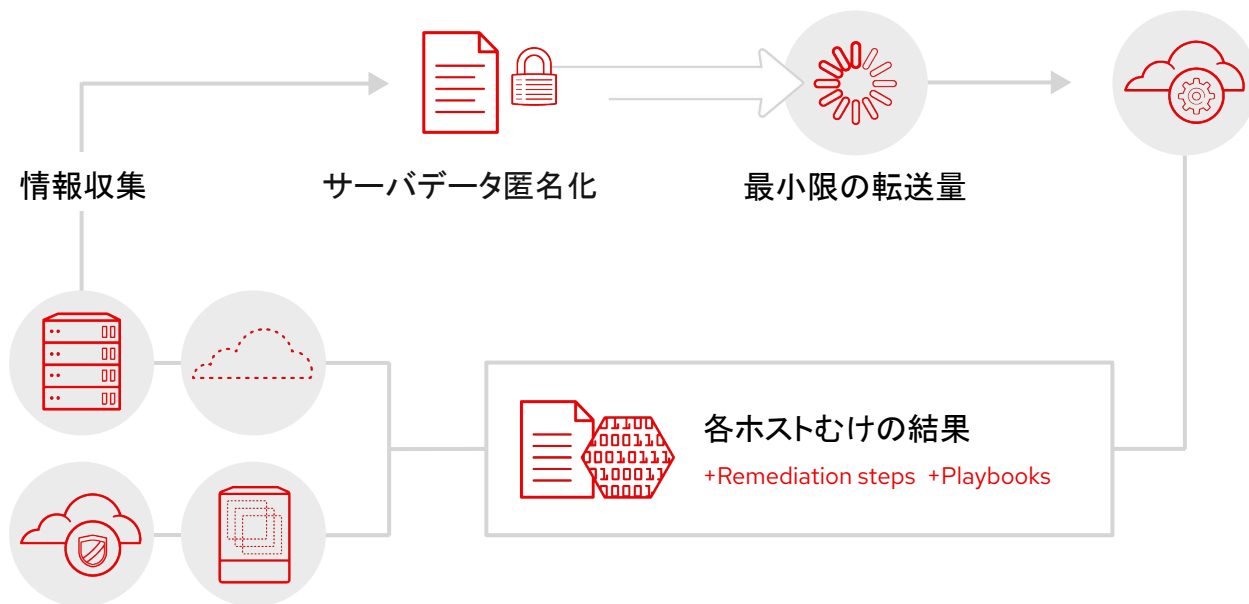
Red Hat製品のアドバイザリ適用状況

Red Hat Insightsの特徴

- RHELやOpenShift等の一部として提供され、追加の費用は発生しません
- SaaS形式でのみ提供されます
- Ansibleによる実行可能な修正スクリプトを生成します
 - 発見された問題の内対応するものはAnsible Playbookを生成
 - 脆弱性に対するワークアラウンド
 - 非推奨設定の変更
 - 問題に関連するパッケージの更新 など
 - Playbookの実行方法
 - Playbookをダウンロードして実行
 - Ansible Tower との連携による実行
 - Red Hat Satellite との連携による実行

Red Hat Insightsの仕組み

- エージェントを各システムに導入し、データを送信します
- Red Hatの作成したルールによりデータが解析されます
- 解析結果のレポートをWebブラウザで閲覧できます



健康診断にたどってみると.....



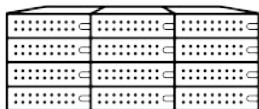
採血



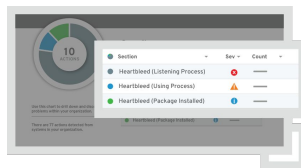
診断票



対策



insights-clientでの
情報収集



レポート



レポートに対応手順や
Playbookも記載

Red Hat Insightsが特に有益なシーン

- 構築時: 抜け漏れ防止
 - 重要な修正の適用漏れを検出
 - 典型的な設定ミスを検出
 - 古いファームウェアの検出など、一般的な障害予防
- 運用時: 最新情報へのキャッチアップ
 - プロアクティブなチェックと警告
 - Red Hatが持つ最新のナレッジを基とした診断

