Static Analysis Results Interchange Format (SARIF) Version 2.0

Committee Specification Draft 02 (2.0.0-csd.2.beta.2019-03-13)

13 March 2019

Technical Committee:

[OASIS Static Analysis Results Interchange Format (SARIF) TC](https://www.oasis-open.org/committees/sarif/)

Chairs:

David Keaton ([dmk@dmk.com](mailto:dmk@dmk.com)), Individual Member

Luke Cartey ([luke@semmle.com](mailto:luke@semmle.com)), [Semmle](http://www.semmle.com/)

Editors:

Michael Fanning ([mikefan@microsoft.com](mailto:mikefan@microsoft.com)), [Microsoft](http://www.microsoft.com/)

Laurence J. Golding ([v-lgold@microsoft.com](mailto:v-lgold@microsoft.com)), [Microsoft](http://www.microsoft.com)

Additional artifacts:

This prose specification is one component of a Work Product that also includes:

* JSON schemas:
  + sarif-schema.json
  + sarif-external-property-file-schema.json

Related work:

This specification replaces or supersedes:

* None

This specification is related to:

* None

Declared XML namespaces:

* None

Abstract:

This document defines a standard format for the output of static analysis tools. The format is referred to as the “Static Analysis Results Interchange Format” and is abbreviated as SARIF.

Status:

This [Working Draft](https://www.oasis-open.org/policies-guidelines/oasis-defined-terms-2017-05-26#dWorkingDraft) (WD) has been produced by one or more TC Members; it has not yet been voted on by the TC or [approved](https://www.oasis-open.org/policies-guidelines/tc-process#committeeDraft) as a Committee Draft (Committee Specification Draft or a Committee Note Draft). The OASIS document [Approval Process](https://www.oasis-open.org/policies-guidelines/tc-process#standApprovProcess) begins officially with a TC vote to approve a WD as a Committee Draft. A TC may approve a Working Draft, revise it, and re-approve it any number of times as a Committee Draft.

This Working Draft is being developed under the [RF on RAND Terms](https://www.oasis-open.org/policies-guidelines/ipr#RF-on-RAND-Mode) Mode of the [OASIS IPR Policy](https://www.oasis-open.org/policies-guidelines/ipr), the mode chosen when the Technical Committee was established. All members of the TC should be familiar with this document, which may create obligations regarding the disclosure and availability of a member's patent, copyright, trademark and license rights that read on an approved OASIS specification. For information on whether any patents have been disclosed that may be essential to implementing this specification, and any offers of patent licensing terms, please refer to the Intellectual Property Rights section of the TC’s web page (<https://www.oasis-open.org/committees/sarif/ipr.php>).

Any machine-readable content ([Computer Language Definitions](https://www.oasis-open.org/policies-guidelines/tc-process#wpComponentsCompLang)) declared Normative for this Work Product must also be provided in separate plain text files. In the event of a discrepancy between such plain text file and display content in the Work Product's prose narrative document(s), the content in the separate plain text file prevails.

URI patterns:

Initial publication URI:  
http://docs.oasis-open.org/sarif/sarif/v2.0/csd01/sarif-v2.0-csd01.docx

Permanent “Latest version” URI:  
http://docs.oasis-open.org/sarif/sarif/v2.0/sarif-v2.0.docx

Copyright © OASIS Open 2017. All Rights Reserved.

All capitalized terms in the following text have the meanings assigned to them in the OASIS Intellectual Property Rights Policy (the "OASIS IPR Policy"). The full [Policy](https://www.oasis-open.org/policies-guidelines/ipr) may be found at the OASIS website.

This document and translations of it may be copied and furnished to others, and derivative works that comment on or otherwise explain it or assist in its implementation may be prepared, copied, published, and distributed, in whole or in part, without restriction of any kind, provided that the above copyright notice and this section are included on all such copies and derivative works. However, this document itself may not be modified in any way, including by removing the copyright notice or references to OASIS, except as needed for the purpose of developing any document or deliverable produced by an OASIS Technical Committee (in which case the rules applicable to copyrights, as set forth in the OASIS IPR Policy, must be followed) or as required to translate it into languages other than English.

The limited permissions granted above are perpetual and will not be revoked by OASIS or its successors or assigns.

This document and the information contained herein is provided on an "AS IS" basis and OASIS DISCLAIMS ALL WARRANTIES, EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO ANY WARRANTY THAT THE USE OF THE INFORMATION HEREIN WILL NOT INFRINGE ANY OWNERSHIP RIGHTS OR ANY IMPLIED WARRANTIES OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE.

Table of Contents

[1 Introduction 14](#_Toc4689930)

[1.1 IPR Policy 14](#_Toc4689931)

[1.2 Terminology 14](#_Toc4689932)

[1.3 Normative References 20](#_Toc4689933)

[1.4 Non-Normative References 21](#_Toc4689934)

[2 Conventions 22](#_Toc4689935)

[2.1 General 22](#_Toc4689936)

[2.2 Format examples 22](#_Toc4689937)

[2.3 Property notation 22](#_Toc4689938)

[2.4 Syntax notation 22](#_Toc4689939)

[2.5 Commonly used objects 22](#_Toc4689940)

[3 File format 24](#_Toc4689941)

[3.1 General 24](#_Toc4689942)

[3.2 SARIF file naming convention 24](#_Toc4689943)

[3.3 artifactContent object 24](#_Toc4689944)

[3.3.1 General 24](#_Toc4689945)

[3.3.2 text property 24](#_Toc4689946)

[3.3.3 binary property 24](#_Toc4689947)

[3.3.4 rendered property 25](#_Toc4689948)

[3.4 artifactLocation object 25](#_Toc4689949)

[3.4.1 General 25](#_Toc4689950)

[3.4.2 Constraints 25](#_Toc4689951)

[3.4.3 uri property 26](#_Toc4689952)

[3.4.4 uriBaseId property 26](#_Toc4689953)

[3.4.5 artifactIndex property 27](#_Toc4689954)

[3.4.6 Guidance on the use of artifactLocation objects 28](#_Toc4689955)

[3.5 String properties 29](#_Toc4689956)

[3.5.1 General 29](#_Toc4689957)

[3.5.2 Localizable strings 29](#_Toc4689958)

[3.5.3 Redactable strings 29](#_Toc4689959)

[3.5.4 GUID-valued strings 29](#_Toc4689960)

[3.5.5 Hierarchical strings 29](#_Toc4689961)

[3.5.5.1 General 29](#_Toc4689962)

[3.5.5.2 Versioned hierarchical strings 30](#_Toc4689963)

[3.6 Object properties 30](#_Toc4689964)

[3.7 Array properties 30](#_Toc4689965)

[3.7.1 General 30](#_Toc4689966)

[3.7.2 Default value 31](#_Toc4689967)

[3.7.3 Array properties with unique values 31](#_Toc4689968)

[3.7.4 Array indices 31](#_Toc4689969)

[3.8 Property bags 31](#_Toc4689970)

[3.8.1 General 31](#_Toc4689971)

[3.8.2 Tags 31](#_Toc4689972)

[3.8.2.1 General 31](#_Toc4689973)

[3.8.2.2 Tag metadata 32](#_Toc4689974)

[3.9 Date/time properties 32](#_Toc4689975)

[3.10 URI-valued properties 33](#_Toc4689976)

[3.10.1 General 33](#_Toc4689977)

[3.10.2 URIs that use the file scheme 34](#_Toc4689978)

[3.10.3 URIs that use the sarif scheme 35](#_Toc4689979)

[3.10.4 Internationalized Resource Identifiers (IRIs) 35](#_Toc4689980)

[3.11 message object 35](#_Toc4689981)

[3.11.1 General 35](#_Toc4689982)

[3.11.2 Constraints 35](#_Toc4689983)

[3.11.3 Plain text messages 35](#_Toc4689984)

[3.11.4 Formatted messages 36](#_Toc4689985)

[3.11.4.1 General 36](#_Toc4689986)

[3.11.4.2 Security implications 36](#_Toc4689987)

[3.11.5 Messages with placeholders 36](#_Toc4689988)

[3.11.6 Messages with embedded links 37](#_Toc4689989)

[3.11.7 Message string lookup 39](#_Toc4689990)

[3.11.8 text property 40](#_Toc4689991)

[3.11.9 markdown property 40](#_Toc4689992)

[3.11.10 messageId property 40](#_Toc4689993)

[3.11.11 arguments property 40](#_Toc4689994)

[3.12 multiformatMessageString object 40](#_Toc4689995)

[3.12.1 General 40](#_Toc4689996)

[3.12.2 Localizable multiformatMessageStrings 40](#_Toc4689997)

[3.12.3 text property 41](#_Toc4689998)

[3.12.4 markdown property 41](#_Toc4689999)

[3.13 sarifLog object 41](#_Toc4690000)

[3.13.1 General 41](#_Toc4690001)

[3.13.2 version property 41](#_Toc4690002)

[3.13.3 $schema property 42](#_Toc4690003)

[3.13.4 runs property 42](#_Toc4690004)

[3.13.5 inlineExternalProperties property 42](#_Toc4690005)

[3.14 run object 43](#_Toc4690006)

[3.14.1 General 43](#_Toc4690007)

[3.14.2 externalPropertyFileReferences property 44](#_Toc4690008)

[3.14.2.1 Rationale 44](#_Toc4690009)

[3.14.2.2 Property definition 44](#_Toc4690010)

[3.14.3 automationDetails property 47](#_Toc4690011)

[3.14.4 aggregateIds property 47](#_Toc4690012)

[3.14.5 baselineGuid property 47](#_Toc4690013)

[3.14.6 tool property 47](#_Toc4690014)

[3.14.7 language 47](#_Toc4690015)

[3.14.8 taxonomies property 48](#_Toc4690016)

[3.14.9 translations property 48](#_Toc4690017)

[3.14.10 policies property 48](#_Toc4690018)

[3.14.11 invocations property 48](#_Toc4690019)

[3.14.12 conversion property 48](#_Toc4690020)

[3.14.13 versionControlProvenance property 48](#_Toc4690021)

[3.14.14 originalUriBaseIds property 49](#_Toc4690022)

[3.14.15 artifacts property 50](#_Toc4690023)

[3.14.16 logicalLocations property 51](#_Toc4690024)

[3.14.17 addresses property 52](#_Toc4690025)

[3.14.18 threadFlowLocations property 52](#_Toc4690026)

[3.14.19 graphs property 52](#_Toc4690027)

[3.14.20 results property 52](#_Toc4690028)

[3.14.21 defaultEncoding property 53](#_Toc4690029)

[3.14.22 defaultSourceLanguage property 53](#_Toc4690030)

[3.14.23 newlineSequences property 53](#_Toc4690031)

[3.14.24 columnKind property 54](#_Toc4690032)

[3.14.25 redactionToken property 54](#_Toc4690033)

[3.15 externalPropertyFileReference object 55](#_Toc4690034)

[3.15.1 General 55](#_Toc4690035)

[3.15.2 location property 55](#_Toc4690036)

[3.15.3 guid property 55](#_Toc4690037)

[3.15.4 itemCount property 55](#_Toc4690038)

[3.16 runAutomationDetails object 55](#_Toc4690039)

[3.16.1 General 55](#_Toc4690040)

[3.16.2 Constraints 56](#_Toc4690041)

[3.16.3 description property 56](#_Toc4690042)

[3.16.4 id property 56](#_Toc4690043)

[3.16.5 guid property 57](#_Toc4690044)

[3.16.6 correlationGuid property 57](#_Toc4690045)

[3.17 tool object 57](#_Toc4690046)

[3.17.1 General 57](#_Toc4690047)

[3.17.2 driver property 58](#_Toc4690048)

[3.17.3 extensions property 58](#_Toc4690049)

[3.18 toolComponent object 58](#_Toc4690050)

[3.18.1 General 58](#_Toc4690051)

[3.18.2 Taxonomies 59](#_Toc4690052)

[3.18.3 Translations 61](#_Toc4690053)

[3.18.4 Policies 62](#_Toc4690054)

[3.18.5 guid property 63](#_Toc4690055)

[3.18.6 name property 63](#_Toc4690056)

[3.18.7 fullName property 63](#_Toc4690057)

[3.18.8 semanticVersion property 64](#_Toc4690058)

[3.18.9 version property 64](#_Toc4690059)

[3.18.10 dottedQuadFileVersion property 64](#_Toc4690060)

[3.18.11 releaseDateUtc 64](#_Toc4690061)

[3.18.12 downloadUri property 64](#_Toc4690062)

[3.18.13 informationUri property 65](#_Toc4690063)

[3.18.14 organization property 65](#_Toc4690064)

[3.18.15 product property 65](#_Toc4690065)

[3.18.16 productSuite property 65](#_Toc4690066)

[3.18.17 shortDescription property 65](#_Toc4690067)

[3.18.18 fullDescription property 65](#_Toc4690068)

[3.18.19 language property 65](#_Toc4690069)

[3.18.20 globalMessageStrings property 66](#_Toc4690070)

[3.18.21 rules property 66](#_Toc4690071)

[3.18.22 notifications property 67](#_Toc4690072)

[3.18.23 taxa 67](#_Toc4690073)

[3.18.24 supportedTaxonomies 68](#_Toc4690074)

[3.18.25 translationMetadata property 69](#_Toc4690075)

[3.18.26 artifactIndices property 69](#_Toc4690076)

[3.18.27 contents property 69](#_Toc4690077)

[3.18.28 isComprehensive property 70](#_Toc4690078)

[3.18.29 localizedDataSemanticVersion property 70](#_Toc4690079)

[3.18.30 minimumRequiredLocalizedDataSemanticVersion property 71](#_Toc4690080)

[3.18.31 associatedComponent property 71](#_Toc4690081)

[3.19 invocation object 72](#_Toc4690082)

[3.19.1 General 72](#_Toc4690083)

[3.19.2 commandLine property 72](#_Toc4690084)

[3.19.3 arguments property 72](#_Toc4690085)

[3.19.4 responseFiles property 73](#_Toc4690086)

[3.19.5 ruleConfigurationOverrides property 73](#_Toc4690087)

[3.19.6 notificationConfigurationOverrides property 73](#_Toc4690088)

[3.19.7 startTimeUtc property 73](#_Toc4690089)

[3.19.8 endTimeUtc property 74](#_Toc4690090)

[3.19.9 exitCode property 74](#_Toc4690091)

[3.19.10 exitCodeDescription property 74](#_Toc4690092)

[3.19.11 exitSignalName property 74](#_Toc4690093)

[3.19.12 exitSignalNumber property 74](#_Toc4690094)

[3.19.13 processStartFailureMessage property 75](#_Toc4690095)

[3.19.14 toolExecutionSuccessful property 75](#_Toc4690096)

[3.19.15 machine property 75](#_Toc4690097)

[3.19.16 account property 75](#_Toc4690098)

[3.19.17 processId property 75](#_Toc4690099)

[3.19.18 executableLocation property 75](#_Toc4690100)

[3.19.19 workingDirectory property 76](#_Toc4690101)

[3.19.20 environmentVariables property 76](#_Toc4690102)

[3.19.21 toolExecutionNotifications property 76](#_Toc4690103)

[3.19.22 toolConfigurationNotifications property 77](#_Toc4690104)

[3.19.23 stdin, stdout, stderr, and stdoutStderr properties 78](#_Toc4690105)

[3.20 attachment object 78](#_Toc4690106)

[3.20.1 General 78](#_Toc4690107)

[3.20.2 description property 78](#_Toc4690108)

[3.20.3 artifactLocation property 79](#_Toc4690109)

[3.20.4 regions property 79](#_Toc4690110)

[3.20.5 rectangles property 79](#_Toc4690111)

[3.21 conversion object 79](#_Toc4690112)

[3.21.1 General 79](#_Toc4690113)

[3.21.2 tool property 80](#_Toc4690114)

[3.21.3 invocation property 80](#_Toc4690115)

[3.21.4 analysisToolLogFiles property 80](#_Toc4690116)

[3.22 versionControlDetails object 80](#_Toc4690117)

[3.22.1 General 80](#_Toc4690118)

[3.22.2 Constraints 80](#_Toc4690119)

[3.22.3 repositoryUri property 80](#_Toc4690120)

[3.22.4 revisionId property 80](#_Toc4690121)

[3.22.5 branch property 81](#_Toc4690122)

[3.22.6 revisionTag property 81](#_Toc4690123)

[3.22.7 asOfTimeUtc property 81](#_Toc4690124)

[3.22.8 mappedTo property 81](#_Toc4690125)

[3.23 artifact object 83](#_Toc4690126)

[3.23.1 General 83](#_Toc4690127)

[3.23.2 artifactLocation property 83](#_Toc4690128)

[3.23.3 parentIndex property 83](#_Toc4690129)

[3.23.4 offset property 84](#_Toc4690130)

[3.23.5 length property 85](#_Toc4690131)

[3.23.6 roles property 85](#_Toc4690132)

[3.23.7 mimeType property 86](#_Toc4690133)

[3.23.8 contents property 86](#_Toc4690134)

[3.23.9 encoding property 86](#_Toc4690135)

[3.23.10 sourceLanguage property 86](#_Toc4690136)

[3.23.10.1 General 86](#_Toc4690137)

[3.23.10.2 Source language identifier conventions and practices 87](#_Toc4690138)

[3.23.11 hashes property 87](#_Toc4690139)

[3.23.12 lastModifiedTimeUtc property 88](#_Toc4690140)

[3.24 translationMetadata object 89](#_Toc4690141)

[3.24.1 General 89](#_Toc4690142)

[3.24.2 name property 89](#_Toc4690143)

[3.24.3 fullName property 89](#_Toc4690144)

[3.24.4 shortDescription property 89](#_Toc4690145)

[3.24.5 fullDescription property 89](#_Toc4690146)

[3.24.6 downloadUri property 89](#_Toc4690147)

[3.24.7 informationUri property 90](#_Toc4690148)

[3.25 result object 90](#_Toc4690149)

[3.25.1 General 90](#_Toc4690150)

[3.25.2 Distinguishing logically identical from logically distinct results 90](#_Toc4690151)

[3.25.3 guid property 90](#_Toc4690152)

[3.25.4 correlationGuid property 91](#_Toc4690153)

[3.25.5 ruleId property 91](#_Toc4690154)

[3.25.6 ruleIndex property 92](#_Toc4690155)

[3.25.7 rule property 92](#_Toc4690156)

[3.25.8 taxa 93](#_Toc4690157)

[3.25.9 kind property 94](#_Toc4690158)

[3.25.10 level property 95](#_Toc4690159)

[3.25.11 message property 97](#_Toc4690160)

[3.25.12 locations property 98](#_Toc4690161)

[3.25.13 analysisTarget property 99](#_Toc4690162)

[3.25.14 fingerprints property 99](#_Toc4690163)

[3.25.15 partialFingerprints property 100](#_Toc4690164)

[3.25.16 codeFlows property 102](#_Toc4690165)

[3.25.17 graphs property 102](#_Toc4690166)

[3.25.18 graphTraversals property 102](#_Toc4690167)

[3.25.19 stacks property 102](#_Toc4690168)

[3.25.20 relatedLocations property 102](#_Toc4690169)

[3.25.21 suppressions property 103](#_Toc4690170)

[3.25.22 baselineState property 104](#_Toc4690171)

[3.25.23 rank property 104](#_Toc4690172)

[3.25.24 attachments property 105](#_Toc4690173)

[3.25.25 workItemUris property 105](#_Toc4690174)

[3.25.26 hostedViewerUri property 105](#_Toc4690175)

[3.25.27 provenance property 105](#_Toc4690176)

[3.25.28 fixes property 105](#_Toc4690177)

[3.25.29 occurrenceCount property 105](#_Toc4690178)

[3.26 location object 106](#_Toc4690179)

[3.26.1 General 106](#_Toc4690180)

[3.26.2 physicalLocation property 106](#_Toc4690181)

[3.26.3 logicalLocation property 106](#_Toc4690182)

[3.26.4 message property 107](#_Toc4690183)

[3.26.5 annotations property 107](#_Toc4690184)

[3.27 physicalLocation object 107](#_Toc4690185)

[3.27.1 General 107](#_Toc4690186)

[3.27.2 id property 107](#_Toc4690187)

[3.27.3 artifactLocation property 107](#_Toc4690188)

[3.27.4 region property 108](#_Toc4690189)

[3.27.5 contextRegion property 108](#_Toc4690190)

[3.27.6 address property 109](#_Toc4690191)

[3.28 region object 109](#_Toc4690192)

[3.28.1 General 109](#_Toc4690193)

[3.28.2 Text regions 109](#_Toc4690194)

[3.28.3 Binary regions 112](#_Toc4690195)

[3.28.4 Independence of text and binary regions 112](#_Toc4690196)

[3.28.5 startLine property 112](#_Toc4690197)

[3.28.6 startColumn property 112](#_Toc4690198)

[3.28.7 endLine property 113](#_Toc4690199)

[3.28.8 endColumn property 113](#_Toc4690200)

[3.28.9 charOffset property 113](#_Toc4690201)

[3.28.10 charLength property 113](#_Toc4690202)

[3.28.11 byteOffset property 113](#_Toc4690203)

[3.28.12 byteLength property 113](#_Toc4690204)

[3.28.13 snippet property 113](#_Toc4690205)

[3.28.14 message property 114](#_Toc4690206)

[3.28.15 sourceLanguage property 114](#_Toc4690207)

[3.29 rectangle object 114](#_Toc4690208)

[3.29.1 General 114](#_Toc4690209)

[3.29.2 top, left, bottom, and right properties 114](#_Toc4690210)

[3.29.3 message property 115](#_Toc4690211)

[3.30 address object 115](#_Toc4690212)

[3.30.1 baseAddress property 115](#_Toc4690213)

[3.30.2 offset property 115](#_Toc4690214)

[3.30.3 fullyQualifiedName property 115](#_Toc4690215)

[3.30.4 name property 115](#_Toc4690216)

[3.30.5 kind property 115](#_Toc4690217)

[3.30.6 index property 116](#_Toc4690218)

[3.30.7 parentIndex property 116](#_Toc4690219)

[3.31 logicalLocation object 116](#_Toc4690220)

[3.31.1 General 116](#_Toc4690221)

[3.31.2 Constraints 116](#_Toc4690222)

[3.31.3 Logical location naming rules 117](#_Toc4690223)

[3.31.4 name property 117](#_Toc4690224)

[3.31.5 index property 118](#_Toc4690225)

[3.31.6 fullyQualifiedName property 118](#_Toc4690226)

[3.31.7 decoratedName property 119](#_Toc4690227)

[3.31.8 kind property 120](#_Toc4690228)

[3.31.9 parentIndex property 122](#_Toc4690229)

[3.32 suppression object 123](#_Toc4690230)

[3.32.1 General 123](#_Toc4690231)

[3.32.2 kind property 123](#_Toc4690232)

[3.32.2.1 suppressedInSource value 123](#_Toc4690233)

[3.32.2.2 suppressedExternally value 123](#_Toc4690234)

[3.32.3 location property 124](#_Toc4690235)

[3.32.4 guid property 124](#_Toc4690236)

[3.33 codeFlow object 125](#_Toc4690237)

[3.33.1 General 125](#_Toc4690238)

[3.33.2 message property 125](#_Toc4690239)

[3.33.3 threadFlows property 126](#_Toc4690240)

[3.34 threadFlow object 126](#_Toc4690241)

[3.34.1 General 126](#_Toc4690242)

[3.34.2 id property 126](#_Toc4690243)

[3.34.3 message property 126](#_Toc4690244)

[3.34.4 initialState property 126](#_Toc4690245)

[3.34.5 immutableState property 126](#_Toc4690246)

[3.34.6 locations property 127](#_Toc4690247)

[3.35 graph object 127](#_Toc4690248)

[3.35.1 General 127](#_Toc4690249)

[3.35.2 description property 127](#_Toc4690250)

[3.35.3 nodes property 127](#_Toc4690251)

[3.35.4 edges property 127](#_Toc4690252)

[3.36 node object 127](#_Toc4690253)

[3.36.1 General 127](#_Toc4690254)

[3.36.2 id property 127](#_Toc4690255)

[3.36.3 label property 128](#_Toc4690256)

[3.36.4 location property 128](#_Toc4690257)

[3.36.5 children property 128](#_Toc4690258)

[3.37 edge object 128](#_Toc4690259)

[3.37.1 General 128](#_Toc4690260)

[3.37.2 id property 128](#_Toc4690261)

[3.37.3 label property 128](#_Toc4690262)

[3.37.4 sourceNodeId property 128](#_Toc4690263)

[3.37.5 targetNodeId property 129](#_Toc4690264)

[3.38 graphTraversal object 129](#_Toc4690265)

[3.38.1 General 129](#_Toc4690266)

[3.38.2 Constraints 129](#_Toc4690267)

[3.38.3 resultGraphIndex property 129](#_Toc4690268)

[3.38.4 runGraphIndex property 129](#_Toc4690269)

[3.38.5 description property 130](#_Toc4690270)

[3.38.6 initialState property 130](#_Toc4690271)

[3.38.7 immutableState property 130](#_Toc4690272)

[3.38.8 edgeTraversals property 130](#_Toc4690273)

[3.39 edgeTraversal object 131](#_Toc4690274)

[3.39.1 General 131](#_Toc4690275)

[3.39.2 edgeId property 132](#_Toc4690276)

[3.39.3 message property 132](#_Toc4690277)

[3.39.4 finalState property 132](#_Toc4690278)

[3.39.5 stepOverEdgeCount property 132](#_Toc4690279)

[3.40 stack object 134](#_Toc4690280)

[3.40.1 General 134](#_Toc4690281)

[3.40.2 message property 134](#_Toc4690282)

[3.40.3 frames property 134](#_Toc4690283)

[3.41 stackFrame object 134](#_Toc4690284)

[3.41.1 General 134](#_Toc4690285)

[3.41.2 location property 134](#_Toc4690286)

[3.41.3 module property 134](#_Toc4690287)

[3.41.4 threadId property 134](#_Toc4690288)

[3.41.5 parameters property 134](#_Toc4690289)

[3.42 threadFlowLocation object 135](#_Toc4690290)

[3.42.1 General 135](#_Toc4690291)

[3.42.2 index property 135](#_Toc4690292)

[3.42.3 location property 135](#_Toc4690293)

[3.42.4 module property 136](#_Toc4690294)

[3.42.5 stack property 136](#_Toc4690295)

[3.42.6 kinds property 136](#_Toc4690296)

[3.42.7 state property 138](#_Toc4690297)

[3.42.8 nestingLevel property 138](#_Toc4690298)

[3.42.9 executionOrder property 139](#_Toc4690299)

[3.42.10 executionTimeUtc property 139](#_Toc4690300)

[3.42.11 importance property 139](#_Toc4690301)

[3.43 resultProvenance object 139](#_Toc4690302)

[3.43.1 General 139](#_Toc4690303)

[3.43.2 firstDetectionTimeUtc property 140](#_Toc4690304)

[3.43.3 lastDetectionTimeUtc property 140](#_Toc4690305)

[3.43.4 firstDetectionRunGuid property 140](#_Toc4690306)

[3.43.5 lastDetectionRunGuid property 140](#_Toc4690307)

[3.43.6 invocationIndex property 140](#_Toc4690308)

[3.43.7 conversionSources property 141](#_Toc4690309)

[3.44 reportingDescriptor object 142](#_Toc4690310)

[3.44.1 General 142](#_Toc4690311)

[3.44.2 Constraints 142](#_Toc4690312)

[3.44.3 id property 142](#_Toc4690313)

[3.44.4 deprecatedIds property 143](#_Toc4690314)

[3.44.5 guid property 145](#_Toc4690315)

[3.44.6 deprecatedGuids property 145](#_Toc4690316)

[3.44.7 name property 145](#_Toc4690317)

[3.44.8 deprecatedNames property 145](#_Toc4690318)

[3.44.9 shortDescription property 145](#_Toc4690319)

[3.44.10 fullDescription property 146](#_Toc4690320)

[3.44.11 messageStrings property 146](#_Toc4690321)

[3.44.12 helpUri property 147](#_Toc4690322)

[3.44.13 help property 147](#_Toc4690323)

[3.44.14 defaultConfiguration property 147](#_Toc4690324)

[3.44.15 taxa property 147](#_Toc4690325)

[3.44.16 optionalTaxa 147](#_Toc4690326)

[3.45 reportingConfiguration object 148](#_Toc4690327)

[3.45.1 General 148](#_Toc4690328)

[3.45.2 enabled property 148](#_Toc4690329)

[3.45.3 level property 148](#_Toc4690330)

[3.45.4 rank property 148](#_Toc4690331)

[3.45.5 parameters property 149](#_Toc4690332)

[3.46 configurationOverride object 149](#_Toc4690333)

[3.46.1 General 149](#_Toc4690334)

[3.46.2 reportingDescriptorReference property 150](#_Toc4690335)

[3.46.3 configuration property 150](#_Toc4690336)

[3.47 reportingDescriptorReference object 150](#_Toc4690337)

[3.47.1 General 150](#_Toc4690338)

[3.47.2 Constraints 151](#_Toc4690339)

[3.47.3 reportingDescriptor lookup 151](#_Toc4690340)

[3.47.4 id 151](#_Toc4690341)

[3.47.5 index 152](#_Toc4690342)

[3.47.6 guid 153](#_Toc4690343)

[3.47.7 toolComponent 153](#_Toc4690344)

[3.48 toolComponentReference object 153](#_Toc4690345)

[3.48.1 General 153](#_Toc4690346)

[3.48.2 toolComponent lookup 153](#_Toc4690347)

[3.48.3 name property 153](#_Toc4690348)

[3.48.4 index property 154](#_Toc4690349)

[3.48.5 guid property 154](#_Toc4690350)

[3.49 fix object 154](#_Toc4690351)

[3.49.1 General 154](#_Toc4690352)

[3.49.2 description property 154](#_Toc4690353)

[3.49.3 artifactChanges property 154](#_Toc4690354)

[3.50 artifactChange object 156](#_Toc4690355)

[3.50.1 General 156](#_Toc4690356)

[3.50.2 artifactLocation property 156](#_Toc4690357)

[3.50.3 replacements property 157](#_Toc4690358)

[3.51 replacement object 157](#_Toc4690359)

[3.51.1 General 157](#_Toc4690360)

[3.51.2 Constraints 158](#_Toc4690361)

[3.51.3 deletedRegion property 158](#_Toc4690362)

[3.51.4 insertedContent property 158](#_Toc4690363)

[3.52 notification object 159](#_Toc4690364)

[3.52.1 General 159](#_Toc4690365)

[3.52.2 descriptor property 159](#_Toc4690366)

[3.52.3 associatedRule property 159](#_Toc4690367)

[3.52.4 physicalLocation property 160](#_Toc4690368)

[3.52.5 message property 160](#_Toc4690369)

[3.52.6 level property 160](#_Toc4690370)

[3.52.7 threadId property 160](#_Toc4690371)

[3.52.8 timeUtc property 160](#_Toc4690372)

[3.52.9 exception property 160](#_Toc4690373)

[3.53 exception object 161](#_Toc4690374)

[3.53.1 General 161](#_Toc4690375)

[3.53.2 kind property 161](#_Toc4690376)

[3.53.3 message property 161](#_Toc4690377)

[3.53.4 stack property 161](#_Toc4690378)

[3.53.5 innerExceptions property 161](#_Toc4690379)

[4 External property file format 162](#_Toc4690380)

[4.1 General 162](#_Toc4690381)

[4.2 External property file naming convention 162](#_Toc4690382)

[4.3 externalProperties object 162](#_Toc4690383)

[4.3.1 General 162](#_Toc4690384)

[4.3.2 $schema property 163](#_Toc4690385)

[4.3.3 version property 163](#_Toc4690386)

[4.3.4 guid property 163](#_Toc4690387)

[4.3.5 runGuid property 163](#_Toc4690388)

[4.3.6 The property value properties 164](#_Toc4690389)

[5 Conformance 165](#_Toc4690390)

[5.1 Conformance targets 165](#_Toc4690391)

[5.2 Conformance Clause 1: SARIF log file 165](#_Toc4690392)

[5.3 Conformance Clause 2: SARIF producer 165](#_Toc4690393)

[5.4 Conformance Clause 3: Direct producer 165](#_Toc4690394)

[5.5 Conformance Clause 4: Deterministic producer 166](#_Toc4690395)

[5.6 Conformance Clause 5: Converter 166](#_Toc4690396)

[5.7 Conformance Clause 6: SARIF post-processor 166](#_Toc4690397)

[5.8 Conformance Clause 7: SARIF consumer 166](#_Toc4690398)

[5.9 Conformance Clause 8: Viewer 166](#_Toc4690399)

[5.10 Conformance Clause 9: Result management system 166](#_Toc4690400)

[5.11 Conformance Clause 10: Engineering system 166](#_Toc4690401)

[Appendix A. (Informative) Acknowledgments 167](#_Toc4690402)

[Appendix B. (Normative) Use of fingerprints by result management systems 168](#_Toc4690403)

[Appendix C. (Informative) Use of SARIF by log file viewers 169](#_Toc4690404)

[Appendix D. (Informative) Production of SARIF by converters 170](#_Toc4690405)

[Appendix E. (Informative) Locating rule and notification metadata 171](#_Toc4690406)

[Appendix F. (Normative) Producing deterministic SARIF log files 172](#_Toc4690407)

[F.1 General 172](#_Toc4690408)

[F.2 Non-deterministic file format elements 172](#_Toc4690409)

[F.3 Array and dictionary element ordering 173](#_Toc4690410)

[F.4 Absolute paths 173](#_Toc4690411)

[F.5 Compensating for non-deterministic output 173](#_Toc4690412)

[F.6 Interaction between determinism and baselining 174](#_Toc4690413)

[Appendix G. (Informative) Guidance on fixes 175](#_Toc4690414)

[Appendix H. (Informative) Diagnosing results in generated files 176](#_Toc4690415)

[Appendix I. (Informative) Sample sourceLanguage values 179](#_Toc4690416)

[Appendix J. (Informative) Examples 181](#_Toc4690417)

[J.1 Minimal valid SARIF log file 181](#_Toc4690418)

[J.2 Minimal recommended SARIF log file with source information 181](#_Toc4690419)

[J.3 Minimal recommended SARIF log file without source information 182](#_Toc4690420)

[J.4 Comprehensive SARIF file 183](#_Toc4690421)

[Appendix K. (Informative) Revision History 194](#_Toc4690422)

# Introduction

Software developers use a variety of analysis tools to assess the quality of their programs. These tools report results which can indicate problems related to program qualities such as correctness, security, performance, compliance with contractual or legal requirements, compliance with stylistic standards, understandability, and maintainability. To form an overall picture of program quality, developers often need to aggregate the results produced by all of these tools. This aggregation is more difficult if each tool produces output in a different format.

This document defines a standard format for the output of static analysis tools, called the Static Analysis Results Interchange Format, or “SARIF”[[1]](#footnote-1). The goals of the format are:

* Comprehensively capture the range of data produced by commonly used static analysis tools.
* Be a useful format for analysis tools to emit directly, and also an effective interchange format into which the output of any analysis tool can be converted.
* Be suitable for use in a variety of scenarios related to analysis result management, and be extensible for use in new scenarios.
* Reduce the cost and complexity of aggregating the results of various analysis tools into common workflows.
* Capture information that is useful for assessing a project’s compliance with corporate policy or certification standards.
* Adopt a widely used serialization format that can be parsed by readily available tools.
* Represent analysis results for all kinds of artifacts, including source code and object code.
* Represent the logical location in which a result is produced, such as a function, class, or namespace.
* Represent the physical location at which a result is produced, including problems that are detected in nested files (such as a source file within a compressed container).

Although most static analysis tools analyze files on disk, SARIF can represent results detected in any URI-addressable artifact (for example, the text returned by an HTTP query). This specification uses the term “artifact” to refer to any item that a tool might analyze. It uses the more restrictive term “file” when referring specifically to a file on disk.

## IPR Policy

This Working Draft is being developed under the [RF on RAND Terms](https://www.oasis-open.org/policies-guidelines/ipr#RF-on-RAND-Mode) Mode of the [OASIS IPR Policy](https://www.oasis-open.org/policies-guidelines/ipr), the mode chosen when the Technical Committee was established.

For information on whether any patents have been disclosed that may be essential to implementing this specification, and any offers of patent licensing terms, please refer to the Intellectual Property Rights section of the TC’s web page (<https://www.oasis-open.org/committees/sarif/ipr.php>).

## Terminology

The key words “MUST”, “MUST NOT”, “REQUIRED”, “SHALL”, “SHALL NOT”, “SHOULD”, “SHOULD NOT”, “RECOMMENDED”, “NOT RECOMMENDED”, “MAY”, and “OPTIONAL” in this document are to be interpreted as described in [[BCP14](#BCP14)] [[RFC2119](#RFC2119)] [[RFC8174](#RFC8174)] when, and only when, they appear in all capitals, as shown here.

For purposes of this document, the following terms and definitions apply:

analysis target

[artifact](#def_artifact) which an [analysis tool](#def_static_analysis_tool) is instructed to analyze

artifact

sequence of bytes addressable *via* a URI

Examples: A physical file in a file system such as a source file, an object file, a configuration file or a data file; a specific version of a file in a version control system; a database table; a stream of bytes returned from an HTTP request.

baseline

set of [results](#def_result) produced by a single [run](#def_run) of a set of [analysis tools](#def_static_analysis_tool) on a set of [artifacts](#def_artifact)

NOTE: A [result management system](#def_result_management_system) can compare the results of a subsequent [run](#def_run) to a baseline produced by a [baseline run](#def_baseline_run) to determine whether new results have been introduced.

baseline run

[run](#def_run) that produces a [baseline](#def_baseline) to which subsequent runs can be compared

binary artifact

[artifact](#def_artifact) considered as a sequence of bytes

binary region

[region](#def_region) representing a contiguous range of zero or more bytes in a [binary artifact](#def_binary_file)

call stack

sequence of nested function calls

camelCase name

name that begins with a lowercase letter, in which each subsequent word begins with an uppercase letter

Example: camelCase, version, fullName.

code flow

set of one or more [thread flows](#def_thread_flow) which together specify a pattern of code execution relevant to detecting a [result](#def_result)

column

1-based index of a character within a [line](#def_line)

configuration file

file, typically textual, that configures the execution of an [analysis tool](#def_static_analysis_tool) or [tool component](#def_tool_component)

converter

[SARIF producer](#def_sarif_producer) that transforms the output of an [analysis tool](#def_static_analysis_tool) from its native output format into the SARIF format

custom taxonomy

[taxonomy](#def_taxonomy) defined by and intended for use with a particular [analysis tool](#def_static_analysis_tool)

deterministic producer

[SARIF producer](#def_sarif_producer) which, given identical inputs, repeatedly produces an identical [SARIF log file](#def_sarif_log_file)

direct producer

[analysis tool](#def_static_analysis_tool) which acts as a [SARIF producer](#def_sarif_producer)

driver

[tool component](#def_tool_component) containing an [analysis tool](#def_static_analysis_tool)’s or [converter](#def_converter)’s primary executable, which controls the tool’s or converter’s execution, and which in the case of an analysis tool typically defines a set of analysis [rules](#def_rule)

embedded link

syntactic construct which enables a [message string](#def_message_string) to refer to a location within an [artifact](#def_artifact) mentioned in a [result](#def_result)

engineering system

software development environment within which [analysis tools](#def_static_analysis_tool) execute

NOTE: An engineering system might include a build system, a source control system, a [result management system](#def_result_management_system), a bug tracking system, a test execution system, and so on.

empty array

array that contains no elements, and so has a length of 0

empty object

object that contains no properties

empty string

string that contains no characters, and so has a length of 0

(end) user

person who uses the information in a [log file](#def_log_file) to investigate, [triage](#def_triage), or resolve [results](#def_result)

extension

[tool component](#def_tool_component) other than the [driver](#def_driver) (for example, a [plugin](#def_plugin), a [configuration file](#def_configuration_file), or a [taxonomy](#def_taxonomy))

external property file

file containing the values of one or more [externalized properties](#def_externalized_property)

externalizable property

property that can be contained in an [external property file](#def_external_property_file)

externalized property

property stored outside of the [SARIF log file](#def_log_file) to which it logically belongs

false positive

[result](#def_result) which an [end user](#def_end_user) decides does not actually represent a [problem](#def_problem)

fingerprint

[stable value](#def_stable_value) that can be used by a [result management system](#def_result_management_system) to uniquely identify a [result](#def_result) over time, even if the [artifact](#def_artifact)[def\_programming\_artifact](#def_programming_artifact) in which it occurs is modified

formatted message

[message string](#def_message_string) which contains formatting information such as Markdown formatting characters

fully qualified logical name

string that that fully identifies the programmatic construct specified by a [logical location](#def_logical_location), typically by means of a hierarchical identifier.

Example: The fully qualified logical name of the C# method f(void) in class C in namespace N is "N.C.f(void)". Its [logical name](#def_logical_name) is "f(void)".

hierarchical string

string in the format <component>{/<component>}\*

line

contiguous sequence of characters, starting either at the beginning of an [artifact](#def_artifact) or immediately after a [newline sequence](#def_newline_sequence), and ending at and including the nearest subsequent newline sequence, if one is present, or else extending to the end of the artifact

localizable

subject to being translated from one natural language to another

log file

output file produced by an [analysis tool](#def_static_analysis_tool), which enumerates the [results](#def_result) produced by the tool

(log file) viewer

[SARIF consumer](#def_sarif_consumer) that reads a [log file](#def_log_file), displays a list of the [results](#def_result) it contains, and allows an [end user](#def_end_user) to view each result in the context of the [artifact](#def_artifact)[def\_programming\_artifact](#def_programming_artifact) in which it occurs

logical location

location specified by reference to a programmatic construct, without specifying the [artifact](#def_artifact) within which that construct occurs

Example: A class name, a method name, a namespace.

logical name

string that partially identifies the programmatic construct specified by a [logical location](#def_logical_location) by specifying most specific (often the rightmost) component of its [fully qualified logical name](#def_fully_qualified_logical_name).

Example: The logical name of the C# method f(void) in class C in namespace N is "f(void)". Its [fully qualified logical name](#def_fully_qualified_logical_name) is "N.C.f(void)".

message string

human-readable string that conveys information relevant to an element in a SARIF file

nested artifact

[artifact](#def_artifact) that is contained within another artifact

nested logical location

[logical location](#def_logical_location) that is contained within another logical location

Example: A method within a class in C++

newline sequence

sequence of one or more characters representing the end of a line of text

NOTE: Some systems represent a newline sequence with a single newline character; others represent it as a carriage return character followed by a newline character.

notification

[reporting item](#def_reporting_item) that describes a condition encountered by a [tool](#def_static_analysis_tool) during its execution

parent (artifact)

[artifact](#def_artifact) which contains one or more [nested artifacts](#def_nested_artifact)

physical location

location specified by reference to an [artifact](#def_artifact)[def\_programming\_artifact](#def_programming_artifact), possibly together with a [region](#def_region) within that artifact

plain text message

[message string](#def_message_string) which does not contain any formatting information

plugin

[tool component](#def_tool_component) that defines additional [rules](#def_rule)

policy

set of [rule configurations](#def_rule_configuration) that specify how [results](#def_result) that violate the [rules](#def_rule) defined by a particular [tool component](#def_tool_component) are to be treated

problem

[result](#def_result) which indicates a condition that has the potential to detract from the quality of the program

Example: A security vulnerability, a deviation from contractual or legal requirements, a deviation from stylistic standards.

property

attribute of an object consisting of a name and a value associated with the name

property bag

object consisting of an unordered set of non-standardized [properties](#def_property) with arbitrary [camelCase names](#def_camelCase_name)

redactable property

[property](#def_property) that potentially contains sensitive information that a SARIF [direct producer](#def_direct_producer) or a [SARIF post-processor](#def_post_processor) might wish to redact

region

contiguous portion of an [artifact](#def_artifact)

reporting item

unit of output produced by a [tool](#def_static_analysis_tool), either a [result](#def_result) or a [notification](#def_notification)

reporting configuration

the subset of [reporting metadata](#def_reporting_metadata) that a [tool](#def_static_analysis_tool) can configure at runtime, before performing its scan  
  
Examples: severity level, rank

reporting descriptor

container for [reporting metadata](#def_reporting_metadata)

reporting metadata

information that describes a class of related [reporting items](#def_reporting_item)  
  
Examples: id, description

repository

container for a related set of files in a version control system

response file

file containing arguments for a [tool](#def_static_analysis_tool), which are interpreted as if they had appeared directly on the command line

result

[reporting item](#def_reporting_item) that describes a condition present in an [artifact](#def_artifact)

result file

[artifact](#def_artifact) in which an [analysis tool](#def_static_analysis_tool) detects a [result](#def_result)

result management system

software system that consumes the [log files](#def_log_file) produced by [analysis tools](#def_static_analysis_tool), produces reports that enable engineering teams to assess the quality of their software [artifacts](#def_programming_artifact) at a point in time and to observe trends in the quality over time, and performs functions such as filing bugs and displaying information about individual [results](#def_result)

NOTE: A result management system can interact with a [log file viewer](#def_log_file_viewer) to display information about individual defects.

root file

[SARIF log file](#def_log_file) to which one or more [external property files](#def_external_property_file) logically belong

rule

specific criterion for correctness verified by an [analysis tool](#def_static_analysis_tool)

NOTE 1: Many analysis tools associate a [rule id](#def_rule_id) with each [result](#def_result) they report, but some do not.

NOTE 2: Some rules verify generally accepted criteria for correctness; others verify conventions in use in a particular team or organization.

Example: “Variables must be initialized before use”, “Class names must begin with an uppercase letter”.

rule configuration

[reporting configuration](#def_reporting_configuration) that applies to a [rule](#def_rule)

rule id

[stable value](#def_stable_value) which an [analysis tool](#def_static_analysis_tool) associates with a [rule](#def_rule)

NOTE: A rule id is more likely to remain stable if it is a symbolic or numeric value, as opposed to a descriptive string.

Example: CA2001

rule metadata

[reporting metadata](#def_reporting_metadata) that describes a [rule](#def_rule)

run

1. invocation of a specified [analysis tool](#def_static_analysis_tool) on a specified version of a specified set of [analysis targets](#def_analysis_target), with a specified set of runtime parameters

2. set of [results](#def_result) produced by such an invocation

SARIF consumer

program that reads and interprets a SARIF log file

SARIF log file

[log file](#def_log_file) in the format defined by the SARIF specification

SARIF post-processor

[SARIF producer](#def_sarif_producer) that transforms an existing [SARIF log file](#def_sarif_log_file) into a new SARIF log file, for example, by removing or redacting security-sensitive elements.

SARIF producer

program that emits output in the SARIF format

stable value

value which, once established, never changes over time

standard taxonomy

[taxonomy](#def_taxonomy) defined without reference to a particular [analysis tool](#def_static_analysis_tool)

(static analysis) tool

program that examines [artifacts](#def_artifact) to detect problems, without executing the program

Example: Lint

taxon (pl. taxa)

one of a set of categories which together comprise a [taxonomy](#def_taxonomy)

taxonomy

classification of analysis results into a set of categories

tag

string that conveys additional information about the SARIF [log file](#def_log_file) element to which it applies

text artifact

[artifact](#def_artifact) considered as a sequence of characters organized into [lines](#def_line) and [columns](#def_column)

text region

[region](#def_region) representing a contiguous range of zero or more character in a [text artifact](#def_text_file)

thread flow

temporally ordered set of code locations specifying a possible execution path through the code, which occur within a single thread of execution, such as an operating system thread or a fiber

tool component

component of an [analysis tool](#def_static_analysis_tool) or [converter](#def_converter), either its [driver](#def_driver) or an [extension](#def_extension), consisting of one or more files

top-level artifact

[artifact](#def_artifact) which is not contained within any other artifact

top-level logical location

[logical location](#def_logical_location) that is not nested within another logical location

Example: A global function in C++

translation

rendering of a [tool component](#def_tool_component)’s [localizable](#def_localizable) strings into another language

triage

decide whether a [result](#def_result) indicates a [problem](#def_problem) that needs to be corrected

user

see [end user](#def_end_user).

VCS

version control system

viewer

see [log file viewer](#def_log_file_viewer).

## Normative References

[BCP14] Bradner, S., “Key words for use in RFCs to Indicate Requirement Levels”, March 1997, https://tools.ietf.org/html/bcp14.

[GFM] “GitHub-Flavored Markdown spec”, Version 0.28-gfm (2017-08-01), <https://github.github.com/gfm/>.

[IANA-ENC] Freed, Ned and Dürst, Martin, “Character Sets”, 2017-12-20, <https://www.iana.org/assignments/character-sets/character-sets.xhtml>.

[IANA-HASH] “Hash Function Textual Names”, <https://www.iana.org/assignments/hash-function-text-names/hash-function-text-names.xhtml>, July 4, 2017.

[ISO8601:2004] “Data elements and interchange formats -- Information interchange -- Representation of dates and times”, ISO 8601:2004, December 2004, <https://www.iso.org/standard/40874.html>.

