SIEMENS
Ingenuity for life

Version 1.0
April 2019

Usage of Metadata in Siemens' Scapolite format

(presented @NIST SCAP v2 Workshop April 30th to May 2nd 2019)

Dr. Bernd Grobauer, Siemens CT RDA ITS

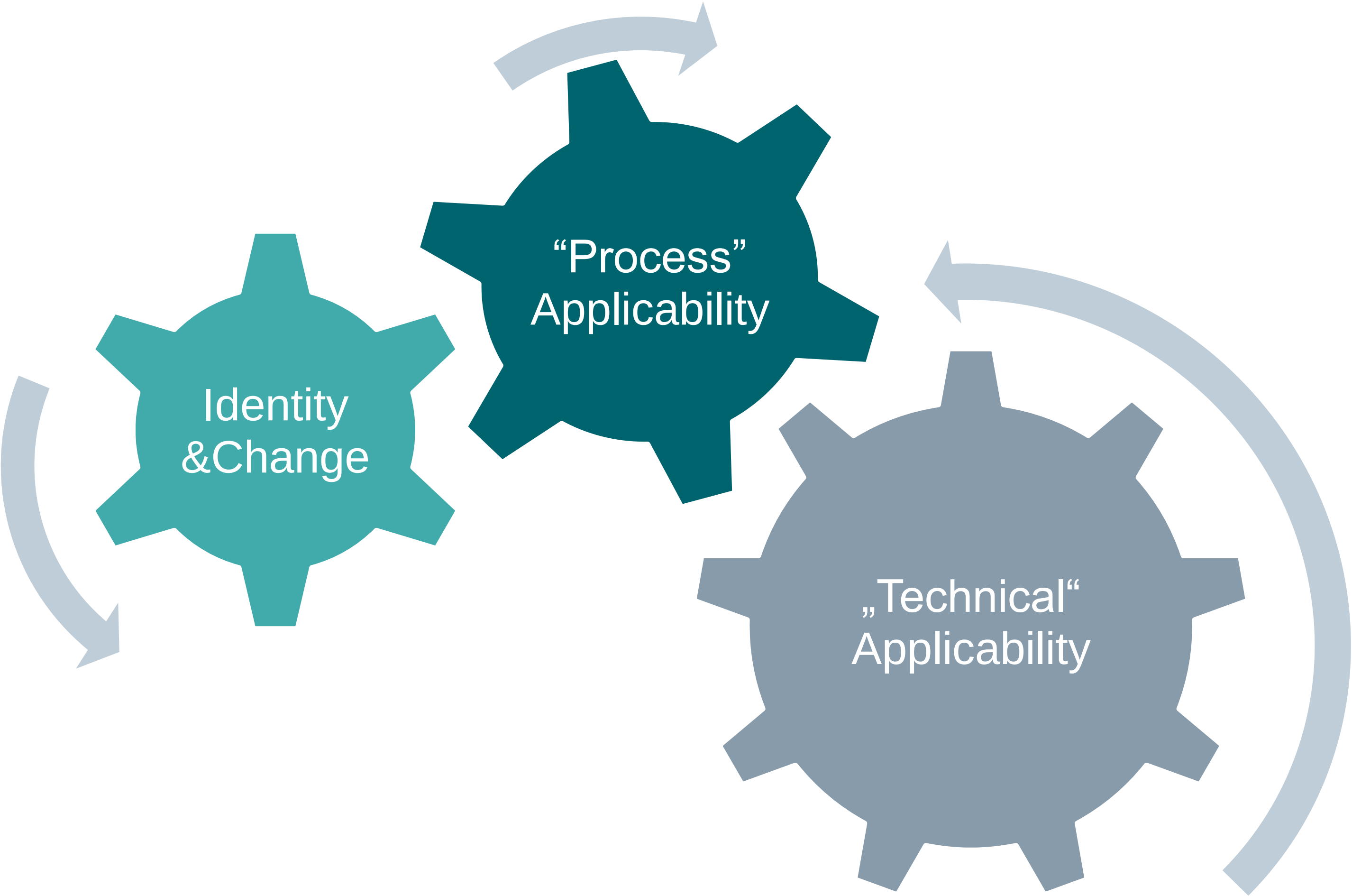
A necessary aside: What is Scapolite?