Red Hat Insightsの使い方

導入

1. insights-client パッケージを導入
2. insights-client --register でシステムを登録 → 1日1回情報を送信

運用

1. メール通知Advisorからメールによる通知を受信 (イベント毎/週次)
2. Webレポート画面を閲覧
 - 問題の原因となりうる課題が表示されます
 - 一部の問題については対策用のAnsible Playbookを提供
3. 対策の実施
 - 課題に対する対策をAnsibleや手作業等で実施

機密情報の隠匿

Red Hat Insightsは必要最低限の情報を収集します。設定によりホスト名、IPv4アドレスの難読化が可能です。

さらに収集対象を制限して機密情報をRed Hatへ渡さない設定が可能です。

1. `insights-client --no-upload`オプションによる素振り
2. お客様にて収集情報をレビュー
3. 収集禁止ルールを設定

収集禁止ルール:

- コマンド名、ファイル名による指定
- 正規表現、キーワードによる行単位の指定

まとめ

- Red Hat Insightsは定期的な情報収集とレポートで、障害が発生する前にプロアクティブなサポートを提供するサービスです
- Red Hatのサポートで蓄積されたナレッジをもとにルールが提供されます
- 早速使ってみましょう

<https://cloud.redhat.com>

Appendix

Red Hat Insightsの対象製品

- Red Hat Insightsは以下の製品を対象としています
 - Red Hat Enterprise Linux 6.4以降 および 7以降
 - Red Hat Virtualization 3.6以降
 - Red Hat OpenStack Platform 7以降
 - OpenShift Container Platform 全て

ネットワーク接続

- Firewallでは api.access.redhat.com:443 および cert-api.access.redhat.com:443 へのアクセス許可が必要です
 - <https://access.redhat.com/solutions/1583183>
- Red Hat Satelliteまたは一般的なHTTPプロキシサーバをプロキシとして利用可能です
 - <https://access.redhat.com/solutions/1606693>

Red Hat Insights関連ドキュメント

- Red Hat Insights ドキュメント
 - https://access.redhat.com/documentation/ja-jp/red_hat_insights/2021/
- Red Hat Insightsが収集するデータ
 - <https://access.redhat.com/articles/1598863>
- 特定ファイルのアップロードを禁止する方法
 - <https://access.redhat.com/articles/4511681>
- Firewall, Proxy経由での接続
 - <https://access.redhat.com/solutions/1583183>

Appendix

レポートで報告される問題の例

例 1: 既知の脆弱性を検出

linux kernelの脆弱性を検出

 Security > Kernel keychain vulnerability (CVE-2016-0728) 

DETECTED ISSUE

A vulnerability in the Linux kernel rated **Important** was discovered. The use-after-free flaw relates to the way the Linux kernel's key management subsystem handles keyring object reference counting in certain error paths of the `join_session_keyring()` function. A local, unprivileged user could use this flaw to escalate their privileges on the system. The issue was reported as [CVE-2016-0728](#).

The host is vulnerable as it is running **kernel-3.10.0-229.20.1.el7**.

STEPS TO RESOLVE

Red Hat recommends that you update **kernel** and reboot. If you cannot reboot now, consider applying the [systemtap patch](#) to update your running kernel.

```
# yum update kernel
# reboot
-or-
# debuginfo-install kernel
(or equivalent)
# stap -vgt -Gfix_p=1
-Gtrace_p=0 cve20160728e.stp
```

 **Related Knowledgebase articles:** [Use after free vulnerability in Linux kernel keychain management \(CVE-2016-0728\)](#)

例 2: 設定内容の問題検出 脆弱な暗号化方式を許可している設定を検出

Security > Insecure SSH ciphers

DETECTED ISSUE

An insecure SSH cipher was detected on this host and could be more susceptible to attack.

The current host is configured with the following ciphers:

- aes128-cbc,blowfish-cbc,cast128-cbc,aes192-cbc,aes256-cbc,hmac-md5,hmac-md5-96,hmac-sha1-96

STEPS TO RESOLVE


Red Hat recommends that you modify `/etc/ssh/sshd_config` to remove the listed insecure ciphers and then restart `sshd` services.