[ISO14977:1996] “Information technology – Syntactic metalanguage – Extended BNF”, ISO/IEC 14977:1996(E), December 1996, <https://www.iso.org/standard/26153.html>.

[JSCHEMA01]Wright, A., “JSON Schema: A Media Type for Describing JSON Documents”, April 2017 (expires October 2017), <http://json-schema.org/latest/json-schema-core.html>.

[RFC2119] Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels", BCP 14, RFC 2119, DOI 10.17487/RFC2119, March 1997, <http://www.ietf.org/rfc/rfc2119.txt>.

[RFC2045] Freed, N. and N. Borenstein, "Multipurpose Internet Mail Extensions (MIME) Part One: Format of Internet Message Bodies", RFC 2045, DOI 10.17487/RFC2045, November 1996, <http://www.rfc-editor.org/info/rfc2045>.

[RFC3629] Yergeau, F., "UTF-8, a transformation format of ISO 10646", STD 63, RFC 3629, DOI 10.17487/RFC3629, November 2003, <http://www.rfc-editor.org/info/rfc3629>.

[RFC3986] Berners-Lee, T., Fielding, R., and L. Masinter, "Uniform Resource Identifier (URI): Generic Syntax", STD 66, RFC 3986, DOI 10.17487/RFC3986, January 2005, <http://www.rfc-editor.org/info/rfc3986>.

[RFC3987] Duerst, M. and Suignard, M., "Internationalized Resource Identifiers (IRIs)", RFC 3987, DOI 10.17487/RFC3987, January 2005, <https://www.rfc-editor.org/info/rfc3987>.

[RFC4122] Leach, P., Mealling, M., and Salz, R., "A Universally Unique IDentifier (UUID) URN Namespace", RFC 4122, DOI 10.17487/RFC4122, July 2005, <http://www.rfc-editor.org/info/rfc4122>.

[RFC5646] Phillips, A., Ed., and M. Davis, Ed., "Tags for Identifying Languages", BCP 47, RFC 5646, DOI 10.17487/RFC5646, September 2009, <http://www.rfc-editor.org/info/rfc5646>.

[RFC6901] Bryan, P., Ed., Zyp, K., and Nottingham, M., Ed., " JavaScript Object Notation (JSON) Pointer ", RFC 6901, DOI 10.17487/RFC6901, April 2013, <http://www.rfc-editor.org/info/rfc6901>.

[RFC8174] Leiba, B., "Ambiguity of Uppercase vs Lowercase in RFC 2119 Key Words", BCP 14, RFC 8174, DOI 10.17487/RFC8174, May 2017, <http://www.rfc-editor.org/info/rfc8174>.

[RFC8089] Kerwin, M., "The "file" URI Scheme", RFC 8089, DOI 10.17487/RFC8089, February 2017, <http://www.rfc-editor.org/info/rfc8089>.

[RFC8259] Bray, T., "The JavaScript Object Notation (JSON) Data Interchange Format", RFC 8259, DOI 10.17487/RFC8259, December 2017, <http://www.rfc-editor.org/info/rfc8259>.

[SEMVER] “Semantic Versioning 2.0.0”, <http://semver.org/>.

[UNICODE10] Unicode 10.0, June 2017, <http://www.unicode.org/versions/Unicode10.0.0/>

## Non-Normative References

[CMARK] “CommonMark Spec”, Version 0.28, (2017-08-01), <http://spec.commonmark.org/0.28/>.

[CWE] “Common Weakness Enumeration”, <https://cwe.mitre.org>.

[GFMCMARK] “GitHub's fork of cmark, a CommonMark parsing and rendering library and program in C”, <https://github.com/github/cmark>.

[GFMENG] “GitHub Engineering: A formal spec for GitHub Flavored Markdown”, <https://githubengineering.com/a-formal-spec-for-github-markdown/>.

[ISO9899:2011] “Information technology – Programming languages – C”, ISO/IEC 9899, December 2011, <https://www.iso.org/standard/57853.html>.

[ISO14882:2017] “Information technology – Programming languages – C++”, ISO/IEC 14882, December 2017, <https://www.iso.org/standard/68564.html>.

[ISO23270:2006] “Information technology – Programming languages – C#”, ISO/IEC 23270, September 2006, <https://www.iso.org/standard/42926.html>.

# Conventions

## General

The following conventions are used within this document.

## Format examples

This document contains several partial examples of the JSON serialization of the SARIF format. The examples are formatted for clarity, as permitted by [[RFC8259](#RFC8259)], which allows “insignificant whitespace” before or after any token; implementations do not need to follow the whitespace convention used in these examples. In these examples, an ellipsis (…) is used to indicate that portions of the log file text required by this specification have been omitted for brevity. A ‘#’ character introduces a comment that extends to the end of the line. These comments are present for explanatory purposes and are not part of the SARIF file format. When a JSON string is too long to fit on a line, it is broken into multiple lines. This is not part of the SARIF format, since JSON strings cannot contain control characters such as newlines.

## Property notation

A SARIF object consists of a set of properties. The value of a property can itself be an object, allowing arbitrary nesting. When necessary for clarity or to avoid ambiguity, we use the “dot” notation to refer to nested values. For example, the physicalLocation object defines a property region whose value is a region object, which in turn contains a charLength property. For clarity, we can refer to the charLength property as physicalLocation.region.charLength.

## Syntax notation

Where this specification describes a syntactic construct, it uses the extended Backus-Naur form (EBNF) defined in [[ISO14977:1996](#ISO14977)].

In all EBNF definitions in this spec:

* The following syntax rules are assumed:

decimal digit = '0' | '1' | '2' | '3' | '4' | '5' | '6' | '7' | '8' | '9';

non negative integer =

"0"

| decimal digit – '0', { decimal digit };

* The following “special sequence” (see [[ISO14977:1996](#ISO14977)], §4.19 and §5.11) refers to any character that can appear in a JSON string according to [[ECMA404](#ECMA404)]:

? JSON string character ?

## Commonly used objects

This specification uses the following notation for certain commonly used objects:

|  |  |
| --- | --- |
| theSarifLog | The root object of the SARIF log file. |
| theRun | The run object (§3.14) containing the object under discussion. |
| theTool | The value of theRun.tool (§3.14.6) |
| theDescriptor | The reportingDescriptor object (§3.44) identified by the reportingDescriptorReference object (§3.47) under discussion. |
| theComponent | The toolComponent object (§3.18) identified by the toolComponentReference object (§3.48) under discussion. |
| theResult | The result object (§3.25) containing the object under discussion. |
| thisObject | The object containing the property under discussion.  NOTE: Usually when the description of a property refers to another property of the same object, the other property is referred to by its unqualified name. When necessary to avoid confusion, the name of the other property is qualified with "thisObject." to emphasize that it is a property of the object under discussion. For an example, see §3.25.7. |

# File format

## General

SARIF defines an object model, the top level of which is the sarifLog object (§3.13), which contains the results of a one or more analysis runs. The runs do not need to be produced by the same analysis tool.

A SARIF log file **SHALL** contain a serialization of the SARIF object model into the JSON format.

NOTE 1: In the future, other serializations might be defined.

The top-level value in the log file, representing the sarifLog object, **SHALL** conform to the JSON object grammar; that is, it **SHALL** consist of a comma-separated sequence of name/value pairs, enclosed in curly brackets, as described in [[RFC8259](#RFC8259)].

A SARIF log file **SHALL** be encoded in UTF-8 [[RFC3629](#RFC3629)].

NOTE 2: [[RFC8259](#RFC8259)] requires this encoding for any JSON text “exchanged between systems that are not part of a closed ecosystem.”

## SARIF file naming convention

The file name of a SARIF log file **SHOULD** end with the extension ".sarif".

EXAMPLE 1: output.sarif

The file name **MAY** end with the additional extension ".json".

EXAMPLE 2: output.sarif.json

## artifactContent object

### General

Certain properties in this specification represent the contents of portions of artifacts external to the log file, for example, artifacts that were scanned by an analysis tool. SARIF represents such content with an artifactContent object. Depending on the circumstances, the SARIF log file might need to represent this content as readable text, raw bytes, or both.

### text property

If the external artifact is a text artifact, an artifactContent object **SHOULD** contain a property named text whose value is a string containing the relevant text. Since SARIF log files are encoded in UTF-8 ([[RFC3629](#RFC3629)]; see §3.1), this means that if the external artifact is a text artifact in any encoding other than UTF-8, the SARIF producer **SHALL** transcode the text to UTF-8 before assigning it to the text property. The SARIF producer **SHALL** escape any characters that [[RFC8259](#RFC8259)] requires to be escaped.

Notwithstanding any necessary transcoding and escaping, the SARIF producer **SHALL** preserve the text artifact’s line breaking convention (for example, "\n" or "\r\n").

If the external artifact is a binary artifact, the text property **SHALL** be absent.

### binary property

If the external artifact is a binary artifact, or if the SARIF producer cannot determine whether the external artifact is a text artifact or a binary artifact, an artifactContent object **SHALL** contain a property named binary whose value is a string containing the MIME Base64 encoding [[RFC2045](#RFC2045)] of the bytes in the relevant portion of the artifact.

If the external artifact is a text artifact in an encoding other than UTF-8, the binary property **MAY** be present, in which case it **SHALL** contain the MIME Base64 encoding of the bytes representing the relevant text in its original encoding.

If the external artifact is a UTF-8 text artifact, the binary property **SHOULD** be absent. If it is present, it **SHALL** contain the MIME Base64 encoding of the UTF-8 bytes representing the relevant text.

### rendered property

An artifactContent object **MAY** contain a property named rendered whose value is a multiformatMessageString object (§3.12) that provides a rendered view of the contents.

EXAMPLE: In this example, a physicalLocation object (§3.27) denotes a memory address. Its region.snippet.rendered property (§3.27.4, §3.28.13) offers a hex view of the relevant address range. The markdown property (§3.12.4) emphasizes a byte of particular interest.

{ # A physicalLocation object (§3.27).

"address": { # See §3.27.6.

"baseAddress": "0x00402180", # See §3.30.1.

"offset": "0x0040" # See §3.30.2.

},

"region": { # See §3.27.4.

"snippet": { # See §3.28.13.

"rendered": { # A multiformatMessageString object (§3.12).

"text": "00 00 01 00 00 00 00 00",

"markdown": "00 00 \*\*01\*\* 00 00 00 00 00"

}

}

}

}

## artifactLocation object

### General

Certain properties in this specification specify the location of an artifact. SARIF represents an artifact’s location with an artifactLocation object. The most important member of an artifactLocation object is its uri property (§3.4.3). If the uri property contains a relative reference (the term used in [[RFC 3986](#RFC3986)] for what is commonly called a “relative URI”), the uriBaseId property (§3.4.4) can sometimes be used to resolve the relative reference to an absolute URI.

### Constraints

At least one of the uri property (§3.4.3) or the artifactIndex property (§3.4.5) **SHALL** be present. In certain circumstances (see §3.4.4 and §3.4.5), they **MAY** both be present.

NOTE: Providing both uri and artifactIndex makes the log file more readable at the expense of increased size. Providing only artifactIndex reduces log file size but makes it less readable to an end user, who has to determine the URI by locating the artifact object (§3.23) at the index within theRun.artifacts (§3.14.15) specified by artifactIndex.

If both uri and artifactIndex are present, they **SHALL** both denote the same artifact. That is, let URI1 be the fully resolved URI of the artifact specified by an artifactLocation object as determined by the uriBaseId resolution procedure described in §3.4.4. Let URI2 be the fully resolved URI of the artifact specified by the artifact object (§3.23) indicated by artifactIndex, determined in the same way. Then URI1 and URI2 **SHALL** be equivalent in the sense described in §3.10.1.

### uri property

Depending on the circumstances, an artifactLocation object either **SHALL**, **SHALL NOT**, or **MAY** contain a property named uri whose value is a string containing a URI [[RFC3986](#RFC3986)] that specifies the location of the artifact. If the artifactLocation object describes a nested artifact whose location within its parent container can be expressed by a path from the root of the container, then if uri is present, it **SHALL** specify a relative reference [[RFC3986](#RFC3986)] expressing that path.

If the artifactIndex property (§3.4.5) is absent, uri **SHALL** be present.

NOTE 1: This ensures that there is a way to locate the artifact specified by the artifactLocation object.

If the artifactLocation object represents a nested artifact whose location within its parent container can be expressed only by means of a byte offset, then uri **SHALL NOT** be present.

NOTE 2: This implies that artifactIndex will be present; see §3.4.5.

Otherwise, uri **MAY** be present.

### uriBaseId property

If this artifactLocation object describes a top-level artifact and the value of its uri property (§3.4.3) is a relative reference, the artifactLocation object **SHOULD** contain a property named uriBaseId whose value is a string which indirectly specifies the absolute URI with respect to which that relative reference is interpreted. If the uri property contains an absolute URI, the uriBaseId property **SHALL** be absent.If this artifactLocation object describes a nested artifact, uriBaseId **SHALL** be absent.

If a SARIF consumer requires an absolute URI (for example, to display the specified artifact to a user), then it needs to resolve uriBaseId to an absolute URI, which it can then combine with the relative reference stored in the uri property.

A SARIF consumer **SHALL** use the following procedure to resolve a uriBaseId to an absolute URI:

1. If the end user has configured the SARIF consumer with a value for the uriBaseId (for example, on the consumer’s command line or through a user interface prompt), then the consumer **SHALL** use the configured value.

EXAMPLE 1: In this example the SARIF consumer’s command line specifies that any uriBaseId property whose value is "SRCROOT" refers to the absolute URI "file:///C:/browser/src/":

C:> SarifAnalyzer --input log.sarif --uriBaseId SRCROOT="file:///C:/browser/src/"

1. If uriBaseId is not yet resolved and theRun.originalUriBaseIds (§3.14.14) is present, the consumer **SHALL** attempt to resolve the uriBaseId from the information in originalUriBaseIds, in the manner specified in §3.14.14.
2. If uriBaseId is not yet resolved, the consumer **MAY** use other information or heuristics to locate the artifact.

The uriBaseId property can be any string; it does not need to have any particular syntax or follow any particular naming convention. In particular, it does not need to designate a machine environment variable or similar value, although it might. The SARIF producer and any SARIF consumers need to agree on the meanings of any values for the uriBaseId property that appear in the log file.

EXAMPLE 2: In this example, the analysis tool has set the uri property of an artifactLocation object (§3.4) to a relative reference. The tool has also set the uriBaseId property to "%srcroot%". The analysis tool and the SARIF consumers have agreed upon a convention whereby this indicates that the relative reference is expressed relative to the root of the source tree in which the file appears.

"artifactLocation": {

"uri": "drivers/video/hidef/driver.c",

"uriBaseId": "%srcroot%"

}

NOTE: There are various reasons for providing the uriBaseId property:

* Portability: A log file that contains relative references together with uriBaseId properties can be interpreted on a machine where the files are located at a different absolute location.
* Determinism: A log file that uses uriBaseId properties has a better chance of being “deterministic”; that is, of being identical from run to run if none of its inputs have changed, even if those runs occur on machines where the files are located at different absolute locations. For more information on this point, see [Appendix F](#AppendixDeterminism), “Producing deterministic SARIF log files”.
* Security: The use of uriBaseId properties avoids the persistence of absolute path names in the log file. Absolute path names can reveal information that might be sensitive.
* Semantics: Assuming the reader of the log file (an end user or another tool) has the necessary context, they can understand the meaning of the location specified by the uri property, for example, “this is a source file”.

For more guidance on the intended use of the uriBaseId property, see §3.4.6.

### artifactIndex property

Depending on the circumstances, an artifactLocation object either **SHALL**, **SHALL NOT**, or **SHOULD** contain a property named artifactIndex whose value is the array index (§3.7.4) within theRun.artifacts (§3.14.15) of the artifact object (§3.23), if any, that describes the artifact specified by this artifactLocation object.

If the uri property (§3.4.3) is absent, then artifactIndex **SHALL** be present.

NOTE 1: This ensures that there is a way to locate the artifact specified by the artifactLocation object.

If theRun.artifacts is absent or does not contain an element that describes the artifact specified by this artifactLocation object, then artifactIndex **SHALL NOT** be present.

NOTE 2: This implies that uri is present.

Otherwise, artifactIndex **SHOULD** be present.

NOTE 3: If artifactIndex is absent, the SARIF consumer will not be able to locate the information contained in the artifact object about the artifact specified by this artifactLocation object.

EXAMPLE: In this example, results[0].locations[0].physicalLocation.artifactLocation.artifactIndex specifies the artifact object located at artifacts[0].

{ # A run object (§3.14).

"artifacts": [

{

"artifactLocation": {

"uri": "file:///C:/Code/main.c"

},

"mimeType": "text/x-c",

}

],

"results": [

{

"ruleId": "CA2101",

"level": "error",

"locations": [

{

"physicalLocation": {

"artifactLocation": {

"uri": "file:///C:/Code/main.c",

"artifactIndex": 0

},

"region: {

"startLine": 24,

"startColumn": 9

}

}

}

]

}

]

}

### Guidance on the use of artifactLocation objects

Some URIs are “deterministic” in the sense that they will be the same from one run to the next and are independent of machine-specific information such as volume names or drive letters. Internet addresses are typically deterministic.

In contrast, file system paths are typically non-deterministic. For example, a source code enlistment might exist at different paths on different machines.

artifactLocation objects represent non-deterministic URIs. The uri property (§3.4.3) **SHOULD** contain a relative reference that *is* deterministic, for example, the relative path from the root of a source code enlistment to the file. The uriBaseId property (§3.4.4) **SHOULD** capture the non-deterministic portion of the URI, for example, the absolute path to the root of the source code enlistment.

EXAMPLE: In this example, the location of a result detected by a tool is specified by a relative reference together with a uriBaseId that specifies the root of the source code enlistment.

{ # A run object (§3.14).

"originalUriBaseIds": { # See §3.14.14.

"SRCROOT": {

"uri": "file:///C:/browser/src/"

}

},

"results": [ # See §3.14.20.

{ # A result object (§3.25).

"locations": [ # See §3.25.12.

{ # A location object (§3.26).

"physicalLocation": { # See §3.26.2.

"artifactLocation": { # An artifactLocation object.

"uri": "ui/window.cpp",

"uriBaseId": "SRCROOT"

}

}

}

]

}

]

}

## String properties

### General

Unless otherwise specified in the description of a specific property, all properties whose values are of type "string" **SHALL** have a non-empty value.

### Localizable strings

Certain string-valued properties in this specification, for example, toolComponent.name (§3.18.6), can be translated into other languages. We describe these properties as being “localizable.” The description of every localizable property will state that it is localizable.

### Redactable strings

Certain string-valued properties in this specification (for example, invocation.commandLine (§3.19.2)) might contain sensitive information that a SARIF producer or a SARIF post-processor might choose to redact. We describe these properties as being “redactable.” The description of every redactable property will state that it is redactable.

If a SARIF producer or a SARIF post-processor chooses to redact sensitive information in a redactable property, it **SHALL** replace the sensitive information with the string whose value is provided by theRun.redactionToken (§3.14.25).

### GUID-valued strings

Certain string-valued properties in this specification provide unique stable identifiers in the form of a GUID or UUID [[RFC4122](#RFC4122)]. This document uses the term “GUID”.

EXAMPLE: "f81d4fae-7dec-11d0-a765-00a0c91e6bf6"

NOTE: RFC4122 allows hex digits in either upper or lower case. It does not permit delimiters such as curly braces ("{", "}") around the value.

The description of every GUID-valued property will state that it is GUID-valued.

### Hierarchical strings

#### General

Certain string-valued properties and certain property names in this specification (for example, the value of the runAutomationDetails.id property (§3.16.4), and the property names in a property bag (§3.8)) are said to be “hierarchical.” This means that the string consists of a sequence of forward-slash-separated components, with this syntax:

hierarchical string = component, { "/", component };

component = { component character };

component character = ? JSON string character ? - "/";

NOTE 1: The grammar prohibits a component from containing a forward slash. There is no escape mechanism to allow a component to include a forward slash.

For examples, see §3.8.2 and §3.16.4.

The description of every hierarchical string will state that it is hierarchical.

A SARIF consumer **SHALL** interpret the values of a hierarchical string as forming a logical hierarchy. The first component represents the top level of the hierarchy, the second component represents the second level, and so on.

NOTE 2: A hierarchical string does not need to include any forward slashes. The syntax permits a single string of non-forward-slash characters. The purpose of this section is to define the semantics of the forward slash character in those properties that respect it.

In string-valued properties and property names that are *not* described as hierarchical, the forward slash character has no special meaning, and a SARIF consumer **SHALL NOT** interpret it as dividing the value into hierarchical components.

#### Versioned hierarchical strings

Certain hierarchical strings in this specification (for example, the property names in result.fingerprints (§3.25.14) and result.partialFingerprints (§3.25.15)) are said to be “versioned.” This means that if the last component of the string is of the form

version component = "v", non negative integer;

then a SARIF consumer **SHALL** consider that component to represent the version number of the entity specified by the string.

The description of every versioned hierarchical string will state that it is versioned.

In string-valued properties and property names that are described as hierarchical but *not* as versioned, a final component matching the syntax of version component has no special meaning, and a SARIF consumer **SHALL NOT** interpret it as a version number.

NOTE 1: A versioned hierarchical string does not need to include a version component. The syntax permits but does not require it.

A hierarchical string without a version component **SHALL** be considered older than any corresponding string with a version component.

EXAMPLE: In this example, the partial fingerprint whose property name is "prohibitedWordHash" is considered to have been computed with an older version of the “prohibited word hash” algorithm than the partial fingerprint whose property name is "prohibitedWordHash/v1".

{ # A result object (§3.25).

"partialFingerprints": { # See §3.25.15.

"prohibitedWordHash": "4efcc21977b55",

"prohibitedWordHash/v1": "097886bc876fe"

}

}

NOTE 2: When a previously unversioned string is later versioned, as in the example above, it might be clearer to specify "v2" for the first explicitly versioned string.

## Object properties

Certain properties in this specification are defined to be objects whose property names satisfy certain conditions. Examples are run.artifacts (§3.14.15) and reportingDescriptor.messageStrings (§3.44.11). Unless otherwise specified in the description of a specific property, if any such object is empty, then either the property **SHALL** be represented as an empty object {}, or it **SHALL** be absent.

## Array properties

### General

Certain properties in this specification are defined to be arrays. Examples are the invocation.toolExecutionNotifications property (§3.19.21) and the property bag tags property (§3.8.2).

### Default value

If an array-valued property is absent, it **SHALL** default to an empty array unless the property’s description specifies otherwise.

### Array properties with unique values

Certain array-valued properties in this specification are described as having “unique” elements. When a property is so described, it means that no two elements of the array **SHALL** have equal values. For purposes of this specification, two array elements **SHALL** be considered equal when they satisfy the condition for equality described in [[JSCHEMA01](#JSCHEMA01)], §4.3, “Instance equality”. In particular, two strings are considered equal when they consist of the same sequence of Unicode [[UNICODE10](#UNICODE10)] code points.

### Array indices

If any property in this specification is described as an “array index,” it **SHALL** contain an integer that is a zero-based index into the specified array. If any such property is absent, it **SHALL** default to -1 (which is otherwise not a valid value for that property), unless the property’s description specifies otherwise.

## Property bags

### General

Certain properties in this specification are defined to be “property bags”. A property bag is an object (§3.6) containing an unordered set of properties with arbitrary names.

The property names are hierarchical strings (§3.5.5). The components of the property names **SHOULD** be camelCase strings, but see [Appendix D](#AppendixConverters) for exceptions.

The property values **MAY** be of any JSON type, including strings, numbers, arrays, objects, Booleans, and null. If a property value is a string, it **MAY** be an empty string.

In addition to those properties that are explicitly documented, every object defined in this specification **MAY** contain a property named properties whose value is a property bag. This allows SARIF producers to include information about each object that is not explicitly specified in the SARIF format.

### Tags

#### General

If a property bag contains a property named tags, the property value **SHALL** be an array of zero or more unique (§3.7.3), hierarchical (§3.5.5) strings. Two strings **SHALL** be considered the same if they consist of the same sequence of Unicode [[UNICODE10](#UNICODE10)] code points.

EXAMPLE: In this example, the SARIF producer tags a result with the string "shipBlocking". Note that anything a tag expresses can also be expressed with a named property bag entry, for example "shipBlocking": true.

{ # A result object (§3.25).

"ruleId": "CA2124",

...

"properties": {

"tags": [

"shipBlocking"

]

}

}

#### Tag metadata

A SARIF log file **MAY** provide additional information about any tag value by including a property whose name is the same as that tag value and whose value is any JSON value. If present, this property **SHALL** be located either in the same property bag that contains the tag, or in the property bag of any SARIF element which lexically contains the element containing the tag.

EXAMPLE: Continuing the example from §3.8.2.1, suppose the tool wishes to provide additional information about ship blocking bugs. It might provide that information within the property bag containing the tag (the property bag belonging to the result object):

{ # A result object (§3.25).

"ruleId": "DB2124",

...

"properties": {

"tags": [

"shipBlocking"

],

"shipBlocking": {

"informationUri":

"http://www.example.com/procedures/shipBlockingBugs.html"

}

}

}

However, there might be several ship blocking bugs. To avoid duplicating information, the tool might choose to place it in the property bag belonging to theRun:

{ # A run object (§3.14).

"results": [

{ # A result object (§3.25).

"ruleId": "DB2124",

...

"properties": {

"tags": [

"shipBlocking"

]

}

],

"properties": {

"shipBlocking": {

"informationUri":

"http://www.example.com/procedures/shipBlockingBugs.html"

}

}

}

## Date/time properties

Certain properties in this specification specify a date and time. The value of every such property, if present, **SHALL** be a string in the following format, which is compatible with [[ISO8601:2004](#ISO86012004)]:

date time = date, [ "T", time, "Z" ] (\* UTC time \*);

date = year, "-", month, "-", day;

year = 4 \* decimal digit;

month = 2 \* decimal digit (\* from 01 to 12 \*);

day = 2 \* decimal digit (\* from 01 to 31 \*);

time = hour, ":", minute, [ ":", second, [ ".", fraction ] ];

hour = 2 \* decimal digit (\* from 00 to 12 \*);

minute = 2 \* decimal digit (\* from 00 to 59 \*);

second = 2 \* decimal digit (\* from 00 to 60, to accommodate leap second \*);

fraction = decimal digit, { decimal digit };

EXAMPLES:  
2016-02-08  
2016-02-08T16:08Z  
2016-02-08T16:08:25Z  
2016-02-08T16:08:25.943Z

The time component of every date/time-valued property **SHALL** be expressed in Coordinated Universal Time (UTC).

NOTE 1: The name of every date/time-valued property ends in “Utc” to emphasize thos requirement.

The time components of date/time-valued properties in property bags (§3.8) **SHOULD** also be expressed in UTC.

NOTE 2: This might not always be possible if the property comes from a source that does not provide time zone information.

A SARIF producer **SHOULD NOT** provide more digits in fraction than warranted by the precision of the clock on the computer on which it runs.

## URI-valued properties

### General

Certain properties in this specification specify either an absolute URI or a URI reference (the term used in [[RFC3986](#RFC3986)] to describe either an absolute URI or a relative reference). The value of every such property, if present, **SHALL** be a string in the format specified by [[RFC3986](#RFC3986)].

If a URI reference refers to a file stored in a version control system (VCS), its value **SHALL** preserve relevant details that permit the correct version of the target file to be retrieved from the VCS. If a URI reference refers to a file stored on a physical file system, it **MAY** be specified as a relative reference that omits root information details (such as hard drive letter and an arbitrarily named root directory associated with a source code enlistment).

NOTE 1: A URI reference (even a relative reference) might contain information that represents unwanted information disclosure, particularly in cases where a tool is analyzing files stored on a physical file system. For example, a file path might contain the account name of a developer.

The URI **SHALL** specify the location of the file at the time the analysis was performed.

Two URI references **SHALL** be considered equivalent if their normalized forms are the same, as described in [[RFC3986](#RFC3986)].

NOTE 2: Some features of this normalized form are:

* Percent-encoded characters use upper-case hexadecimal digits.
* Characters in the ALPHA and DIGIT ranges are not be percent-encoded, nor are hyphen, underscore, or tilde.
* The “:” delimiter is omitted if the port component of the authority is empty.
* In the host component, registered names and hexadecimal addresses use lower-case.
* The scheme component is lower-case.
* "." segments are removed.

For the full specification of the normalized URI form, see [[RFC3986](#RFC3986)].

For additional normalization requirements for URIs that use the "file" scheme, see §3.10.2.

When two URI references are not equivalent in this sense (that is, when their normalized forms are not the same), we will say that they are “distinct.”

Aside from normalization, SARIF producers **SHALL NOT** make any other changes to the text of a URI reference; for example, they **SHALL NOT** convert the path to upper case or to lower case.

NOTE 3: This is especially important when the same SARIF file might be consumed on multiple platforms, for example, a platform such as Microsoft Windows ®, whose NTFS file system is case-insensitive but case-preserving, and a platform such as Linux ®, whose file system is case-sensitive. Consider a scenario where a tool runs on a Windows system using NTFS, and the tool decides to lower-case the file names in the log. If the source files and the SARIF log were transferred to a Linux system, the URI references in the log file would not match the path names on the destination system.

### URIs that use the file scheme

If a URI uses the "file" scheme [[RFC8089](#RFC8089)] and the specified path is network-accessible, the SARIF producer **SHALL** include the host name.

EXAMPLE 1: A file-based URI that references a network share.

file://build.example.com/drops/Build-2018-04-19.01/src

If a URI uses the "file" scheme and the specified path is *not* network-accessible, the SARIF producer **SHOULD NOT** include the host name.

EXAMPLE 2: A file-based URI that references the local file system.

file:///C:/src

A SARIF producer **MAY** choose to omit the hostname (authority) from a file URI, for example, for security reasons. If it does so, then to maximize interoperability with previous version of the URI specification, the URI **SHOULD** start with "file:///", as in EXAMPLE 2. See [[RFC8089](#RFC8089)] for more information on this point.

SARIF direct producers **SHALL** create "file" schema URIs as follows:

1. Resolve the file name to an absolute path, preserving the file system’s casing (even if the file system is case-insensitive), and resolving ".." segments.
2. Create a URI from that path.
3. Optionally, divide the resulting URI into a base URI and a relative URI (preserving case in both parts), and create an entry for the base URI in theRun.originalUriBaseIds (§3.14.14).

SARIF converters might not have the information available to produce a full, normalized absolute path, so they **SHOULD** create "file" schema URIs as follows:

1. Preserve the casing specified in the analysis tool’s native output format.
2. Remove everything to the left of the rightmost ".." segment.
3. Optionally, create an entry for the removed portion of the path in theRun.originalUriBaseIds.

### URIs that use the sarif scheme

In certain circumstances, a URI can refer to an element of the current SARIF log file (for example, see §3.15.2). Such a URI uses the sarif scheme, followed by a JSON pointer [[RFC6901](#RFC6901)] that specifies the element.

EXAMPLE: The URI "sarif:/inlineExternalProperties/0" refers to the 0th element of the array contained in the inlineExternalProperties property (§3.13.5) at the root of the log file.

### Internationalized Resource Identifiers (IRIs)

If a URI-valued property refers to resource identified by an Internationalized Resource Identifier (IRI) [[RFC3987](#RFC3987)], the SARIF producer **SHALL** first transform the IRI into a URI, using the mapping mechanism specified in [[RFC3987](#RFC3987)] §3.1, and then assign the transformed value to the property. The string value of a URI-valued property **SHALL NOT** include Unicode characters such as "é"; such characters are permitted in IRIs but are not permitted in URIs. [[RFC3987](#RFC3987)] §3.1 describes how to replace such characters with “percent-encoded” equivalents to produce a valid URI.

EXAMPLE: Suppose a URI-valued property needs to refer to a resource identified by the string "http://www.example.com/hu/sör.txt". This string contains the character "ö", so it is a valid IRI but not a valid URI. Following the procedure in [[RFC3987](#RFC3987)] §3.1, a SARIF producer would transform this string to the valid URI "http://www.example.com/hu/s%C3%B6r.txt" before assigning it to the property.

## message object

### General

Certain objects in this specification define messages intended to be viewed by a user. SARIF represents such a message with a message object, which offers the following features:

* Message strings in plain text (“plain text messages”) (§3.11.3).
* Message strings that incorporate formatting information (“formatted messages”) in GitHub Flavored Markdown [[GFM](#GFM)] (§3.11.4).
* Message strings with placeholders for variable information (§3.11.5).
* Message strings with embedded links (§3.11.6).

### Constraints

At least one of the text (§3.11.8) and messageId (§3.11.10) properties **SHALL** be present.

NOTE: This ensures that a SARIF consumer can locate the text of the message.

### Plain text messages

A plain text message **SHOULD** be expressed as a single paragraph of plain text, consisting of one or more complete sentences, each ending with a period (or appropriate punctuation for the language in which the message is written). The message **SHALL NOT** contain formatting information such as HTML tags.

The message **SHOULD NOT** contain JSON escaped line breaks (for example, "\r" or "\n"). However, if line breaks are present, they **MAY** follow any convention (for example, "\n" or "\r\n"). A SARIF post-processor **MAY** normalize line breaks to any desired convention, including escaping or removing the line breaks so that the entire message renders on a single line.

The message string **MAY** contain placeholders (§3.11.5) and embedded links (§3.11.6).

If the message consists of more than one sentence, its first sentence **SHOULD** provide a useful summary of the message, suitable for display in cases where UI space is limited.

NOTE 1: If a tool does not construct the message in this way, the initial portion of the message that a viewer displays where UI space is limited might not be understandable.

NOTE 2: The rationale for these guidelines is that the SARIF format is intended to make it feasible to merge the outputs of multiple tools into a single user experience. A uniform approach to message authoring enhances the quality of that experience.

### Formatted messages

#### General

Formatted messages **MAY** be of arbitrary length and **MAY** contain formatting information. The message string **MAY** also contain placeholders (§3.11.5) and embedded links (§3.11.6).

Formatted messages **SHALL** be expressed in GitHub-Flavored Markdown [[GFM](#GFM)]. Since GFM is a superset of CommonMark [[CMARK](#CMARK)], any CommonMark Markdown syntax is acceptable.

#### Security implications

For security reasons, SARIF producers and consumers **SHALL** adhere to the following:

* SARIF producers **SHALL NOT** emit messages that contain HTML, even though all variants of Markdown permit it.
* Deeply nested markup can cause a stack overflow in the Markdown processor [[GFMENG](#GFMENG)]. To reduce this risk, SARIF consumers **SHALL** use a Markdown processor that is hardened against such attacks.

NOTE: One example is the GitHub fork of the cmark Markdown processor [[GFMCMARK](#GFMCMARK)].

* To reduce the risk posed by possibly malicious SARIF files that do contain arbitrary HTML (including, for example, javascript: links), SARIF consumers **SHALL** either disable HTML processing (for example, by using an option such as the --safe option in the cmark Markdown processor) or run the resulting HTML through an HTML sanitizer.

SARIF consumers that are not prepared to deal with the security implications of formatted messages **SHALL NOT** attempt to render them and **SHALL** instead fall back to the corresponding plain text messages.

### Messages with placeholders

A message string **MAY** include or more “placeholders.” The syntax of a placeholder is:

placeholder = "{", index, "}";

index = non negative integer;

index represents a zero-based index into the array of strings contained in the arguments property (§3.11.11).

When a SARIF consumer displays the message, it **SHALL** replace every occurrence of the placeholder {n} with the string value at index n in the arguments array (§3.11.11). Within both plain text and formatted message strings, the characters “{” and “}” **SHALL** be represented by the character sequences “{{” and “}}” respectively.

Within a given message object:

* The plain text and formatted message strings **MAY** contain different numbers of placeholders.
* A given placeholder index **SHALL** have the same meaning in the plain text and formatted message strings (so they can be replaced with the same element of the arguments array).

EXAMPLE 1: Suppose a message object’s text property (§3.11.8) contains this string:

"The variable \"{0}\" defined on line {1} is never used. Consider removing \"{0}\"."

There are two distinct placeholders, {0} and {1} (although {0} occurs twice). Therefore, the arguments array will have at least two elements, the first corresponding to {0} and the second corresponding to {1}.

EXAMPLE 2: In this example, the SARIF consumer will replace the placeholder {0} in message.text with the value "pBuffer" from the 0 element of message.arguments.

{ # A run object (§3.14).

"results": [ # See §3.14.20.

{ # A result object (§3.25).

"ruleId": "CA2101", # See §3.25.5.

"message": { # See §3.25.11.

"text": "Variable '{0}' is uninitialized.", # See §3.11.8.

"arguments": [ "pBuffer" ] # See §3.11.11.

}

}

]

}

### Messages with embedded links

A message string **MAY** include one or more links to locations within artifacts mentioned in the enclosing result object (§3.25). We refer to these links as “embedded links”.

Within a formatted message (§3.11.4), an embedded link **SHALL** conform to the syntax of a GitHub Flavored Markdown link (see [[GFM](#GFM)], §6.6, “Links”), with the restriction that the “link destination” **SHALL** be a non-negative integer (whose interpretation is defined below).

NOTE 1: The GFM link syntax is very flexible. Since a SARIF viewer that renders formatted messages will presumably rely on a full-featured GFM processor, there is no need to restrict the embedded link syntax in SARIF formatted messages.

Within a plain text message (§3.11.3), an embedded link **SHALL** conform to the following syntax (which is a greatly restricted subset of the GFM link syntax) before JSON encoding:

escaped link character = "\" | "[" | "]";

normal link character = ? JSON string character ? – escaped link character;

link character = normal link character | ("\", escaped link character);

link text = { link character };

link destination = ? Any valid URI ?;

embedded link = "[", link text, "](", link destination, ")";

link text is the message text visible to the user.

Literal square brackets ("[" and "]") in the link text of a plain text message **SHALL** be escaped with a backslash ("\").

NOTE 2: When a SARIF log file is serialized as JSON, JSON encoding doubles the backslash.

EXAMPLE 1: Consider this embedded link whose link text contains square brackets and backslashes:

"message": {

"text": "Prohibited term used in [para\\[0\\]\\\\spans\\[2\\](1)."

}

A SARIF viewer would render it as follows:

Prohibited term used in [para[0]\spans[2]](1).

Literal square brackets and (doubled) backslashes **MAY** appear anywhere else in a plain text message without being escaped.

If link destination is a non-negative integer, it **SHALL** refer to a physicalLocation object (§3.27) whose id property (§3.27.2) equals the value of link destination. In this case, theResult **SHALL** contain exactly one physicalLocation object with that id.

NOTE 3: Negative values are forbidden because their use would suggest some non-obvious semantic difference between positive and negative values.

EXAMPLE 2: In this example, a plain text message contains an embedded link to a location with a file. There is exactly one physicalLocation object whose id property matches the link destination.

{

"version": "2.0.0",

"runs": [

{

"results": [

{

"ruleId": "TNT0001",

"message": {

"text": "Tainted data was used. The data came from [here](3)."

},

"locations": [

{

"physicalLocation": {

"uri": "file:///C:/code/main.c",

"region": {

"startLine": 15,

"startColumn": 9

}

}

}

],

"relatedLocations": [

{

"physicalLocation": {

"id": 3,

"uri": "file:///C:/code/input.c",

"region": {

"startLine": 15,

"startColumn": 9

}

}

}

]

}

]

}

]

}

The link destination in embedded links in both plain text messages and formatted messages **MAY** use the "sarif" URI scheme (§3.10.3). This allows a message to refer to any content elsewhere in the SARIF log file.

EXAMPLE 1: A result.message (§3.25.11) can refer to another result in the same run (or, for that matter, in another run within the same log file) as follows:

"There was [another result](sarif:/runs/0/results/42) found by this code flow."

A SARIF viewer executing in an IDE might respond to a click on such a link by selecting the target result in an error list window and navigating the editor to that result’s location.

Because the "sarif" URI scheme users JSON pointer [[RFC6901](#RFC6901)], which locates array elements by their array index, these URIs are potentially fragile if the SARIF log file is transformed by a post-processor.

EXAMPLE 2: If a post-processor concatenates two runs into a single log file, the links within the run at index 1 will be incorrect, and will need to be updated from "sarif:/runs/0/…" to "sarif:/runs/1/…".

EXAMPLE 3: If a post-processor removes results from a run, any links that refer to results at indices following the removed results will need to be adjusted. For example, sarif:/runs/0/results/54 might need to be adjusted to sarif:/runs/0/results/42.

### Message string lookup

A message object can directly contain message strings in its text (§3.11.8) and markdown (§3.11.9) properties. It can also indirectly refer to message strings through its messageId (§3.11.10) property. We refer to the contents of messageId as a “message identifier.”

When a SARIF consumer needs to locate a message string, it **SHALL** follow the string lookup procedure specified in this section. The run object **SHALL** contain enough information for the string lookup procedure to succeed. The string lookup procedure depends on whether the consumer can render formatted messages.

In this procedure, the lookup occurs entirely within the context of a single toolComponent object (§3.18) which we refer to as theComponent. If the SARIF consumer is displaying messages in the language specified by theRun.language (§3.14.7), then theComponent is the tool component that defines the message. If the consumer is displaying messages in any other language – in which case a translation (§3.18.3) is in use – then theComponent is the tool component that contains the translation.

If the consumer can render formatted messages, the lookup procedure is:

1. If message.markdown (§3.11.9) is present, use its value.
2. Otherwise, if message.messageId (§3.11.10) is present, and theComponent. globalMessageStrings (§3.18.20) is present and contains a property whose name matches message.messageId, and if the multiformatMessageString (§3.12) that is the value of that property contains a markdown property (§3.12.4), use the value of that markdown property.
3. Otherwise, execute the lookup procedure for plain text messages, below.

If the consumer cannot render formatted text messages, the string lookup procedure is:

1. If message.text is present, use its value.
2. Otherwise, if message.messageId is present, and theComponent.globalMessageStrings is present and contains a property whose name matches message.messageId, and if the multiformatMessageString that is the value of that property contains a text property (§3.12.3) (which it is required to do), use the value of that property.
3. Otherwise, the string lookup procedure fails (which means that the SARIF log file is invalid).

If the message object occurs as the value of result.message (§3.25.11), then messageId should be looked up first in theRule.messageStrings (§3.44.11), where theRule is a reportingDescriptor object (§3.44), an element of theComponent.rules (§3.18.21), which defines the rule that was violated by this result. If messageId is not found, only then should it be looked up in theComponent.globalMessageStrings as above.

If the message object occurs as the value of notification.message (§3.52.5), then messageId should be looked up first in theNotification.messageStrings (§3.44.11), where theNotification is a reportingDescriptor object (§3.44), an element of theComponent.notifications (§3.18.22), which defines this notification. If messageId is not found, only then should it be looked up in theComponent.globalMessageStrings as above.

### text property

A message object **MAY** contain a property named text whose value is a non-empty string containing a plain text message (§3.11.3).

### markdown property

A message object **MAY** contain a property named markdown whose value is a non-empty string containing a formatted text message (§3.11.4) expressed in GitHub-Flavored Markdown [[GFM](#GFM)].

If the markdown property is present, the text property (§3.11.8) **SHALL** also be present.

NOTE: This ensures that the message is viewable even in contexts that do not support the rendering of formatted text.

SARIF consumers that cannot (or choose not to) render formatted text **SHALL** ignore the markdown property and use the text property instead.

### messageId property

A message object **MAY** contain a property named messageId whose value is a non-empty string containing the message identifier (§3.11.7) for the desired message (§3.11.3). See §3.11.7 for details of the message string lookup procedure.

### arguments property

If the message string specified by any of the properties text (§3.11.8), markdown (§3.11.9), or messageId (§3.11.10) contains any placeholders (§3.11.5), the message object **SHALL** contain a property named arguments whose value is an array of strings. §3.11.5 specifies how a SARIF consumer combines the contents of the arguments array with the message string to construct the message that it presents to the end user, and provides an example.

If none of the properties text, markdown, or messageId contains any placeholders, then arguments **MAY** be absent; if it is present, its value **SHALL** be an empty array.

The arguments array **SHALL** contain as many elements as required by the maximum placeholder index among all the message strings specified by the text, markdown, and messageId properties.

EXAMPLE: If the highest numbered placeholder in the text message string is {3} and the highest numbered placeholder in the markdown message string is {5}, the arguments array must contain at least 6 elements.

## multiformatMessageString object

### General

A multiformatMessageString object groups together all available textual formats for a message string.

### Localizable multiformatMessageStrings

Certain multiformatMessageString-valued properties in this specification, for example, reportingDescriptor.shortDescription (§3.44.9), can be translated into other languages. We describe these properties as being “localizable.” The description of every localizable property will state that it is localizable.

### text property

A multiformatMessageString object **SHALL** contain a property named text whose value is a non-empty string containing a plain text representation of the message.

NOTE: This property is required to ensure that the message is viewable even in contexts that do not support the rendering of formatted text.

### markdown property

A multiformatMessageString object **MAY** contain a property named markdown whose value is a non-empty string containing a formatted message (§3.11.4) expressed in GitHub-Flavored Markdown [[GFM](#GFM)].

SARIF consumers that cannot (or choose not to) render formatted text **SHALL** ignore the markdown property and use the text property (§3.12.3) instead.

## sarifLog object

### General

A sarifLog object specifies the version of the file format and contains the output from one or more runs.

EXAMPLE:

{

"version": "2.0.0", # See §3.13.2.

"runs": [ # See §3.13.4.

{

... # A run object (§3.14)

},

...

{

... # Another run object

}

]

}

### version property

A sarifLog object **SHALL** contain a property named version whose value is a string designating the version of the SARIF specification to which this log file conforms. This string **SHALL** have the value "2.0.0".

Although the order in which properties appear in a JSON object value is not semantically significant, the version property **SHOULD** appear first.

NOTE: This will make it easier for parsers to handle multiple versions of the SARIF format if new versions are defined in the future.  
  
**NOTE: Throughout this specification, the version "2.0.0" is used. However, until this specification is finalized, producers SHOULD use the version value "2.0.0-csd.2.beta.YYYY-MM-DD" (found on the title page of this document) to denote the specific draft version to which their output conforms. This note will be removed in the final version of the specification.**

### $schema property

A sarifLog object **MAY** contain a property named $schema whose value is a string containing an absolute URI from which a JSON schema document describing the version of the SARIF format to which this log file conforms can be obtained.

If the $schema property is present, the JSON schema obtained from the specified URI **SHALL** describe the version of the SARIF format specified by the version property (§3.13.2).

NOTE: The purpose of the $schema property is to allow JSON schema validation tools to locate an appropriate schema against which to validate the log file. This is useful, for example, for tool authors who wish to ensure that logs produced by their tools conform to the SARIF format.

### runs property

A sarifLog object **SHALL** contain a property named runs whose value is either null or an array of zero or more run objects (§3.14).

The value of runs **SHALL** be an array with at least one element except in the following circumstances:

* If theSarifLog is the output of a query on a result management system, and the query did not match any runs stored in the result management system, then the value of runs **SHALL** be an empty array.
* If theSarifLog is the output of a query on a result management system, and the result management system was unable to execute the query (for example, because the query was malformed) then the value of runs **SHALL** be null.

### inlineExternalProperties property

A sarifLog object **MAY** contain a property named inlineExternalProperties whose value is an array of zero or more unique (§3.7.3) externalProperties objects (§4.3).

NOTE: This property allows multiple runs to share large data sets in a single, self-contained log file.

EXAMPLE: In this example, two tools analyze the same set of image files, stored in sarifLog.inlineExternalProperties[0].artifacts. The first tool locates the inline externalProperties object by means of a URI with the sarif scheme (see §3.10.3). The second tool locates the object by means of its guid property (§4.3.4).

{

"$schema": "http://json.schemastore.org/sarif-2.0.0",

"version": "2.0.0",

"inlineExternalProperties": [

{

"guid": "00001111-2222-3333-4444-555566667777", # See §4.3.4.

"artifacts": [ # See §4.3.6.

{

"artifactLocation": {

"uri": "apple.png"

},

"mimeType": "image/png"

},

{

"artifactLocation": {

"uri": "banana.png"

},

"mimeType": "image/png"

}

]

}

],

"runs": [ # See §3.13.4.

{ # A run object (§3.14).

"tool": { # See §3.14.6.

"name": "ImageAccessibilityScanner"

},

"externalPropertyFileReferences": [ # See §3.14.2.

{

"location": {

"uri": "sarif:/inlineExternalPropertyFiles/0"

}

}

],

"results": [

...

]

},

{

"tool": {

"name": "ImageSuitabilityScanner"

},

"externalPropertyFileReferences": [

{

"guid": "00001111-2222-3333-4444-555566667777"

}

],

"results": [

...

]

}

]

}

## run object

### General

A run object describes a single run of an analysis tool and contains the output of that run.

EXAMPLE:

{

"tool": { # See §3.14.6.

... # A tool object (§3.17).

},

"results": [ # See §3.14.20.

{

... # A result object (§3.25).

},

...

{

... # Another result object.