- **Scapolite** = A format based on **Markdow**n and its **YAML preamble**
- with **precise syntax and semantics**. Think of it as a form of XCCDF in YAML+Markdown that can be
  - maintained as many files rather than one huge file,
  - along with extensions for describing machine-readable stuff such as implementations and checks.

- Every document in the Scapolite format is a valid Markdown (or YAML) document.

- Used at Siemens for authoring and maintaining all Siemens-internal IS polices and baselines using
  - Git as repository
  - a stand-alone command-line tool "scaptain" for processing Scapolite
  - a web application "SFeRA" that ingests content from Scapolite and makes it available to users at Siemens as IS Policy Framework.

Some categories of Metadata we are dealing with



Identity: PLEEEEEEEEEASE don’t change identifiers

SIEMENS
Ingenuity for life

Rule number changes when going from v1.3 to v1.4 of CIS Windows 10 Benchmark (same content, different number)

5.38	5.39
5.40	5.41
5.41	5.42
5.42	5.43
5.43	5.44
5.44	5.45
5.45	5.46
17.6.1	17.6.3
18.1.2.1	18.1.2.2
18.5.4.1	18.5.4.2
18.5.4.2	18.5.4.1
18.5.11.3	18.5.11.4
18.5.11.5	18.5.11.3
18.8.6.1.1	18.8.7.1.1
18.8.6.1.2	18.8.7.1.2
18.8.6.1.3	18.8.7.1.3
18.8.6.1.4	18.8.7.1.4
18.8.6.1.5	18.8.7.1.5
18.8.6.1.6	18.8.7.1.6
18.8.13.1	18.8.14.1
18.8.20.2	18.8.21.2
18.8.20.3	18.8.21.3
18.8.20.4	18.8.21.5
18.8.20.5	18.8.21.4
18.8.21.1.1	18.8.22.1.1
18.8.21.1.2	18.8.22.1.2
18.8.21.1.3	18.8.22.1.3
18.8.21.1.4	18.8.22.1.4
18.8.21.1.5	18.8.22.1.5
18.8.21.1.6	18.8.22.1.6
18.8.21.1.7	18.8.22.1.7
18.8.21.1.8	18.8.22.1.8
18.8.21.1.9	18.8.22.1.9
18.8.21.1.12	18.8.22.1.12
18.8.21.1.13	18.8.22.1.13
18.8.21.1.14	18.8.22.1.14

18.8.24.1	18.8.25.1
18.8.25.1	18.8.26.1
18.8.26.1	18.8.27.2
18.8.26.2	18.8.27.3
18.8.26.3	18.8.27.4
18.8.26.4	18.8.27.5
18.8.26.5	18.8.27.7
18.8.26.6	18.8.27.1
18.8.31.5.1	18.8.33.6.3
18.8.31.5.2	18.8.33.6.4
18.8.31.5.3	18.8.33.6.5
18.8.31.5.4	18.8.33.6.6
18.8.31.5.5	18.8.33.6.2
18.8.31.5.6	18.8.33.6.1
18.8.33.1	18.8.35.1
18.8.33.2	18.8.35.2
18.8.34.1	18.8.36.1
18.8.34.2	18.8.36.2
18.8.41.5.1	18.8.44.5.1
18.8.41.11.1	18.8.44.11.1
18.8.43.1	18.8.46.1
18.8.46.1.1	18.8.49.1.1
18.8.46.1.2	18.8.49.1.2
18.9.34.1	18.9.35.1
18.9.42.1	18.9.44.1
18.9.43.1	18.9.45.1
18.9.43.2	18.9.45.2
18.9.43.4	18.9.45.3
18.9.43.5	18.9.45.4
18.9.43.6	18.9.45.5
18.9.43.7	18.9.45.6
18.9.43.8	18.9.45.7