For more information about vulnerable ciphers and for assistance with these necessary modifications see [SSH vulnerabilities: HMAC algorithms and CBC ciphers](#).

Related Knowledgebase articles: [SSH vulnerabilities: HMAC algorithms and CBC ciphers](#)

例 3: 設定と実態の比較による問題検出

設定意図に反してTHPが有効であることを検出


 Performance > Transparent Huge Pages unsuccessfully disabled ☰

DETECTED ISSUE

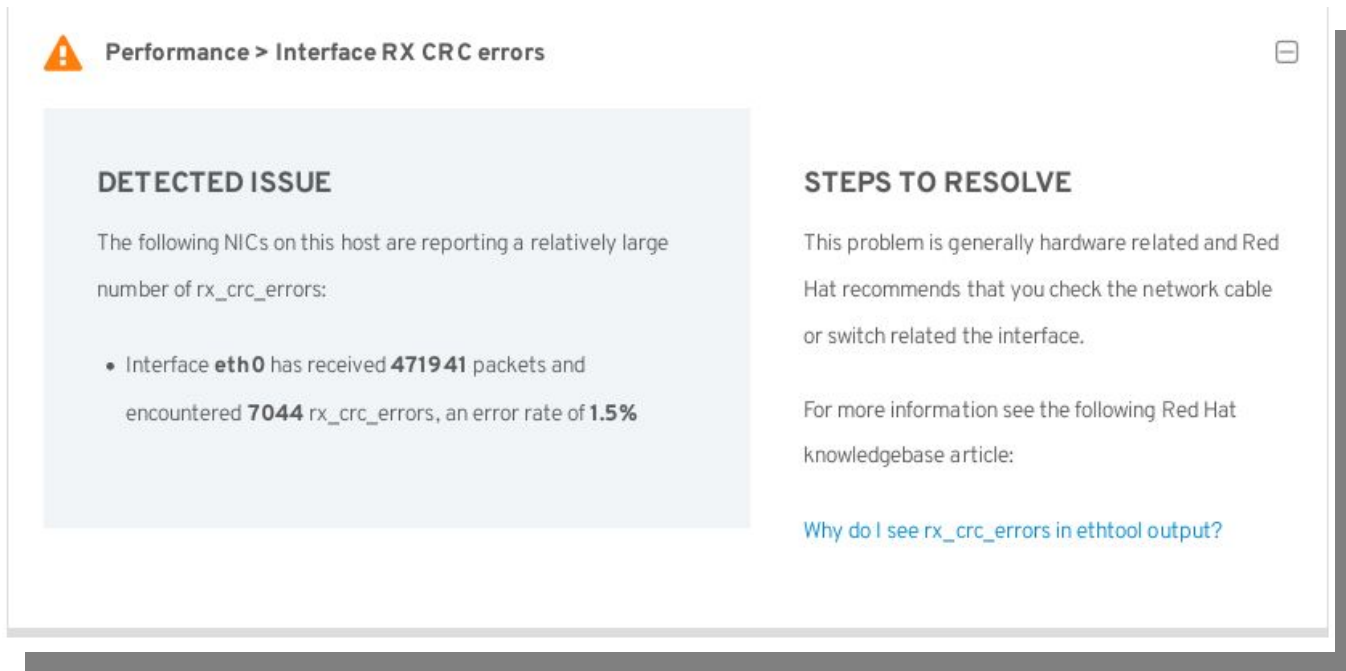
Transparent Huge Pages (THP) is enabled even after appending 'transparent_hugepage=never' to the kernel command line in /boot/grub/grub.conf file. This might cause performance issues with services that require THP to be disabled.

STEPS TO RESOLVE

The ktune service enables Transparent Huge Pages (THP) by default for all profiles. Red Hat recommends that you create a customized tuned profile with disabled THP or by disabling ktune and tuned services.