}

]

}

### externalPropertyFileReferences property

#### Rationale

In some engineering environments, a single tool run might analyze hundreds of thousands of files and produce millions of results. This causes problems for both producers and consumers of such large SARIF log files:

* The log file might be too large for a consumer to hold in memory and might take several minutes to read.
* During production, some information (such as the complete set of artifacts that were analyzed, the complete set of rules that were violated, or the end time of the run) cannot be known until the run is complete. Therefore, it is likely to be serialized at the end of the log file. However, consumers might need to access some of that information before reading the entire file. For example, a SARIF viewer might need to display rule metadata along with each result it displays, or to display the start and end times of a set of tool runs.

To mitigate these problems, SARIF allows certain properties of a run object and its sub-objects to be stored in separate files. We refer to these files as “external property files”, and we refer to the file containing the run object itself as the “root file”. We refer to a property that can be stored in an external property file as an “externalizable property.” We refer to a property that *has* been stored in an external property file as an “externalized property.”

An external property file **SHALL** contain one or more externalized properties. The format of an external property file is described in §4.

A SARIF consumer **SHALL** treat the contents of a property stored in an external property file exactly as if they had appeared inline in the root file as the value of the corresponding property.

#### Property definition

A run object **MAY** contain a property named externalPropertyFileReferences whose value is an object (§3.6) each of whose property names specifies an externalized property and whose corresponding property values specify the locations of one or more external property files that hold the values of those properties.

The following table lists all the externalizable properties together with their corresponding property names in this object:

|  |  |  |
| --- | --- | --- |
| **Externalizable property** | **Property name in**  **externalPropertyFileReferences** | **Type** |
| run.addresses | addresses | array |
| run.artifacts | artifacts | array |
| run.conversion | conversion | object |
| run.graphs | graphs | array |
| run.logicalLocations | logicalLocations | array |
| run.policies | policies | array |
| run.properties | externalizedProperties | object |
| run.results | results | array |
| run.taxonomies | taxonomies | array |
| run.threadFlowLocations | threadFlowLocations | array |
| run.translations | translations | array |
| run.tool.driver | driver | object |
| run.tool.extensions | extensions | array |

NOTE 1: run.properties is externalized under the property name externalizedProperties to allow this object to have a property bag named properties, consistent with all other objects in this specification.

NOTE 2: Note that run.conversion.tool.driver and run.conversion.tool.extensions are not separately externalizable. Rather, the run.conversion property as a whole is externalizable.

Every externalizable property whose type is shown in the table as “object” **SHALL**, if externalized, be stored in a single external property file. In that case, the value of the corresponding property in externalPropertyFileReferences **SHALL** be an externalPropertyFileReference object (§3.15) specifying the location of the external property file.

Every externalizable property whose type is shown in the table as “array” **SHALL**, if externalized, be stored in one or more external property files. In that case, the value of the corresponding property in externalPropertyFileReferences **SHALL** be an array of one or more externalPropertyFileReference objects specifying the locations of those external property files.

EXAMPLE 1: In this example, run.conversion is stored in the file C:\logs\scantool.conversion.sarif-external-properties and run.results is divided into the files C:\logs\scantools.results-1.sarif-external-properties and C:\logs\scantools.results-2.sarif-external-properties.

{ # A run object.

"originalUriBaseIds": { # See §3.14.14.

"LOGSDIR": {

"uri": "file:///C:/logs/"

}

},

"externalPropertyFileReferences": {

"conversion": { # An externalPropertyFileReference object (§3.15).

"location": { # See §3.15.2.

"uri": "scantool.conversion.sarif-external-properties",

"uriBaseId": "LOGSDIR",

"artifactIndex": 0

},

"guid": "11111111-1111-1111-1111-111111111111" # See §3.15.3.

},

"results": [

{

"location": {

"uri": "scantool.results-1.sarif-external-properties",

"uriBaseId": "LOGSDIR",

"artifactIndex": 1

},

"guid": "22222222-2222-2222-2222-222222222222",

"itemCount": 10000

},

{

"location": {

"uri": "scantool.results-2.sarif-external-properties",

"uriBaseId": "LOGSDIR",

"artifactIndex": 2

},

"guid": "333333333333-3333-3333-3333-333333333333",

"itemCount": 4277

}

]

}

...

}

If a property appears inline in the root file, its name **SHALL NOT** appear as one of the property names in externalPropertyFileReferences. Even if the property name erroneously appears in externalPropertyFileReferences, a SARIF consumer **SHALL** ignore the contents of the external property file. Since an external property file can contain multiple externalized properties, externalPropertyFileReference objects belonging to distinct properties **MAY** denote the same external property file. However, if an array-valued externalizable property is divided among multiple external property files, the externalPropertyFileReference objects belonging to that property **SHALL** denote distinct external property files.

EXAMPLE 2: In this example, theRun.conversion and theRun.properties are stored in the same external property file.

{ # A run object (§3.14).

"originalUriBaseIds": { # See §3.14.14.

"LOGSDIR": {

"uri": "file:///C:/logs/"

}

},

"externalPropertyFileReferences": {

"conversion": { # An externalPropertyFileReference object (see §3.15).

"location": { # See §3.15.2.

"uri": "scantool.sarif-external-properties",

"uriBaseId": "LOGSDIR",

"artifactIndex": 0

},

"guid": "11111111-1111-1111-1111-111111111111" # See §3.15.3.

},

"externalizedProperties": {

"location": {

"uri": "scantool.sarif-external-properties",

"uriBaseId": "LOGSDIR",

"artifactIndex": 0

},

"guid": "11111111-1111-1111-1111-111111111111"

}

}

...

}

EXAMPLE 3: This example represents invalid SARIF because both elements of the array belonging to the results property denote the same external property file.

{ # A run object (§3.14).

"originalUriBaseIds": { # See §3.14.14.

"LOGSDIR": {

"uri": "file:///C:/logs/"

}

},

"externalPropertyFileReferences": {

"results": [

{ # An externalPropertyFileReference object (see §3.15).

"location": {

"uri": "scantool.results.sarif-external-properties",

"uriBaseId": "LOGSDIR",

"artifactIndex": 0

},

"guid": "22222222-2222-2222-2222-222222222222"

},

{ # INVALID: The two external property files are the same.

"location": {

"uri": "scantool.results.sarif-external-properties",

"uriBaseId": "LOGSDIR",

"artifactIndex": 0

},

"guid": "22222222-2222-2222-2222-222222222222"

}

]

}

...

}

### automationDetails property

A run object **MAY** contain a property named automationDetails whose value is an runAutomationDetails object (§3.16) that describes this run.

For an example, see §3.16.1.

### aggregateIds property

A run object **MAY** contain a property named aggregateIds whose value is an array of zero or more unique (§3.7.3) runAutomationDetails objects (§3.16) each of which describes an aggregate of runs to which this run belongs.

For an example, see §3.16.1.

### baselineGuid property

A run object **MAY** contain a property named baselineGuid whose value is a GUID-valued string (§3.5.4) which **SHALL** equal the automationDetails.guid property (§3.14.3, §3.16.5) of some previous run.

NOTE: This ensures that only “similar” runs are compared.

If baselineGuid is present, the result.baselineState property (§3.25.22) of every result object (§3.25) in theRun **SHALL** be computed with respect to the run specified by baselineGuid.

### tool property

A run object **SHALL** contain a property named tool whose value is a tool object (§3.17) that describes the analysis tool that was run.

### language

A run object **MAY** contain a property named language whose value is a string specifying the language of the localizable strings (§3.5.2) in theRun (except for localizable strings that occur within theRun.translations (§3.14.9)), in the format specified by [[RFC5646](#RFC5646)]. If this property is absent, it **SHALL** default to "en-US".

EXAMPLE 1: The language is region-neutral English:

"language": "en"

EXAMPLE 2: The language is French as spoken in France:

"language": "fr-FR"

### taxonomies property

A run object **MAY** contain a property named taxonomies whose value is an array of zero or more unique (§3.7.3) toolComponent objects (§3.18) each of which represents a standard taxonomy (§3.18.2).

NOTE: Analysis tools can define their own custom taxonomies; see §3.18.2 and §3.18.23.

### translations property

A run object **MAY** contain a property named translations whose value is an array of zero or more unique (§3.7.3) toolComponent objects (§3.18) each of which represents a translation (§3.18.3).

### policies property

A run object **MAY** contain a property named policies whose value is an array of zero or more unique (§3.7.3) toolComponent objects (§3.18) each of which represents a policy (§3.18.4).

### invocations property

A run object **MAY** contain a property named invocations whose value is an array of zero or more invocation objects (§3.19) that describe the invocation of the analysis tool that was run.

Normally, an analysis tool runs as a single process, and the invocations array requires only one element. The invocations property is defined as an array, rather than as a single invocation object, to accommodate tools which execute a sequence of programs to produce results. For example, a tool might run one program to determine the set of artifacts to analyze and another program to analyze those artifacts.

The elements of the invocations array **SHOULD**, as far as possible, be arranged in chronological order according to the start time of each process. If some of the processes run in parallel, this might not be possible.

### conversion property

If a run object was produced by a converter, it **MAY** contain a property named conversion whose value is a conversion object (§3.20) that describes how the converter transformed the analysis tool’s native output format into the SARIF format.

A direct producer **SHALL NOT** emit the conversion property.

### versionControlProvenance property

A run object **MAY** contain a property named versionControlProvenance whose value is an array of zero or more unique (§3.7.3) versionControlDetails objects (§3.22). Each array entry specifies a revision in a repository containing files that were scanned during the run.

NOTE 1: This property allows an engineering system to reproduce a scan by retrieving the specified revision of the required files from of each repository before repeating the analysis run.

NOTE 2: This property is an array, rather than a single versionControlDetails object, to support scenarios where a tool scans files from multiple repositories in a single run.

NOTE 3: This specification refers to a container for a related set of files in a VCS as a “repository.” Different VCSs use different terms; for example, Visual Studio Team Services Version Control calls it a “team project”.

NOTE 4: This specification refers to a fixed revision of a set of files as a “revision”. Different VCSs use different terms; for example, Git calls it a “commit”.

EXAMPLE: In this example, an analysis tool has scanned files from one repository: the GitHub repository example/browser.

{ # A run object.

"versionControlProvenance": [

{ # A versionControlDetails object (§3.22).

"repositoryUri": "https://github.com/example/browser", # See §3.22.3.

"revisionId": "fd3fbae" # See §3.22.4.

"branch": "master" # See §3.22.5.

}

]

}

### originalUriBaseIds property

A run object **MAY** contain a property named originalUriBaseIds whose value is an object (§3.6) each of whose property names designates a URI base id (§3.4.4) and each of whose property values is an artifactLocation object (§3.4) that specifies (in the manner described below) the absolute URI [[RFC3986](#RFC3986)] of that URI base id on the machine where the SARIF producer ran.

If the artifactLocation object’s uri property (§3.4.3) is a relative reference, its uriBaseId property **SHALL** be present. Otherwise (that is, if uri is an absolute URI), uriBaseId **SHALL** be absent.

The values of the uriBaseId properties in the artifactLocation objects in originalUriBaseIds **SHALL NOT** form a loop, in the sense described in the URI base id resolution procedure below.

This property allows SARIF consumers to resolve any relative references which appear in any artifactLocation objects elsewhere in the run, as long as the consumer runs either on the same machine as the producer, or on a machine with an identical file system layout. This is useful for individual developers who wish to run analysis tools and examine the results in a viewer. It is also useful for teams which share a convention for their file system layout.

A SARIF consumer **SHALL** use the following procedure to resolve a URI base id from the information in originalUriBaseIds:

NOTE 1: This procedure is part of an overall URI base id resolution procedure described in §3.4.4.

NOTE 2: In this procedure, we refer to the resolved URI value by the variable name resolvedUri.

1. Set resolvedUri to an empty string.
2. Fetch the artifactLocation object whose property name within originalUriBaseIds is the value of uriBaseId. If there is no such property, the resolution procedure fails.
3. Prepend artifactLocation.uri to resolvedUri.
4. If artifactLocation.uri is an absolute URI, resolvedUri is the final resolved URI, and the procedure succeeds.  
     
   Otherwise:
5. If uriBaseId is absent, the resolution procedure fails.

NOTE 3: This would not occur in a valid SARIF file, but the file might not be valid.

1. If the value of uriBaseId has already been encountered during this resolution procedure (that is, if there is a loop in the sequence of URI base ids), the resolution procedure fails.

NOTE 4: This would not occur in a valid SARIF file, but the file might not be valid.

1. Otherwise (that is, if uriBaseId is present and its value has not previously been encountered during this resolution), return to Step 2.

EXAMPLE: In this example, the URI base id "SRCROOT" on the machine where the SARIF producer ran was "file:///C:/code/MyProject/src/". The producer detected a result in a file whose location relative to that URI base id was "lib/memory.c". A viewer which wished to display that file would first attempt to locate it on the local file system at "C:\code\MyProject\src\lib\memory.c". If the file did not exist at that location, the viewer might prompt the user for the location.

{ # A run object.

"originalUriBaseIds": {

"PROJECTROOT": {

"uri": "file:///C:/code/MyProject/"

},

"SRCROOT": {

"uri": " src/",

"uriBaseId": "PROJECTROOT"

}

},

"results": [

{ # A result object (§3.25).

"ruleId": "CA1001",

"locations": [

{ # A location object (§3.26).

"physicalLocation": { # See §3.26.2.

"artifactLocation": { # An artifactLocation object (§3.3).

"uri": "lib/memory.c",

"uriBaseId": "SRCROOT"

}

}

}

]

}

]

}

### artifacts property

A run object **SHOULD** contain a property named artifacts whose value is an array of zero or more unique (§3.7.3) artifact objects (§3.23) each of which represents an artifact relevant to the run.

The array **SHOULD** contain elements representing at least those artifacts in which results were detected, but it **MAY** contain elements representing all artifacts examined by the tool (whether or not results were detected in those artifacts), or any subset of those artifacts. It **MAY** also include other artifacts relevant to the run, such as attachments (§3.25.24).

NOTE: artifact objects contain information that is useful for viewers. Viewers will be able to provide the most information to users if the artifacts property is present and contains information for every artifact in which results were detected.

EXAMPLE:

"artifacts": [

{

"artifactLocation": {

"uri": "file:///C:/Code/main.c"

},

"mimeType": "text/x-c",

"hashes": {

"sha-256": "b13ce2678a8807ba0765ab94a0ecd394f869bc81"

}

}

}

In some cases, an artifact might be nested within another artifact (for example, a compressed container), referred to as its “parent.” An artifact that is not nested within another artifact is referred to as a “top-level artifact”. An artifact that is nested within another artifact is referred to as a “nested artifact”. Within the artifacts array, an artifact object representing a nested artifact is linked to its parent *via* its parentIndex property (§3.23.3). For an example, see §3.23.3.

If a nested artifact appears in the artifacts array, then the artifacts array **SHALL** also contain elements describing each of its parents, up to and including the top-level artifact.

### logicalLocations property

Depending on the circumstances, a run object either **MAY** or **SHOULD** contain a property named logicalLocations whose value is an array of zero or more unique (§3.7.3) logicalLocation objects (§3.31) each of which represents a logical location relevant to one or more results detected during the run.

If the tool has source location information available, and therefore can produce results with physical location information (such as the source file name, line, and column), logicalLocations **MAY** be present.

If the tool does not have source location information available, and therefore can only produce results with logical location information (such as a namespace, type, and method name), logicalLocations **SHOULD** be present.

In some cases, a logical location might be nested within another logical location (for example, a class nested within a namespace), referred to as its “parent.” A logical location that is not nested within another logical location is referred to as a “top-level logical location”. A logical location that is nested within another logical location is referred to as a “nested logical location”. Within the logicalLocations array, a logicalLocation object representing a nested logical location is linked to its parent *via* its parentIndex property (§3.31.9).

If a nested logical location appears in the logicalLocations array, then the logicalLocations array **SHALL** also contain elements describing each of its parents, up to and including the top-level logical location.

EXAMPLE: In this example, a result was detected in the C++ class namespaceA::namespaceB::classC. The logicalLocations array contains not only an element describing the class, but also elements describing its containing namespaces.

"logicalLocations": [

{

"name": "classC",

"fullyQualifiedName": "namespaceA::namespaceB::classC",

"kind": "type",

"parentIndex": 1

},

{

"name": "namespaceB",

"fullyQualifiedName": "namespaceA::namespaceB",

"kind": "namespace"

"parentIndex": 2

},

{

"fullyQualifiedName": "namespaceA",

"kind": "namespace"

}

]

NOTE: The detailed information in logicalLocations is useful, even though much of it is captured in logicalLocation.fullyQualifiedName (§3.31.6), because it allows results management systems and other SARIF consumers to organize analysis results, for example, by asking questions such as “How many results were found in the namespace namespaceA::namespaceB?”. Programs can ask these questions without having to know how to parse the fullyQualifiedName string.

### addresses property

A run object **MAY** contain a property named addresses whose value is an array of zero or more unique (§3.7.3) address objects (§3.42) representing addresses that appear in physicalLocation objects (§3.27) within theRun.

In some cases, an address might be nested within another address (for example, an offset within a table within a section). An address that is nested within another address is referred to as a “nested address”. Within the addresses array, an address object representing a nested address is linked to its parent *via* its parentIndex property (§3.30.7).

If a nested address appears in the addresses array, then addresses **SHALL** also contain elements describing each of its parents, up to and including the top-level address.

### threadFlowLocations property

A run object **MAY** contain a property named threadFlowLocations whose value is an array of zero or more unique (§3.7.3) threadFlowLocation objects (§3.42) representing locations that appear in threadFlow objects (§3.34) within the run.

The threadFlowLocations array may contain all or any subset of the threadFlowLocation objects in the run.

NOTE: Defining threadFlowLocation objects within run.threadFlowLocations can reduce the size of the log file if certain locations occur frequently, either within a single thread flow (for example, if the thread flow represents a loop) or across thread flows (for example, if all thread flows start at the program entry point and share their first few locations).

### graphs property

A run object **MAY** contain a property named graphs whose value is an array of zero or more unique (§3.7.3) graph objects (§3.35). A graph object represents a directed graph: a network of nodes and directed edges that describes some aspect of the structure of the code (for example, a call graph).

A graph object defined at the run level **MAY** be referenced by a graphTraversal object (§3.38) defined in the graphTraversals property (§3.25.18) of any result object (§3.25) in the run.

### results property

A run object **SHALL** contain a property named results whose value is either null or an array of zero or more result objects (§3.25), each of which represents a single result detected in the course of the run.

NOTE: The results array is not defined to contain unique (§3.7.3) elements because some tools report a line number but not a column number for a result’s location. Such a tool might report the same result twice on the same line, in some cases producing multiple identical result objects.

If the tool failed to start, and if the engineering system system responsible for running the tool synthesized a SARIF file to record the failure, then results **SHALL** be null. See §3.19.13, invocation.processStartFailureMessage, for more about this scenario.

If the tool started but failed to begin its analysis (for example, because its command line was invalid), then again results **SHALL** be null.

In all other circumstances, results **SHALL** be present and **SHALL** contain all results detected by the tool. If the tool did not detect any results, results **SHALL** be an empty array.

### defaultEncoding property

A run object **MAY** contain a property named defaultEncoding whose value is a string that provides a default for the encoding property (§3.23.9) of any artifact object (§3.23) in run.artifacts (§3.14.15) that refers to a text artifact. The string **SHALL** be one of the character set names specified in [[IANA-ENC](#IANA_ENC)]. The property value **SHALL** be case-insensitive.

If this property is absent, it **SHALL** be interpreted as meaning that there is no default file encoding. In that case, the encoding of any artifact object that does not contain an encoding property **SHALL** be taken to be unknown.

For an example, see §3.23.9.

### defaultSourceLanguage property

A run object **MAY** contain a property named defaultSourceLanguage whose value is a hierarchical string (§3.5.5) that provides a default value for the sourceLanguage property (§3.23.10) of any artifact object (§3.23) in run.artifacts (§3.14.15) which refers to a text artifact that contains source code.

If defaultSourceLanguage is present, its value **SHOULD** conform to the conventions defined in §3.23.10.2.

If defaultSourceLanguage is absent, it **SHALL** be taken to mean that there is no default source language. In that case, the source language of any artifact object that does not contain a sourceLanguage property **SHALL** be taken to be unknown. In that case, a SARIF viewer **MAY** use any method or heuristic to determine the source language of each file, for example by examining the file’s file name extension or MIME type, or by prompting the user.

### newlineSequences property

A run object **MAY** contain a property named newlineSequences whose value is an array of one or more unique (§3.7.3) strings, each of which specifies a character sequence that the tool treated as a line break during this run.

If this property is absent, it **SHALL** default to the array [ "\r\n", "\n" ].

The order of the elements in the array is significant. It **SHALL** mean that at potential line breaks, the tool “greedily” attempted to match each element of the array in order.

EXAMPLE 1: If newlineSequences has the value [ "\r\n", "\r", "\n" ], the character sequence "\r\n" counts as one line break, not two.

NOTE: This property is useful for SARIF consumers that are sensitive to the value of the line number properties startLine (§3.28.5) and endLine (§3.28.7) in region objects (§3.28). It ensures that the consumer counts lines in the same way as the producer. A SARIF viewer might use this property when highlighting a region to ensure that it highlights the correct lines. More critically, a tool that applies fixes (see §3.49), especially one that applies them automatically, can use this property to ensure that it inserts and removes content on the correct lines.

EXAMPLE 2: In this example, the SARIF producer accepts the Unicode characters NEXT LINE (U+0085) and LINE SEPARATOR (U+2028) as line separators in addition to the usual values.

{ # A run object (§3.14).

...

"newlineSequences": [ "\r\n", "\n", "\u0085", "\u2028" ],

...

}

### columnKind property

If a SARIF producer processes text artifacts, the run object **SHALL** contain a property named columnKind whose value is a string that specifies the unit in which the analysis tool measures columns.

columnKind **SHALL** have one of the following values, with the specified meanings:

* "utf16CodeUnits": Each UTF-16 code unit is considered to occupy one column. This means that a surrogate pair is considered to occupy two columns.
* "unicodeCodePoints": Each Unicode code point (abstract character) is considered to occupy one column. This means that even a character that is represented in UTF-16 by a surrogate pair is considered to occupy one column.

If the SARIF producer does not process text artifacts, columnKind **SHALL** be absent.

If the SARIF producer processes text artifacts and columnKind is absent, it **SHALL** default to unicodeCodePoints.

If a SARIF consumer uses a column measurement unit other than that specified by columnKind, and if the consumer is required to interact with the artifact’s contents (for example, by displaying the artifact in an editor and highlighting a region), the consumer **SHALL** recompute column numbers in its (the consumer’s) native measurement unit.

### redactionToken property

If the value of any redactable property (§3.5.3) in the run has been redacted, the run object **SHALL** contain a property named redactionToken whose value is the string used to replace the redacted text. If no text in the run has been redacted, the redactionToken property **SHALL** be absent.

The value of redactionToken **SHOULD** be the string "[REDACTED]". If for any reason a different value is used, it **MAY** be any readily identifiable string. An example of a situation where a SARIF producer might choose a different redaction token is if the string "[REDACTED]" occurs in the value of any redactable property in the run.

EXAMPLE 1: In this example, the leading portion of a full path name has been redacted from the redactable property invocation.commandLine to avoid revealing information about the machine.

{ # A run object (§3.14).

"redactionToken": "[REDACTED]",

"invocation": {

"commandLine": "SourceScanner --input [REDACTED]/src/ui"

}

...

}

## externalPropertyFileReference object

### General

An externalPropertyFileReference object contains information that enables a SARIF consumer to locate the external property file (see §3.14.2) that contains the value of an externalized property.

### location property

Depending on the circumstances, an externalPropertyFileReference object either **SHALL** or **MAY** contain a property named location whose value is an artifactLocation object (§3.4) that specifies the location of the external property file.

If the externalized properties are persisted in a separate file, location **SHALL** be present. In that case, if the artifactLocation object’s uri property (§3.4.3) specifies a relative reference and its uriBaseId property (§3.4.4) is absent, then uri **SHALL** be interpreted relative to the location of the root file.

Otherwise (that is, if the externalized properties are persisted as an element of theSarifLog.inlineExternalProperties (§3.13.5), then location **MAY** be present. If location is present, its uri property **SHALL** be an absolute URI using the sarif scheme (§3.10.3), and its uriBaseId property **SHALL** be absent. If location is absent, then a SARIF consumer that needs to locate the externalized properties **SHALL** do so using the guid property (§3.15.3).

### guid property

An externalPropertyFileReference object **SHALL** contain a property named guid whose value is a GUID-valued string (§3.5.4) which provides a unique, stable identifier for the external property file.

### itemCount property

If an externalPropertyFileReference object specifies an external property file that contains all or a portion of an array-valued property, it **MAY** contain a property named itemCount whose value is an integer greater than or equal to 1 that specifies the number of items in the externalized property array in that file. If the externalPropertyFileReference object specifies an external property file that contains an object-valued property, itemCount **SHALL** be absent.

NOTE: This information is useful to a SARIF consumer that needs to locate the item at a specified array index in an externalized array-valued property. Without this information, the consumer would have to open in turn each external property file belonging to that property, counting the number of array elements in each, until it reached the file containing the desired element.

EXAMPLE: In EXAMPLE 1 in §3.14.2.2, the array-valued property results is divided into two files, the first containing 10,000 elements and the second containing 4,277 elements. A SARIF consumer that needs to access element 12,000 knows immediately that it is contained in the second file, at index 2,000.

## runAutomationDetails object

### General

A runAutomationDetails object contains information that specifies theRun’s identity and role within an engineering system.

EXAMPLE: In this example, a run contains the results from one nightly execution of a single security tool over a specified set of binaries. theRun.automationId describe the run. Its id and guid properties both identify the run; the former in human-readable form, the latter in a form that might be more useful in an engineering system’s database. Its correlationGuid property specifies the set of runs identified by *all but the last component* of id’s hierarchical string; that is, it identifies the set of runs "Nightly CredScan run for sarif-sdk/master/x86/debug".

The run in this example is part of an aggregate of runs which together comprise the nightly execution of the engineering system’s full suite of security tools. theRun.aggregateIds[0] describes that aggregate. Its id and guid properties both identify the aggregate. Its correlationGuid property specifies the collection of such aggregates identified by *all but the last component* of id’s hierarchical string; this is, it identifies the collection of aggregates "Nightly security tools run for sarif-sdk/master/x86/debug".

{ # A run object (§3.14).

"automationId": { # See §3.14.3.

"description": {

"text": "This is the {0} nightly run of the Credentaial Scanner tool on

all product binaries in the '{1}' branch of the '{2}' repo. The

scanned binaries are architecture '{3}' and build type '{4}'.",

"arguments": [

"October 10, 2018",

"master",

"sarif-sdk",

"x86",

"debug"

]

},

"id": "Nightly CredScan run for sarif-sdk/master/x86/debug/2018-10-05",

"guid": "11111111-...",

"correlationGuid": "22222222-...."

},

"aggregateIds": [ # See §3.14.4.

{

"id":

"Nightly security tools run for sarif-sdk/master/x86/debug/2018-10-05"

"guid": "33333333-...",

"correlationGuid": "44444444-...."

}

]

}

### Constraints

At least one of the id (§3.16.4), guid (§3.16.5), or correlationGuid (§3.16.6) properties **SHALL** be present.

### description property

An runAutomationDetails object **MAY** contain a property named description whose value is a message object (§3.11) that describes the role played within the engineering system by theRun.

### id property

An runAutomationDetails object **MAY** contain a property named id whose value is a hierarchical string (§3.5.5) that uniquely identifies theRun within the engineering system.

A result management system or other components of the engineering system **MAY** use run.automationDetails.id to associate the information in the log with additional information not provided by the analysis tool that produced it.

An engineering system **MAY** define any number of components and interpret them in any way desired.

NOTE: The intent is to use the components of id to group results from similar runs, such as “all nightly Credential Scanner runs.” A SARIF viewer might display a set of runs in a tree view, grouped by the components of id.

EXAMPLE 1: A run whose id is "My Nightly Run/Debug/x64/2018-10-10" belongs to the category "My Nightly Run/Debug/x64". Presumably, this is the run from October 10, 2018.

The trailing component of id **MAY** be empty; note that the grammar for a hierarchical identifier (§3.5.5.1) permits any component to be empty. This **SHALL** be taken to signify that the run belongs to the specified category, but that the run itself has no unique identifier.

EXAMPLE 2: A run whose id is "My Nightly Run/Debug/x64/" belongs to the category "My Nightly Run/Debug/x64" but is not distinguished from other runs in that category.

id **MAY** consist of a single component. This **SHALL** be taken to specify a unique identifier for the run, withough specifying any category that the run belongs to.

EXAMPLE 3: A run whose id is "My Nightly Run Debug x64 2018-10-10" has a unique identifier but cannot be inferred to belong to any category.

### guid property

An runAutomationDetails object **MAY** contain a property named guid whose value is a GUID-valued string (§3.5.4) that provides a unique, stable identifier for theRun.

A result management system or other components of the engineering system **MAY** use run.automationDetails.guid to associate the information in the log with additional information not provided by the analysis tool that produced it.

### correlationGuid property

An runAutomationDetails object **MAY** contain a property named correlationGuid whose value is a GUID-valued string (§3.5.4) which is shared by all such runs of the same type, and differs between any two runs of different types.

If id (§3.16.4) is present, correlationGuid **SHALL** identify the category of runs specified by all but the last hierarchical component of id.

NOTE: Consider an engineering system that allows engineers to define “build definitions”, and that assigns a GUID to each build definition. In such a system, the build definition’s GUID could serve as run.automationDetails.correlationGuid. It would be the same for all runs that produced by the same build definition, and different between any two runs produced by different build definitions.

## tool object

### General

A tool object describes the analysis tool or converter that was run. The tool object in run.tool (§3.14.6) describes an analysis tool; the tool object in run.conversion.tool (§3.21.2) describes a converter.

A tool consists of one or more “tool components,” each of which consists of one or more files. We refer to the component that contains the tool’s primary executable file as the “driver.” It controls the tool’s execution and typically defines a set of analysis rules. We refer to all other tool components as “extensions.” Extensions can include:

* Libraries of additional rules, which we refer to as “plugins.”
* Files that affect the behavior of the tool, which we refer to as “configuration files.”

Each tool component is represented by a toolComponent object (§3.18).

If another tool post-processes the log file (for example, by removing certain results, or by adding information that was not known to the analysis tool), the post-processing tool **SHOULD NOT** alter any part of the tool object.

EXAMPLE:

{ # A tool object.

"driver": { # See §3.17.2.

"name": "CodeScanner",

"fullName": "CodeScanner 1.1, Developer Preview (en-US)",

"semanticVersion": "1.1.2-beta.12",

"version": "1.1.2b12",

...

},

"extensions": [ # See §3.17.3.

{

"name": "CodeScanner Security Rules",

"version": "3.1",

...

}

]

}

### driver property

A tool object **SHALL** contain a property named driver whose value is a toolComponent object (§3.18) that describes the component containing the tool’s primary executable file.

### extensions property

If the tool used any extensions during the run, the tool object **SHOULD** contain a property named extensions whose value is an array of one or more unique (§3.7.3) toolComponent objects (§3.18) that describe those extensions. If the tool did not use any extensions during the run, then extensions **SHALL** either be absent or an empty array.

## toolComponent object

### General

A toolComponent object represents one of the components which comprise an analysis tool or a converter, either its driver or one of its extensions. For more information, see §3.17.1.

SARIF also uses toolComponent objects to represent other components that participate in the analysis, including:

* Taxonomies (§3.18.2)
* Translations (§3.18.3)
* Polices (§3.18.4)

NOTE: SARIF makes this design choice because toolComponent objects contain properties that are useful in all of these other types of components: properties that represent the component’s identity, localizable properties (§3.5.2) that label the component and describe its purpose, and properties that define rules and similar items that participate in the analysis. Not every property is useful in every component type; for example, translationMetadata (§3.18.25) is useful only in toolComponent objects that represent translations.

### Taxonomies

A taxonomy is a classification of results into a set of categories. Some taxonomies are defined publicly, without reference to any particular tool; we refer to these as “standard taxonomies.” An example is the Common Weakness Enumeration [[CWE](#CWE)]. A tool can also define its own classification (in addition to the classification implied by its rule definitions); we refer to this as a “custom taxonomy.” We refer to a category within a taxonomy as a “taxon” (*pl.* “taxa”).

A taxonomy is represented by a toolComponent object. Its taxa are stored in the taxa property (§3.18.23).

A taxon is represented by a reportingDescriptor object (§3.44); hence toolComponent.taxa is an array of reportingDescriptor objects. This is the same object that represents rules and notifications, so a taxon can specify identify properties such as id (§3.44.3) and guid (§3.44.5), localizable (§3.5.2) descriptive properties such as name (§3.44.7) and fullDescription (§3.44.10), and configuration properties in defaultConfiguration (§3.44.14).

A reportingDescriptor object in toolComponent.taxa **SHALL** not itself contain taxa (§3.44.15) or optionalTaxa (§3.44.16) properties. These properties apply only to reportingDescriptor objects that describe rules.

Standard taxonomies **SHALL** be stored in the run.taxonomies array (§3.14.8). Every toolComponent object in this array **SHALL** contain a taxa property (§3.18.23), and **SHALL NOT** contain rules (§3.18.21) or notifications (§3.18.22) properties.

A custom taxonomy is represented by providing a toolComponent object in tool.driver (§3.17.2) or tool.extensions (§3.17.3) with a taxa property. Such a toolComponent object **MAY** still contain rules and/or notifications as usual.

EXAMPLE: In this example, the tool driver supports the CWE taxonomy, and also supports a custom taxonomy that it defines. The driver’s rule "CA2101" falls into the "MemoryManagement" taxon of its custom taxonomy, so any result that violates that rule will also fall into that taxon.

{ # A run object (§3.14).

"tool": { # See §3.14.6.

"driver": { # See §3.17.2.

"name": "CodeScanner",

"semanticVersion": "3.3", # See §3.18.8.

"guid": "11111111-1111-1111-1111-111111111111",

...

"rules": [

{

"id": "CA2101",

"shortDescription": {

"text": "Failed to release dynamic memory."

},

"taxa": [

{

"id": "MemoryManagement",

"guid": "66666666-6666-6666-6666-666666666666",

"toolComponent": {

"name": "CodeScanner",

"guid": "11111111-1111-1111-1111-111111111111"

}

}

]

},

...

],

"taxa": [

{

"id": "MemoryManagement",

"guid": "66666666-6666-6666-6666-666666666666",

"shortDescription": {

"text": "Improper usage of dynamic memory."

}

},

{

"id": "Cryptography",

"guid": "77777777-7777-7777-7777-777777777777",

"shortDescription": {

"text": "Insecure use of cryptography."

}

}

],

"supportedTaxonomies": [

{

"name": "CodeScanner",

"guid": "11111111-1111-1111-1111-111111111111"

},

{

"name": "CWE",

"index": 1,

"guid": "33333333-0000-0000-0000-000000000000"

}

]

}

},

"taxonomies": [

{

"name": "CWE",

"version": "3.2",

"releaseDateUtc": "2019-01-03",

"guid": "33333333-0000-0000-0000-000000000000",

"informationUri": "https://cwe.mitre.org/data/published/cwe\_v3.2.pdf/",

"downloadUri": "https://cwe.mitre.org/data/xml/cwec\_v3.2.xml.zip",

"organization": "MITRE",

"shortDescription": {

"text": "The MITRE Common Weakness Enumeration"

},

"contents": [

"localizedData",

"nonLocalizedData"

],

"isComprehensive": true,

"minimumRequiredLocalizedDataSemanticVersion": "3.2",

"taxa": [

{

"id": "327",

"guid": "33333333-0000-0000-0000-111111111111",

"name": "BrokenOrRiskyCryptographicAlgorithm",

"shortDescription": {

"text": "Use of a Broken or Risky Cryptographic Algorithm."

},

"defaultConfiguration": {

"level": "warning"

}

},

{

"id": "924",

"guid": "33333333-0000-0000-0000-222222222222",

"name": "TransmittedMessageIntegrity",

"shortDescription": {

"text": "Improper Enforcement of Message Integrity ..."

},

"defaultConfiguration": {

"level": "warning"

}

},

...

]

}

],

"results": [

{

}

]

}

### Translations

A translation is the rendering of a toolComponent object’s localizable strings (§3.5.2) into another language.

A translation is itself represented by a toolComponent object whose localizable properties are the translated versions of the corresponding properties in the component being translated.

Translations **SHALL** be stored in the run.translations array (§3.14.9).

A translation **SHALL** specify the component that it translates by way of its associatedComponent property (§0). associatedComponent **SHALL NOT** refer to another translation.

A translation component **SHALL** contain the translations over every localizable string in the translated component, even if the translated string is identical to the original string.

To some degree, translations and the components they translate can version independently. The versioning relationship between a translation and the translated component is explained in the sections describing localizedDataSemanticVersion (§3.18.29), populated by translations, and requiredMinimumLocalizedDataSemanticVersion (§3.18.30), populated by translated components.

A translation **SHOULD** populate its contents property (§3.18.27) with the value [ "localizedData" ].

To facilitate the identification of translations that are associated with a given component, a toolComponent **SHOULD** populate its guid property (§3.18.5), and a translation for that component **SHOULD** set its guid property to the same value.

In many cases, a new version of a toolComponent defines new localizable strings or requires changes to existing ones (for example, when the tool defines new analysis rules). But in some cases, a new version of a toolComponent can use existing translations (for example, in the case of a bug fix release). To ensure that new translations are created only when necessary, a translation component **SHOULD** populate localizedDataSemanticVersion (§3.18.29), and a translatable component **SHOULD** populate minimumRequiredLocalizedDataSemanticVersion (§3.18.30). See the descriptions of those two properties for an explanation of the interaction between them.

EXAMPLE: In this example, a French translation is available. It translates localizable component-level properties such as toolComponent.name (§3.18.6), as well as rule-level properties such as reportingDescriptor.shortDescription (§3.44.9). The translation can be used because its localizedDataSemanticVersion property (§3.18.29) is compatible with the translated component’s minimumRequiredLocalizedDataSemantic version property (§3.18.30).

{ # A run object (§3.14).

"tool": { # See §3.14.6.

"driver": { # See §3.17.2.

"name": "CodeScanner",

"semanticVersion": "3.3", # See §3.18.8.

"minimumRequiredLocalizedDataSemanticVersion": "3.1",

...

"rules": [

{

"id": "CA2101",

"shortDescription": {

"text": "Do not do dangerous things."

}

}

]

}

},

"translations": [

{ # A toolComponent object.

"language": "fr-FR",

"semanticVersion": "3.1.3",

"localizedDataSemanticVersion": "3.1.2",

"contents": [

"localizedData"

],

"translationMetadata": {

"name": "French translation for CodeScanner"

},

"name": "<*'CodeScanner' translated into French*>",

...

"rules": [

{

"id": "CA2101",

"shortDescription": {

"text": "<*'Do not do dangerous things.' Translated into French*>"

}

}

]

}

],

...

}

### Policies

A policy is a set of rule configurations that specify how results that violate the rules defined by a particular tool component are to be treated.

A policy is represented by a toolComponent object. A policy **SHALL** specify the tool component to which it applies by way of its associatedComponent property (§0). associatedComponent **SHALL** refer either to theTool.driver (§3.17.2) or to an element of theTool.extensions (§3.17.3).

A policy **SHALL** contain a rules property (§3.18.21), each reportingDescriptor-valued (§3.44) element of which in turn contains a defaultConfiguration property (§3.44.14). Each element of the rules array **SHALL** correspond to a rule defined by the associated component. The rules array **MAY** contain elements describing any or all of the rules defined by the associated component.

Policies **SHALL** be stored in the run.policies array (§3.14.10).

A SARIF consumer **MAY** offer the user the option of treating results according to the associated component’s default rule configuration (possibly modified by command line options stored in theInvocation.ruleConfigurationOverrides (§3.19.5)), or according to the configuration defined by a selected element of run.policies. If the user selects a policy, then for any result that violates a rule covered by that policy, the SARIF consumer **SHALL** treat the result according to the policy, regardless of the associated component’s default configuration, regardless of any configuration overrides, and regardless of whether the result object (§3.25) itself specifies a configuration property such as level (§3.25.10).

NOTE: The rationale is that when a user asks to see how a policy views a set of results, they want to see exactly what the policy has to say, regardless of any configuration options that might have been selected when the log was created.

EXAMPLE: In this example, the tool driver defines rule "CA2101" to be a warning. However, the corporate security policy specifies that a violation of this rule is an error. The presence of run.policies allows a SARIF viewer to display the results according to the tool’s view or the policy’s view.

{ # A run object.

"tool": { # See §3.14.6.

"driver": { # See §3.17.2.

"name": "CodeScanner",

"rules": [ # See §3.18.21.

{ # A reportingDescriptor object (§3.44).

"id": "CA2101",

"defaultConfiguration" { # See §3.44.14.

"level": "warning"

}

}

]

}

},

"policies": [

{ # A toolComponent object (§3.18).

"name": "Example Corp. Security Policy",

"semanticVersion": "7.0",

"rules": [

{

"id": "CA2101",

"defaultConfiguration" {

"level": "error"

}

}

]

}

]

}

### guid property

A toolComponent object **MAY** contain a property named guid whose value is a GUID-valued string (§3.5.4) that uniquely identifies the component.

### name property

A toolComponent object **SHALL** contain a property named name whose value is a localizable string (§3.5.2) containing the name of the tool component.

EXAMPLE 1: "CodeScanner"

EXAMPLE 2: "CodeScanner Security Rules Plugin"

EXAMPLE 3: "CodeScanner configuration file"

### fullName property

A toolComponent object **MAY** contain a property named fullName whose value is a localizable string (§3.5.2) containing the name of the tool component along with its version and any other useful identifying information, such as its locale.

EXAMPLE: "CodeScanner 1.1, Developer Preview (en-US)"

### semanticVersion property

A toolComponent object **MAY** contain a property named semanticVersion whose value is a string containing the tool component’s version in a format that conforms to the syntax and semantics specified by [[SEMVER](#SEMVER)].

EXAMPLE: "semanticVersion": "1.1.2-beta.12"

NOTE 1: Semantic versions are sortable in chronological order of release. The presence of the semanticVersion property allows results management systems to (for example) restrict the results they display to versions newer than a specified version, or to restrict the results to a particular major version.

Unless the author of the converter knows that the version number of the tool from which it converts is intended to be interpreted according to SemVer [[SEMVER](#SEMVER)], the converter **SHALL NOT** emit the semanticVersion property in run.tool (§3.14.6), although of course it may emit its own semanticVersion property (the one in run.conversion.tool (§3.21.2)).

### version property

A toolComponent object **MAY** contain a property named version whose value is a string containing the tool component’s version in whatever format the component natively provides.

NOTE: Plugins are typically executable files whose version can be determined; configuration files are typically text files with no embedded version information.

### dottedQuadFileVersion property

If the operating system on which the tool runs provides a value for the file version of the tool component's primary executable file, and if that value logically consists of an ordered set of four non-negative integers, then the toolComponent object **MAY** contain a property named dottedQuadFileVersion whose value is a string representation of that file version in this syntax:

dottedQuadFileVersion = non negative integer, 3\*(".", non negative integer);

where the non negative integers follow the logical order of the components of the file version.

If the operating system does not provide such a value, the dottedQuadFileVersion property **SHALL** be absent.

EXAMPLE: On the Microsoft Windows ® platform, this information is available in the FILEVERSION member of the VERSIONINFO structure.

### releaseDateUtc

A toolComponent object **MAY** contain a property named releaseDateUtc whose value is a string in the format specified in §3.9, specifying the UTC date (and optionally, the time) of the component’s release.

### downloadUri property

A toolComponent object **MAY** contain a property named downloadUri whose value is a localizable string (§3.5.2) containing the absolute URI [[RFC3986](#RFC3986)] from which this version of the tool component can be downloaded.

NOTE: This property is localizable to allow different language versions of a tool to be downloaded from their own URIs.

### informationUri property

A toolComponent object **MAY** contain a property named informationUri whose value is a localizable string (§3.5.2) containing the absolute URI [[RFC3986](#RFC3986)] at which information about this version of the tool component can be found.

NOTE: This property is localizable to allow tool information in different languages to be found at different URIs.

### organization property

A toolComponent object **MAY** contain a property named organization whose value is a localizable string (§3.5.2) containing the name of the company or organization that produced the tool component.

EXAMPLE: "organization": "Example Software Corp."

### product property

A toolComponent object **MAY** contain a property named product whose value is a localizable string (§3.5.2) containing the name of the product to which the tool component belongs.

EXAMPLE: "product": "Example Software Corp. Security Scanner"

### productSuite property

A toolComponent object **MAY** contain a property named product whose value is a localizable string (§3.5.2) containing the name of the suite of products to which the tool component belongs.

EXAMPLE: "productSuite": "Example Software Corp. Quality Tools"

### shortDescription property

A toolComponent object **MAY** contain a property named shortDescription whose value is a localizable multiformatMessageString object (§3.12, §3.12.2) containing a brief description of the tool component.

The shortDescription property **SHOULD** be a single sentence that is understandable when visible space is limited to a single line of text.

### fullDescription property

A toolComponent object **MAY** contain a property named fullDescription whose value is a localizable multiformatMessageString object (§3.12, §3.12.2) containing a comprehensive description of the tool component.

The first sentence of fullDescription **SHOULD** provide a concise description of the tool component, suitable for display in cases where available space is limited. Tools that construct fullDescription in this way do not need to provide a value for shortDescription (§3.18.17). Tools that do not construct fullDescription in this way **SHOULD** provide a value for shortDescription, because otherwise, the initial portion of fullDescription that a viewer displays where available space is limited might not be understandable.

### language property

Depending on the circumstances, a toolComponent object either **SHALL** or **MAY** contain a property named language whose value is a string specifying the language of the localizable strings (§3.5.2) contained in the component (except for those in the translationMetadata property (§3.18.25)), in the format specified by [[RFC5646](#RFC5646)].

If this object represents a translation (see §3.14.9), language **SHALL** be present; otherwise it **MAY** be present.

If this property is absent, it **SHALL** default to "en-US".

EXAMPLE 1: The language is region-neutral English:

"language": "en"

EXAMPLE 2: The language is French as spoken in France:

"language": "fr-FR"

### globalMessageStrings property

A toolComponent object **MAY** contain a property named globalMessageStrings whose value is an object (§3.6) each of whose property values is a localizable multiformatMessageString object (§3.12, §3.12.2). The property names correspond to message identifiers (§3.11.7) within message objects (§3.11).

EXAMPLE:

"driver": { # A toolComponent object (§3.18).

"globalMessageStrings": {

"call": { # A multiformatMessageString object (§3.12).

"text": "Function call",

"markdown": "Function \*\*call\*\*"

},

"return": {

"text": "Function return",

"markdown": "Function \*\*return\*\*

}

}

}

NOTE: The message strings in this property are not associated with a single rule (hence the “global” in the property name.

### rules property

A toolComponent object **MAY** contain a property named rules whose value is an array of zero or more unique (§3.7.3) reportingDescriptor objects (§3.44), each of which provides information about an analysis rule supported by the tool component.

Some tools use the same identifier to refer to multiple distinct (although logically related) rules. Therefore the id properties (§3.44.3) of the reportingDescriptor objects do not need to be unique within the array.

EXAMPLE: In this example, two distinct but related rules have the same rule id. They are distinguished by their message strings.

"driver": { # A toolComponent object (§3.18).

"name": "CodeScaner",

"rules": [

{ # A reportingDescriptor object (§3.44).

"id": "CA1711",

"shortDescription": {

"text": "Certain type name suffixes should not be used."

},

"messageStrings": {

"default": {

"text": "Rename type name {0} so that it does not end in '{1}'"

}

}

},

{

"id": "CA1711",

"shortDescription": {

"text": "Certain type name suffixes have preferred alternatives."

},

"messageStrings": {

"default": {

"text": "Either replace the suffix '{0}' in member name '{1}' with

the suggested numeric alternate or provide

a more meaningful suffix"

}

}

}

]

}

### notifications property

A toolComponent object **MAY** contain a property named notifications whose value is an array of zero or more unique (§3.7.3) reportingDescriptor objects (§3.44), each of which provides information about a notification provided by the tool component.

A tool might use the same identifier to refer to multiple distinct (although logically related) notifications. Therefore the id properties (§3.44.3) of the reportingDescriptor objects do not need to be unique within the array.

EXAMPLE: In this example, two distinct but related notifications have the same id. They are distinguished by their descriptions and message strings.

"driver": # A toolComponent object (§3.18).

"notifications": [

{ # A reportingDescriptor object (§3.44).

"id": "ERR0001",

"shortDescription": {

"text": "A plugin could not be loaded because it does not exist."

},

"messageStrings": {

"default": "Cannot load plugin '{0}' because it was not found."

}

},

{

"id": "ERR0001",

"shortDescription": {

"text": "A plugin could not be loaded because it is not signed."