18.9.43.9	18.9.45.8
18.9.43.10	18.9.45.9
18.9.43.11	18.9.45.10
18.9.49.1	18.9.52.1
18.9.54.2.2	18.9.58.2.2
18.9.54.3.2.1	18.9.58.3.2.1
18.9.54.3.3.1	18.9.58.3.3.1
18.9.54.3.3.2	18.9.58.3.3.2
18.9.54.3.3.3	18.9.58.3.3.3
18.9.54.3.3.4	18.9.58.3.3.4
18.9.54.3.9.1	18.9.58.3.9.1
18.9.54.3.9.2	18.9.58.3.9.2
18.9.54.3.9.3	18.9.58.3.9.3
18.9.54.3.10.1	18.9.58.3.10.1
18.9.54.3.10.2	18.9.58.3.10.2
18.9.54.3.11.1	18.9.58.3.11.1
18.9.54.3.11.2	18.9.58.3.11.2
18.9.55.1	18.9.59.1
18.9.56.2	18.9.60.3
18.9.56.3	18.9.60.4
18.9.56.4	18.9.60.5
18.9.56.5	18.9.60.6
18.9.61.1	18.9.65.1
18.9.64.1	18.9.68.1
18.9.64.2	18.9.68.2
18.9.64.3	18.9.68.3
18.9.64.4	18.9.68.4
18.9.72.3.1	18.9.76.3.2
18.9.72.9.1	18.9.76.9.1
18.9.74.1.1	18.9.80.1.1
18.9.74.2.1	18.9.80.2.1
18.9.74.2.2	18.9.80.2.2
18.9.74.2.3	18.9.80.2.3
18.9.76.1	18.9.82.1
18.9.78.1	18.9.84.2
18.9.78.2	18.9.84.1
18.9.79.1	18.9.85.1
18.9.79.2	18.9.85.2

18.9.79.3	18.9.85.3
18.9.80.1	18.9.86.1
18.9.89.1	18.9.95.1
18.9.89.2	18.9.95.2
18.9.91.1.1	18.9.97.1.1
18.9.91.1.2	18.9.97.1.2
18.9.91.1.3	18.9.97.1.3
18.9.91.2.1	18.9.97.2.1
18.9.91.2.2	18.9.97.2.2
18.9.91.2.3	18.9.97.2.3
18.9.91.2.4	18.9.97.2.4
18.9.92.1	18.9.98.1
18.9.95.1.2	18.9.101.1.3
18.9.95.2	18.9.101.2
18.9.95.3	18.9.101.3
18.9.95.4	18.9.101.4

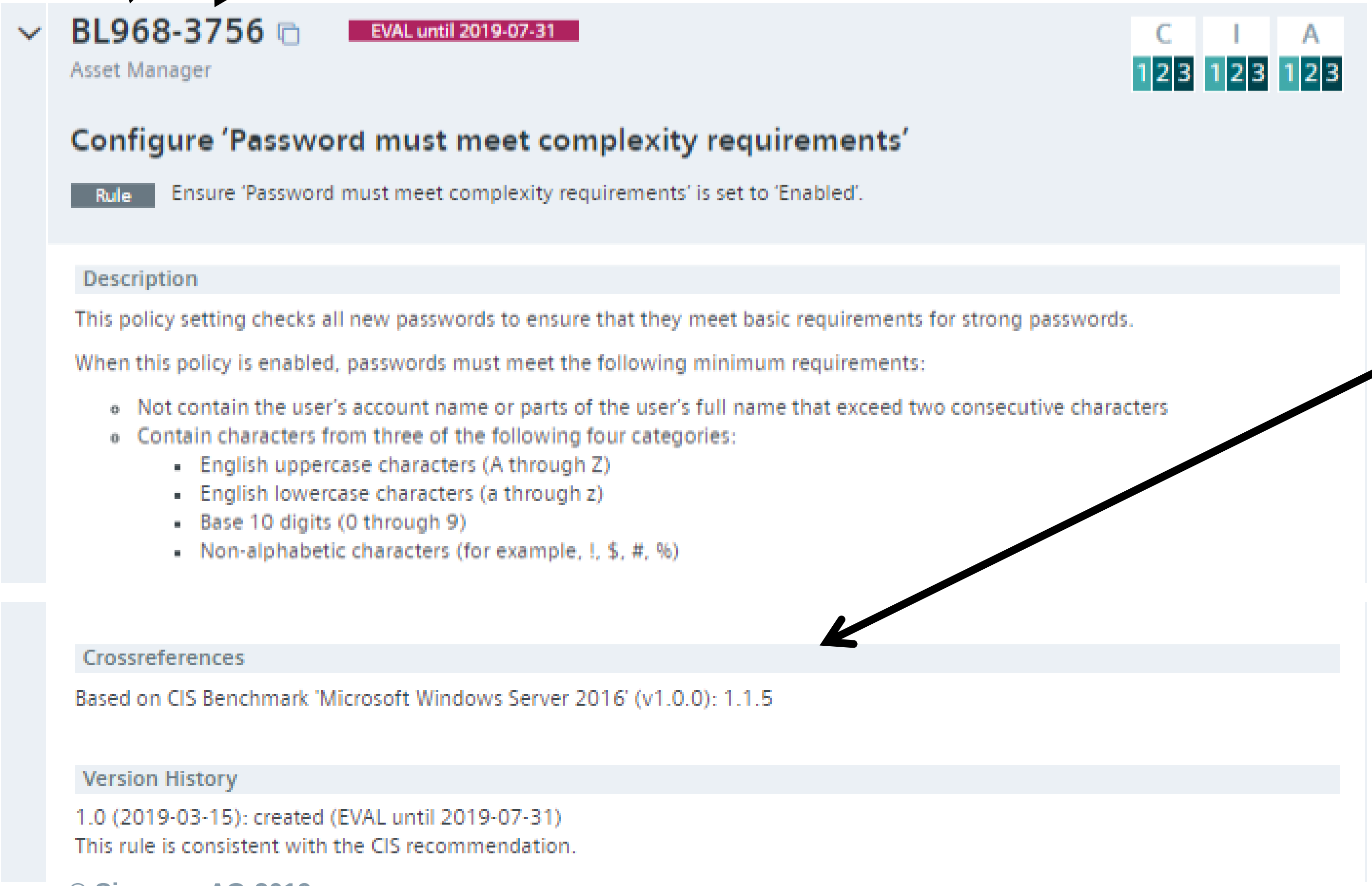
Some rules of thumb:

- Do not change rule identifiers within different iterations of the same baseline
- Don‘t change ***even*** if the rule contents change: you don‘t change your name either just because you have new haircut and now look different (identifiers are not the same as CCE numbers!!!)
- If you derive one document from another document (e.g., Windows Sever 2016 baseline from Windows Server 2012 baseline),
  - provide crossreference back to originating rule
  - consider making relationships explicit in ID scheme

Example usage: Ids and backwards-references

Document number; changes for other Windows releases

Rule-id suffix (random number): stays the same between documents corresponding to different Windows releases



BL968-3756 EVAL until 2019-07-31

Asset Manager

Configure 'Password must meet complexity requirements'

Rule Ensure 'Password must meet complexity requirements' is set to 'Enabled'.

Description

This policy setting checks all new passwords to ensure that they meet basic requirements for strong passwords.

When this policy is enabled, passwords must meet the following minimum requirements:

- Not contain the user's account name or parts of the user's full name that exceed two consecutive characters
- Contain characters from three of the following four categories:
  - English uppercase characters (A through Z)
  - English lowercase characters (a through z)
  - Base 10 digits (0 through 9)
  - Non-alphabetic characters (for example, !, $, #, %)

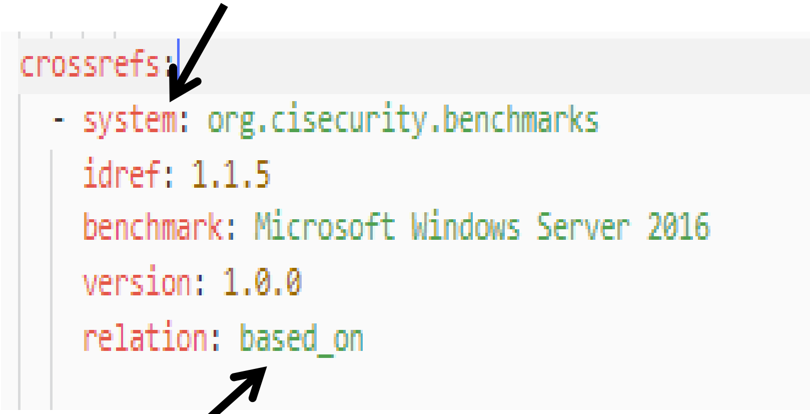
Crossreferences

Based on CIS Benchmark 'Microsoft Windows Server 2016' (v1.0.0): 1.1.5

Version History

1.0 (2019-03-15): created (EVAL until 2019-07-31)
This rule is consistent with the CIS recommendation.