 **Related Knowledgebase articles:**
[Disabling transparent hugepages \(THP\) on Red Hat Enterprise Linux 6 is not taking effect.](#)

例 4: 統計情報による問題検出 NICでのCRCエラー頻発を検出



Performance > Interface RX CRC errors

DETECTED ISSUE

The following NICs on this host are reporting a relatively large number of rx_crc_errors:

- Interface **eth0** has received **471941** packets and encountered **7044** rx_crc_errors, an error rate of **1.5%**

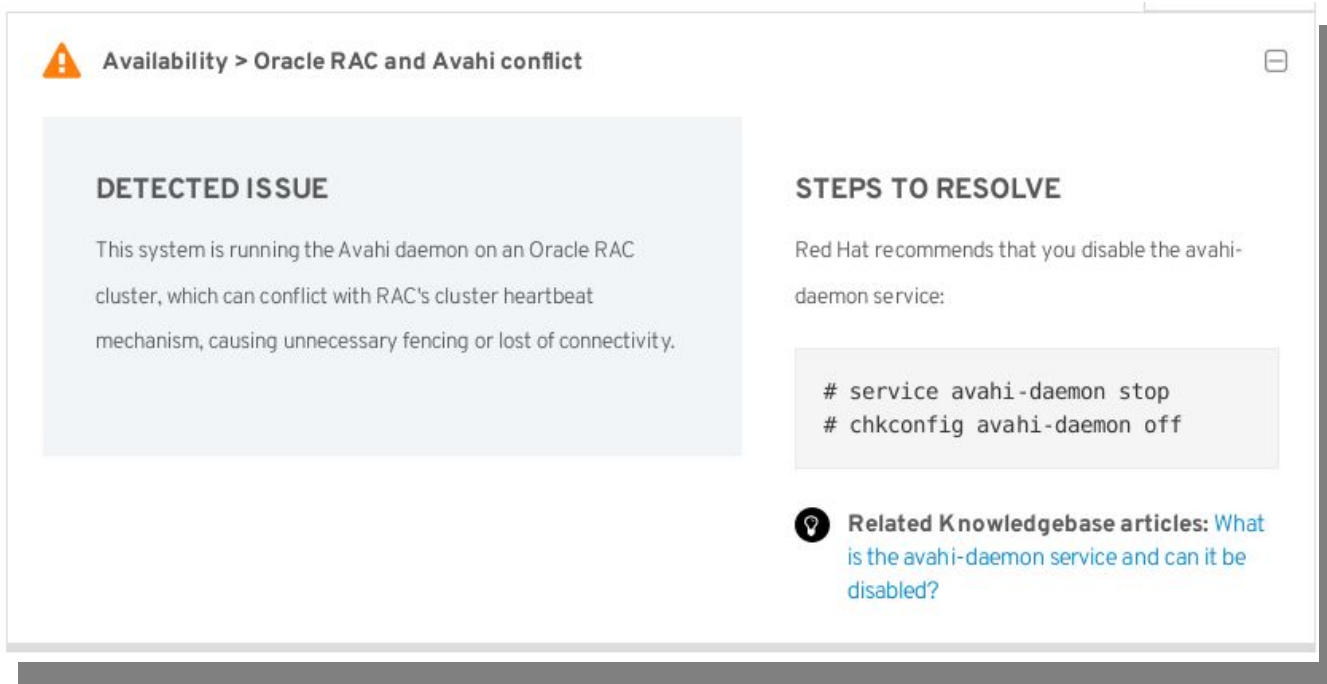
STEPS TO RESOLVE

This problem is generally hardware related and Red Hat recommends that you check the network cable or switch related the interface.

For more information see the following Red Hat knowledgebase article:

[Why do I see rx_crc_errors in ethtool output?](#)

例 5: 他社製品ナレッジ、サービス状態による検出 競合するOracle RACとAvahiの併存を検出



Availability > Oracle RAC and Avahi conflict

DETECTED ISSUE

This system is running the Avahi daemon on an Oracle RAC cluster, which can conflict with RAC's cluster heartbeat mechanism, causing unnecessary fencing or lost of connectivity.

STEPS TO RESOLVE

Red Hat recommends that you disable the avahi-daemon service:

```
# service avahi-daemon stop  
# chkconfig avahi-daemon off
```

Related Knowledgebase articles: [What is the avahi-daemon service and can it be disabled?](#)