},

"messageStrings": {

"default": "Cannot load plugin '{0}' because it is not signed."

}

}

]

}

### taxa

A toolComponent object **MAY** contain a property named taxa whose value is an array of zero or more unique (§3.7.3) reportingDescriptor objects (§3.44), each of which provides information about a taxon defined by the component.

If the toolComponent describes a standard taxonomy such as the Common Weakness Enumeration [[CWE](#CWE)], it **SHALL NOT** contain rules (§3.18.21) or notifications (§3.18.22).

NOTE: Tool components representing standard taxonomies are stored in run.taxonomies (§3.14.8), but will typically be persisted to external property files (see §3.14.2).

If the toolComponent describes a tool driver or plugin that defines its own custom taxonomy, it **MAY** contain all of rules, notifications, and taxa.

EXAMPLE: In this example, a toolComponent object represents the Common Weakness Enumeration.

{ # A toolComponent object.

"name": "CWE",

"version": "3.2",

"guid": "11111111-1111-1111-1111-111111111111",

"releaseDateUtc": "2019-01-03",

"informationUri": "https://cwe.mitre.org/data/published/cwe\_v3.2.pdf/",

"downloadUri": "https://cwe.mitre.org/data/xml/cwec\_v3.2.xml.zip",

"organization": "MITRE",

"shortDescription": {

"text": "The MITRE Common Weakness Enumeration"

},

"taxa": [

{

"id": "327",

"name": "BrokenOrRiskyCryptographicAlgorithm",

"shortDescription": {

"text": "Use of a broken or risky cryptographic algorithm."

},

"defaultConfiguration": {

"level": "warning"

}

},

...

]

}

### supportedTaxonomies

A toolComponent object **MAY** contain a property named supportedTaxonomies whose value is an array of zero or more unique (§3.7.3) toolComponentReference objects, each of which refers to a taxonomy that the component uses to classify results.

A toolComponent object that contains a supportedTaxonomies property **SHALL** declare which taxa (if any) each of its rules falls into by providing taxa (§3.44.15) and/or optionalTaxa (§**Error! Reference source not found.**) properties as appropriate on each reportingDescriptor object (§3.44) in its rules array (§3.18.21).

NOTE: A SARIF consumer could infer the set of taxonomies that a component supports by examining the set of taxa and optionalTaxa properties of each element of toolComponent.rules. The supportedTaxonomies property is a convenience, intended to enable consumers to see this information at a glance.

If a toolComponent supports a custom taxonomy, it **SHOULD** include a reference to itself in supportedTaxonomies.

EXAMPLE: In this example, a toolComponent claims to support the Common Weakness Enumeration [[CWE](#CWE)], and also supports a custom taxonomy.

{ # A run object (§3.14)

"tool": { # See §3.14.6.

"driver": { # See §3.17.2.

"name": "CodeScanner",

"guid": "22222222-2222-2222-222222222222",

"rules": [ # See §3.18.21.

...

],

"taxa": [ # See §**Error! Reference source not found.**. Here, defines a custom

... # taxonomy.

]

"supportedTaxonomies": [

{ # A toolComponentReference object (§3.48).

"name": "CWE", # Declares support for CWE.

"index": 0,

"guid": "11111111-1111-1111-1111-111111111111"

},

{

"name": "CodeScanner", # Declares support for its custom taxonomy.

"guid": "22222222-2222-2222-222222222222"

}

]

}

},

"taxonomies": [

{ # A toolComponentReference object.

"name": "CWE",

"version": "3.2",

"guid": "11111111-1111-1111-1111-111111111111",

...

"taxa": [

...

]

}

],

...

}

### translationMetadata property

If a toolComponent object represents a translation, it **SHALL** contain a property named translationMetadata whose value is a translationMetadata object (§3.24) that contains descriptive information about the translation itself, as opposed to describing the component whose localizable strings (§3.5.2) it translates. Otherwise, translationMetadata **SHALL** be absent.

### artifactIndices property

Depending on the circumstances, a toolComponent object either **SHOULD** or **SHALL NOT** contain a property named artifactIndices whose value is an array of one or more integers each of which specifies the array index (§3.7.4) within theRun.artifacts (§3.14.15) of an artifact object (§3.23) that describes one of the files comprising this tool component.

If theRun.artifacts is present and contains elements that describe one or more of the files comprising the tool component, then artifactIndices **SHOULD** be present.

NOTE: If artifactIndices is absent, the SARIF consumer will be unable to locate the artifact objects that describes this component’s files.

Otherwise, artifactIndices **SHALL NOT** be present.

### contents property

A toolComponent object **SHOULD** contain a property named contents whose value is an array of zero or more unique (§3.7.3) strings each of which is one of the following values with the specified meanings:

* "localizedData": The component includes localizable strings (§3.5.2) such as rule messages.
* "nonLocalizedData": The component includes non-localizable properties such as rule severity levels.

If contents is absent, it **SHALL** default to [ "localizedData", "nonLocalizedData" ].

NOTE: The purpose of this property is to help components protect themselves from misuse. Within a SARIF file, the component types are all stored in their own properties, so there is no danger of mistaking, for example, a translation (stored in run.translations (§3.14.9)) for a policy (stored in run.policies (§3.14.10)). But components such as translations and policies are typically authored independently from a tool and stored separately from its log files. The author of a translation (which contains only "localizedData") can help prevent its misuse as a policy (which requires "nonLocalizedData") by setting contents to [ "localizedData" ].

### isComprehensive property

A toolComponent object **SHOULD** contain a property named isComprehensive whose value is a Boolean that is true if the component contains complete information for the content types specified by contents (§3.18.27) and false otherwise.

If isComprehensive is absent it **SHALL** default to false.

NOTE: This property is useful because tools are permitted to emit rules (§3.18.21), notifications (§3.18.22), or taxa (§3.18.23) properties that contain only those items relevant to the current log file. For example, a tool might define hundreds of rules, but if a scan detects violations of only two of them, then the rules property (if it is present at all, which it need not be) need only contain metadata for those two rules.

So, for example, the author of a translation (§3.18.3) would want to work from a log file whose contents array includes "localizedData" and whose isComprehensive property is set to true. Similarly, the author of a policy (§3.18.4) would want to work from a log file whose contents array contains "nonLocalizedData" and whose isComprehensive property is set to true.

### localizedDataSemanticVersion property

If a toolComponent object represents a translation (§3.18.3), it **SHOULD** contain a property named localizedDataSemanticVersion whose value is a string that specifies the semantic version [[SEMVER](#SEMVER)] of the translated strings. Otherwise, localizedDataSemanticVersion **MAY** be present, in which case it represents the semantic version of the localizable strings (§3.5.2) that are present in this component.

If localizedDataSemanticVersion is absent, it **SHALL** default to thisObject.semanticVersion (§3.18.8).

NOTE 1: See the description of minimumRequiredLocalizedDataSemanticVersion (§3.18.30) for an explanation of how these two properties interact.

NOTE 2: In a translation, localizedDataSemanticVersion will usually be the same as semanticVersion. They will differ only if it is necessary to revise the translation component to correct an error unrelated to the translated strings, for example, an error in its translationMetadata (§3.18.25). In that case, semanticVersion would be incremented but localizedDataSemanticVersion would not.

### minimumRequiredLocalizedDataSemanticVersion property

If a toolComponent object does not represent a translation (§3.18.3), it **SHOULD** contain a property named minimumRequiredLocalizedDataSemanticVersion whose value is a string that specifies the minumum semantic version [[SEMVER](#SEMVER)] of the translated strings that it requires. Otherwise, minimumRequiredLocalizedDataSemanticVersion **SHALL** be absent.

If minimumRequiredLocalizedDataSemanticVersion is absent, it **SHALL** default to thisObject.semanticVersion (§3.18.8).

When a SARIF consumer is seeking a translation for this object, it **SHALL** only accept one whose localizedDataSemanticVersion (§3.18.29) is greater than (in the SEMVER sense) but has the same major version component as thisObject.minimumRequiredLocalizedDataSemanticVersion.

NOTE: minimumRequiredocalizedDataSemanticVersion can differ from semanticVersion for two reasons. First, successive versions of a translated component (even versions whose minor version component is incremented) might be able to use the same set of translated strings. Second, the translation itself might be versioned if, for example, the translation author discovers a typo or decides to clarify a message string.

EXAMPLE: In this example, the tool is at version 3.3, but it only requires strings at version 3.1, because tool versions 3.2 and 3.3 didn’t affect any user-facing localizable strings. Therefore the translation at index 0 in theRun.translations (§3.14.9) is acceptable.

{ # A run object (§3.14).

"tool": { # See §3.14.6.

"driver": { # See §3.17.2.

"name": "CodeScanner",

"semanticVersion": "3.3", # See §3.18.8.

"minimumRequiredLocalizedDataSemanticVersion": "3.1",

...

}

},

"translations": [

{ # A toolComponent object.

"language": "fr-FR",

"localizedDataSemanticVersion": "3.1.2",

...

}

],

...

}

### associatedComponent property

If this toolComponent object represents a plugin (see §3.17.1), a translation (§3.18.3), or a policy (§3.18.4), it **SHOULD** contain a property named associatedComponent whose value is a toolComponentReference object (§3.48) which identifies the component to which this plugin, translation, or policy applies.

The associated toolComponent object **MAY** itself contain an associatedComponent property; for example, a translation might be associated with a plugin which in turn is associated with the driver (see §3.17.1).

## invocation object

### General

An invocation object describes the invocation of the analysis tool that was run.

### commandLine property

An invocation object **MAY** contain a property named commandLine whose value is a string containing the completely specified command line used to invoke the tool, starting with the name of the tool's executable or script file, optionally qualified by the relative or absolute path to the file.

NOTE 1: The information in the commandLine property helps to precisely repeat a run of an analysis tool, and to verify that the results reported in the log file were generated by an appropriate invocation of the tool.

The commandLine property is redactable (§3.5.3) because it might contain information which it is not appropriate to disclose, such as passwords, tokens, database connection strings, or in some circumstances even the fully qualified path to the tool's executable or script file.

NOTE 2: Redacting sensitive information from commandLine makes it more difficult to precisely reproduce an analysis run. The value of commandLine would have to be combined with information from another source to allow the run to be repeated.

EXAMPLE 1: Suppose a tool is invoked with the command line

C:\Users\mary\Tools\DbScanner.exe /ConnectionString  
 "Server=Corp;Db=Accounting;User=Admin;Password=S3cr#t"  
 /input \*.sql

Then commandLine might contain the redacted string

[REDACTED]\DbScanner.exe /connectionString=[REDACTED] /input=\*.sql

The commandLine property might describe a command that would be harmful if it were executed. For this reason, a SARIF consumer that receives of a SARIF log file from an untrusted source **SHOULD NOT** execute the command line without first examining it carefully. In particular, an automated SARIF consumer **SHALL NOT** execute a command line in a SARIF log file from an untrusted source.

EXAMPLE 2: An example of a harmful command line:

{ # An invocation object

"commandLine": "rm -rf /"

}

### arguments property

An invocation object **MAY** contain a property named arguments whose value is either null or an array of zero or more strings, containing in order the command line arguments passed to the tool from the operating system.

If arguments is absent, it **SHALL** default to null.

An empty array **SHALL** mean that the tool was invoked with no command line arguments. null **SHALL** mean that the command line arguments, if any, are not known.

EXAMPLE: If the tool is implemented as a C# or Java program, arguments would contain the contents of the args array passed to entry point method.

NOTE: Although the commandLine property (§3.19.2) contains the same information, parsing it is error prone even if one understands the command shell’s quoting and escaping conventions. SARIF consumers might find the pre-parsed arguments property easier to use.

### responseFiles property

An invocation object **MAY** contain a property named responseFiles whose value is either null or an array of zero or more unique (§3.7.3) artifactLocation objects (§3.4), each of which represents a response file specified on the tool's command line.

If responseFiles is absent, it **SHALL** default to null.

An empty array **SHALL** mean that the tool was invoked with no command line arguments that specified response files. null **SHALL** mean that it is not known whether any command line arguments specified a response file.

A SARIF producer **MAY** embed the contents of a response file in the SARIF log file by mentioning the response file in run.artifacts (§3.14.15) and providing a value for artifact.contents (§3.23.8).

EXAMPLE:

{ # An invocation object.

"commandLine": "/quiet @analyzer.rsp @strict.rsp" @options.rsp,

"responseFiles": [

{ # An artifactLocation object (§3.4)..

"uri": "analyzer.rsp",

"uriBaseId": "RESPONSEFILEDIR"

},

{

"uri": "strict.rsp",

"uriBaseId": "RESPONSEFILEDIR"

},

{

"uri": "options.rsp",

"uriBaseId": "RESPONSEFILEDIR"

}

}

...

}

### ruleConfigurationOverrides property

An invocation object **MAY** contain a property named ruleConfigurationOverrides whose value is an array of zero or more unique (§3.7.3) configurationOverride objects (§3.46), each of which overrides the defaultConfiguration property (§3.44.14) of a reportingDescriptor object (§3.43.7) that describes a rule (that is, a reportingDescriptor object that is an array element of the rules property (§3.18.21) of some toolComponent object (§3.18)).

### notificationConfigurationOverrides property

An invocation object **MAY** contain a property named notificationConfigurationOverrides whose value is an array of zero or more unique (§3.7.3) configurationOverride objects (§3.46), each of which overrides the defaultConfiguration property (§3.44.14) of a reportingDescriptor object (§3.43.7) that describes a notification (that is, a reportingDescriptor object that is an array element of the notifications property (§3.18.22) of some toolComponent object (§3.18)).

### startTimeUtc property

An invocation object **MAY** contain a property named startTimeUtc whose value is a string in the format specified in §3.9, specifying the UTC date and time at which the tool’s execution started.

### endTimeUtc property

An invocation object **MAY** contain a property named endTimeUtc whose value is a string in the format specified in §3.9, specifying the UTC date and time at which the tool’s execution ended.

### exitCode property

If the SARIF producer process did not exit due to a signal, an invocation object **SHOULD** contain a property named exitCode whose value is an integer specifying the process exit code.

If the SARIF producer process exited due to a signal, the exitCode property **SHALL** be absent.

For examples, see §3.19.10.

### exitCodeDescription property

If the SARIF producer process did not exit due to a signal, an invocation object **MAY** contain a property named exitCodeDescription whose value is a string describing the reason for the process exit.

EXAMPLE 1:

{ # An invocation object

"exitCode": 0,

"exitCodeDescription": "Normal successful completion"

}

EXAMPLE 2:

{ # An invocation object

"exitCode": 2,

"exitCodeDescription": "File not found"

}

### exitSignalName property

If the SARIF producer process exited due to a signal, an invocation object **SHOULD** contain a property named exitSignalName whose value is a string containing the name of the signal that caused the process to exit.

If the SARIF producer process did not exit due to a signal, the exitSignalName property **SHALL** be absent.

For an example, see §3.19.12.

### exitSignalNumber property

If the SARIF producer process exited due to a signal, an invocation object **MAY** contain a property named exitSignalNumber whose value is an integer specifying the numeric value of the signal that caused the process to exit.

If the SARIF producer process did not exit due to a signal, the exitSignalNumber property **SHALL** be absent.

EXAMPLE:

{ # An invocation object

"exitSignalNumber": 3,

"exitSignalName": "SIGQUIT"

}

### processStartFailureMessage property

If the analysis tool process failed to start, an invocation object **MAY** contain a property named processStartFailureMessage whose value is a string containing the operating system’s message describing the failure.

NOTE: In this case, the SARIF file would not be produced by the analysis tool (since it failed to start), but rather by some other component of the user’s engineering system which is responsible for monitoring the operation of the analysis tool.

If the analysis tool process started successfully (regardless of whether or how it subsequently failed), the processStartFailureMessage property **SHALL** be absent.

EXAMPLE:

{ # An invocation object

"processStartFailureMessage": "WebScan.exe is not recognized as a command."

}

### toolExecutionSuccessful property

An invocation object **SHOULD** contain a property named toolExecutionSuccessful whose value is a Boolean that is true if the engineering system that started the process knows that the analysis tool succeeded, and false if the engineering system knows that the tool failed.

NOTE: This property is needed because not all programs exit with an exit code of 0 on success and non-0 on failure.

If this property is absent, it **SHALL** default to false if the exitCode property (§3.19.9) is present and has a non-zero value; otherwise it **SHALL** default to true.

EXAMPLE:

{

"exitCode": 1,

"exitCodeDescription": "Scan successful; warnings detected.",

"toolExecutionSuccessful": true

}

### machine property

An invocation object **MAY** contain a property named machine whose value is a string containing the name of the machine on which the tool was run.

### account property

An invocation object **MAY** contain a property named account whose value is a string containing the name of the account under which the tool was run.

### processId property

An invocation object **MAY** contain a property named processId whose value is an integer containing the id of the process in which the tool was run.

### executableLocation property

An invocation object **MAY** contain a property named executableLocation whose value is an artifactLocation object (§3.4) specifying the location of the tool's primary executable file.

NOTE 1: This property is defined in the invocation object rather than in the toolComponent object (§3.18) because the identical tool might be invoked from different paths on different machines.

NOTE 2: This property might duplicate information in the commandLine property (§3.19.2). It is necessary because the command line might not explicitly specify the path to the tool (for example, if the tool directory is on the execution path), and this information is important for troubleshooting.

NOTE 3: Absolute path names can reveal information that might be sensitive.

### workingDirectory property

An invocation object **MAY** contain a property named workingDirectory whose value is an artifactLocation object (§3.4) specifying the fully qualified path name of the directory in which the analysis tool was invoked.

NOTE: Absolute path names can reveal information that might be sensitive.

### environmentVariables property

An invocation object **MAY** contain a property named environmentVariables whose value is an object. The property names in this object **SHALL** contain the names of all the environment variables in the tool's execution environment. The value of each property **SHALL** be a string containing the value of the specified environment variable. If the value of the environment variable is an empty string, the corresponding property value **SHALL** be an empty string.

NOTE 1: Environment variable names and values are likely to reveal highly sensitive information. For example, on a machine running Microsoft Windows ®, environment variables reveal the directories on the execution path, user account name, machine name, logon domain controller, *etc.*

NOTE 2: The result of setting an environment variable to an empty string is operating system-dependent. On Microsoft Windows ®, it removes the variable from the environment. In Unix ®, an environment variable can have an empty value.

### toolExecutionNotifications property

An invocation object **MAY** contain a property named toolExecutionNotifications whose value is an array of zero or more notification objects (§3.52). Each element of the array represents a runtime condition detected by the invoked process, either by the tool’s driver or by one of its extensions. The presence within this array of any notification object whose level property (§3.52.6) is "error" **SHALL** mean that the run failed.

The information in toolExecutionNotifications is primarily intended for the developers of the analysis tool, to aid them in diagnosing bugs in the tool. This contrasts with the information in results, which is intended for the developers of the code being analyzed. However, viewers **MAY** still present tool notifications to users, so users are aware of any tool problems. At a minimum, viewers **SHOULD** make users aware of tool notifications whose level property is "error".

NOTE: Depending on the nature of the error, a tool that encounters a runtime error might or might not be able to continue running.  
  
If the error occurs in the course of evaluating a rule, the tool might report the error in toolExecutionNotifications, disable the rule, and continue to execute the remaining rules.  
  
If the error occurs outside of the evaluation of a rule, the tool might report the error in toolExecutionNotifications and then halt. If the tool exits abnormally, it might not have the opportunity to report the error. But if the tool is running under the control of an orchestration process that can detect the error, that process might add a notification for the error to the log file, or even synthesize a log file to hold the error, if the tool did not have the opportunity to create one.

### toolConfigurationNotifications property

An invocation object **MAY** contain a property named toolConfigurationNotifications whose value is an array of zero or more notification objects (§3.52). Each element of the array represents a condition relevant to the configuration of the tool's driver or one of its extensions. The presence within this array of any notification object whose level property (§3.52.6) is "error" **SHALL** mean that the run failed.

The information in toolConfigurationNotifications is primarily intended for the engineers who configure the analysis tool, to aid them in diagnosing errors in the configuration. This contrasts with the information in results, which is intended for the developers of the code being analyzed. However, viewers **MAY** still present configuration notifications to users, so users are aware of any configuration problems. At a minimum, viewers **SHOULD** make users aware of configuration notifications whose level property is "error".

NOTE: Many tools can be parameterized with information about which rules to run, and how those rules should be configured. In some cases, if the configuration information is invalid, the tool can ignore the invalid information and continue to run.

EXAMPLE 1: A tool is invoked with a configuration file which specifies that the tool should disable rule ABC0001, but there is no rule whose id is ABC0001. The tool reports the problem in toolConfigurationNotifications. The tool might continue to run, reporting results for the rules that are correctly configured.

"toolConfigurationNotifications": [

{ # A notification object (§3.52).

"descriptor": {

"id": "UnknownRule"

},

"associatedRule": {

"ruleId": "ABC0001"

},

"level": "warning",

"message": {

"text": "Could not disable rule \"ABC0001\"

because there is no rule with that id."

}

]

EXAMPLE 2: A tool is invoked with an unknown command-line argument. The tool reports the problem in toolConfigurationNotifications. The tool might report the problem as a warning and continue to run, or it might report the problem as an error and terminate.

"toolConfigurationNotifications": [

{ # A notification object (§3.52).

"descriptor": {

"id": "UnknownCommandLineArgument"

},

"level": "error",

"message": {

"text": "Command line argument \"/X\" is unknown."

}

}

]

EXAMPLE 3: A tool is invoked with a command-line argument that specifies the name of a directory containing files to analyze, but the user who invoked the tool does not have read access to that directory. The tool reports the problem as an error in toolConfigurationNotifications and then terminates.

"toolConfigurationNotifications": [

{ # A notification object (§3.52).

"descriptor": {

"id": "CannotFindRulePlugin"

},

"level": "error",

"message": {

"text": "Cannot find rule plugin \"C:\\AnalysisTool\\CustomChecks.dll."

}

}

]

### stdin, stdout, stderr, and stdoutStderr properties

An invocation object **MAY** contain any or all of the properties stdin, stdout, stderr, and stdoutStderr, whose values are artifactLocation objects (§3.4) referring to files that contain the input to and output from the SARIF producer process. stdin, stdout, and stderr refer, respectively, to files containing the contents of the standard input, standard output, and standard error streams. stdoutStderr refers to a file containing the interleaved contents of the standard output and standard error streams. This is useful when the output of those two streams was written to the same file by means of command shell redirection syntax such as "> output.txt 2>&1".

A SARIF producer **MAY** embed the stream contents in the log file by mentioning the corresponding file in run.artifacts (§3.14.15) and providing a value for artifact.contents (§3.23.8).

## attachment object

### General

An attachment object describes an artifact relevant to the detection of a result (see §3.25.24).

A SARIF producer **MAY** embed the contents of an attachment in the log file by mentioning the attachment in run.artifacts (§3.14.15) and providing a value for artifact.contents (§3.23.8).

EXAMPLE: In this example, image001.png is a screen shot of the program being analyzed at the point where the result was detected. Note that this example is more appropriate to a dynamic analysis tool than to a static analysis tool.

{ # A result object (§3.25).

...

"attachments": [ # See §3.25.24.

{ # An attachment object.

"description": { # See §3.20.2.

"text": "Screen shot"

},

"artifactLocation": { # See §3.20.3.

"uri": "file:///C:/ScanOutput/image001.png"

}

}

]

}

### description property

An attachment object **SHOULD** contain a property named description whose value is a message object (§3.11) describing the role played by the attachment.

### artifactLocation property

An attachment object **SHALL** contain a property named artifactLocation whose value is an artifactLocation object (§3.3) that specifies the location of the attachment.

### regions property

An attachment object **MAY** contain a property named regions whose value is an array of zero or more unique (§3.7.3) region objects (§3.28), each of which **SHALL** specify a region of interest within the attachment, and **SHOULD** contain a message property (§3.28.14) so a user can understand its relevance.

### rectangles property

An attachment object **MAY** contain a property named rectangles whose value is an array of zero or more unique (§3.7.3) rectangle objects (§3.29). If the attachment is an image (for example .png or .svg), each rectangle object **SHALL** specify an area of interest within the image, and **SHOULD** contain a message property (§3.29.3) so a user can understand its relevance.

If the attachment is not an image, and rectangles is present, its value **SHALL** be an empty array.

## conversion object

### General

A conversion object describes how a converter transformed the output of an analysis tool from the analysis tool’s native output format into the SARIF format.

EXAMPLE: In this example, a converter has converted an AndroidStudio output file into a SARIF log file:

{

...

"runs": [

{

"tool": {

"driver": {

"name": "AndroidStudio"

}

},

"conversion": {

"tool": { # see §3.21.2

"driver": {

"name": "SARIF SDK Multitool"

}

},

# see §3.21.3

"invocation":

"Sarif.Multitool.exe convert -t AndroidStudio northwind.log"

"analysisToolLogFileLocation": { # see §3.21.4

"uri": "northwind.log",

"uriBaseId": "$LOG\_DIR$"

}

},

"results": [

...

]

}

]

}

### tool property

A conversion object **SHALL** contain a property named tool whose value is a tool object (§3.17) that describes the converter.

### invocation property

A conversion object **MAY** contain a property named invocation whose value is an invocation object (§3.19) that describes the invocation of the converter.

### analysisToolLogFiles property

Some analysis tools produce one or more output files that describe the analysis run as a whole; we refer to these as “per-run” files. Some tools produce one or more output files for each result; we refer to these as “per-result” files. Some tools produce both per-run and per-result files.

A conversion object **MAY** contain a property named analysisToolLogFiles whose value is an array of zero or more unique (§3.7.3) artifactLocation objects (§3.3) that specify the locations of the per-run files.

If the analysis tool did not produce any per-run files, and analysisToolLogFiles is present, its value **SHALL** be an empty array.

Per-result files are handled by the resultProvenance.conversionSources property (§3.43.7).

## versionControlDetails object

### General

A versionControlDetails object specifies the information necessary to retrieve from a version control system (VCS) the correct revision of the files that were scanned during the run.

For an example, see §3.14.13.

### Constraints

A versionControlDetails object **SHALL** contain sufficient information to uniquely and permanently identify the revision of the files that were scanned.

NOTE: The required set of properties depends on the VCS and on the engineering system within which it is used. Consider Git as an example. The revisionId property (containing a commit id) would suffice. The branch property (§3.22.5) might not suffice because a Git branch is a pointer to the latest commit along a line of development; however, branch together with asOfTimeUtc (§3.22.7) might suffice (although that is not an idiomatic use of Git). Similarly, revisionTag (§3.22.6) might not suffice because a Git tag can be removed, but if the engineering system guaranteed that certain tags (such as those specifying public releases) were stable, then revisionTag might suffice.

### repositoryUri property

A versionControlDetails object **SHALL** contain a property named repositoryUri whose value is a string containing an absolute URI [[RFC3986](#RFC3986)] that specifies the location of the repository containing the scanned files.

### revisionId property

A versionControlDetails object **SHOULD** contain a property named revisionId whose value is a string that uniquely and permanently identifies the appropriate revision of the scanned files.

### branch property

A versionControlDetails object **MAY** contain a property named branch whose value is a string containing the name of a branch containing the correct revision of the scanned files.

### revisionTag property

A versionControlDetails object **MAY** contain a property named revisionTag whose value is a string containing a tag that has been applied to the revision in the VCS.

NOTE 1: This specification refers to an identifier for a revision in a VCS as a “tag”. Different VCSs use different terms; for example, Visual Studio Team Services Version Control calls it a “label”.

NOTE 2: Although VCSs generally allow a revision to have more than one tag, the revisionTag property is not an array. The purpose of revisionTag is to aid in identifying a revision so that a scan can be reproduced, not to exhaustively describe the revision.

### asOfTimeUtc property

A versionControlDetails object **MAY** contain a property named asOfTimeUtc whose value is a string in the format specified in §3.9, specifying a UTC date and time that can be used to synchronize an enlistment to the state of the repository as of that time.

NOTE: In some VCSs, the “synchronize by date” feature requires the time to be expressed in the server’s time zone. In such a case, the SARIF producer would need to know the server’s time zone to correctly populate asOfTimeUtc.

### mappedTo property

A versionControlDetails object **MAY** contain a property named mappedTo whose value is an artifactLocation object (§3.4) that specifies the location in the local file system to which the root of the repository was mapped at the time of the analysis.

This property makes it possible to map any artifactLocation to the repository, if any, to which the file belongs. The mapping algorithm **SHALL** be as follows, or any algorithm with equivalent effect (a clarifying example follows):

1. Resolve the artifactLocation as far as possible using the procedure specified in §3.14.14. Denote the resolved artifactLocation by a.
2. For every versionControlDetails object vcd in theRun.versionControlProvenance (§3.14.13), resolve the artifactLocation object specified by vcd.mappedTo, again using the procedure specified in §3.14.14. Denote each such resolved artifactLocation object by v.
3. Let S be the set of all versionControlDetails objects vcd for which v.uriBaseId equals a.uriBaseId and v.uri is a prefix of a.uri.
4. If S is the empty set, then the file specified by artifactLocation does not belong to any repository.
5. Otherwise, the file specified by artifactLocation belongs to the repository specified by the member of S with the longest v.uri.

EXAMPLE: This example illustrates the mapping algorithm. Consider this SARIF file:

{

"originalUriBaseIds": {

"HOME": {

"uri": "file:///home/user"

}

"PACKAGE\_ROOT": {

"uri": "package",

"uriBaseId": "HOME"

},

},

"versionControlProvenance": [

{

"repositoryUri": "https://github.com/example-corp/package",

"revisionId": "b87c4e9"

"mappedTo": {

"uriBaseId": "PACKAGE\_ROOT"

},

},

{

"repositoryUri": "https://github.com/example-corp/plugin1",

"revisionId": "cafdac7"

"mappedTo": {

"uriBaseId": "PACKAGE\_ROOT"

"uri": "plugin1",

},

{

"repositoryUri": "https://github.com/example-corp/plugin2",

"revisionId": "d0dc2c0"

"mappedTo": {

"uriBaseId": "PACKAGE\_ROOT"

"uri": "plugin2",

}

],

"results": [

{

"ruleId": "CA1000",

"locations": [

{

"physicalLocation": {

"artifactLocation": {

"uri": "plugin1/x.c",

"uriBaseId": "PACKAGE\_ROOT"

}

}

}

]

}

]

}

The object is to determine to which repository, if any, the file plugin1/x.c specified by the result location belongs. The algorithm proceeds as follows, using a simplified notation (*uriBaseId*, *uri*) to denote an artifactLocation:

1. Use the information in originalUriBaseIds and the procedure specified in §3.14.14 to calculate the “resolved the artifact location” a:  
     
   (PACKAGE\_ROOT, plugin1/x.c) → (HOME, package/plugin1/x.c) → (null, file:///home/user/package/plugin1/x.c).
2. In the same way, calculate the resolved artifact location v from the mappedTo property of each element vcd of the versionControlProvenance array:
   1. (PACKAGE\_ROOT, null) → (HOME, package) → (null, file:///home/user/package)
   2. (PACKAGE\_ROOT, plugin1) → (HOME, package/plugin1) → (null, file:///home/user/package/plugin1)
   3. (PACKAGE\_ROOT, plugin2) → (HOME, package/plugin2) → (null, file:///home/user/package/plugin2)
3. The set of vcd for which v.uriBaseId equals a.uriBaseId (which is null) and for which v.uri is a *prefix* of a.uri (which is file:///home/user/package/plugin1/x.c) contains the objects at indices 0 and 1. It does not contain the object at index 2 because file:///home/user/package/plugin2 is not a prefix of file:///home/user/package/plugin1/x.c.
4. The set is not empty (it contains indices 0 and 1).
5. The member of the set for with the longest v.uri is the object at index 1, because file:///home/user/package/plugin1 is longer than file:///home/user/package.

Therefore, the specified file belongs to the repository specified by the versionControlDetails object at index 1, namely https://github.com/example-corp/plugin1.

## artifact object

### General

An artifact object represents a single artifact.

### artifactLocation property

Depending on the circumstances, an artifact object either **SHALL**, **MAY**, or **SHALL NOT** contain a property named artifactLocation whose value is an artifactLocation object (§3.3).

If the artifact object represents a top-level artifact, then artifactLocation **SHALL** be present.

If the artifact object represents a nested artifact whose location relative to its parent can be expressed only by means of a path, then artifactLocation **SHALL** be present, and the value of its uri property **SHALL** be a relative reference [[RFC3986](#RFC3986)] expressing that path.

If the artifact object represents a nested artifact whose location within its parent can be expressed only by a byte offset from the start of the parent, and not by means of a path, then the artifactLocation property **SHALL** be absent.

If the artifact object represents a nested artifact whose location within its parent can be expressed either by means of a path or by means of a byte offset from the start of the parent, then either the artifactLocation property or the offset property (§3.23.4) or both **SHALL** be present; they **SHALL NOT** both be absent. If the artifactLocation property is present, the value of its uri property **SHALL** be a relative reference expressing the path of the nested artifact within the parent.

For an example, see §3.23.3.

### parentIndex property

If this artifact object represents a nested artifact, then it **SHALL** contain a property named parentIndex whose value is the array index (§3.7.4) of the parent artifact's artifact object within theRun.artifacts (§3.14.15).

If this artifact object represents a top-level artifact, then parentIndex **SHALL** be absent.

NOTE: parentIndex makes it possible to navigate from the artifact object representing a nested artifact to the artifact objects representing each of its parent artifacts in turn, up to the top-level artifact.

EXAMPLE: This example demonstrates two levels of artifact nesting. The top-level artifact is a ZIP archive represented by the artifact object at index 0 in the artifacts array. The archive contains a word processing document at the specified absolute path from its root; the document is represented by the artifact object at index 1. Finally, the document contains an embedded media object of the specified length at the specified offset from its beginning; the media object is represented by the artifact object at index 2. The media object’s parentIndex property refers to its parent document; the document’s parentIndex property refers to its parent ZIP archive, and the ZIP archive does not have a parentIndex property.

"artifacts": [

{

"artifactLocation": {

"uri": "file:///C:/Code/app.zip"

},

"mimeType": "application/zip",

},

{

"artifactLocation": {

"uri": "/docs/intro.docx",

},

"mimeType":

"application/vnd.openxmlformats-officedocument.wordprocessingml.document",

"parentIndex": 0

},

{

"offset": 17522,

"length": 4050,

"mimeType": "application/x-contoso-animation",

"parentIndex": 1

}

}

### offset property

Depending on the circumstances, an artifact object either **SHALL**, **MAY**, or **SHALL NOT** contain a property named offset whose value is a non-negative integer.

If the artifact object represents a top-level artifact, then the offset property **SHALL** be absent.

If the artifact object represents a nested artifact whose location relative to its parent can be expressed only by means of a byte offset from the start of its parent artifact, then the offset property **SHALL** be present, and its value **SHALL** be that byte offset.

If the artifact object represents a nested artifact whose location within its parent can only be expressed by means of a path, and not by means of a byte offset from the start of the parent, then the offset property **SHALL** be absent.

If the artifact object represents a nested artifact whose location within its parent can be expressed either by means of a path or by means of a byte offset from the start of the parent, then either the artifactLocation property (§3.23.2) or the offset property or both **SHALL** be present; they **SHALL NOT** both be absent. If the offset property is present, its value **SHALL** be that byte offset.

### length property

An artifact object **MAY** contain a property named length whose value is a non-negative integer specifying the length of the artifact in bytes.

### roles property

An artifact object **MAY** contain a property named roles whose value is an array of zero or more unique (§3.7.3) strings, each of which specifies a role that this artifact played in the analysis.

Each array element **SHALL** have one of the following values, with the specified meanings:

* "analysisTarget": The analysis tool was instructed to scan this artifact.
* "attachment": The artifact is an attachment mentioned in result.attachments (§3.25.24).
* "directory": The artifact object represents a directory (a container for other files and directories) rather than a file.

NOTE 1: URIs do not represent “directories” in the file system sense. Even if the URI https://www.example.com/dir/file addresses a resource, the URI https://www.example.com/dir might also address a resource. Nonetheless, if the analysis tool knows that https://www.example.com/dir is not itself a resource, but only a prefix for other URIs that *are* resources, it is appropriate for the tool to mark https://www.example.com/dir with the "directory" role.

* "responseFile": The artifact contains command line arguments to a program, as specified in invocation.responseFiles (§3.19.4).
* "referencedOnCommandLine": The artifact was referenced on the command line.
* "resultFile": A result was detected in this artifact.
* "standardStream": The artifact contains the contents of one of the standard input or output streams, as specified in invocation.stdin, invocation.stdout, invocation.stderr, or invocation.stdoutStderr (§3.19.23).
* "driver": The file belongs to the analysis tool’s driver (§3.17.2).
* "extension": The file belongs to one of the analysis tool’s extensions (§3.17.3).
* "taxonomy": The file belongs to a taxonomy (§3.18.2).
* "translation": The file belongs to a translation (§3.18.3).
* "policy": The file belongs to a policy (§3.18.4).
* "traceFile": The analysis tool traced through this artifact while executing or simulating the execution of the code under test.
* "memoryContents": The artifact contains the contents of a portion of memory.

The following role values denote artifacts that have changed since the baseline run. If theRun.baselineGuid (§3.14.5), its value **SHALL** specify the baseline run. If any of these role values are present but baselineGuid is absent, the engineering system **SHALL** provide out of band information that determines the baseline run.

* "unmodified": The artifact has not been modified since the baseline run.
* "modified": The artifact was modified after the baseline run.
* "added": The artifact was added after the baseline run.
* "deleted": The artifact was deleted after the baseline run.
* "renamed": The artifact was renamed after the baseline run. In this case, the artifact object specifies the new name.
* "uncontrolled": The artifact is not under version control.

NOTE 2: The information conveyed by these values could be extracted from a VCS. These properties exist so SARIF consumers can have this information without needing access to the VCS.

### mimeType property

An artifact object **SHOULD** contain a property named mimeType whose value is a string that specifies the artifact’s MIME type [[RFC2045](#RFC2045)].

### contents property

An artifact object **MAY** contain a property named contents whose value is an artifactContent object (§3.3) representing the entire contents of the artifact.

### encoding property

If an artifact object represents a text artifact, it **MAY** contain a property named encoding whose value is a string that specifies the artifact’s text encoding. The string **SHALL** be one of the character set names specified in [[IANA-ENC](#IANA_ENC)]. The property value **SHALL** be case-insensitive.

If the artifact object represents a text artifact and this property is absent, it **SHALL** default to the value of theRun.defaultEncoding (§3.14.21), if that property is present; otherwise, the artifact’s encoding **SHALL** be taken to be unknown.

If the artifact object represents a binary artifact, encoding **SHALL** be absent.

EXAMPLE: In this example, the encoding of output.txt is UTF-16BE (obtained from the default), but the encoding of data.txt is UTF-16LE:

{ # A run object (§3.14)

"defaultEncoding": "UTF-16BE", # See §3.14.21.

"artifacts": [ # See §3.14.15.

{

"artifactLocation": {

"uri": "output.txt"

}

# encoding property omitted

},

{

"artifactLocation": {

"uri": "data.txt"

},

"encoding": "UTF-16LE"

}

]

}

### sourceLanguage property

#### General

If an artifact object represents a text artifact that contains source code, it **MAY** contain a property named sourceLanguage whose value is a hierarchical string (§3.5.5) that specifies the programming language in which the source code is written. If the artifact object does not represent a text artifact containing source code, sourceLanguage **SHALL** be absent.

For the remainder of this section, we assume that the artifact object represents a text artifact that contains source code.

NOTE 1: This property is intended to help SARIF viewers to render code snippets (§3.28.13) with appropriate syntax coloring.

If the artifact contains source code in a mix of languages, and if it is possible to identify one of those languages as the “primary” language of the artifact, then sourceLanguage **SHALL** specify that language.

NOTE 2: Typically, this is the language implied by the file name extension.

EXAMPLE: In an HTML file that contains embedded JavaScript, sourceLanguage would be "html".

If it is not possible to identify a primary language, sourceLanguage **MAY** specify any language used in the artifact, or it **MAY** be absent.

NOTE 3: In either case, it is possible to specify a source language for any region by using region.sourceLanguage (see §3.28.15).

If sourceLanguage is absent, it **SHALL** default to the value of theRun.defaultSourceLanguage (§3.14.22). If both artifact.sourceLanguage and theRun.defaultSourceLanguage are absent, the artifact’s source language **SHALL** be taken to be unknown. In that case, a SARIF viewer **MAY** use any method or heuristic to determine the artifact’s source language, for example, by examining its file name extension or MIME type, or by prompting the user.

#### Source language identifier conventions and practices

To maximize interoperability, SARIF producers and consumers **SHOULD** conform to the following conventions and practices with respect to the value of this property:

* Producers:
  + Use only lower-case letters, and numbers (for example, "c" rather than "C").
  + Spell out symbols (for example, "csharp" rather than "c#").
  + To denote a language variant, use the hierarchical string mechanism (for example, "c#/7").
  + Do not abbreviate (for example, "visualbasic"™ rather than "vb").
* Consumers
  + Accept source language identifiers that conform to the above producer conventions.
  + In addition, accept a variety of common industry forms, for example, {"cplusplus", "c++", "cpp"}, or {"javascript", "js"}.
  + Compare source language identifiers case-insensitively.

[Appendix I](#AppendixSourceLanguage), “Sample sourceLanguage values,” provides sample values for common programming languages.

### hashes property

An artifact object **MAY** contain a property named hashes whose value is a non-empty object (§3.6) each of whose property names specifies the name of a hash function, and each of whose property values represents the value produced by that hash function.

EXAMPLE: In this example, each of the hash functions SHA-256 and SHA-512 were used to compute hash values for the file.

{ # A file object.

"hashes": {

"sha-256": "...",

"sha-512": "..."

}

}

To maximize interoperability, the property names **SHOULD** appear in the IANA registry of hash function textual names [[IANA-HASH](#IANA_HASH)]. SARIF consumers that need to verify hash values **SHOULD** be able to compute any hash function whose name appears in the IANA registry.

The object **SHOULD** contain a property named "sha-256". SARIF consumers that need to verify hash values **SHALL** be able to compute a SHA-256 hash.

The object **MAY** contain properties whose names do not appear in the IANA registry, but at the expense of interoperability. A SARIF consumer **MAY** implement any hash function, but it does not have to implement any hash function that does not appear in the IANA registry.

If the hash function is one whose name appears in the IANA registry, the property name **SHALL** equal the name as it appears in the registry (for example, "sha-256" rather than "sha256"); otherwise the property name **MAY** be any suitable name, but it **SHALL NOT** equal any name defined in the IANA registry.

SARIF consumers **SHALL** treat the property name as case insensitive (even when comparing to hash function names in the IANA registry).

Each property value **SHALL** be a string representation of the hash digest of the artifact, computed by the hash function specified by the property name. Numeric hash values **SHALL** be represented in hexadecimal. The hexadecimal string representation **SHALL NOT** include a hexadecimal prefix such as "0x" or a suffix such as "h". A SARIF consumer **SHALL** treat a hexadecimal string value as case insensitive.

NOTE 1: The value is represented as a string because hash values are typically represented in hexadecimal notation, and JSON integer values must be decimal.

NOTE 2: A hash value for an analysis target can be useful when a log file is processed by a result management system. The value can be used as a key when persisting results in a database. This allows a build system to use cached results, rather than repeating the analysis, when a target has not changed. A file hash can also be useful for validating results in a policy compliance system, allowing an auditor to validate that rerunning analysis against a target that hashes to a specific value reproduces the provided results.  
  
The artifact object defines a set of hash values, rather than a single hash value, to allow a log file to be consumed by multiple tool chains that might expect hash values produced by differing hash function. Compliance systems, for example, will favor the use of more secure hash functions (such as SHA-256) that minimize the possibility that two different targets will produce the same hash (at the expense of speed to produce the hash). In situations where compliance and security are not a concern, a system might prefer to use a fast hash function (such as MD5 or SHA-1) even though they have known weaknesses that allow adversaries to more easily generate hash collisions.  
  
To populate the hashes property, an analysis tool needs the ability to produce hashes for its analysis targets. Alternatively, the hashes could be added to the log file as a post-processing step.  
  
To make the best use of such an analysis tool, a user (such as a build engineer) would determine what systems in their build environment will consume the log file. The user would then configure the tool to produce hashes using the hash functions required by those systems. Analysis tools that are configurable to produce hashes with a variety of commonly used hash functions will interoperate most easily with such systems.

### lastModifiedTimeUtc property

An artifact object **MAY** contain a property named lastModifiedTimeUtc whose value is a string in the format specified in §3.9, specifying the UTC date and time at which the artifact was most recently modified.

NOTE: In scenarios where a tool has analyzed files on a network file share or on a local disk, an engineering system might use this property, rather than hashes (§3.23.11), as the most lightweight mechanism to determine whether the analysis needs to be repeated.

## translationMetadata object

### General

A translationMetadata object describes a translation. It is necessary because in a toolComponent object that represents a translation, the usual descriptive properties name (§3.18.6), fullName (§3.18.7), *etc.* contain the translations of the corresponding strings in the toolComponent being translated; therefore they are not available to hold descriptive information for the translation itself.

Because they occur only in toolComponent objects that represent translations, the properties of a translationMetadata object are not themselves localized (§3.5.2).

EXAMPLE:

{ # A toolComponent object (§3.18).

"language": "fr-FR", # The language of the translation (see (§3.18.19).

"translationMetadata": { # A translation metadata object.

"name": "CodeScanner translation for fr-FR ",

"fullName": "CodeScanner translation for fr-FR by Example Corp.",

"shortDescription": {

"text": "A good translation"

},

"fullDescription": {

"text": "A good translation performed by native en-US speakers."

}

},

"name": "(fr-FR translation of translated component’s name)",

"fullName": "(fr-FR translation of translated component’s full name)",

...

}

### name property

A translationMetadata object **SHALL** contain a property named name whose value is a string containing a name for the translation.

### fullName property

A translationMetadata object **MAY** contain a property named fullName whose value is a string containing the name of the translation along with any other useful identifying information.

### shortDescription property

A translationMetadata object **MAY** contain a property named shortDescription whose value is a multiformatMessageString object (§3.12) containing a brief description of the translation.

### fullDescription property

A translationMetadata object **MAY** contain a property named fullDescription whose value is a multiformatMessageString object (§3.12) containing a comprehensive description of the translation.

### downloadUri property

A translationMetadata object **MAY** contain a property named dowloadUri whose value is a string containing the absolute URI [[RFC3986](#RFC3986)] from which this the translation can be downloaded.

### informationUri property

A translationMetadata object **MAY** contain a property named dowloadUri whose value is a string containing the absolute URI [[RFC3986](#RFC3986)] at which information about this the translation can be found.

## result object

### General

A result object describes a single result detected by an analysis tool.

Each result is produced by the evaluation of a rule. If theTool contains a reportingDescriptor object (§3.44) that describes that rule, we refer to that object as theDescriptor, and we refer to the toolComponent object (§3.18) that defines theDescriptor as theComponent.

### Distinguishing logically identical from logically distinct results

Successive runs of the same tool, or even runs of different tools, might detect the same condition in the code. When two result objects represent the same condition, we say that the results are “logically identical;” when they represent different conditions, we say that the results are “logically distinct.” Two results can be logically identical even if the result objects are not identical. For example, if code is inserted into a file between runs, the same condition might be reported on two different lines.

To avoid reporting the same condition repeatedly, result management systems typically group results into equivalence classes such that results in any one class are logically identical and results in different classes are logically distinct.

Some result management systems do this by calculating a “fingerprint” for each result and considering results with the same fingerprint to be logically identical. A fingerprint is calculated from information contained in the result and might contain readable information from the result.

Other result management systems group results into equivalence classes *without* associating a computed fingerprint with each result, and they denote each equivalence class with an arbitrary unique identifier. This identifier is opaque: it is ­*not* calculated from information stored in the result, and hence contains no readable information about the result.

Still other result management systems compute a fingerprint, associate an arbitrary unique identifier with the fingerprint, and use that identifier rather than the fingerprint to identify the equivalence class of results.

SARIF accommodates all these types of result management systems. Result management systems that compute fingerprints **SHOULD** populate the fingerprints property (§3.25.14). Result management systems that group results into equivalence classes based on an arbitrary unique identifier **SHOULD** populate the correlationGuid property (§3.25.4), regardless of whether they also compute a fingerprint.

### guid property

A result object **MAY** contain a property named guid whose value is a GUID-valued string (§3.5.4) defining a unique, stable identifier for the result.

Direct SARIF producers and SARIF converters **SHOULD NOT** set this property. A result management system **SHOULD** set this property when it ingests a SARIF log file. If it does so, then later, when a SARIF consumer retrieves results in SARIF format from the result management system, the result management system **SHALL** set this property to the value it assigned.

A result management system **MAY** store multiple results with identical fingerprints (see §3.25.14 and [Appendix B](#AppendixFingerprints)), but the guid properties for those results **SHALL** be distinct.

### correlationGuid property

A result object **MAY** contain a property named correlationGuid whose value is a GUID-valued string (§3.5.4) that is shared by all results that are considered logically identical, and that is different between any two results that are considered logically distinct.