Note that sometimes you need more than an identifier in a reference; Here: document ID and document version



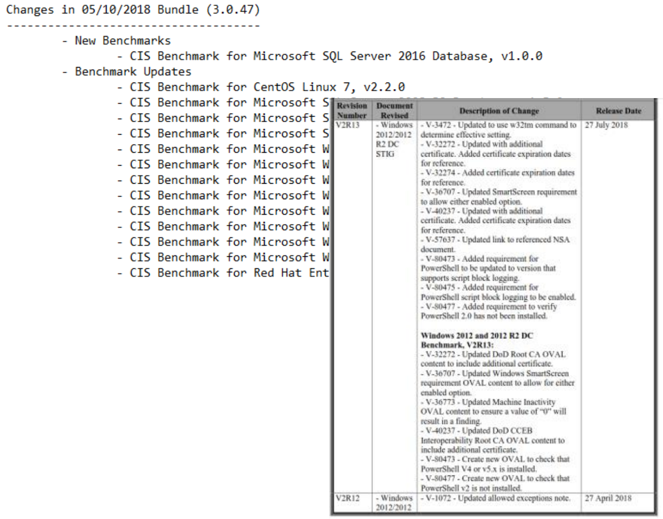
```
crossrefs:
  - system: org.cisecurity.benchmarks
    idref: 1.1.5
    benchmark: Microsoft Windows Server 2016
    version: 1.0.0
    relation: based_on
```

Could be ‚identical‘ in this case, but until we can check this automatically, we have to make a trade-off between precision and maintainability / probability of human error by author/maintainer

Metadata for Change Tracking
Current approaches

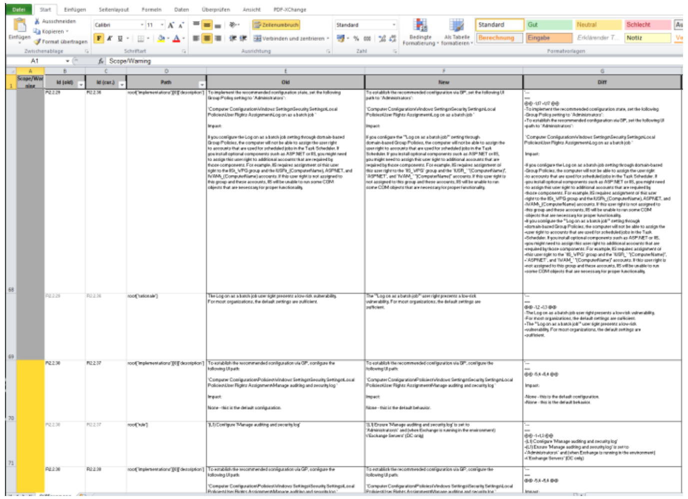
Trust publisher’s release-notes

Use diff tooling to check all differences



```
Changes in 05/10/2018 Bundle (3.0.47)
-------------------------------------
        - New Benchmarks
                - CIS Benchmark for Microsoft SQL Server 2016 Database, v1.0.0
        - Benchmark Updates
                - CIS Benchmark for CentOS Linux 7, v2.2.0
                - CIS Benchmark for Microsoft S
                - CIS Benchmark for Microsoft S
                - CIS Benchmark for Microsoft S
                - CIS Benchmark for Microsoft W
                - CIS Benchmark for Microsoft W
                - CIS Benchmark for Microsoft W
                - CIS Benchmark for Microsoft W
                - CIS Benchmark for Microsoft W
                - CIS Benchmark for Microsoft W
                - CIS Benchmark for Microsoft W
                - CIS Benchmark for Microsoft W
                - CIS Benchmark for Red Hat Ent
```

Revision Number	Document Revised	Description of Change	Release Date
V2R13	- Windows 2012/2012 R2 DC STIG	- V-3472 - Updated to use w32tm command to determine effective setting. - V-32272 - Updated with additional certificate. Added certificate expiration dates for reference. - V-32274 - Added certificate expiration dates for reference. - V-36707 - Updated SmartScreen requirement to allow either enabled option. - V-40237 - Updated with additional certificate. Added certificate expiration dates for reference. - V-57637 - Updated link to referenced NSA document. - V-80473 - Added requirement for PowerShell to be updated to version that supports script block logging. - V-80475 - Added requirement for PowerShell script block logging to be enabled. - V-80477 - Added requirement to verify PowerShell 2.0 has not been installed. **Windows 2012 and 2012 R2 DC Benchmark, V2R13:** - V-32272 - Updated DoD Root CA OVAL content to include additional certificate. - V-36707 - Updated Windows SmartScreen requirement OVAL content to allow for either enabled option. - V-36773 - Updated Machine Inactivity OVAL content to ensure a value of "0" will result in a finding. - V-40237 - Updated DoD CCEB Interoperability Root CA OVAL content to include additional certificate. - V-80473 - Create new OVAL to check that PowerShell V4 or v5.x is installed. - V-80477 - Create new OVAL to check that PowerShell v2 is not installed.	27 July 2018
V2R12	- Windows 2012/2012	- V-1072 - Updated allowed exceptions note.	27 April 2018



Scope/Warning	Id (old)	Id (cur.)	Path	Old	New	Diff
	R2.2.29	R2.2.36	root['implementations'][0]['description']	[illegible]	[illegible]	[illegible]
	R2.2.29	R2.2.36	root['rationale']	[illegible]	[illegible]	[illegible]

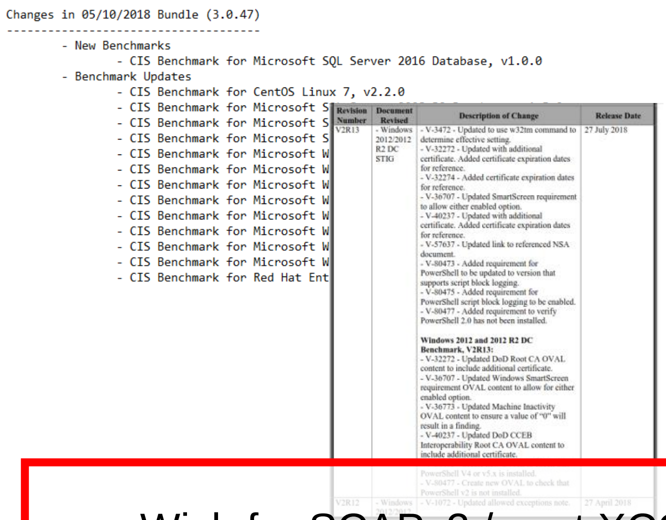
Metadata for Change Tracking
Desired approach: each rule carries meta data about changes

SIEMENS
Ingenuity for life

Trust publisher's release-notes

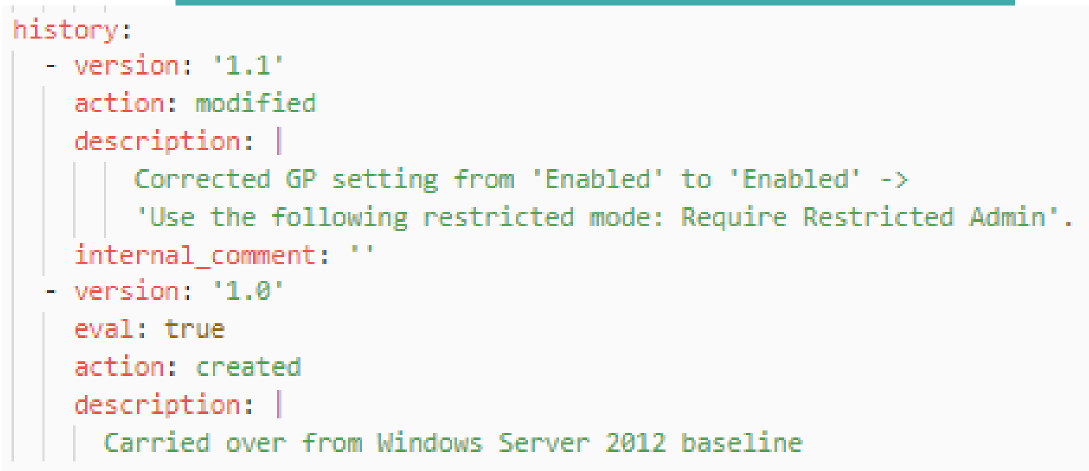
Review per-rule metadata with change-info!!!