Direct SARIF producers and SARIF converters **SHOULD NOT** set this property. A result management system **MAY** set this property when it ingests a SARIF log file. If it does so, then later, when a SARIF consumer retrieves results in SARIF format from the result management system, the result management system **MAY** set this property to the value it assigned.

NOTE: correlationGuid and fingerprints (§3.25.14) provide two different ways for result management systems to associate results that are logically identical. See §3.25.2 for more information.

### ruleId property

Depending on the circumstances, a result object either **SHALL**, **MAY**, or **SHALL NOT** contain a property named ruleId whose value is a hierarchical string (§3.5.5) whose first component is the stable, opaque identifier of the rule that was evaluated to produce the result.

NOTE 1: ruleId will usually consist entirely of the rule’s stable opaque identifier. In some cases, it might be helpful to specify additional hierarchical components to more precisely describe the rule violation.

A SARIF viewer or result management system **MAY** use the additional hierarchical components to allow a user to suppress a subset of the violations of a given rule. A result result management system **MAY** also use the additional components to more precisely match results between runs.

EXAMPLE: In this example, the first result describes a violation of rule CA2101. Its ruleId consists entirely of the rule’s identifier. The second and third results both describe violations of rule CA5350. Each of their ruleIds specifies an additional hierarchical component that more precisely describes the rule violation. Note that rule.index (§3.25.7, §3.47.5) for both those results is 1; despite the additional hierarchical components in ruleId, both results describe violations of the same rule.

A SARIF viewer or result management system might allow a user to suppress, for example, only those violations of rule CA5350 which specify sha-1 as the second hierarchical component of ruleId; that is, to allow the use of SHA-1 but still warn about the uses of other weak cryptographic algorithms.

{

"tool": {

"driver": {

"name": "CodeScanner",

"rules": [

{

"id": "CA201",

"shortDescription": {

"text": "Specify marshaling for P/Invoke string arguments"

}

},

{

"id": "CA5350",

"shortDescription": {

"text": "Do not use weak cryptographic algorithms"

}

}

]

}

},

"results": [

{

"ruleId": "CA2101",

"rule": {

"index": 0

}

},

{

"ruleId": "CA5350/md5",

"rule": {

"index": 1

}

},

{

"ruleId": "CA5350/sha-1",

"rule": {

"index": 1

}

}

]

]

Direct producers **SHALL** emit either or both of ruleId and rule.id (§3.25.7, §3.47.4). If rule.id is absent, ruleId **SHALL** be present. If rule.id is present, ruleId **MAY** be present.

For an example of the interaction between ruleId and rule.id, see §3.47.4.

Not all existing analysis tools emit the equivalent of a ruleId in their output. A SARIF converter which converts the output of such an analysis tool to the SARIF format **SHALL NOT** set ruleId, and in particular, it **SHALL NOT** attempt to synthesize it from other information available in the original analysis tool's output.

NOTE 2: If a converter were to synthesize a rule id, then two converters for the same tool might synthesize them differently, leading to loss of interoperability. For example, a SARIF consumer might mistakenly conclude that two issues, found in SARIF log files created by those two converters, were logically distinct because they had different rule ids.

### ruleIndex property

If theDescriptor exists (that is, if theTool contains a reportingDescriptor object (§3.44) that describes the rule that was violated), a result object **MAY** contain a property named ruleIndex whose value is the array index (§3.7.4) of theDescriptor within theComponent.ruleDescriptors (§3.18.21). Otherwise, ruleIndex **SHALL** be absent.

The semantics of ruleIndex are identical to the semantics of reportingDescriptorReference.index (§3.47.5), and are described there.

If ruleIndex and rule.index (§3.25.7, §3.47.5) are both present, they **SHALL** be equal.

### rule property

Depending on the circumstances, a result object either **SHALL NOT**, **SHOULD**, or **MAY** contain a property named rule whose value is a reportingDescriptorReference object (§3.47) that identifies theDescriptor. The procedure for looking up a reportingDescriptor from a reportingDescriptorReference is described in §3.47.3.

If theDescriptor does not exist (that is, if theTool does not contain a reportingDescriptor object (§a3.44) that describes the rule that was violated), then rule **SHALL NOT** be present.

If theDescriptor occurs in theTool.extensions (§3.17.3), then rule **SHOULD** be present.

NOTE 1: If theDescriptor occurs in theTool.extensions and ruleDescriptorReference is absent, the SARIF consumer will not be able to locate the rule metadata, even if ruleIndex (§3.25.6) is present, because ruleIndex alone does not specify which extension contains theDescriptor.

If theDescriptor occurs in theTool.driver (§3.17.2) and ruleIndex is absent, then again ruleDescriptorReference **SHOULD** be present.

NOTE 2: If theDescriptor occurs in theTool.driver and ruleIndex is absent, the SARIF consumer will not be able to locate the rule metadata within theTool.driver.ruleDescriptors.

If theDescriptor occurs in theTool.driver and ruleIndex is present, then ruleDescriptorReference **MAY** be present.

NOTE 3: If theDescriptor occurs in theTool.driver, then ruleIndex suffices to locate the rule metadata within theTool.driver.ruleDescriptors.

If rule.id (§3.47.4) is absent, it **SHALL** default to thisObject.ruleId. If rule.id and thisObject.ruleId are both present, they **SHALL** be equal.

If rule.index (§3.47.5) is absent, it **SHALL** default to thisObject.ruleIndex. If rule.index and thisObject.ruleIndex are both present, they **SHALL** be equal.

If rule is absent, it **SHALL** default to a reportingDescriptorReference object whose id property is set to thisObject.ruleId and whose index property is set to thisObject.ruleIndex.

### taxa

A result object **MAY** contain a property named taxa whose value is an array of zero or more unique (§3.7.3) reportingDescriptorReference objects (§3.47) each of which refers to a taxon into which this result falls.

If the toolComponent object (§3.18) theComponent that defines the rule that was violated contains a reportingDescriptor object (§3.44) theDescriptor (a member of toolComponent.rules (§3.18.21)) that describes that rule, then thisObject.taxa **SHALL** contain elements corresponding to those elements of theDescriptor.optionalTaxa (§**Error! Reference source not found.**) that describe taxa into which this result falls. thisObject.taxa **SHALL NOT** contain elements which correspond to theDescriptor.taxa (§3.44.15); rather, the result **SHALL** implicitly be taken to fall into all the taxa described by theDescriptor.taxa.

Otherwise (that is, if theDescriptor does not exist), thisObject.taxa **SHALL** contain elements that describe all taxa into which the result falls.

In either case, if there is no toolComponent that defines the taxonomy to which an element of thisObject.taxa refers, then that element (a reportingDescriptorReference object) **SHALL** contain only an id property (§3.47.4).

EXAMPLE: In this example, a tool defines a custom taxonomy (see §**Error! Reference source not found.**) consisting of three taxa with ids "REQ", "OPT1", and "OPT2". The tool emits a result that falls into the optional taxon "OPT2". The result implicitly falls into the taxon "REQ". theResult.taxa contains "OPT2" but does not contain "REQ".

{ # A run object (§3.14).  
 "tool": {

"driver": {

"name": "CodeScanner",

...

"rules": [

{

"id": "CA2101",

...

"taxa": [

{

"id": "REQ"

}

],

"optionalTaxa": [

{

"id": "OPT1"

},

{

"id": "OPT2"

}

]

}

],

"taxa": [

{

"id": "REQ",

...

},

{

"id": "OPT1",

...

},

{

"id": "OPT2",

...

}

]

}

},

"results": [

{

"ruleId": "CA2101",

"taxa": [

{

"id": "OPT2",

"index": 1,

}

]

}

]

}

### kind property

A result object **MAY** contain a property named kind whose value is one of a fixed set of strings that specify the nature of the result.

If present, the kind property **SHALL** have one of the following values, with the specified meanings:

* "pass": The rule specified by ruleId (§3.25.3) was evaluated, and no problem was found.
* "open": The rule specified by ruleId was evaluated, and the tool concluded that there was insufficient information to decide whether a problem exists.

NOTE 1: This value is used by proof-based tools.Sometimes such a tool can prove that there is no violation (kind = "pass"), sometimes it can prove that there is a violation (kind = "fail"), and sometimes it does not detect a violation but is unable to prove that there is none (kind = "open"). If kind is "open", the user should add additional assertions to enabe the tool to determine if there is a violation.

* "notApplicable": The rule specified by ruleId was not evaluated, because it does not apply to the analysis target.

EXAMPLE: In this example, a binary checker has a rule that applies to 32-bit binaries only. It produces a "notApplicable" result if it is run on a 64-bit binary:

"results": [

{

"ruleId": "ABC0001",

"kind": "notApplicable",

"message": {

"text": "\"MyTool64.exe\" was not evaluated for rule ABC0001

because it is not a 32-bit binary."

},

"locations": [

{

"physicalLocation": {

"uri": "file://C:/bin/MyTool64.exe"

}

}

]

}

]

* "review": The result requires review by a human user to decide if it represents a problem.

NOTE 2: This value is used by tools that are unable to check for certain conditions, but that wish to bring to the user’s attention the possibility that there might be a problem. For example, an accessibility checker might produce a result with the message "Do not use color alone to highlight important information," with kind = "review". A user might address this issue by visually inspecting the UI.

* "fail": The result represents a problem whose severity is specified by the level property (§3.25.10).

If kind is absent, it **SHALL** default to "fail".

If level has any value other than "none" and kind is present, then kind **SHALL** have the value "fail".

### level property

A result object **MAY** contain a property named level whose value is one of a fixed set of strings that specify the severity level of the result.

If present, the level property **SHALL** have one of the following values, with the specified meanings:

* "warning": The rule specified by ruleId was evaluated, and a problem was found.
* "error": The rule specified by ruleId was evaluated, and a serious problem was found.
* "note": A purely informational log entry.
* "none": The concept of “severity” does not apply to this result because the kind property (§3.25.9) has a value other than "fail".

If the value of level is "note", then if the note relates to a particular rule, ruleId (§3.25.5) **SHOULD** be present; otherwise ruleId **SHALL** be absent.

EXAMPLE 1: In this example, the tool reports an observation about the code that does not represent a problem.

"results": [

{

"ruleId": "ABC0002",

"kind": "fail",

"level": "note",

"message": {

"text": "Consider using 'nameof(start)' instead of hard-coding

the parameter name 'start'."

},

"locations": [

{

"physicalLocation": {

"uri": "file:///C:/code/a.cs",

"region": {

"startLine": 6

}

}

}

]

}

]

EXAMPLE 2: In this example, the tool reports information that is relevant to a particular rule but does not represent an observation about the code. Also in this example, kind is absent, and since level is present, kind defaults to "fail".

"results": [

{

"ruleId": "ABC0003",

"level": "note",

"message": {

"text": "A new version of rule ABC0003 is available."

}

}

]

EXAMPLE 3: In this example, the tool reports information that is not related to any rule and is not an observation about the code.

"results": [

{

"level": "note",

"message": {

"text": "Version 11.0 of SuperLint is now available."

}

}

]

If kind (§3.25.9) has any value other than "fail", then if level is absent, it **SHALL** default to "none", and if it is present, it **SHALL** have the value "none".

If kind has the value "fail" and level is absent, then level **SHALL** be determined by the following procedure:

IF rule (§3.25.7) is present THEN

LET theDescriptor be the reportingDescriptor object (§3.44) that it specifies.

# Is there a configuration override for the level property?

IF result.provenance.invocationIndex (§3.25.27, §3.43.6) is present THEN

LET theInvocation be the invocation object (§3.19) that it specifies.

IF theInvocation.ruleConfigurationOverrides (§3.19.5) is present

AND it contains a reportingDescriptorConfigurationOverride object (§3.46) whose

reportingDescriptorReference property (§3.46.2) specifies theDescriptor THEN

LET theOverride be that reportingDescriptorConfigurationOverride object.

IF theOverride.configuration.level (§3.46.3, §3.45.3) is present THEN

Set level to theConfiguration.level.

ELSE

# There is no configuration override for level. Is there a default configuration for it?

IF theDescriptor.defaultConfiguration.level (§3.44.14, §, §3.45.3) is present THEN

SET level to theDescriptor.defaultConfiguration.level.

IF level has not yet been set THEN

SET level to "warning".

### message property

A result object **SHALL** contain a property named message whose value is a message object (§3.11) that describes the result.

The message property **SHOULD** provide sufficient details to allow an end user to resolve any problem that the result might indicate. In particular, it **SHALL** include all of the following information that is available and relevant to the result:

* Information sufficient to identify the analysis target, and the location within the target where the problem occurred.
* The condition within the analysis target that led to the problem being reported.
* The risks potentially associated with not fixing the problem.
* The full range of responses to the problem that the end user could take (including the definition of conditions where it might be appropriate not to fix the problem, or to conclude that the result is a false positive).

EXAMPLE 1: This is an example of a message:

"results": [

{

"message": {

"text": "Deleting member 'x' of variable 'y' may compromise

performance on subsequent accesses of 'y'. Consider

setting object member 'x' to null instead, unless this

object is a dictionary or if runtime semantics otherwise

dictate that the existence of a null member is distinct

from one that is not present at all. This violation can

also be ignored for infrequently called code paths."

}

}

]

If the message object contains a messageId property (§3.11.10), then if theDescriptor exists and value of messageId equals one of the property names in theDescriptor.messageStrings (§3.44.11), then that string **SHALL** be used; otherwise, the string SHALL be looked up in theComponent.globalMessageStrings (§3.18.20).

NOTE: This interpretation of message.messageId differs from its interpretation elsewhere in this specification. In every other message object in this specification, messageId always refers to a string within theComponent.globalMessageStrings.

EXAMPLE 2: In this example, message.messageId refers to the property named default defined in the messageStrings property of the reportingDescriptor object identified by "CA2101".

{ # A run object (§3.14).

"tool": { # See §3.14.6.

"driver": { # See §3.17.2.

"name": "CodeScanner",

"rules": [ # See §3.18.21.

{ # A ruleDescriptor object (§3.44).

"id": "CA2101",

"messageStrings": {

"default": { # A multiformatMessageString object (§3.12).

"text": "The default message for this rule.",

"markdown": " The default message for \*this\* rule."

},

"special": {

"text": "Another message, for special cases.",

"markdown": "Another message, for \*special\* cases."

}

}

}

]

}

},

"results": [

{ # A result object (§3.25).

"ruleId": "CA2101",

"message": {

"messageId": "default"

},

...

}

]

}

### locations property

A result object **SHOULD** contain a property named locations whose value is an array of zero or more location objects (§3.26), each of which specifies a location where the result occurred.

NOTE 1: In rare circumstances, it might not be possible to specify a location for a result. However, the locations property contains very valuable information for anyone who needs to diagnose and correct the condition described by the result, so the authors of analysis tools should make every effort to provide it.

EXAMPLE 1: If a C++ analyzer detects that no file defines a global function main, then that result cannot be associated with a file.

NOTE 2: The locations array is not defined to contain unique (§3.7.3) elements because some tools report a line number but not a column number for a result’s location. Such a tool might report the same result twice on the same line, in some cases producing multiple identical location objects.

The locations array **SHALL NOT** contain more than one element unless the condition indicated by the result, if any, can only be corrected by making a change at every location specified in the array.

EXAMPLE 2: In C#, which support “partial” classes, portions of the declaration of a single class can occur at multiple locations in the source code. If an analysis tool reports that the name of such a class does not conform to a specified convention, then the resulting log file might contain a single result object, which would contain a locations array each of whose elements specifies a location in the source code where the class name occurs.

The locations array **SHALL NOT** be used to specify distinct occurrences of the same result which can be corrected independently.

EXAMPLE 3: Consider an analysis tool which locates misspelled words in documentation, and suppose this tool scans a document in which the same word is misspelled in two distinct locations. Then the resulting log file must contain two distinct result objects, each of which contains a locations array containing a single location object specifying the location of one instance of the misspelled word.  
  
EXAMPLE 4: In contrast, consider a tool which locates misspelled words in variable names. If the tool detects a misspelled variable name, it must produce a single result object whose locations array contains the location of every reference to the variable, since fixing some but not all of the references would cause a compilation error.

### analysisTarget property

If the analysis target differs from the result file, a result object **SHOULD** contain a property named analysisTarget whose value is an artifactLocation object (§3.4) that specifies the analysis target.

If the analysis target and the result file are the same, the analysisTarget property **SHOULD** be absent.

EXAMPLE: In this example, the tool’s analysis target was the file mouse.c. In the course of the scan, the tool detected a result in the included file mouse.h.

{ # A result object (§3.25).

"analysisTarget": { # An artifactLocation object (§3.4

"uri": "input/mouse.c",

"uriBaseId": "SRCROOT"

},

"locations": [ # See §3.25.12.

{ # A location object (§3.26).

"physicalLocation": { # See §3.26.2.

"artifactLocation": { # An artifactLocation object.

"uri": "input/mouse.h",

"uriBaseId": "SRCROOT"

},

"region": {

"startLine": 42

}

}

}

]

}

### fingerprints property

A result object **MAY** contain a property named fingerprints whose value is an object (§3.6).

Each property value in this object **SHALL** be a string that provides a stable identifier for the result. This identifier **SHALL**, to the extent that it is feasible, be the same for all results that are logically identical, and different for any two results that are logically distinct. This requirement is intended to ensure that a fingerprint is resistant to changes that do not affect the logical identity of the result, such as the location of the root of a source code enlistment, or the line number where a result appears in a source file.

Each property name in this object **SHALL** be a versioned hierarchical string (§3.5.5.2). A result management system **MAY** use the property names to identify the method used to calculate the fingerprint.

EXAMPLE: In this example, the producer has calculated a fingerprint using version 2 of a fingerprinting method it refers to as "contextRegionHash":

{

"fingerprints": {

"contextRegionHash/v2": "097886bc876fe"

}

}

When a result management system uses fingerprint information to determine whether two results are logically identical, it **SHOULD** use the latest version of the fingerprint available in both results.

EXAMPLE 2: In this example, one result has values for versions 1 and 2 of the “context region hash” fingerprint. Another result has values for versions 2 and 3. A result management system would use version 2 (the greatest common version) to compare the two results.

{ # A run object (§3.14).

"results": [ # See §3.14.20.

{ # A result object (§3.25).

"fingerprints": {

"contextRegionHash/v1": "1234567900abc"

"contextRegionHash/v2": "234567900abcd"

},

{

"fingerprints": {

"contextRegionHash/v2": "234567900abcd"

"contextRegionHash/v3": "34567900abcde"

}

]

}

This property is an array, rather than a single string, to allow a result management system to select among a variety of methods for deciding whether two results are logically identical or logically distinct.

A direct SARIF producer **SHOULD NOT** populate this property. A SARIF converter **MAY** populate this property if the analysis tool’s native output format provides a value that qualifies as a fingerprint (a stable identifier for the result). A result management system **MAY** populate this property when it ingests a SARIF file. If it does so, then later, when a SARIF consumer retrieves results in SARIF format from the result management system, the result management system **MAY** set this property to the value it assigned.

[Appendix B](#AppendixFingerprints) provides requirements for how a result management system computes fingerprints.

NOTE: fingerprints and correlationGuid (§3.25.4) provide two different ways for result management systems to associate results that are logically identical. See §3.25.2 for more information.

### partialFingerprints property

A result object **MAY** contain a property named partialFingerprints whose value is an object (§3.6).

Each property value in this object **SHALL** be a string that contributes to the stable, unique identity, or “fingerprint,” of the result (see §3.25.14). [Appendix B](#AppendixFingerprints) explains how a result management system can compute these fingerprints.

Each property name in this object **SHALL** be a versioned hierarchical string (§3.5.5.2). A SARIF producer **MAY** use the property name to identify the nature of the information used to compute the partial fingerprint.

EXAMPLE 1: In this example, the producer has calculated a partial fingerprint using version 3 of a partial fingerprint value it refers to as "prohibitedWordHash":

{ # A result object (§3.25).

"partialFingerprints": {

"prohibitedWordHash/v3": "097886bc876fe"

}

}

When a result management system uses partial fingerprint information to determine whether two results are logically identical, it **SHOULD** use the latest version of the partial fingerprint available in both results.

EXAMPLE 2: In this example, one result has values for versions 1 and 2 of the “prohibited word hash” partial fingerprint. Another result has values for versions 2 and 3. A result management system would use version 2 (the greatest common version) to compare the two results.

{ # A run object (§3.14).

"results": [ # See §3.14.20.

{ # A result object (§3.25).

"partialFingerprints": {

"prohibitedWordHash/v1": "1234567900abc"

"prohibitedWordHash/v2": "234567900abcd"

},

{

"partialFingerprints": {

"prohibitedWordHash/v2": "234567900abcd"

"prohibitedWordHash/v3": "34567900abcde"

}

]

}

To make use of the information, if any, embodied in the property names, a result management system requires knowledge of the naming convention used by the SARIF producer. A result management system with that knowledge **MAY** use the property names to decide which partial fingerprints to include in its fingerprint computation. A result management system lacking that knowledge **SHALL** include all the partial fingerprints in its fingerprint computation.

Because result management systems might come to depend on the choice of property names, SARIF producers that use property names to identify the nature of the information used to compute the partial fingerprint **SHOULD** adhere to the following guidelines:

* Choose meaningful property names that describe the information used to compute the partial fingerprint.
* Document the property names.
* When introducing a partial fingerprint computed with a different approach, associate it with a new property name.
* Avoid removing existing property names and partial fingerprints, since existing result management systems might rely on them.

EXAMPLE 3: In this example, a SARIF-producing document checker has computed two partial fingerprints, one being a hash of a word that should not appear in a document, and the other being a hash of the document’s language.

{ # A result object

...

"partialFingerprints": {

"wordHash":

"2c26b46b68ffc68ff99b453c1d30413413422d706483bfa0f98a5e886266e7ae",

"langHash":

"5c49f88dafe66e0ecdca8f682ae0b38c38ccd3ad464e3358e899beca88c18560"

}

}

EXAMPLE 4. In this example, the SARIF producer has computed a single partial fingerprint. It has chosen an arbitrary value for the corresponding property name.

{ # A result object

...

"partialFingerprints": {

"1": "56eaf900cc8f6"

}

}

### codeFlows property

A result object **MAY** contain a property named codeFlows whose value is an array of zero or more codeFlow objects (§3.33). The codeFlows property is intended for use by analysis tools that provide execution path details that illustrate a possible problem in the code.

NOTE: The SARIF file format allows multiple codeFlow objects within a single result object to allow for the possibility that more than code flow might be relevant to a single result.

### graphs property

A result object **MAY** contain a property named graphs whose value is an array of zero or more unique (§3.7.3) graph objects (§3.35). A graph object represents a directed graph: a network of nodes and directed edges that describes some aspect of the structure of the code (for example, a call graph).

A graph object defined at the result level **SHALL** be referenced only by graphTraversal objects (§3.38) defined in the graphTraversals property (§3.25.18) of the result object in which it is defined. This contrasts with graph objects defined at the run level (§3.14.19), which **MAY** be referenced by graphTraversal objects defined in the graphTraversals property of any result object in theRun.

### graphTraversals property

If a result object contains a graphs property (§3.25.17), or if theRun contains a graphs property (§3.14.19), then the result object **MAY** contain a property named graphTraversals whose value is an array of one or more unique (§3.7.3) graphTraversal objects (§3.38). If neither the result object nor theRun contains a graphs property, the graphTraversals property **SHALL** be absent. A graph traversal is a path through the code that visits one or more nodes in a specified graph.

### stacks property

A result object **MAY** contain a property named stacks whose value is an array of stacks or more stack objects (§3.40). The stacks property is intended for use by analysis tools that collects call stack information in the process of producing results.

NOTE: The SARIF file format allows multiple stack objects within a single result object to allow for the possibility that more than one call stack might be relevant to a single result.

### relatedLocations property

A result object **MAY** contain a property named relatedLocations whose value is an array of zero or more location objects (§3.26), each of which represents a location relevant to understanding the result.

EXAMPLE: Suppose that a tool for analyzing JavaScript has a rule that reports a problem when a variable declared in an inner scope hides a variable with the same name in an enclosing scope. The tool would report the problem on the line where the inner variable is declared. The tool could choose to add an element to the relatedLocations array, specifying the location where the outer variable was declared.  
  
The result might appear in the log file like this:

results: [

{

"ruleId": "JS3056",

"level": "error",

"message": {

"text": "Name 'index' cannot be used in this scope because

it would give a different meaning to 'index'."

},

"locations": [

{

"physicalLocation": {

"uri": "file:///C:/Code/a.js",

"region": {

"startLine": "6",

"startColumn": "10"

}

}

}

],

"relatedLocations": [ # An array of location objects

# (§3.26)

{ # A location object.

"message": {

"text": "The previous declaration of 'index' was here."

},

"physicalLocation": {

"uri": "file:///C:/Code/a.js",

"region": {

"startLine": "2",

"startColumn": "6"

}

}

}

]

},

...

]

The tool might write messages to the console like this:

C:\Code\a.js(6,10-10): error : JS3056: Name 'index' cannot be used in this scope because it would give a different meaning to 'index'.

C:\Code\a.js(2,6-6): info : JS3056: The previous declaration of 'index' was here.

### suppressions property

A result object **MAY** contain a property named suppressions whose value is an array of zero or more unique (§3.7.3) suppression objects (§3.32), each of which describes a request to “suppress” a result (that is, to exclude it from result lists, bug counts, *etc.*).

If suppressions is absent, it **SHALL** default to an null.

The presence of an array value, whether or not the array is empty, **SHALL** mean that suppression information is available for the result. In this case, if the array is non-empty, a SARIF consumer **SHALL** treat the result as suppressed, and if the array is empty, a consumer **SHALL** treat the result as not suppressed.

The absence of an array value, or the presence of a null value, **SHALL** mean that suppression information is not available for the result. A SARIF consumer **SHALL** treat such a result as not suppressed.

The suppressions values for all result objects in theRun **SHALL** be either all null or all non-null.

NOTE: The rationale is that an engineering system will generally evaluate all results for suppression, or none of them. Requiring that the suppressions values be either all null or all non-null enables a consumer to determine whether suppression information is available for the run by examining a single result object.

### baselineState property

A result object **MAY** contain a property named baselineState whose value is a string that specifies the state of this result with respect to some previous run, which we refer to as the “baseline run.”

If theRun.baselineGuid (§3.14.5), its value **SHALL** specify the baseline run.

This property **SHALL** have one of the following values, with the specified meanings:

* "new": This result was detected in the current run but was not detected in the baseline run.
* "unchanged": This result was detected both in the current run and in the baseline run, and it did not change between those two runs in any way that the tool considers significant.
* "updated": This result was detected both in the current run and in the baseline run, but it changed between those two runs in a way that the tool considers significant.
* "absent": This result was detected in the baseline run but was not detected in the current run.

NOTE 1: The purpose of baselineState is to allow (for example) a measurement of how many new results were introduced in the run, and how many previously existing results no longer appear.

To assign a value to baselineState, a tool needs a way to determine whether a result is logically “the same”, in some sense, as a result that appeared in the baseline. [Appendix B](#AppendixFingerprints) discusses how a result management system can assign a “fingerprint” to each result. See also the description of the fingerprints (§3.25.14) and partialFingerprints (§3.25.15) properties.

An analysis tool that works together with such a result management system can use the fingerprint to determine whether two results are logically the same; two results with the same fingerprint are considered logically the same.

NOTE 2: A result management system might respond to a “new” result by filing an issue in a bug tracking system. It might respond to an “updated” result by editing the details of an existing issue in the bug tracking system, or by attaching an updated SARIF log to the issue. It might respond to an “absent” result by resolving the issue. It might take no action at all for an “unchanged” issue, or it might simply update its internal information about the range of runs that contained the result.

If baselineState is present on any result object in theRun, it **SHALL** be present on every such result object.

NOTE 3: The presence of baselineState on any result implies that the SARIF producer performed a comprehensive comparison between the results in the current run and those in some previous run. A SARIF consumer is entitled to expect that the differencing operation produced a baselineState value for every result.

This is conceptually similar to a tool that compares two text files, and for every line, concludes that it exists in the left-hand file, the right-hand file, or both. The tool must provide this information for every line in both files; it cannot leave some lines “undetermined.”

### rank property

A result object **MAY** contain a property named rank whose value is a number between 0.0 and 100.0 inclusive, representing the priority or importance of the result. 0.0 is the lowest priority and 100.0 is the highest.

If kind (§3.25.9) has any value other than "fail", then if rank is absent, it **SHALL** default to -1.0, and if it is present, it **SHALL** have the value -1.0.

If kind has the value "fail" and rank is absent, rank **SHALL** default to the value determined by the procedure defined for level (§3.25.10), except throughout the procedure, replace "level" with "rank" and replace "warning" with -1.0.

NOTE: rank values produced by different tools are in general not commensurable. If Tool A produces one result with rank 0.65 and a second result with rank 0.70, the consumer is entitled to assume that the second result is of higher priority than the first. But if Tool A produces a result with rank 0.65 and Tool B produces a result with rank 0.70, the result produced by Tool B might or might not be of higher priority than the result produced by Tool A. In an engineering system that aggregates results from multiple tools, rank values might need to be adjusted, either automatically or by end users, so that rank values from different tools can be interleaved in a meaningful way.

### attachments property

A result object **MAY** contain a property named attachments whose value is an array of zero or more unique (§3.7.3) attachment objects (§3.20), each of which describes an artifact relevant to the detection of the result. The array elements **SHALL** refer to distinct artifacts.

### workItemUris property

A result object **MAY** contain a property named workItemUris whose value is either null or an array of zero or more unique (§3.7.3) strings, each containing the absolute URI [[RFC3986](#RFC3986)] of a work item associated with this result.

If workItemUris is absent, it **SHALL** default to null.

An empty array **SHALL** mean that there are no work items associated with this result. null **SHALL** mean that the set of work items associated with this result, if any, is not known.

NOTE: Result management systems are likely to generate work items from at least some of the results in a SARIF log file. Depending on the engineering system, these work items might take the form of Git issues, Jira tickets, TFS work items, or the equivalent in other work item tracking systems.

### hostedViewerUri property

A result object **MAY** contain a property named hostedViewerUri whose value is a string containing an absolute URI [[RFC3986](#RFC3986)] at which the result can be viewed. The URI **SHALL** be valid as of the time the tool generated this result. It is not guaranteed to be valid at later times (for example, the hosting environment might not keep results older than a specified age).

NOTE: This property can be used by tools that provide an online viewing experience for the results they generate. This experience might be specifically designed to display the results from that tool, as opposed to a generic SARIF viewer that displays results from any tool that produces SARIF.

### provenance property

A result object **MAY** contain a property named provenance whose value is a resultProvenance object (§3.43) that contains information about how and when the result was detected.

### fixes property

A result object **MAY** contain a property named fixes whose value is an array of one or more unique (§3.7.3) fix objects (§3.45).

### occurrenceCount property

A result object **MAY** contain a property named occurrenceCount whose value is a positive integer specifying the number of times a result with theResult.correlationGuid (§3.25.4) has been observed.

NOTE: This property is intended for the scenario where multiple SARIF files are being merged into a single SARIF file, with the intent that each logically distinct result (§3.25.2) occurs only once in the merged file. In that case, the system performing the merge would select one occurrence of each logically distinct result to serve as the exemplar for that class of results, and it would set occurrenceCount on that instance to the number of times a result with that correlationGuid occurred in the input files.

## location object

### General

A location object describes a location. Depending on the circumstances, a location object is described by physical location (§3.27), a logical location (§3.31), both, or in rare circumstances, neither (see below).

A logical location specifies a programmatic construct, for example, a class name or a function name, without specifying the artifact within which that construct occurs.

NOTE: There are two reasons to include logical locations in the SARIF format in addition to physical locations:

1. In the absence of symbol information, binary analysis tools might not have source code locations available, so information about line and column numbers might not be present in the log file. In this case, code editors, other programs, or end users can use logical location to navigate from a result to the correct source code location.  
  
2. Logical location information is an important contributor to fingerprinting scenarios because it is typically more resilient to changes in source code than are the line numbers included in physical locations. See [Appendix B](#AppendixFingerprints) for more information about fingerprinting. The logicalLocation.fullyQualifiedName property (§3.31.6) is particularly convenient for fingerprinting.

In rare circumstances, there might be neither physical nor logical location information available for a location object. See §3.42.3 for an example. In that case, the location object **SHOULD** contain a message property (§3.26.4) explaining the significance of this “location.”

### physicalLocation property

Depending on the circumstances, a location object either **SHALL**, **MAY**, or **SHALL NOT** contain a property named physicalLocation whose value is a physicalLocation object (§3.27) that identifies the file within which the location lies. If physical location information is available and the logicalLocation property (§3.26.3) is absent, physicalLocation **SHALL** be present. If physical location is available and logicalLocation is present, physicalLocation **MAY** be present. If physical location information is not available, physicalLocation **SHALL NOT** be present.

### logicalLocation property

Depending on the circumstances, a location object either **SHALL**, **MAY**, or **SHALL NOT** contain a property named logicalLocation whose value is a logicalLocation object (§3.31) that identifies the programmatic construct within which the location lies. If logical location information is available and the physicalLocation property (§3.26.2) is absent, logicalLocation **SHALL** be present. If logical location is available and physicalLocation is present, logicalLocation **MAY** be present. If logical location information is not available, logicalLocation **SHALL NOT** be present.

The logicalLocation object held by this property **MAY** be augmented with information in theRun.logicalLocations (§3.14.16). See §3.31.5 for more information.

### message property

A location object **MAY** contain a property named message whose value is a message object (§3.11) relevant to the location.

### annotations property

A location object **MAY** contain a property named annotations whose value is an array of zero or more unique (§3.7.3) region objects (§3.28), each of which describes a region within the artifact specified by the location object that is relevant to the location. Each of these region objects **SHOULD** contain a message property (§3.28.14) that explains the relevance of the region to the location.

EXAMPLE: Consider a location object which describes the declaration statement

int x = (y + z) \* q;

If the analysis tool wanted to emphasize the expression (y + z), it might set the annotations property to:

"annotations": [ # An array of region objects.

{ # A region object (§3.28).

"startLine": 12,

"startColumn": 13,

"endColumn": 19,

"message": {

"text": "(y + z) = 42"

}

}

]

## physicalLocation object

### General

A physicalLocation object represents the physical location where a result was detected. A physical location specifies a reference to an artifact together with a region within that artifact.

### id property

A physicalLocation object **MAY** contain a property named id whose value is a non-negative integer that **SHALL** be unique among all physicalLocation objects belonging to theResult. The value does not need to be unique across all result objects in theRun.

EXAMPLE: Within a result object, the following property values (among others) are physicalLocation objects, and no two of them can have the same values for their id properties:

result.relatedLocations[0].physicalLocation

result.codeFlows[0].threadFlows[0].locations[0].physicalLocation

result.stacks[0].frames[0].physicalLocation

The purpose of the id property is to enable an embedded link (§3.11.5) within a message object (§3.11) to refer to the location. If no message object within theResult refers to this location *via* an embedded link, the id property does not need to appear.

### artifactLocation property

A physicalLocation object **SHALL** contain a property named artifactLocation whose value is an artifactLocation object (§3.4) that represents the location of the artifact.

### region property

A physicalLocation object **MAY** contain a property named region whose value is a region object (§3.28) that represents a relevant portion of the artifact. In particular, if the physicalLocation object occurs within the locations property (§3.25.12) of a result object (§3.25), the region property **SHALL** specify the region within the artifact where the result was detected.

EXAMPLE 1: In this example, a physicalLocation object specifies the location where a result was detected. Its region property specifies the portion of the file where the result was detected.

{ # A result object (§3.25).

"locations": [ # See §3.25.12.

{ # A location object (§3.26).

"physicalLocation": { # See §3.26.2.

"artifactLocation": { # A physicalLocation object.

"uri": "ui/window.c",

"uriBaseId": "SRCROOT"

},

"region": { # The region specifies the portion of the file

"startLine": 42 # where the result was detected.

}

}

}

]

}

If the physicalLocation object specifies a location in a nested artifact, then the region property **SHALL** specify the location with respect to the innermost nested artifact.

EXAMPLE 2: If a result occurs in a C++ file contained in a compressed archive, then the region would represent the line and column number of the result with the C++ file. It would not represent (for example) the offset of the C++ file from the start of the archive.

If the region property is absent, the physicalLocation object refers to the entire artifact.

### contextRegion property

If a physicalLocation object contains a region property (§3.27.4), it **MAY** also contain a property named contextRegion whose value is a region object (§3.28) which specifies a region that is a proper superset of the region specified by the region property. If region is absent, contextRegion **SHALL** be absent.

The purpose of contextRegion is to enable a viewer to provide visual context when displaying a portion of an artifact.

EXAMPLE In this example, an analysis tool detected a result on line 42. The tool provides additional context SARIF viewers by specifying a range of content surrounding the result line.

{ # A result object (§3.25).

"locations": [ # See §3.25.12.

{ # A location object (§3.26).

"physicalLocation": { # A physicalLocation object (§3.27).

"artifactLocation": { # An artifactLocation object (§3.4).

"uri": "ui/window.c",

"uriBaseId": "SRCROOT"

},

"region": { # See §3.27.4.

"startLine": 42,

"snippet": {

"text": "int n = m + 1;"

}

},

"contextRegion": {

"startLine": 41,

"endLine": 43,

"snippet": {

"text": "int m;\nint n = m + 1\n\n"

}

}

}

}

]

}

### address property

A physicalLocation object **MAY** contain a property named address whose value is an address object (§3.30) that represents the physical or virtual address of this location.

## region object

### General

A region object represents a region, that is, a contiguous portion of an artifact.

The region object defines both “text properties” and “binary properties.” The text properties represent a region as a contiguous range of zero or more characters (a “text region”). The binary properties represent a region as a contiguous range of zero or more bytes (a “binary region”).

For regions in text artifacts, a region object **SHOULD** contain text properties and **MAY** also contain binary properties. If both text properties and binary properties are present, they **SHALL** specify the identical range of bytes in the artifact, as determined by the artifact’s character encoding.

For regions in binary artifacts, a region object **SHALL** contain binary properties and **SHALL NOT** contain text properties.

If any text properties are present, enough text properties **SHALL** be present to fully specify a text region (see §3.28.2). If any binary properties are present, then enough binary properties **SHALL** be present to fully specify a binary region (see §3.28.3).

### Text regions

NOTE 1: The examples in this section assume a text file with the following contents:

abcd\r\nefg\r\nhijk\r\nlmn\r\n

Breaking the lines for the sake of readability, the contents are:

abcd\r\n

efg\r\n

hijk\r\n

lmn\r\n

The file contains four lines, each of which ends with the two-character newline sequence "\r\n", which is explicitly displayed for clarity.

The line number of the first line in a text artifact **SHALL** be 1. The column number of the first character in each line **SHALL** be 1. The character offset of the first character in the artifact **SHALL** be 0.

The values of text properties **SHALL NOT** depend on the presence or absence of a byte order mark (BOM) at the start of the artifact.

Column numbers are expressed in the measurement unit specified by theRun.columnKind (§3.14.24).

A SARIF viewer **MAY** choose to present column numbers that match the visual offset of each character from the beginning of the line. These “visual” column numbers might not match the column numbers contained in the SARIF file.

NOTE 2: Such a mismatch might occur if, for example, the line contains a tab character, or an accented character represented by a base character plus a combining character.

A text artifact’s character encoding determines the number of bytes that represent each character, and therefore determines the range of bytes represented by a text region. A SARIF consumer **SHALL** consider an artifact to have the encoding specified by artifact.encoding (§3.23.9), if present, or else by run.defaultEncoding (§3.14.21), if present. If neither is present, the consumer **MAY** use any heuristic or procedure to determine the encoding, including (for example) prompting the user.

NOTE 3: If a consumer incorrectly determines an artifact’s encoding, it might not display the artifact correctly. For example, when it attempts to highlight a region, it might highlight an incorrect range of characters.

A text region **MAY** be specified in two ways:

* By means of the “line/column” properties startLine (§3.28.5), startColumn (§3.28.6), endLine (§3.28.7), and endColumn (§3.28.8).
* By means of the “offset/length” properties charOffset (§3.28.9) and charLength (§3.28.10).

A text region **SHALL** specify both its start (the location of its first character) and its end (the location of its last character).

A text region does not include the character specified by endColumn (see §3.28.8).

EXAMPLE 1: The following regions (among others) all specify the range of characters "bc".

{

"startLine": 1,

"startColumn": 2,

"endLine": 1,

"endColumn": 4 # The region excludes the character at endColumn.

}

{

"charOffset": 1,

"charLength": 2

}

{

"startLine": 1,

"startColumn": 2,

"endLine": 1,

"endColumn": 4,

"charOffset": 1,

"charLength": 2

}

EXAMPLE 2: The following region is invalid, even though it might appear to specify the same range of characters "bc" as in EXAMPLE 1:

{

"startLine": 1,

"charOffset": 1, # Specifies the "b"

"endColumn": 4 # Specifies the column one past the "c"

}

This is because the line/column properties and the offset/length properties, taken independently, specify different regions:

* "startColumn" is absent, and so defaults 1 (see §3.28.6).
* "endLine" is absent, and so defaults to "startLine", which in this example is 1 (see §3.28.7).
* "charLength" is absent, and so defaults to 0 (see §3.28.10).

In summary, the above region is equivalent to the region

{

"startLine": 1,

"startColumn": 1,

"endLine": 1,

"endColumn": 4,

"charOffset": 1,

"charLength": 0

}

Now we can see that the line/column properties represent the range of characters "abc", while the offset/length properties represent an insertion point before the character "b" (see §3.28.10). Those two regions are not the same, and so the region is invalid.

Incidentally, *neither* of those regions is the same as the "bc" one might expect if it were valid to compose a region partially from a mixture of line/column properties and offset/length properties.

If a region spans more than one line, it **SHALL** include the newline sequences of all but the last line in the region.

EXAMPLE 3: The region

{ "startLine": 2, "endLine": 3 }

includes the characters "efg\r\nhijk".

A region of length 0 is referred to as an “insertion point.” An insertion point **MAY** be specified either by specifying charLength as 0, or by specifying the same values for startColumn and endColumn.

NOTE 4: This is consistent with the rule that a region does not include the character in column endColumn.

EXAMPLE 4: These regions (among others) specify an insertion point before the "b" on line 1.

{ "startLine": 1, "startColumn": 2, "endColumn": 2 }

{ "charOffset": 1, ""charLength": 0 }

EXAMPLE 5: These regions (among others) specify an insertion point at the beginning of the file:

{ "startLine": 1, "startColumn": 1, "endColumn": 1 }

{ "charOffset": 0, "charLength": 0 }

To specify an insertion point after the last character in an artifact, set endLine to the number of the last line in the artifact, and set endColumn to a value one greater than the number of characters on the line, *including* any trailing newline sequence..

EXAMPLE 6: These regions (among others) specify an insertion point at the very end of the file. Note that the last line contains the five characters (including the newline sequence) "lmn\r\n".

{ "startLine": 4, "startColumn": 6, "endColumn": 6 }

{ "charOffset": 22, "charLength": 0 }

### Binary regions

The byte offset of the first byte in an artifact **SHALL** be 0.

To specify a byte region, at least byteOffset (§3.28.11) **SHALL** be present. byteLength (§3.28.12) **MAY** also be present. byteOffset specifies the start of the region. byteLength specifies the end of the region. A byteLength value of 0 represents an insertion point before the byte specified by byteOffset.

### Independence of text and binary regions

The text-related and binary-related properties in a region object **SHALL** be treated independently. That is, the value of a text-related property **SHALL NOT** be inferred from the value of any set of binary-related properties, and *vice versa*.

EXAMPLE: This example is based on the sample text file show in NOTE 1 of §3.28.2. It represents invalid SARIF because the text-related and binary-related properties are inconsistent. At first glance they appear to be consistent because the byte at offset 2 is indeed on line 1:

{ "startLine": 1, "byteOffset": 2, "byteLength": 6 }

However, because the default values for the missing text-related properties are determined entirely from the existing text-related properties, and independently of any binary-related properties, this region is in fact equivalent to this one:

{

"startLine": 1,

"startColumn": 1, // Missing startColumn defaults to 1.

"endLine": 1, // Missing endLine defaults to startLine.

"endColumn": 5, // Missing endColumn defaults to (length of endLine + 1),

// exclusive of newline sequence.

"byteOffset": 2

"byteLength": 6

}

This makes it clear that the text-related and binary-related properties represent different ranges of bytes, and therefore the region is invalid.

### startLine property

When a region object represents a text region specified by line/column properties, it **SHALL** contain a property named startLine whose value is a positive integer equal to the line number of the line containing the first character in the region.

### startColumn property

When a region object represents a text region specified by line/column properties, it **MAY** contain a property named startColumn whose value is a positive integer equal to the column number of the first character in the region.

If startColumn is absent,it **SHALL** default to 1.

### endLine property

When a region object represents a text region specified by line/column properties, it **MAY** contain a property named endLine whose value is a positive integer equal to the line number of the line containing the last character in the region.

If endLine is absent, its value **SHALL** default to startLine.

### endColumn property

When a region object represents a text region specified by line/column properties, it **MAY** contain a property named endColumn whose value is an integer whose value is one greater than the column number of the last character in the region.

If endColumn is absent, it **SHALL** default to a value one greater than the column number of the last character on the line, excluding any newline sequence.

### charOffset property

When a region object represents a text region specified by offset/length properties, it **SHALL** contain a property named charOffset whose value is an integer equal to the zero-based character offset of the first character in the region from the beginning of the artifact.

### charLength property

When a region object represents a text region specified by offset/length properties, it **MAY** contain a property named charLength whose value is a non-negative integer equal to the number of characters in the region.

If charLength is absent, it **SHALL** default to 0, which **SHALL** be interpreted as an insertion point at the position specified by charOffset (§3.28.9)

The sum of charOffset and charLength **SHALL** be greater than or equal to 0 and less than or equal to the number of characters in the artifact.

A region whose charOffset is equal to the number of characters in the artifact and whose charLength is 0 is permitted and **SHALL** represent an insertion point at the end of the artifact.

### byteOffset property

When a region object represents a binary region, it **SHALL** contain a property named byteOffset whose value is an integer equal to the zero-based byte offset of the first byte in the region from the beginning of the artifact.

### byteLength property

When a region object represents a binary region, it **MAY** contain a property named byteLength whose value is an integer equal to the number of bytes in the region. If byteLength is absent, it **SHALL** default to 0, which **SHALL** be interpreted as an insertion point at the position specified by byteOffset (§3.28.11).

The sum of byteOffset and byteLength **SHALL** be greater than or equal to 0 and less than or equal to the number of bytes in the artifact.

A region object whose byteOffset equals the number of bytes in the artifact and whose byteLength is 0 is permitted, and **SHALL** represent an insertion point at the end of the artifact.

### snippet property

A region object **MAY** contain a property named snippet whose value is an artifactContent object (§3.3) representing the portion of the artifact specified by the region object.

NOTE: The purpose of the snippet property is to allow a SARIF viewer to present the contents of the region even if the artifact from which it was taken is not available. It also allows an end user examining a SARIF log file to see the relevant content without opening another file.

### message property

A region object **MAY** contain a property named message whose value is a message object (§3.11) containing a message relevant to the region.

A SARIF viewer **SHOULD** display this message when the user interacts with the region. For example, if the user hovers over the region with the mouse, the viewer might present the message as hover text.

### sourceLanguage property

If the region object represents a portion of a text artifact that contains source code, it **MAY** contain a property named sourceLanguage whose value is a hierarchical string (§3.5.5) that specifies the programming language in which this portion of the source code is written. If the region object does not represent a portion of a text artifact containing source code, then sourceLanguage **SHALL** be absent.

For the remainder of this section, we assume that the region object represents a portion of a text artifact that contains source code.

NOTE: This property is intended to help SARIF viewers to render code snippets (§3.28.13) with appropriate syntax coloring. It is intended for use in mixed-language files, such as HTML files that contains JavaScript. For more information about this usage, see §3.23.10.

if sourceLanguage is absent, it **SHALL** default to the value of the sourceLanguage property (§3.23.10) of the artifact object (§3.23) which describes the artifact that contains the region. artifact.sourceLanguage in turn defaults to theRun.defaultSourceLanguage (§3.14.22). If all three of region.sourceLanguage, artifact.sourceLanguage, and theRun.defaultSourceLanguage are absent, the source language of the region object **SHALL** be taken to be unknown. In that case, a SARIF viewer **MAY** use any method or heuristic to determine the region’s source language, for example, by examining the file’s file name extension or MIME type, or by prompting the user.

For conventions and practices regarding the value of this property, see §3.23.10.2.

## rectangle object

### General

A rectangle object specifies a rectangular area within an image. When a SARIF viewer displays an image, it **SHOULD** indicate the presence of these areas, for example, by highlighting them or surrounding them with a border.