Use diff tooling to check all differences

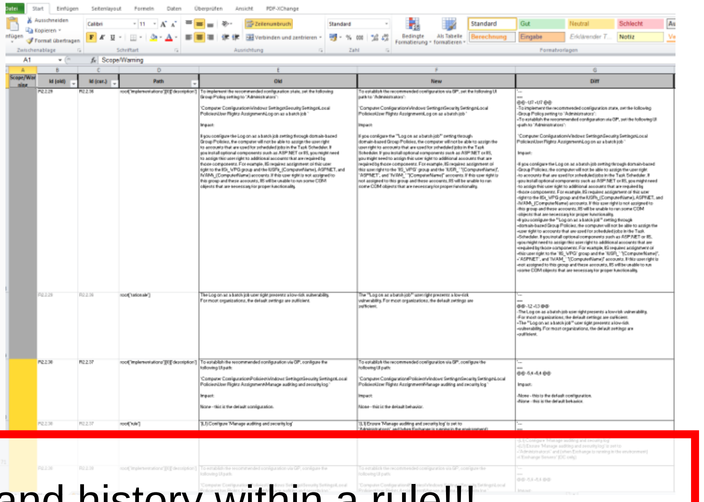


```
Changes in 05/10/2018 Bundle (3.0.47)
-------------------------------------
        - New Benchmarks
                - CIS Benchmark for Microsoft SQL Server 2016 Database, v1.0.0
        - Benchmark Updates
                - CIS Benchmark for CentOS Linux 7, v2.2.0
                - CIS Benchmark for Microsoft S
                - CIS Benchmark for Microsoft S
                - CIS Benchmark for Microsoft S
                - CIS Benchmark for Microsoft W
                - CIS Benchmark for Microsoft W
                - CIS Benchmark for Microsoft W
                - CIS Benchmark for Microsoft W
                - CIS Benchmark for Microsoft W
                - CIS Benchmark for Microsoft W
                - CIS Benchmark for Microsoft W
                - CIS Benchmark for Microsoft W
                - CIS Benchmark for Red Hat Ent
```

Revision Number	Document Revised	Description of Change	Release Date
V2R13	- Windows 2012/2012 R2 DC STIG	- V-3472 - Updated to use w32tm command to determine effective setting. - V-32272 - Updated with additional certificate. Added certificate expiration dates for reference. - V-32274 - Added certificate expiration dates for reference. - V-36707 - Updated SmartScreen requirement to allow either enabled option. - V-40237 - Updated with additional certificate. Added certificate expiration dates for reference. - V-57637 - Updated link to referenced NSA document. - V-80473 - Added requirement for PowerShell to be updated to version that supports script block logging. - V-80475 - Added requirement for PowerShell script block logging to be enabled. - V-80477 - Added requirement to verify PowerShell 2.0 has not been installed. **Windows 2012 and 2012 R2 DC Benchmark, V2R13:** - V-32272 - Updated DoD Root CA OVAL content to include additional certificate. - V-36707 - Updated Windows SmartScreen requirement OVAL content to allow for either enabled option. - V-36773 - Updated Machine Inactivity OVAL content to ensure a value of "0" will result in a finding. - V-40237 - Updated DoD CCEB Interoperability Root CA OVAL content to include additional certificate. PowerShell V4 or v5.x is installed. - V-80477 - Create new OVAL to check that PowerShell v2 is not installed.	27 July 2018
V2R12	- Windows 2012/2012	- V-1072 - Updated allowed exceptions note.	27 April 2018



```
history:
  - version: '1.1'
    action: modified
    description: |
      Corrected GP setting from 'Enabled' to 'Enabled' ->
      'Use the following restricted mode: Require Restricted Admin'.
    internal_comment: ''
  - version: '1.0'
    eval: true
    action: created
    description: |
      Carried over from Windows Server 2012 baseline
```

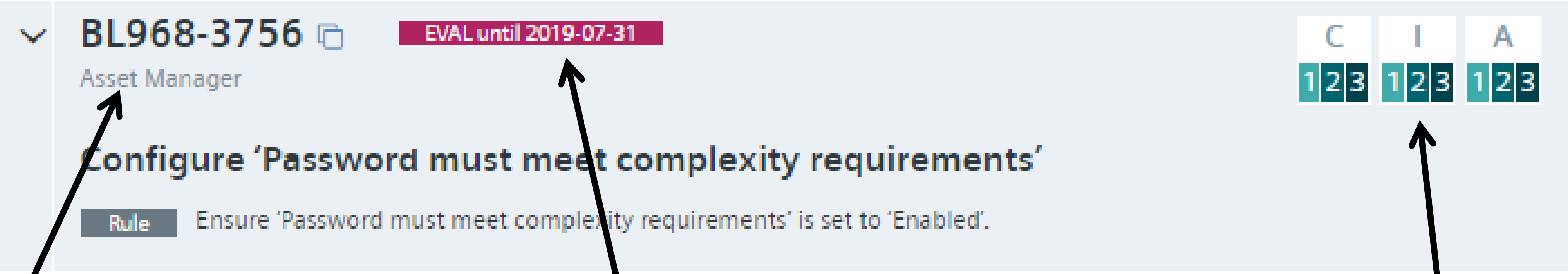


Wish for SCAPv2 / next XCCDF: include capability for keeping metadata on changes and history within a rule!!!