### top, left, bottom, and right properties

A rectangle object **SHALL** contain properties named top, left, bottom, and right, each of which contains a number (as defined by [[JSCHEMA01](#JSCHEMA01)]) specifying one of the coordinates of the rectangle within the image. These properties **SHALL** be measured in the image format’s natural units (for example, pixels for raster-based image formats). These values **MAY** be positive or negative, depending on the natural coordinate system of the image format. They **MAY** increase either from left to right or from right to left, and either from top to bottom or from bottom to top, again depending on the natural coordinate system of the image format.

NOTE: A number in JSON schema can take a variety of forms, including simple integers (42) and floating-point numbers (3.14).

### message property

A rectangle object **SHOULD** contain a property named message whose value is a message object (§3.11) containing a message relevant to this area of the image.

A SARIF viewer **SHOULD** display this message when the user interacts with the area. For example, if the user hovers over the area with the mouse, the viewer might present the message as hover text.

## address object

An address object describes a physical or a virtual address in an executing program.

EXAMPLE:

{ # An address object.

"baseAddress": "0x00402180", # See §3.30.1.

"offset": "0x0040", # See §3.30.2.

"kind": "section", # See §3.30.5.

"name": ".text" # See §3.30.4.

}

### baseAddress property

An address object **MAY** contain a property named baseAddress whose value is a string containing a hexadecimal representation of the base address of the region containing this address.

### offset property

An address object **MAY** contain a property named baseAddress whose value is a string containing a hexadecimal representation of the offset of this address from baseAddress (§3.30.1). If baseAddress is absent, offset **SHALL** represent an absolute address.

### fullyQualifiedName property

An address object **MAY** contain a property named fullyQualifiedName whose value is a string containing the fully qualified name of this address.

This property is useful for nested addresses, for example, an offset from the start of a table which in turn resides within a section.

EXAMPLE: "fullyQualifiedName": "MyDll.dll+0x47"

This name consists of two components. The first component is the name of the address at which the module was loaded into memory. The second component represents an offset from that address.

### name property

An address object **MAY** contain a property named name whose value is a string containing the name of the memory region containing this address.

### kind property

An address object **MAY** contain a property named kind whose value is a string that specifies the kind of memory region in which this address is located.

When possible, SARIF producers **SHOULD** use the following values, with the specified meanings.

* "section": A named portion of a PE or COFF file.
* "segment": A portion of memory.

If none of these values are appropriate, a SARIF producer **MAY** use any value.

### index property

Depending on the circumstances, an address object either **MAY, SHALL NOT**, or **SHALL** contain a property named index whose value is the array index (§3.7.4) within theRun.addresses (§3.14.17) of an address object that provides additional properties for the current address object. We refer to the object in theRun.addresses as the “cached object.”

If the current object is an element of run.addresses, then index **MAY** be present. If present, its value **SHALL** be the index of the current object within theRun.addresses.

Otherwise, if run.addresses is absent, or if it does not contain a cached object for the current object, then index **SHALL NOT** be present.

Otherwise (that is, if the current object is not an element of theRun.addresses, and theRun.addresses does contain a cached object for the current object), then index **SHALL** be present, and its value **SHALL** be the array index within theRun.addresses of the cached object.

If index is present, and if the cached object contains any property that is absent from the current object, then the current object **SHALL** take the value of that property from the cached object.

NOTE: This allows a SARIF producer to reduce the size of the log file by caching properties shared by several address objects, and specifying only the properties that differ in the current object.

### parentIndex property

If this address object represents a nested address, then it **SHALL** contain a property named parentIndex whose value is the array index (§3.7.4) of the parent address object within theRun.addreses (§3.14.17).

If this address object represents a top-level address, then parentIndex **SHALL** be absent.

NOTE: parentIndex makes it possible to navigate from the address object representing a nested address to the address objects representing each of its parent addresses in turn, up to the top-level address.

## logicalLocation object

### General

A logicalLocation object describes a logical location. A logical location is a location specified by a programmatic construct such as a namespace, a type, or a method, without regard to the physical location where the construct occurs.

logicalLocation objects occur in two places: as array elements of the run.logicalLocations property (§3.14.16) and as the value of the location.logicalLocation property (§3.26.3).

### Constraints

If the logicalLocation object does not occur as an array element of run.logicalLocations (§3.14.16), at least one of the index property (§3.31.5) or the fullyQualifiedName property (§3.31.6) **SHALL** be present; they **MAY** both be present.

NOTE: Providing both index and fullyQualifiedName makes the log file more readable at the expense of increased size. Providing only index reduces log file size but makes it less readable to an end user, who has to determine the fully qualified name by locating the logicalLocation object at the index within run.logicalLocations (§3.14.16) specified by index.

### Logical location naming rules

Every logical location has a “fully qualified logical name” (more briefly, a “fully qualified name”) that fully specifies the programmatic construct to which it refers. When programmatic constructs are nested (such as a method within a class within a namespace), the fully qualified name is typically a hierarchical identifier such as "N.C.F(void)" or "N::C::F(void)". We refer to the rightmost component of this hierarchical identifier as the “logical name” (more briefly, the “name”) of the logical location.

Whenever possible, logical names and fully qualified logical names **SHOULD** conform to the syntax of the programming language in which the programmatic construct specified by the logical location was expressed.

EXAMPLE 1: The fully qualified logical name of the C++ method f(void) in class C in namespace N is "N::C::f(void)". Its logical name is "f(void)".

This is not always possible, for two reasons:

* For certain values of logicalLocation.kind (§3.31.8), there is no language syntax to specify the fully qualified name.

EXAMPLE 2: Suppose the logical location is the local variable pBuffer in the C++ method "N::C::f(void)". logicalLocation.kind is "variable". There is no way to express the fully qualified name in C++. The SARIF producer might choose a fully qualified name such as "N::C::f(void)?pBuffer".

* For other values of logicalLocation.kind, it is sometimes but not always possible to express the logical location in language syntax.

EXAMPLE 3: Suppose the logical location is the anonymous callback function in this JavaScript function:

function click\_it() {

$("button").click(function(){

alert("Clicked!");

});

}

logicalLocation.kind is "function", for which it is sometimes possible to specify a fully qualified name. But there is no language syntax to express the name of an anonymous callback. The SARIF producer might choose a fully qualified name such as "click\_it?anon-1".

### name property

A logicalLocation object **SHALL** contain a property named name whose value is the logical name of the programmatic construct specified by this object. For example, this property might contain the name of a class or a method.

The name property **SHALL** be suitable for display and **SHALL** follow the naming rules for logical names described in §3.31.3.

NOTE: A C++ analysis tool might have available both the source code form of a function name and the compiler’s “decorated” function name (which encodes the function signature in a manner that is compiler-dependent and not easily readable). The tool would place the source code form of the function name in the name property, and the decorated name in the decoratedName property (§3.31.8).

EXAMPLE: In this C++ example, the fully qualified name is "b::c(float)", so "name" is the rightmost component, "c(float)".

{ # A logicalLocation object.

"name": "c(float)",

"fullyQualifiedName": "b:c(float)", # See §3.31.6.

"kind": "function" # See §3.31.8

}

### index property

Depending on the circumstances, a logicalLocation object either **MAY, SHALL NOT**, or **SHALL** contain a property named index whose value is the array index (§3.7.4) within theRun.logicalLocations (§3.14.16) of a logicalLocation object that provides additional properties for the current logicalLocation object. We refer to the object in theRun.logicalLocations as the “cached object.”

If the current object is an element of run.logicalLocations, then index **MAY** be present. If present, its value **SHALL** be the index of the current object within theRun.logicalLocations.

Otherwise, if run.logicalLocations is absent, or if it does not contain a cached object for the current object, then index **SHALL NOT** be present.

Otherwise (that is, if the current object is not an element of theRun.logicalLocations, and theRun.logicalLocations does contain a cached object for the current object), then index **SHALL** be present, and its value **SHALL** be the array index within theRun.logicalLocations of the cached object.

If index is present, and if the cached object contains any property that is absent from the current object, then the current object **SHALL** take the value of that property from the cached object.

NOTE: This allows a SARIF producer to reduce the size of the log file by caching properties shared by several logicalLocation objects, and specifying only the properties that differ in the current object.

### fullyQualifiedName property

Depending on the circumstances, a logicalLocation object either **SHALL** or **MAY** contain a property named fullyQualifiedName whose value is the fully qualified name of the logical location. This name **SHALL** follow the naming rules for fully qualified names described in §3.31.3.

If this logicalLocation object represents a top-level logical location, then fullyQualifiedName **MAY** be present. If present, it **SHALL** equal name; if absent, it **SHALL** default to name. If this object does not represent a top-level logical location, fullyQualifiedName **SHALL** be present.

It is possible for two or more distinct logical locations to have the same fully qualified name.

NOTE: This is an extremely rare corner case.

EXAMPLE: Suppose a tool analyzes two C++ source files:

// file1.cpp

namespace A {

class B {

}

}

// file2.cpp

namespace A {

namespace B {

class C {

}

}

}

These could not coexist in the same compilation, but there is no reason two such source files could not exist.

If the tool detected one result in class B in *file1.cpp*, and another result in namespace B in *file2.cpp*, the fullyQualifiedName for both would be A::B. However, they would be distinguished by their parentIndex properties:

"logicalLocations": [

{

"name": "B",

"fullyQualifiedName": "A::B",

"kind": "namespace",

"parentIndex": 1

},

{

"name": "A",

"kind": "namespace"

},

{

"name": "B",

"fullyQualifiedName": "A::B",

"kind": "type",

"parentIndex": 3

},

{

"name": "A",

"kind": "namespace"

}

]

NOTE: There are a few reasons the fullyQualifiedName property exists, even though the information it contains is presented in more detail in the run.logicalLocations property:

* run.logicalLocations might not be present.
* It allows a SARIF viewer to display the logical location in a way that is easily understood by users.
* As mentioned in §3.26.1, fullyQualifiedName is also particularly convenient for fingerprinting, although the more detailed information in run.logicalLocations could be used instead.
* It relieves viewers from having to format the logical location from the more detailed information in run.logicalLocations.
* It is useful for producing readable in-source suppressions (for example, “suppress all instance of rule CA2101 in the class NamespaceA.NamespaceB.ClassC”).

### decoratedName property

A logicalLocation object **MAY** contain a property named decoratedName whose value is a string containing the compiler's internal representation of the logical location associated with this location object. Some compilers refer to this representation as a “mangled name.”

EXAMPLE: In this example, the decoratedName property contains a “mangled” name emitted by a C++ compiler:

{ # A "logicalLocation" object

"name": "c(float)",

"fullyQualifiedName": "b::c(float)",

"decoratedName": "?c@b@@AAGXM@Z"

}

### kind property

A logicalLocation object **SHOULD** contain a property named kind whose value is one of the following strings, if any of those strings accurately describes the construct identified by this object.

* Values for locations within executable code:
  + "function"
  + "member"
  + "module"
  + "namespace"
  + "resource"
  + "type"
  + "returnType"
  + "parameter"
  + "variable"
* Values for locations within XML documents:
  + "element"
  + "attribute"
  + "text"
  + "comment"
  + "processingInstruction"
  + "dtd"

EXAMPLE 1: Consider the following XML document:

1. <?xml version="1.0"?>

2. <orders>

3. <order number="">

4. <total>-$3.25</total>

5. </order>

6. </order>

Suppose that an analysis tool detects errors on line 3 (the order number is blank) and line 4 (the total is negative). It might represent the logical locations of these errors as XML Paths (although this is not required), as follows:

{ # A run object (§3.14)

"results": [ # See §3.14.20.

{ # A result object (§3.25).

"locations": [ # See §3.25.12.

{ # A location object (§3.26).

"logicalLocation": { # See §3.26.3.

"fullyQualifiedName": "/orders/order[1]/@number",

"index": 2

}

}

]

},

{

"locations": [

{

"logicalLocation": {

"fullyQualifiedName": "/orders/order[1]/total/text()",

"index": 3

}

}

]

}

],

"logicalLocations": [ # See §3.14.16.

{ # A logicalLocation object (§3.31).

"name": "orders",

"fullyQualifiedName": "/orders",

"kind": "element"

},

{

"name": "order[1]",

"fullyQualifiedName": "/orders/order[1]",

"kind": "element",

"parentIndex": 0

},

{

"name": "number",

"fullyQualifiedName": "/orders/order[1]/@number",

"kind": "attribute",

"parentIndex": 1

},

{

"name": "text",

"fullyQualifiedName": "/orders/order[1]/text()",

"kind": "text",

"parentIndex": 1

}

]

}

* Values for locations within JSON documents:
  + "object"
  + "array"
  + "property"
  + "value"

EXAMPLE 2: Consider the following JSON document:

1. {

2. "orders": [

3. {

4. "productIds": [ "A-101", "", "A-223" ],

5. "total": "-$3.25"

6. }

7. ]

8. }

Suppose that an analysis tool detects errors on line 4 (one of the product ids blank) and line 5 (the total is negative). It might represent the logical locations of these errors as JSON Pointers (although this is not required), as follows:

{ # A run object (§3.14)

"results": [ # See §3.14.20.

{ # A result object (§3.25).

"locations": [ # See §3.25.12.

{ # A location object (§3.26).

"logicalLocation": { # See §3.26.3.

"fullyQualifiedName": "/orders/0/number",

"index": 2

}

}

]

},

{

"locations": [

{

"logicalLocation": {

"fullyQualifiedName": "/orders/0/total",

"index": 3

}

}

]

}

],

"logicalLocations": [ # See §3.14.16.

{ # A logicalLocation object (§3.31).

"name": "orders",

"fullyQualifiedName": "/orders",

"kind": "array"

},

{

"name": "0",

"fullyQualifiedName": "/orders/0",

"kind": "object",

"parentIndex": 0

},

{

"name": "productIds",

"fullyQualifiedName": "/orders/0/productIds",

"kind": "array",

"parentIndex": 1

},

{

"name": "1",

"fullyQualifiedName": "/orders/0/productIds/1",

"kind": "value",

"parentIndex": 2

},

{

"name": "total",

"fullyQualifiedName": "/orders/0/total",

"kind": "property",

"parentIndex": 1

}

]

}

If none of those strings accurately describes the construct, kind **MAY** contain any value specified by the analysis tool.

If a logical location is both a member and a type (for example, a nested class in C++ or C#), the value of kind, if present, **SHALL** be "type".

NOTE: The purpose of this property is to help result management systems group results that occur in the same logical location. If one result specifies the logical location “namespace A”, and another result specifies the logical location “class A”, the difference in the kind property between the two results tells the result management system to sort them into different groups.

### parentIndex property

If this logicalLocation object represents a nested logical location, then it **SHALL** contain a property named parentIndex whose value is the array index (§3.7.4) of the parent logicalLocation object within theRun.logicalLocations (§3.14.16).

If this logicalLocation object represents a top-level logical location, then parentIndex **SHALL** be absent.

NOTE: parentIndex makes it possible to navigate from the logicalLocation object representing a nested logical location to the logicalLocation objects representing each of its parent logical locations in turn, up to the top-level logical location.

EXAMPLE: In this example, the logical location n::f(void) is nested within the top-level logical location n. The logicalLocation object representing n::f(void) contains a parentIndex property that points to the object representing n; the object representing n does not contain a parentIndex property.

{ # A run object (§3.14).

"logicalLocations": [ # See §3.14.16.

{

"name": "f(void)", # See §3.31.4.

"fullyQualifiedName": "n::f(void)", # See §3.31.6.

"kind": "function", # See §3.31.8.

"parentIndex": 1

},

{

"name": "n",

"kind": "namespace"

}

]

}

## suppression object

### General

A suppression object describes a request to suppress a result.

The supported reasons for suppressing a result are:

* The developer has suppressed the result in the source code (see §3.32.2.1).
* The result is marked as suppressed in an external store such as a database (see §3.32.2.2).

NOTE: The treatment of suppressed results depends on the development environment within which the log file is used, for example, a build system, an integrated development environment (IDE), or a result management system. Typically, development environments do not expose suppressed results to the user. For example, they do not include them in build log files, display them in error lists, or include them in bug counts.

### kind property

A suppression object **SHALL** contain a property named kind whose value is a string with one of the following values, which the specified meanings.

#### suppressedInSource value

Some programming languages offer a syntactic construct for suppressing compiler warnings.

EXAMPLE: In C#, #pragma warning is such a construct.

If a suppression is the result of such a construct, kind **SHALL** have the value "suppressedInSource".

#### suppressedExternally value

Some development environments provide a persistent store, for example a database, containing historical information about the results from analysis tools. Such a store might offer the ability to mark a result as “suppressed,” meaning that if the result is encountered again, it is to be ignored.

If a suppression is the result of such externally persisted information, kind **SHALL** have the value "suppressedExternally".

#### underReview

This value indicates that the engineering team is discussing the issue to decide if they will suppress it.

#### suppressionRejected

This value indicates that the engineering team discussed the issue and decided not to suppress it,

### location property

A suppression object **MAY** contain a property named location whose value is a location object (§3.26) that specifies the location where the suppression is persisted.

NOTE: In the common scenario, a suppression is represented by a source code construct (which we will refer to as a “suppression construct”) such as an attribute or a specially formatted comment at the location where the result was detected. In this scenario, location is unnecessary, although it is permitted, because an end user who navigates from the result to the source code location will see the suppression attribute or comment near the relevant code.

Nevertheless, there are several scenarios where location is useful. Here are some examples:

When the suppression construct is placed in a separate compiled source file, kind (§3.32.2) is "suppressedInSource", and location.physicalLocation (§3.26.2) specifies the location of the suppression attribute in that separate file.

Even when the suppression construct is adjacent to the result line, location.physicalLocation can be useful because it allows you to include in the log file a source code snippet containing the suppression construct, using location.physicalLocation.region.snippet (§3.27.4, §3.28.13).

When a tool detects a result within a method, but the suppression construct is applied to some higher-level construct such as the enclosing class, then kind is again "suppressedInSource", location.logicalLocation (§3.26.3) can specify the construct to which the suppression was applied, and location.physicalLocation can still usefully specify the location of the suppression construct in the source file, since it is distant from the result.

In a similar case, a binary analysis tool that detected the suppression within an executable file’s metadata could provide location.logicalLocation even if it could not provide location.physicalLocation.

If a suppression is stored in a separate, non-compiled file, sometimes called a “sidecar file,” kind is "suppressedExternally", and location.physicalLocation specifies the location of the suppression within the sidecar file. The sidecar file might even be another SARIF file.

If a suppression is stored in a database, kind is again "suppressedExternally", and and location.physicalLocation might specify the URI of a query that returns the database information that describes the suppression.

### guid property

A suppression object **MAY** contain a property named guid whose value is a GUID-valued string (§3.5.4).

NOTE: This can be used, for example, to link a suppression object in a SARIF file to suppression information in a result management system’s database.

## codeFlow object

### General

A codeFlow object describes the progress of one more programs through one or more thread flows, which together result in the detection of a result in the system being analyzed. We define a thread flow as a temporally ordered sequence of code locations occurring within a single thread of execution, typically an operating system thread or a fiber. The thread flows in a code flow **MAY** lie within a single process, within multiple processes on the same machine, or within multiple processes on multiple machines.

EXAMPLE

{ # A result object (§3.25).

"codeFlows": [ # See §3.25.16.

{ # A codeFlow object (§3.33).

"message": { # See §3.33.2.

"text": "..."

},

"threadFlows": [ # See §3.33.3.

{ # A threadFlow object (§3.34).

"id": "thread-123", # See §3.34.2.

"message": { # See §3.34.3.

"text": "..."

},

"locations": [ # See §3.34.6.

{ # A threadFlowLocation object (§3.42).

"location": { # See §3.42.3.

"physicalLocation": { # See §3.26.2.

"artifactLocation": {

"uri": "ui/window.c",

"uriBaseId": "SRCROOT"

},

"region": {

"startLine": 42

}

}

},

"state": { # See §0.

"x": "42",

"y": "54",

"x + y": "96"

},

"nestingLevel": 0, # See §3.42.8.

"executionOrder": 2 # See §3.42.9.

}

]

}

]

}

]

}

### message property

A codeFlow object **MAY** contain a property named message whose value is a message object (§3.11) relevant to the code flow.

### threadFlows property

A codeFlow object **SHALL** contain a property named threadFlows whose value is an array of one or more threadFlow objects (§3.34), each of which describes the progress of a program through a single thread of execution such as an operating system thread or a fiber.

## threadFlow object

### General

A thread flow is a sequence of code locations that specify a possible path through a single thread of execution such as an operating system thread or a fiber.

For an example, see §3.33.1.

### id property

A threadFlow object **MAY** contain a property named id whose value is a string that uniquely identifies this threadFlow within its containing codeFlow object (§3.33).

NOTE: A tool might choose to use an operating system thread id for this purpose. However, if thread ids are reused on a single machine, or if the code flow includes thread flows from more than one machine, the thread id might not be unique.

### message property

A threadFlow object **MAY** contain a property named message whose value is a message object (§3.11) relevant to the thread flow.

### initialState property

A threadFlow object **MAY** contain a property named initialState whose value is an object (§3.6) each of whose properties is a string that represents the value of a relevant expression prior to the first location in the thread flow. This property, together with threadFlowLocation.state (§0), enables a SARIF viewer to present a debugger-like “watch window” experience as the user traverses a thread flow.

This property **SHOULD NOT** include expressions whose value remains constant throughout the thread flow. Such values **SHOULD** be stored in the immutableState property (§3.34.5).

For details of how properties within a “state” object are represented, see EXAMPLE 1 in §0.

### immutableState property

A threadFlow object **MAY** contain a property named immutableState whose value is an object (§3.6) each of whose properties is a string that represents the value of a relevant expression that remains constant throughout the thread flow.

EXAMPLE: In this example, immutableState holds the values of the HTTP headers of the web request that caused the thread flow. Note that, although the property names in this example contain slashes, the property names are not formally specified as being hierarchical strings (§3.5.5).

{ # A threadFlow object.

"immutableState": {

"Headers/Host": "www.example.com",

"Headers/Accept-Language": "en-US",

"Headers/Pragma": "no-cached"

}

}

### locations property

A threadFlow object **SHALL** contain a property named locations whose value is an array of one or more threadFlowLocation objects (§3.42). Each element of the array **SHALL** represent a single location visited by the tool in the course of producing the result. This array does not need to include every location visited by the tool, but the elements that are present **SHALL** occur in the execution order that demonstrates the problem. The elements do need to be unique within the array.

NOTE: The locations array might include multiple identical elements if, for example, the analysis tool simulated the execution of a loop in the course of producing the result.

## graph object

### General

A graph object represents a directed graph, a network of nodes and directed edges that describes some aspect of the structure of the code (for example, a call graph). graph objects **MAY** be defined both at the run level in run.graphs (§3.14.19) and at the result level in result.graphs (§3.25.17).

A path through a graph, called a “graph traversal,” is represented by a graphTraversal object (§3.38).

### description property

A graph object **MAY** contain a property named description whose value is a message object (§3.11) that describes the graph.

### nodes property

A graph object **MAY** contain a property named nodes whose value is an array of zero or more unique (§3.7.3) node objects (§3.36) which represent the nodes of the graph.

### edges property

A graph object **MAY** contain a property named edges whose value is an array of zero or more unique (§3.7.3) edge objects (§3.37) which represent the edges of the graph.

## node object

### General

A node object represents a node in the graph represented by the containing graph object (§3.35).

### id property

A node object **SHALL** contain a property named id whose value is a string that uniquely identifies the node within the containing graph object (§3.35). id **SHALL** be unique among all nodes in the graph, regardless of nesting (see §3.36.5).

EXAMPLE: This graph is invalid because two nodes have the same id, even though the nodes are within unrelated nested graphs.

{ # A graph object (§3.35).

"nodes": [ # See §3.35.3.

{ # A node object.

"id": "n1",

"children": [ # See §3.36.5.

{

"id": "n3"

}

]

},

{

"id": "n2",

"children": [

{

"id": "n3" # INVALID: duplicate id.

}

]

}

],

...

}

### label property

A node object **MAY** contain a property named label whose value is a message object (§3.11) that provides a short description of the node.

### location property

A node object **SHOULD** have a property named location whose value is a location object (§3.26) that specifies the location associated with the node.

### children property

A node object **MAY** contain a property named children whose value is an array of zero or more unique (§3.7.3) node objects, referred to as “child nodes.”

Child nodes are logically subordinate to their containing node, and form a “nested graph” within that node.

## edge object

### General

An edge object represents a directed edge in the graph represented by the containing graph object (§3.35).

### id property

An edge object **SHALL** contain a property named id whose value is a string that uniquely identifies the edge within the containing graph object (§3.35).

### label property

An edge object **MAY** contain a property named label whose value is a message object (§3.11) that provides a short description of the edge.

### sourceNodeId property

An edge object **SHALL** contain a property named sourceNodeId whose value is a string that identifies the source node (the node at which the edge starts). It **SHALL** equal the id property (§3.36.2) of one of the node objects (§3.36) in the containing graph object (§3.35). It **MAY** equal the id of any node within the graph, regardless of nesting (see §3.36.5).

EXAMPLE: In this example, an edge connects two nodes defined in unrelated nested graphs.

{ # A graph object (§3.35).

"nodes": [ # See §3.35.3.

{ # A node object.

"id": "n1",

"children": [ # See §3.36.5.

{

"id": "n3"

}

]

},

{

"id": "n2",

"children": [

{

"id": "n4"

}

]

}

],

"edges": [ # See §3.35.4.

{

"sourceNodeId": "n3", # Source node and target node are in separate

"targetNodeId": "n4" # nested graphs: ok.

}

],

...

}

### targetNodeId property

An edge object **SHALL** contain a property named targetNodeId whose value is a string that identifies the target node (the node at which the edge ends). It **SHALL** equal the id property (§3.36.2) of one of the node objects (§3.36) in the containing graph object (§3.35). It **MAY** equal sourceNodeId (§3.37.4).

## graphTraversal object

### General

A graphTraversal object represents a “graph traversal,” that is, a path through a graph specified by a sequence of connected “edge traversals,” each of which is represented by an edgeTraversal object (§3.39). For an example, see §3.38.8.

### Constraints

Exactly one of the resultGraphIndex property (§3.38.3) and the runGraphIndex property (§3.38.4) **SHALL** be present.

### resultGraphIndex property

If a graphTraversal object represents the traversal of a graph object (§3.35) that resides in the theResult.graphs (§3.25.17), the graphTraversal object **SHALL** contain a property named resultGraphIndex whose value is the array index (§3.7.4) within theResult.graphs of that graph object.

### runGraphIndex property

If a graphTraversal object represents the traversal of a graph object (§3.35) that resides in theRun.graphs (§3.14.19), the graphTraversal object **SHALL** contain a property named runGraphIndex whose value is the array index within theRun.graphs of that graph object.

### description property

A graphTraversal object **MAY** contain a property named description whose value is a message object (§3.11) that describes the graph traversal.

### initialState property

A graphTraversal object **MAY** contain a property named initialState whose value is an object (§3.6) each of whose properties is a string that represents the value of a relevant expression at the point of entry to the graph. This property, together with edgeTraversal.finalState (§3.39.4), enables a SARIF viewer to present a debugger-like “watch window” experience as the user traverses a graph.

This property **SHOULD NOT** include expressions whose value remains constant throughout the traversal. Such values **SHOULD** be stored in the immutableState property (§3.38.7).

For details of how properties within a “state” object are represented, see EXAMPLE 1 in §0.

### immutableState property

A graphTraversal object **MAY** contain a property named immutableState whose value is an object (§3.6) each of whose properties is a string that represents the value of a relevant expression that remains constant throughout the traversal.

EXAMPLE: In this example, immutableState holds the values of the HTTP headers of the web request that caused the graph traversal. Note that, although the property names in this example contain slashes, the property names are not formally specified as being hierarchical strings (§3.5.5).

{ # A graphTraversal object.

"immutableState": {

"Headers/Host": "www.example.com",

"Headers/Accept-Language": "en-US",

"Headers/Pragma": "no-cached"

}

}

### edgeTraversals property

A graphTraversal object **MAY** contain a property named edgeTraversals whose value is an array of zero or more edgeTraversal objects (§3.39) which together represent the sequence of edges traversed during this graph traversal.

The edgeTraversal objects **SHALL** be connected end to end; that is, the target node of every traversed edge **SHALL** equal the source node of the next edge.

EXAMPLE: In this example, the graphTraversal contains two edgeTraversal objects. The id of the first traversed edge is "e1", which connects node "n1" to node "n2". The id of the second traversed edge is "e3", which connects node "n2" to node "n4". This is a valid graph traversal because the target node of each traversed edge is the source node of the next.

This example also demonstrates the usage of graphTraversal.initialState (§3.38.6) and edgeTraversal.finalState (§3.39.4).

{ # A result object (§3.25).

"graphs": [ # See §3.25.17.

{ # A graph object (§3.35).

"nodes": [ # See §3.35.3.

{ "id": "n1" }, # A node object (§3.36).

{ "id": "n2" },

{ "id": "n3" },

{ "id": "n4" }

],

"edges": [ # See §3.35.4.

{ # An edge object (§3.37).

"id": "e1", # See §3.37.2.

"sourceNodeId": "n1", # See §3.37.4.

"targetNodeId": "n2" # See §3.37.5.

},

{

"id": "e2",

"sourceNodeId": "n2",

"targetNodeId": "n3"

},

{

"id": "e3",

"sourceNodeId": "n2",

"targetNodeId": "n4"

}

]

}

],

"graphTraversals": [ # See §3.25.18.

{ # A graphTraversal object (§3.38).

"resultGraphIndex": 0, # See §3.38.3.

"initialState": { # See §3.38.6.

"x": "1",

"y": "2",

"x + y": "3”

},

"edgeTraversals": [ # See §3.38.8.

{ # An edgeTraversal object (§3.39).

"edgeId": "e1", # See §3.39.2.

"finalState": { # See §3.39.4.

"x": "4",

"y": "2",

"x + y": "6”

}

},

{

"edgeId": "e3",

"finalState": {

"x": "4",

"y": "7",

"x + y": "11”

}

}

]

}

]

}

## edgeTraversal object

### General

An edgeTraversal object represents the traversal of a single edge during a graph traversal.

### edgeId property

An edgeTraversal object **SHALL** contain a property named edgeId whose value is a string which equals the id property (§3.37.2) of one of the edge objects (§3.37) in the graph identified by the resultGraphIndex property (§3.38.3) or the runGraphIndex property (§3.38.4) of the containing graphTraversal object (§3.38).

### message property

An edgeTraversal object **MAY** contain a property named message whose value is a message object (§3.11) that contains a message to display to the user as the edge is traversed.

### finalState property

An edgeTraversal object **MAY** contain a property named finalState whose value is an object (§3.6) each of whose properties represents the value of a relevant expression after the edge has been traversed.

NOTE:This property, together with graphTraversal.initialState (§3.38.6), enables a viewer to present a debugger-like “watch window” experience as the user traverses a graph.

A SARIF viewer **SHALL** display only those properties that are explicitly present in the finalState property of the current edgeTraversal. It **SHALL NOT** assume that properties present in previous steps are still present with unchanged values.

For details of how properties within a “state” object are represented, see §0.

### stepOverEdgeCount property

An edgeTraversal object **MAY** contain a property named stepOverEdgeCount whose value is an integer specifying the number of edges a user can step over.

This property is intended to enable a viewing experience in which the user can either step over or step into the traversal of a nested graph (§3.36.5). Therefore, this property **SHOULD** be specified only on an edge that leads from a node to one of its child nodes, and its value **SHOULD** be the number of edges the user would need to traverse to return to the current nesting level.

If this property is present, a SARIF viewer **SHOULD** provide a visual cue informing the user that they have the option of either stepping over the current edge and into the nested graph, or of stepping over the entire traversal of the nested graph.

EXAMPLE: This example defines a graph containing two nested graphs, the first representing code locations in function A and the second representing locations in function B. Node na2 in function A represents a call to function B.

The example defines a graph traversal consisting of a set of edge traversals which start at node "na1" in function A, call into function B, and ultimately return to and continue execution in function A.

Suppose the user executes the first edge traversal, which traverses edge ea1.The next edge traversal has a stepOverEdgeCount property value of 4. Therefore, the SARIF viewer informs her that she can now choose to either step into function B by traversing edge "eab", or step over the function call by traversing 4 edges, the last of which (edge "eba") returns to function A at node "na3".

If she chooses to enter the nested graph, she will visit the following nodes, in this order:

[ na1, na2, nb1, nb2, nb3, na3, na4 ]

If she chooses not to enter the nested graph, the traversal of the edges

[ eab, eb1, eb2, eba ]

will be collapsed into a single “step over.” As a result, she will visit the following nodes, in this order:

[ na1, na2, na3, na4 ]

{ # A result object (§3.25).

"graphs": [ # See §3.25.17.

{ # A graph object (§3.35).

"nodes": [

{

"id": "functionA",

"children": [

{ "id": "na1" },

{ "id": "na2", "label": "Call functionB" },

{ "id": "na3" },

{ "id": "na4" }

]

},

{

"id": "functionB",

"nodes": [

{ "id": "nb1" },

{ "id": "nb2" },

{ "id": "nb3" }

],

}

]

"edges": [

{ "id": "ea1", "sourceNodeId": "na1", "targetNodeId": "na2" },

{ "id": "ea2", "sourceNodeId": "na2", "targetNodeId": "na3" },

{ "id": "eab", "sourceNodeId": "na2", "targetNodeId": "nb1" },

{ "id": "ea3", "sourceNodeId": "na3", "targetNodeId": "na4" },

{ "id": "eb1", "sourceNodeId": "nb1", "targetNodeId": "nb2" },

{ "id": "eb2", "sourceNodeId": "nb2", "targetNodeId": "nb3" },

{ "id": "eba", "sourceNodeId": "nb3", "targetNodeId": "na3" }

]

}

],

"graphTraversals": [ # See §3.25.18.

{ # A graphTraversal object (§3.38).

"resultGraphIndex": 0, # The graph being traversed.

"edgeTraversals": [

{ "edgeId": "ea1" },

{

"edgeId": "eab",

"stepOverEdgeCount": 4

},

{ "edgeId": "eb1" },

{ "edgeId": "eb2" },

{ "edgeId": "eba" },

{ "edgeId": "ea3" }

]

}

]

}

## stack object

### General

A stack object describes a single call stack. A call stack is a sequence of nested function calls, each of which is referred to as a stack frame.

### message property

A stack object **MAY** contain a property named message whose value is message object (§3.11) relevant to this call stack.

### frames property

A stack object **SHALL** contain a property named frames whose value is an array of zero or more stackFrame objects (§3.41). This array **SHALL** include every function call in the stack for which the tool has information, and the entries that are present **SHALL** occur in chronological order with the most recent (innermost) call first and the least recent (outermost) call last. The entries in this array do not need to be unique within the array.

NOTE 1: It is possible for the same frame to occur multiple times if the call stack includes a recursion.

NOTE 2: It is possible that the analysis tool will not have location information for every frame in the call stack. This might happen if, for example, application code for which location information is available calls into operating system code for which location information is not available, which in turn calls back into application code.

## stackFrame object

### General

A stackFrame object describes a single stack frame within a call stack (§3.40).

### location property

A stackFrame object **MAY** contain a property named location whose value is a location object (§3.26) specifying the location to which this stack frame refers.

### module property

A stackFrame object **MAY** contain a property named module whose value is a string containing the name of the module that contains the location to which this stack frame refers.

### threadId property

A stackFrame object **MAY** contain a property named threadId whose value is an integer which identifies the thread on which the code at the location specified by this object was executed.

### parameters property

A stackFrame object **MAY** contain a property named parameters whose value is an array of zero or more strings representing the parameters of the function call represented by this stack frame.

## threadFlowLocation object

### General

A threadFlowLocation object represents a location visited by an analysis tool in the course of simulating or monitoring the execution of a program.

### index property

Depending on the circumstances, a threadFlowLocation object either **MAY**, **SHALL NOT**, or **SHALL** contain a property named index whose value is a non-negative integer that specifies the array index (§3.7.4) within theRun.threadFlowLocations (§3.14.18) of a threadFlowLocation object that provides additional properties for the current threadFlowLocation object. We refer to the object in theRun.threadFlowLocations as the “cached object.”

If the current object is an element of theRun.threadFlowLocations, then index **MAY** be present. If present, its value **SHALL** be the index of the current object within run.threadFlowLocations.

Otherwise, if theRun.threadFlowLocations is absent, or if it does not contain a cached object for the current object, then index **SHALL NOT** be present.

Otherwise (that is, if the current object is not an element of run.threadFlowLocations, and run.threadFlowLocations does contain a cached object for the current object), then index **SHALL** be present, and its value **SHALL** be the index with theRun.threadFlowLocations of the cached object.

If index is present, and if the cached object contains any property that is absent from the current object, then the current object **SHALL** take the value of that property from the cached object.

NOTE: This allows a SARIF producer to reduce the size of the log file by caching properties shared by several threadFlowLocation objects, and specifying only the properties that differ in the current object. This could be useful in the case of a loop, where the same physical location is encountered many times, the only difference being variable values in the state property (§0).

### location property

If location information is available, a threadFlowLocation object **SHALL** contain a property named location whose value is a location object (§3.26) that specifies the location to which the threadFlowLocation object refers. If location information is not available, location **SHALL** be absent.

There are analysis tools whose native output format includes the equivalent of a SARIF code flow, but which do not provide location information for every step in the code flow. A SARIF converter for such a format might not be able to populate location. However, if the native output format associates a human readable message with such a step, the SARIF converter **SHOULD** create a location object and populate only its message property (§3.26.4). A SARIF direct producer which creates such code flows **SHOULD** populate location.message, even if no actual location information is available.

EXAMPLE: In this example, a file is locked by another program before a thread attempts to write to it. The analysis tool has no location information for the other program; in fact, the analysis tool might merely be simulating an execution sequence in which a *hypothetical* external program locks the file. Nevertheless, it provides a helpful message.

Note the use of executionOrder (§3.42.9) to ensure that the location in the external program executes before the location in the program being analyzed.

{ # A codeFlow object (§3.33).

"threadFlows": [ # See §3.33.3.

{ # A threadFlow object (§3.34).

"message": { # See §3.34.3.

"text": "An external program."

},

"locations": [ # See §3.34.6.

{ # A threadFlowLocation object.

"executionOrder": 1,

"location": { # A location object with only a message.

"message": {

"text": "File is now locked."

}

}

}

]

},

{ # Another threadFlow object.

"message": {

"text": "The program being analyzed."

},

"locations": [

...

{

"executionOrder": 2,

"message": {

"text": "Attempt to write to the file."

},

"location": {

"physicalLocation": {

"artifactLocation": {

"uri": "io/logger.c",

"uriBaseId": "SRCROOT"

},

"region": {

"startLine": 42,

"snippet": {

"text": " fprintf(fd, "test\\n");\n"

}

}

}

}

}

]

}

]

}

### module property

A threadFlowLocation object **MAY** contain a property named module whose value is a string containing the name of the module that contains the code location specified by this object.

### stack property

A threadFlowLocation object **MAY** contain a property named stack whose value is a stack object (§3.40) that represents the call stack leading to this location.

### kinds property

A threadFlowLocation object **MAY** contain a property named kinds whose value is an array of unique (§3.7.3) strings that describe the meaning of this location. The strings **SHOULD** be a human-readable (as opposed to, for example, GUIDs or hash values).

When possible, SARIF producers **SHOULD** use the following values, with the specified meanings.

Verbs:

* "acquire": Gain ownership of something.
* "release": Relinquish ownership of something.
* "enter": Entry point to a section of the program such as a function.
* "exit": Exit point from a section of the program such as a function.
* "call": Point of call into a section of the program such as a function.
* "return": Point of return from section of the program such as a function.
* "branch": Conditional transfer of control.

NOTE: These values are typically combined with nouns from the list below, as in the examples below.

Nouns:

* "taint": Value obtained from user input.
* "function": Section of a program that can be called into and returned from.
* "handler": Code invoked in response to an exception, signal, or event.
* "lock": Limits access to a resource.
* "memory": Portion of computer’s internal storage.
* "resource": Anything that can be acquired and released.
* "scope": Section of a program that limits the visibility of variables defined within it.

Miscellaneous:

* "implicit": Code was invoked implicitly, for example by a garbage collector.
* "false": A condition evaluated to false.
* "true": A condition evaluated to true.
* "caution": Execution of the code at this location in the current circumstance requires care.
* "danger": Execution of the code at this location in the current circumstance is dangerous.
* "unknown": The state of an item is not known.
* "unreachable": Code at this location is unreachable.

If none of these values are appropriate, a SARIF producer **MAY** use any value. The interpretations of values other than those above depends on the producer. A SARIF consumer that wishes to take action based on such values **SHALL** examine theTool to determine if it (the consumer) knows how to interpret them, unless the consumer has out of band information.

A SARIF producer **MAY** provide additional kind-dependent information by populating threadFlowLocation.properties with properties whose names and values depend on the kind. A SARIF consumer that knows how to interpret kinds for this tool **MAY** use this additional information.

EXAMPLE 1: In this example, tainted data enters the system at this location.

"kinds": [

"acquire",

"taint"

]

EXAMPLE 2: In this example, the “taint” state of a data item at this location is unknown:

"kinds": [

"taint",

"unknown"

]

EXAMPLE 3: In this example, control leaves a function at this location.

"kinds": [

"exit",

"function"

]

### state property

A threadFlowLocation object **MAY** contain a property named state whose value is an object (§3.6) in which each property name represents an expression relevant to the location in the context of the code flow, and the corresponding property value is a string that specifies the value of that expression.

NOTE:This property enables a SARIF viewer to present a debugger-like “watch window” experience as the user navigates through a code flow.

A SARIF viewer **SHALL** display only those properties that are explicitly present in the state property of the current threadFlowLocation. It **SHALL NOT** assume that properties present in previous steps are still present with unchanged values.

EXAMPLE 1: In this example, the state property captures the values of the expressions "x", "y", and "x + y".

{ # A threadFlowLocation object.

"state": {

"x": "42",

"y": "54",

"x + y": "96"

}

}

The format of each property name **SHALL** be consistent with the syntax of an expression in the programming language in which the code being analyzed was written. Each property value **SHALL** be a string whose format is consistent with the syntax of a value in the programming language in which the code being analyzed was written

EXAMPLE 2: In C++, a property name within the state object might be:

* A variable name such as "index".
* An array element reference such as "names[index]".
* An object property reference such as "names[index]->first".
* Any other expression that produces a value.

EXAMPLE 3: In C++, a property value within the state object might be:

* An integer such as "42" (note that the property value is a string).
* A string such as "\"John\"" (the double quotes are escaped as they would be in a JSON serialization; other serializations might represent the double quotes differently).
* A Boolean such as "true".

### nestingLevel property

A threadFlowLocation object **MAY** contain a property named nestingLevel whose value is an integer that represents any type of logical containment hierarchy among the threadFlowLocation objects in the threadFlow. Typically, it represents function call depth.

A viewer that renders a threadFlow **SHOULD** provide a visual representation of the value of nestingLevel. Typically, this would be an indentation indicating the depth of each location in the call tree.

### executionOrder property

A threadFlowLocation object **MAY** contain a property named executionOrder whose value is a positive integer that represents the temporal order in which execution reached this location, across all threadFlowLocation objects within all threadFlow objects belonging to a single codeFlow (§3.33). executionOrder values are assigned in increasing order of time; for example, execution reaches a threadFlowLocation whose executionOrder is 2 occurs before it reaches a threadFlowLocation whose executionOrder is 3. If two threadFlowLocations in different threadFlow objects within the same codeFlow have the same value for executionOrder, it means that execution reached both of those locations simultaneously. For that reason, values of executionOrder within a single threadFlow **SHALL** be unique.

It is only necessary to assign a value to executionOrder when the temporal ordering of a threadFlowLocation relative to a location in a different threadFlow is significant to the detection of a result.

If this property is absent, it **SHALL** default to 0, which is not otherwise a valid value for executionOrder.

### executionTimeUtc property

A threadFlowLocation object **MAY** contain a property named executionTimeUtc whose value is a string in the format specified in §3.9, specifying the UTC date and time at which the thread of execution through the code reached this location.

### importance property

A threadFlowLocation **MAY** contain a property named importance whose value is a string that specifies the importance of this threadFlowLocation in understanding the code flow.

The importance property **SHALL** have one of the following values, with the specified meanings:

* "important": this location is important for understanding the code flow.
* "essential": this location is essential for understanding the code flow.
* "unimportant": this location contributes to a more detailed understanding of the code flow but is not normally needed.

If this property is absent, it **SHALL** be considered to have the value "important".

NOTE: A viewer might use this property to offer the user three options for viewing a lengthy code flow:

* A “normal view,” which omits locations whose importance property is "unimportant".
* An “abbreviated view,” which displays only those locations whose importance property is "essential".
* A “verbose view,” which displays all the locations in the code flow.

## resultProvenance object

### General

A resultProvenance object contains information about the how and when theResult was detected.

NOTE: This information is useful to various human and automated participants in an engineering system. For example:

* A build engineer might use the information to understand the specific tool invocation that produced the result, for example, if the violated rule should not have been configured to run at all.
* A developer reviewing results might use the information to determine how long an issue has existed in the code.
* A result management system might be responsible for associating logically identical results from one run to the next, making it possible for the developer to determine how long the result has existed. Such a result management system might populate this information.

### firstDetectionTimeUtc property

A resultProvenance object **MAY** contain a property named firstDetectionTimeUtc whose value is a string in the format specified in §3.9, specifying the UTC date and time at which the result was first detected. It **SHOULD** specify the start time of the run in which the result was first detected, as opposed to, for example, the time within the run at which the result was actually generated.

NOTE: Using the run’s start time makes it possible to group together results that were first detected in the same run.

### lastDetectionTimeUtc property

A resultProvenance object **MAY** contain a property named lastDetectionTimeUtc whose value is a string in the format specified in §3.9, specifying the UTC date and time at which the result was most recently detected. It **SHOULD** specify the start time of the run in which the result was most recently detected, as opposed to, for example, the time within the run at which the result was actually generated.

NOTE: Using the run’s start time makes it possible to group together results that were detected in the same run.

If lastDetectionTimeUtc is absent, its default value **SHALL** be determined as follows:

1. If run.invocations is present, and if the startTimeUtc property (§3.19.7) is present on any of the invocation objects (§3.19) in that array, then the default is the earliest of those times.
2. Otherwise, there is no default.

### firstDetectionRunGuid property

A resultProvenance object **MAY** contain a property named firstDetectionRunGuid whose value is a GUID-valued string (§3.5.4) which **SHALL** equal the automationDetails.guid property (§3.14.3, §3.16.5) of the run in which theResult was first detected (either the current run or some previous run).

### lastDetectionRunGuid property

A resultProvenance object **MAY** contain a property named lastDetectionRunGuid whose value is a GUID-valued string (§3.5.4) which **SHALL** equal the automationDetails.guid property (§3.14.3, §3.16.5) of the run in which theResult was most recently detected (either the current run or some previous run).

### invocationIndex property

If theRun.invocations (§3.14.11) is present, a resultProvenance object **MAY** contain a property named invocationIndex whose value is the array index (§3.7.4) within the invocations property of the invocation object (§3.19) that describes the tool invocation as a result of which theResult was detected.

If theRun.invocations is absent, invocationIndex **SHALL** be absent.

NOTE 1: The purpose of this property is to allow a result to be associated with the tool invocation that produced it.

If invocationIndex is absent and theRun.invocations is present and contains a single element, it **SHALL** default to 0; otherwise it **SHALL** default to -1, which is otherwise not a valid value for this property.

NOTE 2: This provides a sensible default in the common case where there is only a single tool invocation in the run.

### conversionSources property

Some analysis tools produce output files that describe the analysis run as a whole; we refer to these as “per-run” files. Some tools produce one or more output files for each result; we refer to these as “per-result” files. Some tools produce both per-run and per-result files.

A resultProvenance object **MAY** contain a property named conversionSources whose value is an array of one or more unique (§3.7.3) physicalLocation objects (§3.27).

If theResult was produced by a converter, and if the analysis tool whose output was converted to SARIF produced any per-result files for this result, then the physicalLocation objects in the array **SHALL** specify the relevant portions of the per-result files for this result.

Otherwise (that is, if the run object was not produced by a converter, or if there were no per-run files for this result), then if conversionProvenance is present, its value **SHALL** be an empty array.

Per-run files are handled by the conversion.analysisToolLogFiles property (§3.21.4).

NOTE: This property is intended to be useful to developers of converters, to help them debug the conversion from the analysis tool’s native output format to the SARIF format.

EXAMPLE: Given this analysis tool’s output file:

<?xml version="1.0" encoding="UTF-8"?>

<problems>

<problem>

<file></file>

<line>242</line>

...

<problem\_class ...>Assertions</problem\_class>

...

<description>Assertions are unreliable. ...</description>

</problem>

</problems>

a SARIF converter might transform it into the following SARIF log file:

{

...

"runs": [

{

"tool": {

"driver": {

"name": "CodeScanner"

}

},

"conversion": { # A conversion object (see §3.20)

...

},

"results": [

{

"ruleId": "Assertions",

"message": {

"text": "Assertions are unreliable. ..."

},

...

"provenance": { # See §3.25.27.

"conversionSources": [ # An array of physicalLocation objects

{ # (§3.27).

"artifactLocation": { # See §3.27.3.

"uri": "CodeScanner.log",

"uriBaseId": "$LOGSROOT"

},

"region": { # See §3.27.4.

"startLine": 3,

"startColumn": 3,

"endLine": 12,

"endColumn": 13,

"snippet": {

"text": "<problem>\n ... \n </problem>"

}

}

}

],

...

}

}

]

}

]

}

## reportingDescriptor object

### General

A reportingDescriptor object contains information that describes a “reporting item” generated by a tool. A reporting item is either a result produced by the tool’s analysis (see §3.25), or a notification of a condition encountered by the tool (§3.52). We refer to this descriptive information as “reporting item metadata.” When referring to the metadata that describes a result, we use the more specific term “rule metadata.”

Some of the properties of the reportingDescriptor object are interpreted differently depending on whether the object represents a rule or a notification. The description of each property will specify any such differences.

### Constraints

Either the shortDescription property (§3.44.9) or the fullDescription property (§3.44.10) or both **SHALL** be present.

### id property

A reportingDescriptor object **SHALL** contain a property named id whose value is a string. In the case of a rule, id **SHALL** contain a containing a stable, opaque identifier for the rule. In the case of a notification, id need not be a stable, opaque identifier; it **MAY** be a user-readable identifier.

EXAMPLE: "id": "CA2101"

NOTE: Rule identifiers must be stable for two reasons:

* So build automation scripts can refer to specific checks, for example, to disable them, without the risk of a script breaking if a rule id changes.
* So result management systems can compare results from one run to the next, without erroneously designating results as “new” because a rule id has changed.

Rule identifiers should be opaque – that is, they should not convey information to a user – because a rule's implementation might change over time. Suppose a rule id is "DoNotDoXOrY", suppose circumstances change so that “Y” is now acceptable, and suppose the implementation of the rule changes accordingly. Because the rule id must not change, the string "DoNotDoXOrY" will continue to be persisted to logs, where it will convey outdated guidance to users in a way that an opaque identifier such as "CA2101" would not.

In contrast to rule identifiers, notification identifiers need not be stable or opaque, because the reasoning that leads to those requirements for rules does not apply to notifications. A tool notification with level "error" should always be treated as a failure, and tools should not allow them to be disabled. And tool authors are free to change the notification ids at any time, so there is no reason for them to be opaque; to the contrary, they are more useful if they convey information to the user.

### deprecatedIds property

A reportingDescriptor object **MAY** contain a property named deprecatedIds whose value is an array of zero or more unique (§3.7.3) strings, each of which contains an id (see §3.44.3) by which this reporting item was known in some previous version of the analysis tool.

NOTE: This property is most useful for rules. It addresses the scenario where rule ids change from one version of a tool to the next. For example, a tool developer might decide that a rule is too general, covering too many concepts. In the next version of the tool, the tool developer might break this rule into a set of more specific rules.

Now the result management system has the problem of matching results between the newer and the older versions of the tool. deprecatedIds solves this problem.

EXAMPLE: In this example, version 1 of an analysis tool defines rule CA1000. A run of this tool finds two results.The result management system decides that neither result was previously detected, so it marks them as with "baselineState": "new" (§3.25.22), producing this log:

{

"tool": {

"driver": {

"name": "CodeScanner",

"version": "1",

"rules": [

{

"id": "CA1000",

...

}

]

}

},

"results": [

{

"ruleId": "CA1000",

"rule": {

"index": 0

},

"baselineState": "new",

...

},

{

"ruleId": "CA1000",

"rule": {

"index": 0

},

"baselineState": "new",

...

}

]

}

The engineering team decides that these results are false positive, so they add in-source suppressions, for example (in C#):

[SuppressMessage("CA1000", ...)]

...

[SuppressMessage("CA1000", ...)]

Now the tool developers decide that rule CA1000 is too broad, so in version 2 of the tool, they divide it into two new rules, CA1001 and CA1002. The engineering team runs the new tool, and the result management system performs result matching, producing this log:

{

"tool": {

"driver": {

"name": "CodeScanner",

"version": "2",

"rules": [

{

"id": "CA1001",

"deprecatedIds": [

"CA1000"

],

...

},

{

"id": "CA1002",

"deprecatedIds": [

"CA1000"

],

...

}

]

}

},

"results": [

{

"ruleId": "CA1001",

"rule": {

"index": 0

},

"baselineState": "existing",

"suppressions": [

{

"kind": "suppressedInSource"

}

],

...

},

{

"ruleId": "CA1002",

"rule": {

"index": 1

},

"baselineState": "existing",

"suppressions": [

{

"kind": "suppressedInSource"

}

],

...

}

]

}

There are a few things to notice:

* In tool.driver.rules, each of the new rules is associated with its id from the previous tool version.
* As a result, the analysis tool can determine that the in-source suppressions still apply, even though the rule ids have changed, so it correctly marks each result with "suppresionStates": [ "suppressedInSource" ].
* Furthermore, the result management system can determine that these are the same results it saw in the previous run, so it correctly marks them with "baselineState": "existing".

### guid property

A reportingDescriptor object **MAY** contain a property named guid whose value is a GUID-valued string (§3.5.4) that uniquely identifies the descriptor.

### deprecatedGuids property

A reportingDescriptor object **MAY** contain a property named deprecatedGuids whose value is an array of zero or more unique (§3.7.3) GUID-valued strings (§3.5.4) each of which was used by a previous version of the tool as the value of the guid property (§3.44.5) for this object.

### name property

A reportingDescriptor object **MAY** contain a property named name whose value is a localizable string (§3.5.2) containing an identifier that is understandable to an end user. If the name of a rule contains implementation details that change over time, a tool author might alter a rule's name (while leaving the stable id property (§3.44.3) unchanged).

NOTE: A rule name is suitable in contexts where a readable identifier is preferable and where the lack of stability is not a concern.

EXAMPLE: "name": "SpecifyMarshalingForPInvokeStringArguments"

### deprecatedNames property

A reportingDescriptor object **MAY** contain a property named deprecatedNames whose value is an array of zero or more unique (§3.7.3) localizable (§3.5.2) strings each of which was used by a previous version of the tool as the value of the name property (§3.44.7) for this object.

The array elements **SHALL** occur in the same order in every language translation.

### shortDescription property

A reportingDescriptor object **MAY** contain a property named shortDescription whose value is a localizable multiformatMessageString object (§3.12, §3.12.2) that provides a concise description of the reporting item. The shortDescription property **SHOULD** be a single sentence that is understandable when visible space is limited to a single line of text.

EXAMPLE:

{ # A reportingDescriptor object

"shortDescription": {

"text": "Specify marshaling for P/Invoke string arguments"

}

}

### fullDescription property

A reportingDescriptor object **SHOULD** contain a property named fullDescription whose value is a localizable multiformatMessageString object (§3.12, §3.12.2) that comprehensively describes the reporting item.

The fullDescription property **SHOULD**, as far as possible, provide details sufficient to enable resolution of any problem indicated by the reporting item.

The first sentence of fullDescription **SHOULD** provide a concise description of the reporting item, suitable for display in cases where available space is limited. Tools that construct fullDescription in this way do not need to provide a value for shortDescription (§3.44.9). Tools that do not construct fullDescription in this way **SHOULD** provide a value for shortDescription, because otherwise, the initial portion of fullDescription that a viewer displays where available space is limited might not be understandable.

### messageStrings property

A reportingDescriptor object **MAY** contain a property named messageStrings whose value is an object (§3.6) consisting of a set of properties with arbitrary names, each of whose values is a localizable multiformatMessageString object (§3.12, §3.12.2).

If the reportingDescriptor object defines a rule, the set of property names appearing in the messageStrings property **SHALL** contain at least the set of strings which occur as values of result.message.messageId properties (§3.25.11, §3.11.10) in the current run object. The messageStrings property **MAY** contain additional properties whose names do not appear as the value of the result.message.messageId property for any result object in the run.

If the reportingDescriptor object describes a notification, the set of property names appearing in the messageStrings property **SHALL** contain at least the set of strings which occur as values of notification.message.messageId for any notification object in the run.

NOTE: Additional properties are permitted in the messageStrings property for the convenience of tool vendors, who might find it easier to emit the entire set of messages defined in the reporting metadata, rather than restricting it to those messages that happen to appear in the log file.

EXAMPLE:

{ # A reportingDescriptor object for a rule.

"messageStrings": {

"objectCreation": { # A multiformatMessageString object (§3.12).

"text": "{0} creates a new instance of {1} which is never used.

Pass the instance as an argument to another method,

assign the instance to a variable,

or remove the object creation if it is unnecessary."

},

"stringReturnValue": {

"text": "{0} calls {1} but does not use the new string

instance that the method returns.

Pass the instance as an argument to another method,

assign the instance to a variable,

or remove the call if it is unnecessary."

}

}

}

### helpUri property

A reportingDescriptor object **MAY** contain a property named helpUri whose value is a localizable string (§3.5.2) containing the absolute URI [[RFC3986](#RFC3986)] of the primary documentation for the reporting item.

NOTE 1: The documentation might include examples, contact information for the authors, and links to additional information.

NOTE 2: This property is localizable so that help information in different languages can be viewed at different URIs.

### help property

A reportingDescriptor object **MAY** contain a property named help whose value is a localizable multiformatMessageString object (§3.12, §3.12.2) which provides the primary documentation for the reporting item.

NOTE: This property is useful when help information is not available at a URI, for example, in the case of a custom rule written by a developer, as opposed to one supplied by the tool vendor.

### defaultConfiguration property

A reportingDescriptor object **MAY** contain a property named defaultConfiguration whose value is a reportingConfiguration object (§3.45).

If this property is absent, it **SHALL** be taken to be present, and its properties **SHALL** be taken to have the default values specified in §3.45.

The rule- or notification-specific configuration parameters for a reportingDescriptor, if any, **SHALL NOT** be stored in its property bag (§3.8) Rather, they **SHALL** be stored in defaultConfiguration.parameters (§3.45.5).

### taxa property

If a reportingDescriptor object represents a rule, it **MAY** contain a property named taxa whose value is an array of unique (§3.7.3) reportingDescriptorReference objects (§3.47) each of which declares a taxon into which every result which violates the rule described by this reportingDescriptor object **SHALL** fall. Otherwise, taxa **SHALL** be absent.

A rule **MAY** fall into multiple taxa from multiple taxonomies.

For the explanation and an example of how rule taxa are applied to results, see §**Error! Reference source not found.**.

### optionalTaxa

If a reportingDescriptor object represents a rule, it **MAY** contain a property named optionalTaxa whose value is an array of unique (§3.7.3) reportingDescriptorReference objects (§3.47) each of which declares a taxon into which results which violates the rule described by this reportingDescriptor object **MAY** optionally fall. Otherwise, optionalTaxa **SHALL** be absent.

A rule **MAY** fall into multiple taxa from multiple taxonomies.

For the explanation and an example of how rule taxa are applied to results, see §**Error! Reference source not found.**.

## reportingConfiguration object

### General

A reportingConfiguration object contains the information in a reportingDescriptor (§3.44) that a SARIF producer can modify at runtime, before executing its scan. We refer to the reportingDescriptor object whose configuration is established or modified by a reportingConfiguration object as theDescriptor.

When a reportingConfiguration object appears as the value of theDescriptor.defaultConfiguration (§3.44.14), it specifies theReportingDescriptor’s default configuration. When a reportingConfiguration object appears as the value of configurationOverride.configuration (§3.46.3), it overrides the default values in the reportingDescriptor identified by configurationOverride.reportingDescriptorReference (§3.46.2).

For an example, see §3.45.5.

### enabled property

A reportingConfiguration object **MAY** contain a property named enabled whose value is a Boolean that specifies whether the condition described by theDescriptor was checked for during the scan.

If this property is absent, it **SHALL** default to true.

EXAMPLE: In this example, a tool allows the user to enable or disable rules or notifications:

SecurityScanner --disable "SEC4002,SEC4003" --enable SEC6012

### level property

A reportingConfiguration object **MAY** contain a property named level whose value is one of the strings "warning", "error", or "note", with the same meanings as when those strings appear as the value of result.level (§3.25.10) or notification.level (§3.52.6).

If level is absent, it **SHALL** default to "warning".

If theDescriptor describes a rule, then if level is present, it **SHALL** provide the value for the level property of any result object (§3.25) whose rule property (§3.25.7), either explicitly supplied or inferred from its default, identifies theDescriptor and which does not itself specify a level property. For details of the configuration property resolution procedure, see §3.25.10 (which illustrates the procedure for the specific case of the result.level property).

If theDescriptor describes a notification, then if level is present, it **SHALL** provide the value for the level property of any notification object (§3.52) whose descriptor property (§) identifies theDescriptor and which does not itself specify a level property.

EXAMPLE: In this example, a tool allows the user to override a rule or notification’s default level:

WebScanner --level "WEB1002:error,WEB1005:warning"

### rank property

A reportingConfiguration object **MAY** contain a property named rank whose value is a number between 0.0 and 100.0 inclusive, with the same interpretation as the value of the result.rank (§3.25.23).

If rank is absent, it **SHALL** default to -1.0, which is otherwise not a valid value for this property.

If theDescriptor describes a rule, then if rank is present, it **SHALL** provide the value for the rank property of any result object (§3.25) whose rule property (§3.25.7), either explicitly supplied or inferred from its default, identifies theDescriptor and which does not itself specify a rank property.

rank is not applicable to notifications.

### parameters property

A reportingConfiguration object **MAY** contain a property named parameters whose value is a property bag (§3.8). This allows a reportingDescriptor object (§) to define configuration information that is specific to that descriptor.

EXAMPLE: In this example, a rule that specifies the maximum permitted source line length is parameterized by the maximum length.

{ # A reportingDescriptor object (§3.44).

"id": "SA2707",

"name": {

"text": "LimitSourceLineLength"

},

"shortDescription": {

"text": "Limit source line length for readability."

},

"defaultConfiguration": {

"enabled": true,

"level": "warning",

"parameters": {

"maxLength": 120

}

}

}

The rule provides a default value, but the tool allows the user to override it:

StyleScanner \*.c --rule-config "SA2707:maxLength=80"

## configurationOverride object

### General

A configurationOverride object modifies the effective runtime configuration of a specified reportingDescriptor object (§3.44), which we refer to as theDescriptor.

The configurationOverride object’s reportingDescriptorReference property (§3.46.2) identifies theDescriptor. Its configuration property (§3.46.3) overrides the values specified in the theDescriptor.defaultConfiguration (§3.44.14).

EXAMPLE: In this example, rule CA2101 is treated as a warning rather than an error.

{ # A run object (§3.14).

"tool": { # See §3.14.6.

"driver": { # See §3.17.2.

"name": "CodeScanner",

"rules": [ # See §3.18.21.

{ # A reportingDescriptor object (§3.44).

"id": "CA2101",

"defaultConfiguration": {

"level": "error"

}

}

]

}

},

"invocations": [ # See §3.14.11.

{ # An invocation object (§3.19).

"ruleConfigurationOverrides": [ # See §3.19.5.

{ # A configurationOverride object (§3.46).

"reportingDescriptorReference": { # See §3.46.2.

"index": 0

},

"configuration": { # See §3.46.3.

"level": "warning"

}

}

]

}

]

}

### reportingDescriptorReference property

A configurationOverride object **SHALL** contain a property named reportingDescriptorReference whose value is a reportingDescriptorReference object (§3.47) that identifies the reportingDescriptor (§3.44) whose runtime configuration is to be modified, which we refer to as theDescriptor.

### configuration property

A configurationOverride object **SHALL** contain a property named configuration whose value is a reportingConfiguration object (§3.45) each of whose properties overrides the corresponding property in theDescriptor.defaultConfiguration (§3.44.14). If any property of configuration is absent, the corresponding property of theDescriptor.defaultConfiguration is respected.

## reportingDescriptorReference object

### General

A reportingDescriptorReference object identifies a particular reportingDescriptor object (§3.44), which we refer to as theDescriptor, among all reportingDescriptor objects defined by theTool, including those defined by theTool.driver (§3.17.2) and theTool.extensions (§3.17.3).

In some cases, there is no reportingDescriptor object associated with a reportingDescriptorReference object. In that case, the reportingDescriptorReference object **SHALL** contain only the id property (§3.47.4), and theDescriptor does not exist.

EXAMPLE: In this example, a tool emits a tool execution notification that refers to a rule. The tool does not provide rule metadata. Therefore associatedRule (§3.52.3) contains only an id property, whose value is the id of the rule that failed. Similarly, the tool does not provide metadata about its notifications, so "descriptor" (§3.52.2) contains only the id of the notification.

{ # An invocation object (§3.19).

"toolExecutionNotifications": [ # See §3.19.21.

{ # A notification object (§3.52).

"descriptor": { # See §3.52.2.

"id": "CTN9999"

},

"associatedRule": { # See §.3.52.3

"id": "C2001"

},

"level": "error",

"message": {

"text": "Exception evaluating rule 'C2001'. Rule disabled;

run continues."

}

}

]

}

### Constraints

At least one of index (§3.47.5) and guid (§3.47.6) **SHALL** be present. If both are present, they **SHALL** identify the same reportingDescriptor object (§3.44).

### reportingDescriptor lookup

theDescriptor **SHALL** be located within the toolComponent object (§3.18) identified by the toolComponent property (§3.47.7), which we refer to as theComponent. The procedure for looking up a toolComponent from a toolComponentReference is described in §3.48.2.

theDescriptor **SHALL** be located either within theComponent.rules (§3.18.21) or theComponent.notifications (§3.18.22), according to this table:

|  |  |
| --- | --- |
| If the reportingDescriptorReference  occurs in: | … then theDescriptor is an element of: |
| invocation.ruleConfigurationOverrides (§3.19.5) | rules |
| invocation.notificationConfigurationOverrides (§3.19.6) | notifications |
| result.rule (§3.25.7) | rules |
| notification.descriptor (§3.52.2) | notifications |
| notification.associatedRule (§3.52.3) | rules |

### id

A reportingDescriptorReference object **MAY** contain a property named id whose value is a hierarchical string (§3.5.5) that either equals theDescriptor.id (§3.44.3) or equals theDescriptor.id plus one additional hierarchical component.

NOTE: This property does not participate in the lookup, but its presence improves the readability of the log file at the expense of increased file size.

If id is absent and theResult.ruleId (§3.25.5) is present, then id **SHALL** default to theResult.ruleId. If both are present, they **SHALL** be equal.

For more information about the semantics of id when theDescriptor is a rule, in particular the usage of the hierarchical components of id, see the description of result.ruleId (§3.25.5).

EXAMPLE: In this example, the first result object is valid because rule.id (inherited from ruleId) equals theDescriptor.id. The second result object is also valid because rule.id (this time specified directly) equals theDescriptor.id plus one additional hierarchical component ("ghi"). The third result object is invalid because theDescriptor.id is not a “component-wise” prefix of rule.id. The fourth result object is invalid because ruleId does not equal rule.id.

{ # A run object (§3.14).

"tool": { # See §3.14.6.

"driver": { # See §3.17.2.

"name": "CodeScanner",

"rules": [ # See §3.18.21.

{ # A reportingDescriptor object (§3.44).

"id": "abc/def", # See §3.44.3.

...

},

...

]

}

},

"results": [ # See §3.14.20.

{ # A result object (§3.25).

"ruleId": "abc/def", # See §3.25.5.

"rule": {

"index": 0

},

},

{

"rule": {

"id": "abc/def/ghi",

"index": 0

}

},

{

"rule": {

"id": "abc/defg", # INVALID: theDescriptor.id is not a

"index": 0 # "component-wise" prefix of id.

}

},

{

"ruleId": "abc/def",

"rule": {

"id": "abc/defg/hij", # INVALID: Not equal to ruleId.

"index": 0

}

]

}

### index

A reportingDescriptorReference object **MAY** contain a property named index whose value is the array index (§3.7.4) into theComponent.rules (§3.18.21) or theComponent.notifications (§3.18.22), according to the table in §3.47.3.

EXAMPLE 1: In this example, there is more than one rule with id CA1711. index uniquely specifies the relevant rule, whether or not there are multiple rules with the same id.

{ # A run object (§3.14).

"tool": { # See §3.14.6.

"driver": { # See §3.17.2.

"name": "CodeScanner",

"rules": [ # See §3.18.21.

{ # A reportingDescriptor object (§3.44).

"id": "CA1711", # See §3.44.3.

...

},

{ # Another reportingDescriptor with the same id.

"id": "CA1711", # rule.index points to this one.

...

}

]

}

},

"results": [ # See §3.14.20.

{ # A result object (§3.25).

"ruleId": "CA1711", # See §3.25.5.

# A reportingDescriptorReference object.

"rule": {

"index": 1

}

}

]

}

If index is absent and theResult.ruleIndex (§3.25.6) is present, index **SHALL** default to theResult.ruleIndex. If both are present, they **SHALL** be equal.

### guid

A reportingDescriptorReference object **MAY** contain a property named guid whose value is a GUID-valued string (§3.5.4) equal to theDescriptor.guid (§3.44.5).

### toolComponent

A reportingDescriptorReference object **MAY** contain a property named toolComponent whose value is a toolComponentReference object (§3.48) that identifies theComponent.

If toolComponent is absent, theComponent shall be taken to be theTool.driver (§3.17.2).

## toolComponentReference object

### General

A toolComponentReference object identifies a particular toolComponent object (§3.18), either theTool.driver (§3.17.2) or an element of theTool.extensions (§3.17.3). We refer to the identified toolComponent object as theComponent.

### toolComponent lookup

If neither index (§3.48.4) nor guid (§3.48.5) is present, theComponent **SHALL** be theTool.driver (§3.17.2).

If index is present, theComponent **SHALL** be the object at array index index within theTool.extensions (§3.17.3).

If index is absent and guid is present, theComponent **SHALL** be either theTool.driver or an element of theTool.extensions, whichever one has a matching guid property.

### name property

A toolComponentReference object **MAY** contain a property named name whose value is a string equal to theComponent.name (§3.18.6).

NOTE: This property does not participate in the lookup, but its presence improves the readability of the log file at the expense of increased file size.

### index property

If theComponent is an element of theTool.extensions (§3.17.3), a toolComponentReference object **MAY** contain a property named index whose value is the array index (§3.7.4) of that element. Otherwise, index SHALL be absent.

### guid property

A toolComponentReference object **MAY** contain a property named guid whose value is a GUID-valued string (§3.5.4) equal to theComponent.guid (§3.18.5).

## fix object

### General

A fix object represents a proposed fix for the problem indicated by theResult. It specifies a set of artifacts to modify. For each artifact, it specifies regions to remove, and provides new content to insert.

EXAMPLE:

{ # A result object (§3.25).

"fixes": [ # See §3.25.28.

{ # A fix object.

"description": { # See §3.49.2.

"text": "Private member names begin with '\_'"

},

"artifactChanges": [ # See §3.49.3.

{ # An artifactChange object (§3.50).

...

}

]

}

],

...

}

### description property

A fix object **SHOULD** contain a property named description whose value is a message object (§3.11) that describes the proposed fix.

NOTE: The purpose of the description property is to enable a SARIF viewer to present the proposed fix to the end user.

EXAMPLE:

"fix": {

"description": {

"text": "Combine declaration and initialization of variable 'x'."

},

...

}

### artifactChanges property

A fix object **SHALL** contain a property named artifactChanges whose value is an array of one or more unique (§3.7.3) artifactChange objects (§3.50), each of which describes the changes to a single artifact that are necessary to effect the fix.

NOTE: artifactChanges is an array because a fix might require changes to multiple artifacts.

The array elements **SHALL** refer to distinct artifacts.

EXAMPLE 1: In this example, two artifactChange objects make identical changes (commenting out the first line) in two distinct C-language files, src/a.c and src/b.c.

{ # A fix object.

"artifactChanges": [

{ # An artifactChange object (§3.50).

"artifactLocation": { # See §3.50.2.

"uri": "src/a.c"

},

"replacements": [ # See §3.50.3.

{ # A replacement object (§3.51).

"deletedRegion": { # See §3.51.3.

"startLine": 1,

"startColumn": 1,

"endColumn": 1

},

"insertedContent": { # See §3.51.4.

"text": "// "

}

}

}

},

{

"artifactLocation": {

"uri": "src/b.c"

},

"replacements": [

{

"deletedRegion": {

"startLine": 1,

"startColumn": 1,

"endColumn": 1

},

"insertedContent": {

"text": "// "

}

}

}

}

]

}

EXAMPLE 2: This example represents invalid SARIF because the two artifactChange objects refer to the same file, src/a.c. It is invalid even though the artifactChange objects are distinguished by their replacements properties.

{ # A fix object.

"artifactChanges": [

{ # An artifactChange object (§3.50).

"artifactLocation": { # See §3.50.2.

"uri": "src/a.c"

},

"replacements": [ # See §3.50.3.

{ # A replacement object (§3.51).

"deletedRegion": { # See §3.51.3.

"startLine": 1,

"startColumn": 1,

"endColumn": 1

},

"insertedContent": { # See §3.51.4.

"text": "// "

}

}

}

},

{

"artifactLocation": {

"uri": "src/a.c" # Invalid: refers to the same file.

},

"replacements": [

{

"deletedRegion": {

"startLine": 2, # Invalid even though it affects a

"startColumn": 1, # different line.

"endColumn": 1

},

"insertedContent": {

"text": "// "

}

}

}

}

]

}

## artifactChange object

### General

An artifactChange object represents a change to a single artifact.

EXAMPLE:

{ # A fix object (§3.45).

"artifactChanges": [ # See §3.49.3.

{

"artifactLocation": { # See §3.50.2.

"uri": "a.h"

},

"replacements": [ # See §3.50.3.

{ # A replacement object (§3.51).

...

},

{ # Another replacement object.

...

}

]

}

]

}

### artifactLocation property

An artifactChange object **SHALL** contain a property named artifactLocation whose value is an artifactLocation object (§3.4) that represents the location of the artifact.

### replacements property

An artifactChange object **SHALL** contain a property named replacements whose value is an array of one or more replacement objects (§3.51), each of which represents the replacement of a single region of the artifact specified by the artifactLocation property (§3.50.2).

## replacement object

### General

A replacement object represents the replacement of a single region of an artifact. If the region’s length is zero, it represents an insertion point.

If a replacement object specifies both the removal of a region by means of the deletedRegion property (§3.51.3) and the insertion of new content by means of the insertedContent property (§3.51.4), then the effect of the replacement **SHALL** be as if the removal were performed before the insertion.

If a single artifactChange object (§3.50) specifies more than one replacement, then the effect of the replacements **SHALL** be as if they were performed in the order they appear in the replacements array (§3.50.3). The deletedRegion property of each replacement object **SHALL** specify the location of the replacement in the unmodified artifact.

EXAMPLE 1: Suppose an artifactChange object contains a replacements property whose value is the following array of replacement objects:

"artifactChanges": [

{

"deletedRegion": {

"byteOffset": 12,

"byteLength": 5

},

"insertedContent": {

"binary": "ZXhhbXBsZQ=="

}

},

{

"deletedRegion": {

"byteOffset": 20,

"byteLength": 3

}

},

{

"deletedRegion": {

"byteOffset": 312,

"byteLength": 0

},

"insertedContent": {

"binary": "ZXhhbXBsZQ=="

}

}

]

The first replacement object removes 5 bytes starting at offset 12; that is, it removes bytes 12–16. Then it inserts the 7 bytes specified by the MIME Base64-encoded string in the insertedContent.binary property at the same offset.

The second replacement object removes 3 bytes starting at offset 20 *with respect to the unmodified file*. Since 5 bytes were removed and 7 bytes inserted *before* byte 20, the 3 bytes removed actually start at byte 22 of the contents after the first change. Since the insertedContent property is absent, no content is inserted in place of the deleted bytes.

In the third replacement object, the length of the region specified by the deletedRegion property is zero, so the region represents an insertion point. The 7 bytes specified by the insertedContent.binary property are inserted at offset 312 with respect to the unmodified artifact.

A replacement object can represent either a textual replacement or a binary replacement, depending on whether the deletedRegion property (§3.51.3) specifies a text region (§3.28.2) or a binary region (§3.28.3).

EXAMPLE 2: In this example, the replacements property specifies a replacement in a text file.

"replacements": [

{

"deletedRegion": { # The region object represents a text region (§3.28.2).

"startLine": 12,

"startColumn": 5,

"endColumn": 9

},

"insertedContent": {

"text": "example" # The insertedContent property contains a text

} # property instead of a binary property.

}

]

When performing a replacement in a text artifact, the SARIF producer **SHOULD** specify a text replacement rather than a binary replacement. This allows the SARIF producer to specify the region without regard to whether the artifact starts with a byte order mark (BOM).

### Constraints

If the deletedRegion property (§3.51.3) specifies a text region (§3.28.2) and the insertedContent property (§3.51.4) is present, then the insertedContent property **SHOULD** contain a text property (§3.3.2).

If the deletedRegion property specifies a binary region (§3.28.3) and the insertedContent property is present, then the insertedContent property **SHALL** contain a binary property (§3.3.3).

### deletedRegion property

A replacement object **SHALL** contain a property named deletedRegion whose value is a region object (§3.28) specifying the region to delete.

If the length of the region specified by deletedRegion is zero, then deletedRegion specifies an insertion point, and the SARIF consumer performing the replacement **SHALL NOT** remove any content.

### insertedContent property

A replacement object **MAY** contain a property named insertedContent whose value is an artifactContent object (§3.3) that specifies the content to insert in place of the region specified by the deletedRegion property (or at the point specified by deletedRegion, if deletedRegion has a length of zero and therefore specifies an insertion point).

If the inserted content is specified as text, the text **SHALL** be transcoded from UTF-8 (the encoding of all text in all SARIF log files) to the encoding of the target artifact before being inserted.

NOTE: This implies that a text fix cannot be safely applied unless the target artifact’s encoding is known.

If insertedContent is absent or its properties specify content whose length is zero, the SARIF consumer performing the replacement **SHALL NOT** insert any content.

## notification object

### General

A notification object describes a condition encountered during the execution of an analysis tool which is relevant to the operation of the tool itself, as opposed to being relevant to an artifact being analyzed by the tool. Conditions relevant to artifacts being analyzed by a tool are represented by result objects (§3.25).

### descriptor property

Depending on the circumstances, a notification object either **SHOULD** or **SHALL NOT** contain a property named descriptor whose value is a reportingDescriptor object (§3.44), which we refer to as theDescriptor, that describes this notification.

If theDescriptor exists (that is, if theTool contains a reportingDescriptor object that describes this notification), then descriptor **SHOULD** be present. If present, it **SHALL** identify theDescriptor.

If theDescriptor does not exist, descriptor **SHALL NOT** be present.

NOTE: If theDescriptor exists but descriptor is absent, a SARIF consumer will not be able to locate the metadata for this notification.

### associatedRule property

If the condition described by the notification object is relevant to a particular analysis rule, the notification object **SHOULD** contain a property named associatedRule whose value is a reportingDescriptor object (§3.44) that identifies the rule.

EXAMPLE: In this example, there is more than one rule with id CA1711. associatedRule.index uniquely specifies the relevant rule.

{ # A run object (§3.14).

"tool": { # See §3.14.6.

"driver": { # See §3.17.2.

"name": "CodeScanner",

"rules": [ # See §3.18.21.

{ # A reportingDescriptor object (§3.44).

"id": "CA1711",

...

},

{ # Another reportingDescriptor object

"id": "CA1711", # with the same id. associatedRule.id

... # identifies this one.

}

]

}

},

"invocations": [ # See §3.14.11.

{ # An invocation object (§3.19).

"toolConfigurationNotifications": [ # See §3.19.22.

{ # A notification object (§3.52).

"descriptor": {

"id": "CFG0001"

},

"message": {

"text": "Rule configuration is missing."

},

"associatedRule": {

"id": "CA1711",

"index": 1

}

}

],

}

]

}

### physicalLocation property

If the condition described by the notification object is relevant to a particular artifact location, the notification object **SHOULD** contain a property named physicalLocation whose value is a physicalLocation object (§3.27) that identifies the relevant location.

### message property

A notification object **SHALL** contain a property named message whose value is a message object (§3.11) that describes the condition that was encountered.

NOTE: The message object in the notification.message property will typically not contain a markdown property (§3.11.9) because notifications typically appear on the console, where formatted text is not supported.

### level property

A notification object **MAY** contain a property named level whose value is one of a fixed set of strings that specify the severity level of the notification.

If present, the level property **SHALL** have one of the following values, with the specified meanings:

* "error": A serious problem was found. The condition encountered by the tool resulted in the analysis being halted or caused the results to be incorrect or incomplete.
* "warning": A problem that is not considered serious was found. The condition encountered by the tool is such that it is uncertain whether a problem occurred, or is such that the analysis might be incomplete but the results that were generated are probably valid.
* "note": The notification is purely informational. There is no required action.

If level is absent, it **SHALL** default to the value determined by the procedure defined for result.level (§3.25.10), except throughout the procedure, replace ruleConfigurationOverrides with notificationConfigurationOverrides.

Analysis tools **SHOULD** treat notifications whose level property is "error" as failures and treat the entire run as having failed.

### threadId property

A notification object **MAY** contain a property named threadId whose value is an integer which identifies the thread associated with this notification.

### timeUtc property

A notification object **MAY** contain a property named timeUtc whose value is a string in the format specified §3.9, specifying the UTC date and time at which the analysis tool generated the notification.

### exception property

If the notification is a result of a runtime exception, the notification object **MAY** contain a property named exception whose value is an exception object (§3.53).

If the notification is not the result of a runtime exception, the exception property **SHALL** be absent.

## exception object

### General

An exception object describes a runtime exception encountered during the execution of an analysis tool. This includes signals in POSIX-conforming operating systems

### kind property

An exception object **SHOULD** contain a property named kind whose value is a string describing the exception.

If the exception represents a thrown object, kind **SHALL** be the fully qualified type name of the object that was thrown, if that information is available.

EXAMPLE 1: C#: "System.ArgumentNullException"

If the exception represents a POSIX signal, kind **SHALL** be the symbolic name of the signal as specified in <signal.h>.

EXAMPLE 2: POSIX: "SIGFPE"

If the tool does not have access to information about the object that was thrown, the kind property **SHALL** be absent.

### message property

An exception object **SHOULD** contain a property named message whose value is a message object (§3.11) that describes the exception.

If the tool does not have access to an appropriate property of the thrown object, the message property **SHALL** be absent.

EXAMPLE 1: C++: The tool would populate message from the string returned from the what() method of any object derived from std::exception.

EXAMPLE 2: C#: The tool would populate message from the Message property of any object derived from System.Exception.

NOTE: Exception messages, appearing as they do in typical languages and operating systems, are typically plain text, and require no arguments (§3.11.5). Nevertheless, this property is defined to be a message object rather than a simple string for consistency with other message properties in this specification.

### stack property

An exception object **MAY** contain a property named stack whose value is a stack object (§3.40) that describes the sequence of function calls leading to the exception.

### innerExceptions property

An exception object **MAY** contain a property named innerExceptions whose value is an array of zero or more exception objects, each of which is considered a cause of the containing exception.

NOTE: There is commonly no more than one inner exception. This property is an array to accommodate platforms that provide a mechanism for aggregating exceptions, such as the System.AggregateException class from the .NET Framework.

# External property file format

## General

External property files (see §3.14.2) conform to a schema distinct from that of the root file. External property files contain information that makes it possible for a consumer to determine which properties are contained in the file, to parse their contents, and to associate the external properties with the run to which they belong.

## External property file naming convention

The file name of an external property file **SHOULD** end with the extension ".sarif-external-properties".

EXAMPLE 1: scan-results.sarif-external-properties

The file name **MAY** end with the additional extension ".json".

EXAMPLE 2: scan-results.sarif-external-properties.json

## externalProperties object

### General

The top-level element of an external property file **SHALL** be an object which we refer to as an externalProperties object.

EXAMPLE: In this example, run.artifacts and run.properties have been externalized to a file with these contents. Note that run.properties has been externalized under the property name externalizedProperties, as explained in §3.14.2.2.

{ # An externalProperties object

"$schema": # See §4.3.2.

"http:///json.schemastore.org/sarif-external-property-file-2.0.0",

"version": "2.0.0", # See §4.3.3.

# See §4.3.4.

"guid": "00001111-2222-3333-4444-555566667777",

# See §4.3.5.

"runGuid": "88889999-AAAA-BBBB-CCCC-DDDDEEEEFFFF",

"artifacts": { # See §4.3.6.

{

"artifactLocation": {

"uri": "apple.png"

},

"mimeType": "image/png"

},

{

"artifactLocation": {

"uri": "banana.png"

},

"mimeType": "image/png"

}

},

"externalizedProperties": {

"policy": "Web application security policy",

"team": "Security Assurance Team"

}

}

### $schema property

An externalProperties object **MAY** contain a property named $schema whose value is a string containing an absolute URI from which a JSON schema document describing the version of the external property file format to which this external property file conforms can be obtained.

If the $schema property is present, the JSON schema obtained from the specified URI **SHALL** describe the version of the external property file format corresponding to the SARIF version specified by the version property (§4.3.3).

NOTE: The purpose of the $schema property is to allow JSON schema validation tools to locate an appropriate schema against which to validate the external property file. This is useful, for example, for tool authors who wish to ensure that external property files produced by their tools conform to the external property file format.

### version property

Depending on the circumstances, an externalProperties object either **SHALL** or **MAY** contain a property named version whose value is a string designating the version of the SARIF specification to which this external property file conforms. If present, this string **SHALL** have the value "2.0.0".

If this externalProperties object is the root element of an external property file (see §3.14.2.1), then version **SHALL** be present.

Otherwise (that is, if this externalProperties object is an element of theSarifLog.inlineExternalProperties (§3.13.5)), then version **MAY** be present. If absent, it **SHALL** be default to the value of theSarifLog.version (§3.13.2).

Although the order in which properties appear in a JSON object value is not semantically significant, the version property **SHOULD** appear first.

NOTE: This will make it easier for parsers to handle multiple versions of the external property file format if new versions are defined in the future.

### guid property

An externalProperties object **SHALL** contain a property named guid whose value is a GUID-valued string (§3.5.4) that equals the guid property (§3.15.3) of the corresponding externalPropertyFileReference object (§3.15) in the run.externalPropertyFiles property (§3.14.2) in the root file.

### runGuid property

If the externalized properties belongs contained in this externalProperties object are associated with a single run object (§3.14) theRun, and if theRun contains an automationDetails.guid property (§3.14.3, §3.16.5), the externalProperties object **MAY** contain a property named runGuid whose value is a GUID-valued string (§3.5.4) that equals theRun.automationDetails.guid. Otherwise (that is, if this externalProperties object is associated with more than one run object, or if theRun does not define automationDetails.guid, then runGuid **SHALL** be absent.

### The property value properties

An externalProperties object **SHALL** contain one or more externalized properties. The property names in this object, and the names of the corresponding externalized properties, are given in the table in §3.14.2.2.

The corresponding property values are the values of the externalized properties, exactly as they would have appeared had they occurred inline in the root file.

NOTE 2: See the EXAMPLE in §4.3.1, where the externalized properties are run.artifacts and run.properties, the externalized value of run.artifacts is stored in a property named artifacts, and the externalized value of run.properties is stored in a property named externalizedProperties.

# Conformance

## Conformance targets

This specification defines requirements for the SARIF file format and for certain software components that interact with it. The entities (“conformance targets”) for which this specification defines requirements are:

* **SARIF log file**: A log file in the format defined by the SARIF specification.
* **SARIF producer**: A program which emits output in the SARIF format.
* **Direct producer**: An analysis tool which acts as a SARIF producer.
* **Deterministic producer**: A SARIF producer which, given identical inputs, repeatedly produces an identical SARIF log file.
* **Converter**: A SARIF producer that transforms the output of an analysis tool from its native output format into the SARIF format.
* **SARIF post-processor**: A SARIF producer that transforms an existing SARIF log file into a new SARIF log file, for example, by removing or redacting security-sensitive elements.
* **SARIF consumer**: A program that reads and interprets a SARIF log file.
* **Viewer**: A SARIF consumer that reads a SARIF log file, displays a list of the results it contains, and allows an end user to view each result in the context of the artifact in which it occurs.
* **Result management system**: a software system that consumes the log files produced by analysis tools, produces reports that enable engineering teams to assess the quality of their software artifacts at a point in time and to observe trends in the quality over time, and performs functions such as filing bugs and displaying information about individual results.
* **Engineering system**: a software development environment within which analysis tools execute. It might include a build system, a source control system, a [result management system](#def_result_management_system), a bug tracking system, a test execution system, and so on.

The normative content in this specification defines requirements for SARIF log files, except for those normative requirements that are explicitly designated as defining the behavior of another conformance target.

## Conformance Clause 1: SARIF log file

A text file satisfies the “SARIF log file” conformance profile if:

* It conforms to the syntax and semantics defined in §3.

## Conformance Clause 2: SARIF producer

A program satisfies the “SARIF producer” conformance profile if:

* It produces output in the SARIF format, according to the semantics defined in §3.
* It satisfies those normative requirements in §3 that are designated as applying to SARIF producers.

## Conformance Clause 3: Direct producer

An analysis tool satisfies the “Direct producer” conformance profile if:

* It satisfies the “SARIF producer” conformance profile.
* It additionally satisfies those normative requirements in §3 that are designated as applying to “direct producers” or to “analysis tools”.
* It does not emit any objects, properties, or values which, according to §3, are intended to be produced only by converters.

## Conformance Clause 4: Deterministic producer

An analysis tool or a converter satisfies the “Deterministic producer” conformance profile if:

* It satisfies the “Direct producer” conformance profile or the “Converter” conformance profile, as appropriate.
* It satisfies the normative requirements in [Appendix F](#AppendixDeterminism), “Producing deterministic SARIF log files”.

## Conformance Clause 5: Converter

A converter satisfies the “Converter” conformance profile if:

* It satisfies the “SARIF producer” conformance profile.
* It additionally satisfies those normative requirements in §3 that are designated as applying to converters.
* It does not emit any objects, properties, or values which, according to §3, are intended to be produced only by direct producers.

## Conformance Clause 6: SARIF post-processor

A SARIF post-processor satisfies the “SARIF post-processor” conformance profile if:

* It satisfies the “SARIF producer” conformance profile.
* It additionally satisfies those normative requirements in §3 that are designated as applying to post-processors.

## Conformance Clause 7: SARIF consumer

A consumer satisfies the “SARIF consumer” conformance profile if:

* It reads SARIF log files and interprets them according to the semantics defined in §3.
* It satisfies those normative requirements in §3 that are designated as applying to SARIF consumers.

## Conformance Clause 8: Viewer

A viewer satisfies the “viewer” conformance profile if:

* It satisfies the “SARIF consumer” conformance profile.
* It additionally satisfies the normative requirements in §3 that are designated as applying to viewers.

## Conformance Clause 9: Result management system

A result management system satisfies the “result management system” conformance profile if:

* It satisfies the “SARIF consumer” conformance profile.
* It additionally satisfies the normative requirements in §3 and [Appendix B](#AppendixFingerprints) (“Use of fingerprints by result management systems”) that are designated as applying to result management systems.

## Conformance Clause 10: Engineering system

An engineering system satisfies the “engineering system” conformance profile if:

* It satisfies the normative requirements in §3 that are designated as applying to engineering systems.

1. (Informative) Acknowledgments

The following individuals have participated in the creation of this specification and are gratefully acknowledged:

Participants:

Andrew Pardoe, Microsoft

Chris Wysopal, CA Technologies

David Keaton, Individual

Douglas Smith, Kestrel Technology

Duncan Sparrell, sFractal Consulting LLC

Everett Maus, Microsoft

Hendrik Buchwald, RIPS Technologies

Henny Sipma, Kestrel Technology

Jim Kupsch, SWAMP

Jordyn Puryear, Microsoft

Joseph Feiman, CA Technologies

Ken Prole, Code Dx, Inc.

Kevin Greene, Mitre Corporation

Larry Hines, Micro Focus

Laurence J. Golding, Individual

Luke Cartey, Semmle

Mel Llaguno, Synopsys

Michael Fanning, Microsoft

Nikolai Mansourov, Object Management Group

Paul Anderson, GrammaTech, Inc.

Paul Brookes, Microsoft

Paul Patrick, FireEye, Inc.

Philip Royer, Splunk Inc.

Pooya Mehregan, Security Compass

Ram Jeyaraman, Microsoft

Sean Barnum, FireEye, Inc.

Smith Douglas, Kestrel Technology

Stefan Hagen, Individual

Sunny Chatterjee, Microsoft

Tim Hudson, Cryptsoft Pty Ltd.

Trey Darley, New Context Services, Inc.

Vamshi Basupalli, SWAMP

Yekaterina O'Neil, Micro Focus

1. (Normative) Use of fingerprints by result management systems

On large software projects, a single run of a set of analysis tools can produce hundreds of thousands of results or more. To deal with so many results, some engineering teams adopt a strategy whereby they first prevent the introduction of new problems into their code, and then work to address the existing problems.

To prevent the introduction of new problems, it is necessary first to record the results from a designated run. We refer to this as a baseline. It is then necessary to compare the results from a subsequent run with the baseline.

To determine whether a result from a subsequent run is logically the same as a result from the baseline, there must be a way to use information contained in the result to construct a stable identifier for the result. We refer to this identifier as a fingerprint.

A result management system **SHOULD** construct a fingerprint by using information contained in the SARIF file such as

* the name of the tool that produced the result.
* the rule id.
* the file system path to the analysis target.

There are situations where information that would be helpful in uniquely identifying a result is not easily detectable by the result management system. For example, consider a tool which checks documentation for words that are culturally or politically sensitive. The word would most likely occur only in result.message, for example: "The word xxx should not be used in documentation."

The SARIF format provides the partialFingerprints property to allow analysis tools and other components in the SARIF ecosystem to provide additional information which a result management system can incorporate into the fingerprint that it constructs for each result. In this example, the tool might set the value of a property in the partialFingerprints object to the prohibited word. A result management system **SHALL** include the information in partialFingerprints in its fingerprint computation. See §3.25.15 for more requirements on how a result management system decides which partial fingerprints to use.

An analysis tool **SHALL NOT** include in partialFingerprints information that a result management system could deduce from other information in the SARIF file, for example, file hashes. Rather, the result management would use such information, along with partialFingerprints, in its computation of fingerprints.

Some information contained in the result is not useful in constructing a fingerprint. For example, suppose the fingerprint were to include the line number where the result was located, and suppose that after the baseline was constructed, a developer inserted additional lines of code above that location. Then in the next run, the result would occur on a different line, the computed fingerprint would change, and the result management system would erroneously report it as a new result.

A result management system **SHOULD NOT** include an absolute line number (or an absolute byte location in a binary artifact) in its fingerprint computation.

A result management system **SHALL NOT** include non-deterministic file format elements ([Appendix F](#AppendixDeterminism), §F.2) in its fingerprint computation.

A result management system **SHALL NOT** include non-deterministic absolute URIs ([Appendix F](#AppendixDeterminism), §F.4) in its fingerprint computation.

It is difficult to devise an algorithm that constructs a truly stable fingerprint for a result. Fortunately, for practical purposes, the fingerprint does need to be absolutely stable; it only needs to be stable enough to reduce the number of results that are erroneously reported as “new” to a low enough level that the development team can manage the erroneously reported results without too much effort.

1. (Informative) Use of SARIF by log file viewers

It is frequently useful for an end user to view the results produced by an analysis tool in the context of the artifacts in which they occur. A log file viewer is a program that allows an end user to do this.

Typically, the user opens a log file in the viewer, which presents a list of the results in the log file. When the user selects a result from the list, the viewer displays the source code from the file specified in the result, and displays information about the result in the vicinity of the region where the result occurred. For example, the viewer might interleave result information between lines of source code.

There are various reasons why a viewer might need to know the type of information contained in a source file that it displays:

* If the viewer knows the programming language, it can provide services such as syntax highlighting.
* If the result occurs in a source file that is nested within (for example) a compressed container file, then the viewer needs to know the file type of the container so that it can extract the source file.

There are various ways that a viewer might obtain file type information. In the SARIF format, the mimeType property of the artifact object provides this information. In the absence of the mimeType property, a viewer can fall back to examining the filename extension, for example “.zip”. It is recommended that the analysis tool provide the mimeType property (which it must know, because it was able to interpret the artifact in which it detected the result), rather than forcing the viewer to rely on a file name extension.

1. (Informative) Production of SARIF by converters

There are two broad categories of tools that can produce output in the SARIF format. Analysis tools produce SARIF as a result of performing a scan on a set of analysis targets. Converters translate existing data from a non-SARIF format into the SARIF format. That data might come from an analysis tool that produces output in a non-SARIF format, from a bug database, or from any other source.

Converters should populate those elements of the SARIF format for which a direct equivalent exists in the input data.

If the input data includes information for which there is no SARIF equivalent, converters may use it to populate the various property bags and tag lists defined by the SARIF format, or they may simply omit it from the output. When populating a property bag with such information, converters should use a property name that matches the name of that piece of information in the native tool format, even if that name does not conform to the camelCase convention used in the rest of this specification. This makes it easier to match these properties with the source data in the native tool format.

NOTE: The converter must replace any characters that cannot occur in a JSON string with the appropriate escape sequence.

If the input data does not include an equivalent for any SARIF element, the converter should not attempt to synthesize that element. For example, a converter should not attempt to heuristically extract a rule id from the text of an unstructured error message.

If a converter were to synthesize values, it would potentially introduce additional complexity in the implementation of SARIF viewers. The reason is that the viewer itself might examine the analysis tool and its version in the tool object, and attempt to synthesize missing elements.

Now suppose a converter made a bad choice in synthesizing a missing element, and then fixed the problem in an update. As a result, two log files claiming to have been produced by the same version of the same analysis tools might have different elements filled in, or the same elements filled in differently. For that matter, two different converters might make different choices in how to synthesize missing elements. As a result, the viewer would have to take into account both the analysis tool (and its version) and the converter (and its version) in deciding how to synthesize any remaining elements.

By design, to avoid this added complexity, the SARIF standard does not define an element to hold the converter version. This, together with the guidance that converter implementers should not attempt to synthesize missing elements, allows viewer implementers to assume that all files from the same version of the same tool are identical in structure.

This general guidance is embodied in various sections of the specification. For example:

* A converter should not attempt to synthesize a ruleId for a result if the tool does not provide one.
* A converter that knows which artifact a result was detected in, but not which artifact the analysis tool was originally instructed to scan, should populate the location.physicalLocation property, but should not attempt to populate result.analysisTarget (see §3.25.13).
* A converter should not attempt to guess whether the analysis tool's version string is intended to be interpreted as a Semantic Version 2.0.0 version string (see §3.18.8).

1. (Informative) Locating rule and notification metadata

The SARIF format allows rule and notification metadata to be included in a SARIF log file (see §3.18.21 and §3.18.22). A SARIF log file does not need to include any metadata. This raises the questions of when metadata should be included in a log file, and how to locate the metadata if it is not included in the log file.

Metadata should be included in a log file in the following circumstances:

* The log file is intended to be viewed in a tool such as a log file viewer that needs to display metadata related to each result or notification even when the tool is not connected to a network.
* The log file is intended to be uploaded to a result management system which requires information about every rule specified by every result, and which might not have prior knowledge of the rules specified by the results in this log file.
* Neither of the above applies, but the increased log file size due to the metadata is not considered significant.

If metadata is not included in the log file, and if external property files (see §3.14.2) are not used, this specification does not specify a mechanism for locating the metadata. If the SARIF log file is produced in the context of an engineering system that provides a service from which metadata can be obtained (for example, a result management system, or a web service dedicated to metadata), then tooling can be created to merge a log file with the relevant metadata when required (for example, when presenting the results in a log file viewer).

1. (Normative) Producing deterministic SARIF log files
   1. General

In certain circumstances, it is desirable for an analysis tool to produce deterministic output; that is, for it to produce identical output when run repeatedly over identical inputs.

Certain build systems provide an example of when this is desirable. Consider a build system that caches the results of each build step. If the build is rerun, and the inputs to the step are identical (which the build system might determine, for example, by comparing timestamps, or by computing a hash of the inputs to the step and storing it along with the output from the step), then the build system can save time by not re-running the step, and simply using the existing outputs.

In the case of SARIF, one could imagine a sequence of build steps where Steps A, B, and C each run an analysis tool on a different set of targets, producing log files A.sarif, B.sarif, and C.sarif, and then build Step D performs an analysis on the aggregate of those log files. If the targets analyzed in Step B change but the targets analyzed in steps A and C do not, and if the contents of the SARIF log file are deterministic, then when the build is re-run, only Steps B and D need to be performed.

Authors of analysis tools are encouraged to provide a mechanism (for example, a command line option such as --deterministic) which instructs the tool to produce deterministic output.

There are several issues to consider when producing deterministic output:

* Avoiding elements of the SARIF file format whose values are non-deterministic.
* Emitting array and dictionary elements in a deterministic order.
* Avoiding absolute paths.
* Handling baseline information
  1. Non-deterministic file format elements

A tool that produces deterministic output **SHALL NOT** emit the following elements of the SARIF format. All of these elements are **OPTIONAL**.

Not all of these elements are non-deterministic in all cases. For example, some build systems might run all builds on the same machine or under the same account. However, avoiding these elements, in conjunction with the techniques described in subsequent sections of this Appendix, guarantees deterministic output.

* invocation.startTimeUtc
* invocation.endTimeUtc
* invocation.processId
* invocation.machine
* invocation.account
* invocation.fileName (because fileName is specified as being an absolute path, and tools might be stored in different directories on different machines)
* invocation.workingDirectory
* invocation.environmentVariables
* The use of absolute file paths in invocation.commandLine (because builds performed on different machines might use a different root directory)
* threadFlow.threadId
* threadFlowLocation.executionTimeUtc
* notification.threadId
* notification.timeUtc
* result.guid
* run.automationDetails.id
* run.automationDetails.guid
* run.aggregateIds[i].id
* run.aggregateIds[i].guid
* run.baselineGuid
* run.originalUriBaseIds
* stackFrame.threadId
* physicalLocation.address (because security measures such as address space layout randomization (ASLR) might place identical code at different addresses from run to run)
* The presence of any non-deterministic elements in a property bag property
  1. Array and dictionary element ordering

A tool that produces deterministic output **SHALL** emit array and dictionary elements in a deterministic order.

For some arrays, SARIF requires a specific ordering. For example, within stack.Frames, SARIF requires the location object representing the most deeply nested function call to appear first.

For other arrays, for example properties.tags, SARIF does not require a specific ordering. For such arrays, a tool can ensure the order by sorting the array elements before writing them to the log file. For example, it might sort the tags in locale-insensitive alphabetical order.

The array of result objects in the run.results array presents more of a problem. A multi-threaded analysis tool analyzing multiple artifacts in parallel might produce results in any order, and there is no natural order for the results. A tool might choose to order them, for example, first alphabetically by analysis target URI, then numerically by line number, then by column number, then alphabetically by rule id.

For dictionaries such as the artifact.hashes object, a tool might order the property names alphabetically, using a locale-insensitive ordering.

* 1. Absolute paths

The use of non-deterministic absolute file paths (that is, absolute paths which might differ from machine to machine) in artifactLocation.uri properties prevents the production of deterministic output. For example:

* Different build machines might be configured to use different source directories.
* A single build machine might use a different directory for each build.

A tool that produces deterministic output **SHALL NOT** emit non-deterministic absolute file paths. Tools can achieve this by emitting URIs that are relative to one or more root directories (for example, a source root directory and an output root directory), and accompanying each artifactLocation.uri property with the corresponding artifactLocation.uriBaseId property.

* 1. Compensating for non-deterministic output

If an analysis tool does not produce deterministic output, a build system can add additional processing steps to compensate.

There are two scenarios to consider:

* Log equality is determined by a simple comparison of file contents, or by comparing file hashes.
* Log equality is determined by an “intelligent” comparison.

In the first scenario, a post-processing step could produce deterministic output by creating a new file that omits non-deterministic elements, reorders array elements and object properties, removes file path prefixes, and introduces artifactLocation.uriBaseId properties.

In the second scenario, a post-processing step could intelligently compare the newly produced log to the log from a previous build by ignoring non-deterministic elements, ensuring that arrays have the same elements regardless of order, and ignoring file path prefixes.

* 1. Interaction between determinism and baselining

SARIF's baselining feature poses a particular challenge for determinism. We illustrate the problem with the following scenario:

On a particular date, a project's nightly build runs an analysis tool ToolX, which produces a log file, say, log\_20170914.sarif. The next day, a developer modifies one of the files scanned by the tool in a way that introduces a new problem. That night, the nightly build tool runs again, this time producing a log file which compares the current set of results to those that appeared in the previous run:

ToolX --input a.c b.c --baseline log\_20170914.sarif --output log\_20170915.sarif

Because a new problem has been introduced, log\_20170614.sarif will contain a result object whose baselineState is "new". The next night, without any further changes to the source files, the tool is run yet again:

ToolX --input a.c b.c --baseline log\_20170915.sarif --output log\_20170916.sarif

The result object that first appeared in log\_20160615.sarif still appears in log\_20160616.sarif, but since it existed in the baseline, its baselineState will now be "existing".

The result is that even though none of the analysis target files have changed, the log file has changed, or at least, a simple file comparison (such as comparing the hash of the new log with the hash of the baseline) will report that it has changed.

Strictly speaking, this does not violate determinism. After all, the baseline file has changed, and the baseline file is one of the inputs to the analysis. But from a practical standpoint, this is still a problem, albeit a small one.

If the build uses a simple mechanism such as hash value comparison to determine if a file has changed, then on those occasions when the only difference between the newest log and the baseline is that some results that were previously "new" are now "existing", subsequent build steps which consume the SARIF log file will run, even if they might not actually be necessary. For example, a build step which automatically files bugs for new results will run, even though the log contains no new results. Or a build step which tracks the number of open issues will run, even though the number of open issues has not actually changed.

If the build engineers for a project wish to absolutely minimize the execution of unnecessary build steps, they have various options. They might perform an “intelligent” comparison between the baseline and the new log, treating "new" results in the baseline as equivalent to "existing" results. Or they might rewrite the baseline (marking all "new" results as "existing") before performing the comparison. Of course, there is no guarantee that such an “intelligent” comparison or baseline rewriting process will actually take less time than the unnecessary build steps it is intended to avoid.

1. (Informative) Guidance on fixes

Tools that produce SARIF files which include fix objects should take care to structure those fixes in such a way as to affect a minimal range of content. This maximizes the likelihood that an automated tool can safely apply multiple fixes to the same artifact.

The following example will clarify what this means and why it is important. Consider an XML file containing the following element:

<lineItem partNumber=A3101 />

Suppose that a (domain-specific) XML scanning tool reported two results:

* The value of the partNumber attribute is not enclosed in quotes.
* The part numbering scheme has changed, and part numbers beginning with “A” now begin with “AA”.

Fixing only result #1 would produce the element

<lineItem partNumber="A3101" />

Fixing only result #2 would produce the element

<lineItem partNumber=AA3101 />

Fixing both results should produce the element

<lineItem partNumber="AA3101" />

The fix for result #1 might be specified in various ways, for example:

1. As a single replacement:
   * Replace the characters A3101 with the characters "A3101".
2. As a sequence of two replacements:
   1. Insert a quotation mark before A3101.
   2. Insert a quotation mark after A3101.

The fix for result #2 is most simply specified as a single replacement:

* Replace the characters A3101 with the characters AA3101.

Suppose there exists an automated tool which reads a SARIF file containing fix objects and applies as many of the specified fixes as possible to the source files.

If the fix for result #1 were structured as a single replacement, then after applying the fix, the tool would not be able to fix result #2, because the range of characters specified by the fix for result #2 would have been replaced. On the other hand, if the fix for result #1 were structured as two replacements (with a separate insertion for each quotation mark), the tool would still be able to apply the fix for result #2, because the targeted range of characters would still exist.

Therefore, structuring fixes as sequences of minimal, disjoint replacements maximizes the amount of work that can be done by automated fixup tools.

1. (Informative) Diagnosing results in generated files

Sometimes it is desirable to analyze files generated by the build. These files are usually not under source control, and the build might even overwrite them multiple times. This Appendix offers guidance on how to persist enough information in a SARIF log file to facilitate the diagnosis of results in these files.

In what follows, we will refer to files that are generated only once as “singly generated,” and files that are generated multiple times as “multiply generated.”

It can be difficult to diagnose results in generated files for the following reasons:

* The file might not be available to the engineer who diagnoses the result (for example, the engineer might not have a build environment).
* If the file is multiply generated, then at best only the last version is available, but results might have been found in previous versions.
* It might be difficult to tell which instance of a multiply generated file contained the result.

For both singly and multiply generated files, there are two options (which can be used together):

1. Use the physicalLocation object’s region and contextRegion properties to store enough of the generated file’s contents to facilitate diagnosis. The region object’s snippet property holds the relevant portion of the file contents.
2. Use the file object’s contents property to persist the entire contents of the file in run.artifacts.

The first option is more compact; the second allows a SARIF viewer to present results with greater context.

EXAMPLE 1: In this example, the analysis tool populates region.snippet and contextRegion.snippet, allowing a SARIF viewer to display just enough context (one hopes) to diagnose the result.

{ # A run object (§3.14).

"originalUriBaseIds": { # See §3.14.14

"GENERATED": "file:///C:/code/browser/obj"

},

"results": [ # See §3.14.20.

{ # A result object (§3.25).

"ruleId": "CS6789", # See §3.25.5.

"message": { # See §3.25.11.

"text": "Division by 0!"

},

"locations": [ # See §3.25.12.

{ # A location object (§3.26).

"physicalLocation": { # See §3.26.2.

"artifactLocation": {

"uri": "ui/window.g.cs", # A generated file (".g").

"uriBaseId": "GENERATED"

},

"region": {

"startLine": 42,

**"snippet": {**

**"text": " int z = x / y;\r\n"**

**}**

},

"contextRegion": {

"startLine": 40,

"endLine": 42,

**"snippet": {**

**"text": " int x = 54;\r\n int y = 0;\r\n int z = x / y;\r\n"**

**}**

}

}

}

]

}

],

...

}

EXAMPLE 2: In this example, the analysis tool populates artifact.contents, allowing a SARIF viewer to present the result in a larger context at the expense of a larger log file.

{

"originalUriBaseIds": {

"GENERATED": {

"uri": "file:///dev-1.example.com/code/browser/obj/"

}

},

"results": [

{

"ruleId": "CS6789",

"message": {

"text": "Division by 0!"

},

"locations": [

{

"physicalLocation": {

"artifactLocation": {

"uri": "ui/window.g.cs",

"uriBaseId": "GENERATED",

"artifactIndex": 0

},

"region": {

"startLine": 42

},

"contextRegion": {

"startLine": 40,

"endLine": 42

}

}

}

]

}

],

"artifacts": [ # See §3.14.15.

{ # An artifact object (§3.23).

"artifactLocation": { # See §3.23.2.

"uri": "ui/window.g.cs",

"uriBaseId": "GENERATED"

},

**"contents": { # See §3.23.8.**

**"text": "..." # See §3.3.2.**

**}**

}

]

}

Multiply generated files are treated similarly, but they present an additional problem: if more than one version of a given multiply generated file appears in run.artifacts – either because the analysis tool wishes to persist the file contents, or for any other reason – then there must be a way to distinguish them.

The recommended solution is for the analysis tool to create a new URI base id for each version of the generated files. For example, the tool might append an incremented integer to the URI base id for each version of the file. The result might look like the following example.

EXAMPLE 3: In this example, "ui/window.g.cs" is multiply generated. The analysis tool creates URI base ids "GENERATED-1" and "GENERATED-2" to distinguish the two versions.

{

"originalUriBaseIds": {

**"GENERATED-1": {**

**"uri": "file:///dev-1.example.com/code/browser/obj/"**

**},**

**"GENERATED-2": {**

**"uri": "file:///dev-1.example.com/code/browser/obj/"**

**}**

},

"results": [

{

"ruleId": "CS6789",

"message": {

"text": "Division by 0!"

},

"locations": [

{

"physicalLocation": {

"artifactLocation": {

"uri": "ui/window.g.cs",

**"uriBaseId": "GENERATED-1"**

},

"region": {

"startLine": 42

},

"contextRegion": {

"startLine": 40,

"endLine": 42

}

}

}

]

}

],

"artifacts": [

"artifactLocation": {

"uri": "ui/window.g.cs",

**"uriBaseId": "GENERATED-1" # Unique uriBaseId value.**

}

...

},

{

"artifactLocation": {

"uri": ui/window.g.cs",

**"uriBaseId": "GENERATED-2" # Unique uriBaseId value.**

}

...

}

]

}

1. (Informative) Sample sourceLanguage values

This Appendix contains a list of sample values for the artifact.sourceLanguage property (§3.23.10) for some common programming languages. The purpose of this Appendix is to promote interoperability by encouraging SARIF producers to use the same identifiers for these languages.

The names of some of the languages in this list are the trademarks of their respective owners.

* abap
* actionscript
* apex
* c
* cobol
* coldfusion
* cplusplus
* csharp
* css
* fsharp
* fortran
* go
* java
* javascript
* json
* jsp
* markdown (variants: markdown/gfm, markdown/cmark)
* objectivec
* perl
* php
* python
* razor
* ruby
* scala
* sql (variants: sql/tsql, sql/psql).
* swift
* typescript
* yaml
* Markup languages:
  + html
  + sgml
  + xml
* Typesetting languages:
  + latex
  + nroff
  + roff
  + tex
  + troff
* Unix ® shell languages:
  + bash
  + csh
  + ksh
  + sh
  + tcsh
* Windows ® shell languages:
  + cmd
  + powershell

1. (Informative) Examples

This Appendix contains examples of complete, valid SARIF files, to complement the fragments shown in examples throughout this document.

* 1. Minimal valid SARIF log file

This is a minimal valid SARIF log file. It contains only those elements required by the specification (elements which the specification states **SHALL** be present).

The file contains a single run object (§3.14) with an empty results array (§3.14.20), as would happen if the tool detected no issues in any of the artifacts it scanned.

{

"version": "2.0.0",

"runs": [

{

"tool": {

"driver": {

"name": "CodeScanner"

}

},

"results": [

]

}

]

}

* 1. Minimal recommended SARIF log file with source information

This is a minimal recommended SARIF log file for the case where an analysis tool produced results and source location information is available.

The file contains those elements recommended by the specification (elements which the specification states “**SHOULD**” be present), in addition to the required elements.

The file contains a single run object (§3.14) with a results array (§3.14.20). The results array contains a single result object (§3.25) so the recommended elements of the result object can be shown.

Its run.artifacts property (§3.14.15) specifies only those artifacts in which the tool detected a result.

It does not contain a run.logicalLocations property (§3.14.16), because when physical location information is available, that property is optional (it “**MAY**” be present).

This example also includes a toolComponent.rules property (§3.18.21) containing rule metadata, even though rule metadata is optional, to show how a SARIF log file can be self-contained, in the sense of containing all the information necessary to interpret the results.

{

"version": "2.0.0",

"runs": [

{

"tool": {

"driver": {

"name": "CodeScanner",

"rules": [

{

"id": "C2001",

"fullDescription": {

"text": "A variable was used without being initialized. This can result

in runtime errors such as null reference exceptions."

}

}

]

}

},

"artifacts": [

{

"artifactLocation": {

"uri": "file:///build.example.com/work/src/collections/list.cpp"

},

"mimeType": "text/x-c"

}

],

"results": [

{

"ruleId": "C2001",

"rule": {

"index": 0

},

"message": {

"text": "Variable \"count\" was used without being initialized.",

"markdown": "Variable `count` was used without being initialized."

},

"locations": [

{

"physicalLocation": {

"artifactLocation": {

"uri": "file://build.example.com/work/src/collections/list.cpp",

"artifactIndex": 0

},

"region": {

"startLine": 15

}

},

"logicalLocation": {

"fullyQualifiedName": "collections::list:add"

}

}

]

}

]

}

]

}

* 1. Minimal recommended SARIF log file without source information

This is a minimal recommended SARIF file for the case where an analysis tool produced results and source location information is not available.

The file contains those elements recommended by the specification (elements which the specification states “**SHOULD**” be present), in addition to the required elements.

The file contains a single run object (§3.14) with a results array (§3.14.20). The results array contains a single result object (§3.25) so the recommended elements of the result object can be shown.

Its run.artifacts property (§3.14.15) specifies only those artifacts in which the tool detected a result.

It contains a run.logicalLocations property (§3.14.16), because when physical location information is not available, that property is recommended.

{

"version": "2.0.0",

"runs": [

{

"tool": {

"driver": {

"name": "BinaryScanner"

}

},

"artifact": [

{

"artifactLocation": {

"uri": "file://build.example.com/work/bin/example"

},

"mimeType": "application/vnd.microsoft.portable-executable"

}

],

"logicalLocations": [

{

"name": "Example",

"kind": "namespace"

},

{

"name": "Worker",

"fullyQualifiedName": "Example.Worker",

"kind": "type",

"parentIndex": 0

},

{

"name": "DoWork",

"fullyQualifiedName": "Example.Worker.DoWork",

"kind": "function",

"parentIndex": 1

}

],

"results": [

{

"ruleId": "B6412",

"message": {

"text": "The insecure method \"Crypto.Sha1.Encrypt\" should not be used.",

"markdown": "The insecure method `Crypto.Sha1.Encrypt` should not be used."

},

"level": "warning",

"locations": [

{

"logicalLocation": {

"fullyQualifiedName": "Example.Worker.DoWork",

"index": 2

}

}

]

}

]

}

]

}

* 1. Comprehensive SARIF file

The purpose of this example is to demonstrate the usage of as many SARIF elements as possible. Not all elements are shown, because some are mutually exclusive.

Because the purpose is to present as many elements as possibly, the file as a whole does not represent best practices for SARIF usage, nor does it represent the output of a single, coherent analysis. For example, the result presented in the file involves a runtime exception, but at the same time it is marked as suppressedExternally (to demonstrate the result.suppressions property), which is unrealistic.

{

"version": "2.0.0",

"$schema": "http://json.schemastore.org/sarif-2.0.0",

"runs": [

{

"automationId": {

"guid": "BC650830-A9FE-44CB-8818-AD6C387279A0",

"id": "Nightly code scan/2018-10-08"

},

"baselineGuid": "0A106451-C9B1-4309-A7EE-06988B95F723",

"aggregateIds": [

{

"id": "Build/14.0.1.2/Release/20160716-13:22:18",

"correlationGuid": "26F138B6-6014-4D3D-B174-6E1ACE9439F3"

}

],

"tool": {

"driver": {

"name": "CodeScanner",

"fullName": "CodeScanner 1.1 for Microsoft Windows (R) (en-US)",

"version": "2.1",

"semanticVersion": "2.1.0",

"dottedQuadFileVersion": "2.1.0.0",

"releaseDateUtc": "2019-03-17",

"organization": "Example Corporation",

"product": "Code Scanner",

"productSuite": "Code Quality Tools",

"shortDescription": {

"text": "A scanner for code"

},

"fullDescription": {

"text": "A really great scanner for all your code."

},

"properties": {

"copyright": "Copyright (c) 2017 by Example Corporation."

},

"globalMessageStrings": {

"call": {

"text": "Call",

"markdown": "\*\*Call\*\*"

}

"return": {

"text": "Return",

"markdown": "\*\*Return\*\*"

}

},

"rules": [

{

"id": "C2001",

"deprecatedIds": [

"CA2000"

],

"defaultConfiguration": {

"level": "error",

"rank": 95

},

"shortDescription": {

"text": "A variable was used without being initialized."

},

"fullDescription": {

"text": "A variable was used without being initialized. This can result

in runtime errors such as null reference exceptions."

},

"messageStrings": {

"default": {

"text": "Variable \"{0}\" was used without being initialized.",

"markdown": "Variable `{0}` was used without being initialized."

}

}

}

],

"notifications": [

{

"id": "start",

"shortDescription": {

"text": "The run started".

},

"messageStrings": {

"default": {

"text": "Run started."

}

}

},

{

"id": "end",

"shortDescription": {

"text": "The run ended".

},

"messageStrings": {

"default": {

"text": "Run ended."

}

}

}

],

"language": "en-US"

},

"extensions": [

{

"name": "CodeScanner Security Rules",

"version": "3.1",

"rules": [

{

"id": "S0001",

"defaultConfiguration": {

"level": "error"

},

"shortDescription": {

"text": "Do not use weak cryptographic algorithms."

},

"messageStrings": {

"default": {

"text": "The cryptographic algorithm '{0}' should not be used."

}

}

}

]

}

]

},

"language": "en-US",

"versionControlProvenance": [

{

"repositoryUri": "https://github.com/example-corp/browser",

"revisionId": "de67ef7",

"mappedTo": {

"uriBaseId": "PROJECTROOT"

}

}

],

"originalUriBaseIds": {

"PROJECTROOT": {

"uri": "file://build.example.com/work/"

},

"SRCROOT": {

"uri": " src/",

"uriBaseId": "PROJECTROOT"

},

"BINROOT": {

"uri": " bin/",

"uriBaseId": "PROJECTROOT"

}

},

"invocations": [

{

"commandLine": "CodeScanner @build/collections.rsp",

"responseFiles": [

{

"uri": "build/collections.rsp",

"uriBaseId": "SRCROOT",

"artifactIndex": 0

}

],

"startTimeUtc": "2016-07-16T14:18:25Z",

"endTimeUtc": "2016-07-16T14:19:01Z",

"machine": "BLD01",

"account": "buildAgent",

"processId": 1218,

"fileName": "/bin/tools/CodeScanner",

"workingDirectory": {

"uri": "/home/buildAgent/src"

},

"environmentVariables": {

"PATH": "/usr/local/bin:/bin:/bin/tools:/home/buildAgent/bin",

"HOME": "/home/buildAgent",

"TZ": "EST"

},

"toolConfigurationNotifications": [

{

"descriptor": {

"id": "UnknownRule"

},

"associatedRule": {

"ruleId": "ABC0001"

},

"level": "warning",

"message": {

"text": "Could not disable rule \"ABC0001\" because

there is no rule with that id."

}

}

],

"toolExecutionNotifications": [

{

"descriptor": {

"id": "CTN0001"

},

"level": "note",

"message": {

"text": "Run started."

}

},

{

"descriptor": {

"id": "CTN9999"

},

"associatedRule": {

"id": "C2001",

"index": 0,

},

"level": "error",

"message": {

"text": "Exception evaluating rule \"C2001\". Rule disabled;

run continues."

},

"physicalLocation": {

"artifactLocation": {

"uri": "crypto/hash.cpp",

"uriBaseId": "SRCROOT",

"artifactIndex": 4

}

},

"threadId": 52,

"timeUtc": "2016-07-16T14:18:43.119Z",

"exception": {

"kind": "ExecutionEngine.RuleFailureException",

"message": {

"text": "Unhandled exception during rule evaluation."

},

"stack": {

"frames": [

{

"location": {

"message": {

"text": "Exception thrown"

},

"logicalLocation": {

"fullyQualifiedName":

"Rules.SecureHashAlgorithmRule.Evaluate"

},

"physicalLocation": {

"address": {

"offset": "0x40c606"

}

}

},

"module": "RuleLibrary",

"threadId": 52

},

{

"location": {

"logicalLocation": {

"fullyQualifiedName":

"ExecutionEngine.Engine.EvaluateRule"

}

},

"physicalLocation": {

"address": {

"offset": "0x40c80A"

}

},

"module": "ExecutionEngine",

"threadId": 52

}

]

},

"innerExceptions": [

{

"kind": "System.ArgumentException",

"message": "length is < 0"

}

]

}

},

{

"descriptor": {

"id": "CTN0002"

},

"level": "note",

"message": {

"text": "Run ended."

}

}

]

}

],

"artifacts": [

{

"artifactLocation": {

"uri": "build/collections.rsp",

"uriBaseId": "SRCROOT"

},

"mimeType": "text/plain",

"length": 81,

"contents": {

"text": "-input src/collections/\*.cpp -log out/collections.sarif -rules all -disable C9999"

}

},

{

"artifactLocation": {

"uri": "application/main.cpp",

"uriBaseId": "SRCROOT"

},

"mimeType": "text/x-c",

"length": 1742,

"hashes": {

"sha-256": "cc8e6a99f3eff00adc649fee132ba80fe333ea5a"

}

},

{

"artifactLocation": {

"uri": "collections/list.cpp",

"uriBaseId": "SRCROOT"

},

"mimeType": "text/x-c",

"length": 980,

"hashes": {

"sha-256": "b13ce2678a8807ba0765ab94a0ecd394f869bc81"

}

},

{

"artifactLocation": {

"uri": "collections/list.h",

"uriBaseId": "SRCROOT"

},

"mimeType": "text/x-c",

"length": 24656,

"hashes": {

"sha-256": "849be119aaba4e9f88921a99e3036fb6c2a8144a"

}

},

{

"artifactLocation": {

"uri": "crypto/hash.cpp",

"uriBaseId": "SRCROOT"

},

"mimeType": "text/x-c",

"length": 1424,

"hashes": {

"sha-256": "3ffe2b77dz255cdf95f97d986d7a6ad8f287eaed"

}

},

{

"artifactLocation": {

"uri": "app.zip",

"uriBaseId": "BINROOT"

},

"mimeType": "application/zip",

"length": 310450,

"hashes": {

"sha-256": "df18a5e74b6b46ddaa23ad7271ee2b7c5731cbe1"

}

},

{

"artifactLocation": {

"uri": "/docs/intro.docx"

},

"mimeType":

"application/vnd.openxmlformats-officedocument.wordprocessingml.document",

"parentIndex": 5,

"offset": 17522,

"length": 4050

}

],

"logicalLocations": [

{

"name": "add",

"fullyQualifiedName": "collections::list::add",

"decoratedName": "?add@list@collections@@QAEXH@Z",

"kind": "function",

"parentIndex": 1

},

{

"name": "list",

"fullyQualifiedName": "collections::list",

"kind": "type",

"parentIndex": 2

},

{

"name": "collections",

"kind": "namespace"

},

{

"name": "add\_core",

"fullyQualfiedName": "collections::list::add\_core",

"decoratedName": "?add\_core@list@collections@@QAEXH@Z",

"kind": "function",

"parentIndex": 1

},

{

"fullyQualifiedName": "main",

"kind": "function"

}

],

"results": [

{

"ruleId": "C2001",

"rule": {

"index": 0

},

"kind": "fail",

"level": "error",

"message": {

"messageId": "default",

"arguments": [

"ptr"

]

},

"suppressions": [

{

"kind": "suppressedExternally"

}

],

"baselineState": "existing",

"rank": 95,

"analysisTarget": {

"uri": "collections/list.cpp",

"uriBaseId": "SRCROOT",

"artifactIndex": 2

},

"locations": [

{

"physicalLocation": {

"artifactLocation": {

"uri": "collections/list.h",

"uriBaseId": "SRCROOT",

"artifactIndex": 3

},

"region": {

"startLine": 15,

"startColumn": 9,

"endLine": 15,

"endColumn": 10,

"charLength": 1,

"charOffset": 254,

"snippet": {

"text": "add\_core(ptr, offset, val);\n return;"

}

}

},

"logicalLocation": {

"fullyQualifiedName": "collections::list:add",

"index": 0

}

}

],

"relatedLocations": [

{

"message": {

"text": "Variable \"ptr\" was declared here.",

"markdown": "Variable `ptr` was declared here."

},

"physicalLocation": {

"artifactLocation": {

"uri": "collections/list.h",

"uriBaseId": "SRCROOT",

"artifactIndex": 3

},

"region": {

"startLine": 8,

"startColumn": 5

}

},

"logicalLocation": {

"fullyQualifiedName": "collections::list:add",

"index": 0

}

}

],

"codeFlows": [

{

"message": {

"text": "Path from declaration to usage"

},

"threadFlows": [

{

"id": "thread-52",

"locations": [

{

"importance": "essential",

"location": {

"message": {

"text": "Variable \"ptr\" declared.",

"markdown": "Variable `ptr` declared."

},

"physicalLocation": {

"artifactLocation": {

"uri":"collections/list.h",

"uriBaseId": "SRCROOT",

"artifactIndex": 3

},

"region": {

"startLine": 15,

"snippet": {

"text": "int \*ptr;"

}

}

},

"logicalLocation": {

"fullyQualifiedName": "collections::list:add",

"index": 0

}

},

"module": "platform"

},

{

"state": {

"y": "2",

"z": "4",

"y + z": "6",

"q": "7"

},

"importance": "unimportant",

"location": {

"physicalLocation": {

"artifactLocation": {

"uri":"collections/list.h",

"uriBaseId": "SRCROOT",

"artifactIndex": 3

},

"region": {

"startLine": 15,

"snippet": {

"text": "offset = (y + z) \* q + 1;"

}

}

},

"logicalLocation": {

"fullyQualifiedName": "collections::list:add",

"index": 0

},

"annotations": [

{

"startLine": 15,

"startColumn": 13,

"endColumn": 19,

"message": {

"text": "(y + z) = 42",

"markdown": "`(y + z) = 42`"

}

}

],

},

"module": "platform"

},

{

"importance": "essential",

"location": {

"message": {

"text": "Uninitialized variable \"ptr\" passed to

method \"add\_core\".",

"markdown": "Uninitialized variable `ptr` passed to

method `add\_core`."

},

"physicalLocation": {

"artifactLocation": {

"uri":"collections/list.h",

"uriBaseId": "SRCROOT",

"artifactIndex": 3

},

"region": {

"startLine": 25,

"snippet": {

"text": "add\_core(ptr, offset, val)"

}

}

},

"logicalLocation": {

"fullyQualifiedName": "collections::list:add",

"index": 0

}

},

"module": "platform"

}

]

}

]

}

],

"stacks": [

{

"message": {

"text": "Call stack resulting from usage of uninitialized variable."

},

"frames": [

{

"location": {

"message": {

"text": "Exception thrown."

},

"physicalLocation": {

"artifactLocation": {

"uri": "collections/list.h",

"uriBaseId": "SRCROOT",

"artifactIndex": 3

},

"region": {

"startLine": 110,

"startColumn": 15

},

"address": {

"offset": "0x40883A"

}

},

"logicalLocation": {

"fullyQualifiedName": "collections::list:add\_core",

"index": 0

},

},

"module": "platform",

"threadId": 52

"parameters": [ "null", "0", "14" ]

},

{

"location": {

"physicalLocation": {

"artifactLocation": {

"uri": "collections/list.h",

"uriBaseId": "SRCROOT",

"artifactIndex": 3

},

"region": {

"startLine": 43,

"startColumn": 15

},

"address": {

"offset": "0x408894"

}

},

"logicalLocation": {

"fullyQualifiedName": "collections::list:add",

"index": 0

}

},

"module": "platform",

"threadId": 52,

"parameters": [ "14" ]

},

{

"location": {

"physicalLocation": {

"artifactLocation": {

"uri": "application/main.cpp",

"uriBaseId": "SRCROOT",

"artifactIndex": 1

},

"region": {

"startLine": 28,

"startColumn": 9

},

"address": {

"offset": "0x408ACC"

}

},

"logicalLocation": {

"fullyQualifiedName": "main",

"index": 4

}

},

"module": "application",

"threadId": 52

}

]

}

],

"fixes": [

{

"description": {

"text": "Initialize the variable to null"

},

"artifactChanges": [

{

"artifactLocation": {

"uri": "collections/list.h",

"uriBaseId": "SRCROOT",

"artifactIndex": 3

},

"replacements": [

{

"deletedRegion": {

"startLine": 42

},

"insertedContent": {

"text": "A different line\n"

}

}

]

}

]

}

],

"hostedViewerUri":

"https://www.example.com/viewer/3918d370-c636-40d8-bf23-8c176043a2df",

"workItemUris": [

"https://github.com/example/project/issues/42",

"https://github.com/example/project/issues/54"

],

"provenance": {

"firstDetectionTimeUtc": "2016-07-15T14:20:42Z",

"firstDetectionRunGuid": "8F62D8A0-C14F-4516-9959-1A663BA6FB99",

"lastDetectionTimeUtc": "2016-07-16T14:20:42Z",

"lastDetectionRunGuid": "BC650830-A9FE-44CB-8818-AD6C387279A0",

"invocationIndex": 0

}

}

]

}

]

}

1. (Informative) Revision History

|  |  |  |  |
| --- | --- | --- | --- |
| **Revision** | **Date** | **Editor** | **Changes Made** |
| 01 | 2017/09/22 | Laurence J. Golding | Initial version, transcribed from contribution with minor corrections. |
| 02 | 2017/11/29 | Laurence J. Golding | Incorporated changes for GitHub issues [#25](https://github.com/oasis-tcs/sarif-spec/issues/25), [#27](https://github.com/oasis-tcs/sarif-spec/issues/27), and [#56](https://github.com/oasis-tcs/sarif-spec/issues/56). |
| 03 | 2018/01/10 | Laurence J. Golding | Incorporated changes for GitHub issues [#33](https://github.com/oasis-tcs/sarif-spec/issues/33), #[61](https://github.com/oasis-tcs/sarif-spec/issues/61), [#69](https://github.com/oasis-tcs/sarif-spec/issues/69), and [#72](https://github.com/oasis-tcs/sarif-spec/issues/72). Made several minor editorial changes and a few changes to correct inaccuracies. |
| 04 | 2018/01/11 | Laurence J. Golding | Incorporated changes for GitHub issue [#73](https://github.com/oasis-tcs/sarif-spec/issues/73). |
| 05 | 2018/01/15 | Laurence J. Golding | Incorporated changes for GitHub issue [#79](https://github.com/oasis-tcs/sarif-spec/issues/79). |
| 06 | 2018/01/16 | Laurence J. Golding | Two minor editorial changes. |
| 07 | 2018/01/17 | Laurence J. Golding | Incorporated changes for GitHub issue [#65](https://github.com/oasis-tcs/sarif-spec/issues/65). |
| 08 | 2018/02/19 | Laurence J. Golding | Incorporated changes for GitHub issues [#66](https://github.com/oasis-tcs/sarif-spec/issues/66), [#74](https://github.com/oasis-tcs/sarif-spec/issues/74), [#81](https://github.com/oasis-tcs/sarif-spec/issues/81), #[88](https://github.com/oasis-tcs/sarif-spec/issues/88). |
| 09 | 2018/02/28 | Laurence J. Golding | Incorporate changes for GitHub issues [#82](https://github.com/oasis-tcs/sarif-spec/issues/82), [#83](https://github.com/oasis-tcs/sarif-spec/issues/83), [#89](https://github.com/oasis-tcs/sarif-spec/issues/89), [#90](https://github.com/oasis-tcs/sarif-spec/issues/90), [#91](https://github.com/oasis-tcs/sarif-spec/issues/91), [#92](https://github.com/oasis-tcs/sarif-spec/issues/92), [#94](https://github.com/oasis-tcs/sarif-spec/issues/94), and [#104](https://github.com/oasis-tcs/sarif-spec/issues/104). |
| 10 | 2018/03/16 | Laurence J. Golding | Incorporate changes for GitHub issues [#10](https://github.com/oasis-tcs/sarif-spec/issues/10), [#15](https://github.com/oasis-tcs/sarif-spec/issues/15), [#23](https://github.com/oasis-tcs/sarif-spec/issues/23), [#29](https://github.com/oasis-tcs/sarif-spec/issues/29), [#63](https://github.com/oasis-tcs/sarif-spec/issues/63), [#64](https://github.com/oasis-tcs/sarif-spec/issues/64), [#84](https://github.com/oasis-tcs/sarif-spec/issues/84), [#102](https://github.com/oasis-tcs/sarif-spec/issues/102), [#110](https://github.com/oasis-tcs/sarif-spec/issues/110). |
| 11 | 2018/03/28 | Laurence J Golding | Incorporate changes for GitHub issues [#75](https://github.com/oasis-tcs/sarif-spec/issues/75), [#80](https://github.com/oasis-tcs/sarif-spec/issues/80), [#86](https://github.com/oasis-tcs/sarif-spec/issues/86), [#95](https://github.com/oasis-tcs/sarif-spec/issues/95), [#96](https://github.com/oasis-tcs/sarif-spec/issues/96), and [#133](https://github.com/oasis-tcs/sarif-spec/issues/133). |
| 12 | 2018/04/18 | Laurence J. Golding | Incorporate changes for GitHub issues [#46](https://github.com/oasis-tcs/sarif-spec/issues/46), [#98](https://github.com/oasis-tcs/sarif-spec/issues/98), [#99](https://github.com/oasis-tcs/sarif-spec/issues/99), [#107](https://github.com/oasis-tcs/sarif-spec/issues/107), [#108](https://github.com/oasis-tcs/sarif-spec/issues/108), [#11](https://github.com/oasis-tcs/sarif-spec/issues/113)3, [#119](https://github.com/oasis-tcs/sarif-spec/issues/119), [#120](https://github.com/oasis-tcs/sarif-spec/issues/120), [#125](https://github.com/oasis-tcs/sarif-spec/issues/125), and [#130](https://github.com/oasis-tcs/sarif-spec/issues/130). |
| 13 | 2018/05/03 | Laurence J. Golding | Incorporate changes for GitHub issues [#122](https://github.com/oasis-tcs/sarif-spec/issues/122), [#126](https://github.com/oasis-tcs/sarif-spec/issues/126), [#134](https://github.com/oasis-tcs/sarif-spec/issues/134), [#136](https://github.com/oasis-tcs/sarif-spec/issues/136), [#137](https://github.com/oasis-tcs/sarif-spec/issues/137), [#139](https://github.com/oasis-tcs/sarif-spec/issues/139), [#145](https://github.com/oasis-tcs/sarif-spec/issues/145), [#147](https://github.com/oasis-tcs/sarif-spec/issues/147), [#154](https://github.com/oasis-tcs/sarif-spec/issues/154), and [#155](https://github.com/oasis-tcs/sarif-spec/issues/155).  Editorial change in result.ruleMessageId. |
| 14 | 2018/05/08 | Laurence J. Golding | Address GitHub issue [#156](https://github.com/oasis-tcs/sarif-spec/issues/156): editorial |
| 15 | 2018/05/17 | Laurence J. Golding | Incorporate changes for GitHub issues [#103](https://github.com/oasis-tcs/sarif-spec/issues/103), [#138](https://github.com/oasis-tcs/sarif-spec/issues/138), [#141](https://github.com/oasis-tcs/sarif-spec/issues/141), [#143](https://github.com/oasis-tcs/sarif-spec/issues/143), [#153](https://github.com/oasis-tcs/sarif-spec/issues/153), [#157](https://github.com/oasis-tcs/sarif-spec/issues/157), [#159](https://github.com/oasis-tcs/sarif-spec/issues/159), [#160](https://github.com/oasis-tcs/sarif-spec/issues/160), [#161](https://github.com/oasis-tcs/sarif-spec/issues/161), [#162](https://github.com/oasis-tcs/sarif-spec/issues/162), [#163](https://github.com/oasis-tcs/sarif-spec/issues/163), [#165](https://github.com/oasis-tcs/sarif-spec/issues/165), [#166](https://github.com/oasis-tcs/sarif-spec/issues/166), [#167](https://github.com/oasis-tcs/sarif-spec/issues/167), and [#170](https://github.com/oasis-tcs/sarif-spec/issues/170).  Editorial change for “occurs” *vs.* “contains”. |
| 16 | 2018/05/30 | Laurence J. Golding | Incorporate changes for GitHub issues [#93](https://github.com/oasis-tcs/sarif-spec/issues/93), [#149](https://github.com/oasis-tcs/sarif-spec/issues/149), [#160](https://github.com/oasis-tcs/sarif-spec/issues/160) (revised), [#171](https://github.com/oasis-tcs/sarif-spec/issues/171), [#176](https://github.com/oasis-tcs/sarif-spec/issues/176), [#181](https://github.com/oasis-tcs/sarif-spec/issues/181), and [#187](https://github.com/oasis-tcs/sarif-spec/issues/187) (editorial).  Editorial change: Remove “semanticVersion” from all but “Comprehensive” example in Appendix I.  Editorial change: Improve language for default values. |
| 17 | 2018/06/06 | Laurence J. Golding | Incorporate changes for GitHub issues [#158](https://github.com/oasis-tcs/sarif-spec/issues/158), [#164](https://github.com/oasis-tcs/sarif-spec/issues/164), [#172](https://github.com/oasis-tcs/sarif-spec/issues/172), [#175](https://github.com/oasis-tcs/sarif-spec/issues/175), [#178](https://github.com/oasis-tcs/sarif-spec/issues/178), and [#186](https://github.com/oasis-tcs/sarif-spec/issues/186). |
| 18 | 2018/06/08 | Laurence J. Golding | Incorporate changes for GitHub issues #189 and [#191](https://github.com/oasis-tcs/sarif-spec/issues/191). |
| 19 | 2018/11/14 | Laurence J. Golding | Incorporate changes for GitHub issues [#169](https://github.com/oasis-tcs/sarif-spec/issues/169), [#256](https://github.com/oasis-tcs/sarif-spec/issues/256), [#269](https://github.com/oasis-tcs/sarif-spec/issues/269), [#272](https://github.com/oasis-tcs/sarif-spec/issues/272), and [#275](https://github.com/oasis-tcs/sarif-spec/issues/275). |
| 20 | 2018/11/29 | Laurence J. Golding | Incorporate changes for GitHub issues [#186](https://github.com/oasis-tcs/sarif-spec/issues/186), [#188](https://github.com/oasis-tcs/sarif-spec/issues/188), [#274](https://github.com/oasis-tcs/sarif-spec/issues/274), [#279](https://github.com/oasis-tcs/sarif-spec/issues/279), [#280](https://github.com/oasis-tcs/sarif-spec/issues/280), [#284](https://github.com/oasis-tcs/sarif-spec/issues/284), [#285](https://github.com/oasis-tcs/sarif-spec/issues/285), and [#288](https://github.com/oasis-tcs/sarif-spec/issues/288). |
| 21 | 2018/12/13 | Laurence J. Golding | Incorporate changes for GitHub issues [#248](https://github.com/oasis-tcs/sarif-spec/issues/248), [#270](https://github.com/oasis-tcs/sarif-spec/issues/270), [#287](https://github.com/oasis-tcs/sarif-spec/issues/287), #[292](https://github.com/oasis-tcs/sarif-spec/issues/292), #[293](https://github.com/oasis-tcs/sarif-spec/issues/293), and #[297](https://github.com/oasis-tcs/sarif-spec/issues/297). |
| 22 | 2019/01/10 | Laurence J. Golding | Incorporate changes for GitHub issues [#286](https://github.com/oasis-tcs/sarif-spec/issues/286), [#291](https://github.com/oasis-tcs/sarif-spec/issues/291), [#303](https://github.com/oasis-tcs/sarif-spec/issues/303), and [#304](https://github.com/oasis-tcs/sarif-spec/issues/304). |
| 23 | 2019/02/20 | Laurence J. Golding | Incorporate changes for GitHub issues [#146](https://github.com/oasis-tcs/sarif-spec/issues/146), [#312](https://github.com/oasis-tcs/sarif-spec/issues/312), [#317](https://github.com/oasis-tcs/sarif-spec/issues/317), and [#322](https://github.com/oasis-tcs/sarif-spec/issues/322). |
| 24 | 2019/03/15 | Laurence J. Golding | Incorporate changes for GitHub issues [#168](https://github.com/oasis-tcs/sarif-spec/issues/168), [#291](https://github.com/oasis-tcs/sarif-spec/issues/291), [#309](https://github.com/oasis-tcs/sarif-spec/issues/309), [#320](https://github.com/oasis-tcs/sarif-spec/issues/320), [#321](https://github.com/oasis-tcs/sarif-spec/issues/321), [#326](https://github.com/oasis-tcs/sarif-spec/issues/326), [#330](https://github.com/oasis-tcs/sarif-spec/issues/330), [#335](https://github.com/oasis-tcs/sarif-spec/issues/335), [#340](https://github.com/oasis-tcs/sarif-spec/issues/340), and [#341](https://github.com/oasis-tcs/sarif-spec/issues/341). |
| 25 | 2019/03/16 | Laurence J. Golding | Incorporate changes for GitHub issues [#179](https://github.com/oasis-tcs/sarif-spec/issues/179), [#319](https://github.com/oasis-tcs/sarif-spec/issues/319), and [#337](https://github.com/oasis-tcs/sarif-spec/issues/337). |
| 26 | 2019/03/28 | Laurence J. Golding | Incorporate changes for GitHub issues [#202](https://github.com/oasis-tcs/sarif-spec/issues/202), #[302](https://github.com/oasis-tcs/sarif-spec/issues/302), [#311](https://github.com/oasis-tcs/sarif-spec/issues/311), [#314](https://github.com/oasis-tcs/sarif-spec/issues/314), [#315](https://github.com/oasis-tcs/sarif-spec/issues/315), [#318](https://github.com/oasis-tcs/sarif-spec/issues/318), [#324](https://github.com/oasis-tcs/sarif-spec/issues/324), [#325](https://github.com/oasis-tcs/sarif-spec/issues/325), [#327](https://github.com/oasis-tcs/sarif-spec/issues/327), [#338](https://github.com/oasis-tcs/sarif-spec/issues/338), [#344](https://github.com/oasis-tcs/sarif-spec/issues/344), [#346](https://github.com/oasis-tcs/sarif-spec/issues/346), [#347](https://github.com/oasis-tcs/sarif-spec/issues/347), and [#350](https://github.com/oasis-tcs/sarif-spec/issues/350). |

1. Pronounced 'sæ-rɪf (“a” as in “cat”, “i” as in “if”, emphasis on the first syllable). [↑](#footnote-ref-1)