„Process“ Applicability

- Implementation of rules is carried out via processes within an organization
- Processes and thus the required meta-data per rule necessarily vary from organization to organization

➔ **format needs extension points regarding applicability metadata**



BL968-3756

EVAL until 2019-07-31

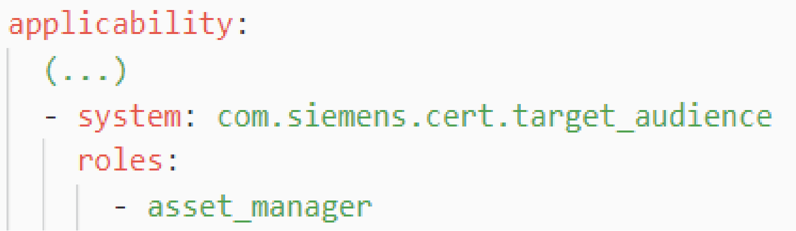
Asset Manager

C	I	A
1 2 3	1 2 3	1 2 3

Configure ‘Password must meet complexity requirements’

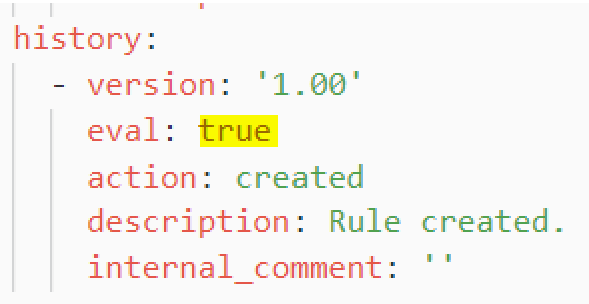
Rule Ensure ‘Password must meet complexity requirements’ is set to ‘Enabled’.

Target audience / responsible person



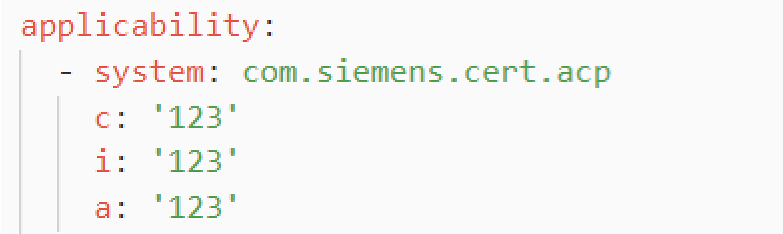
```
applicability:
  (...)
  - system: com.siemens.cert.target_audience
    roles:
      - asset_manager
```

Evaluation-period for new/changed rules



```
history:
  - version: '1.00'
    eval: true
    action: created
    description: Rule created.
    internal_comment: ''
```

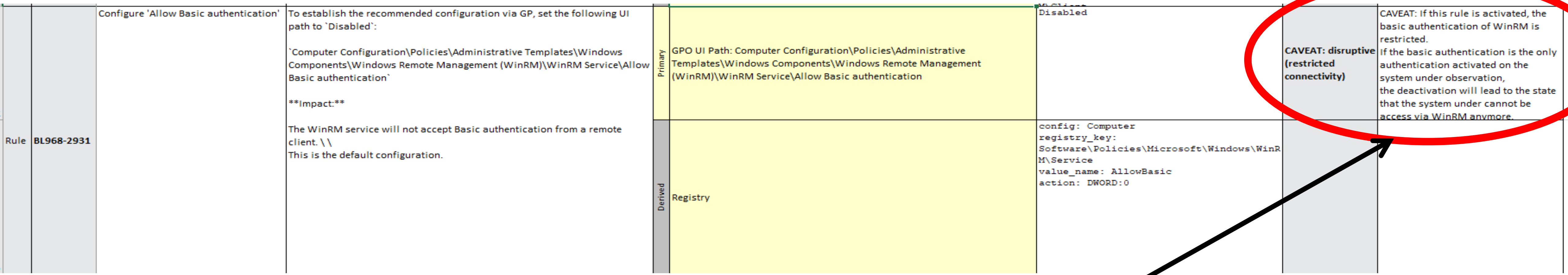
Applicability of rule with respect to Siemens-specific asset-classification



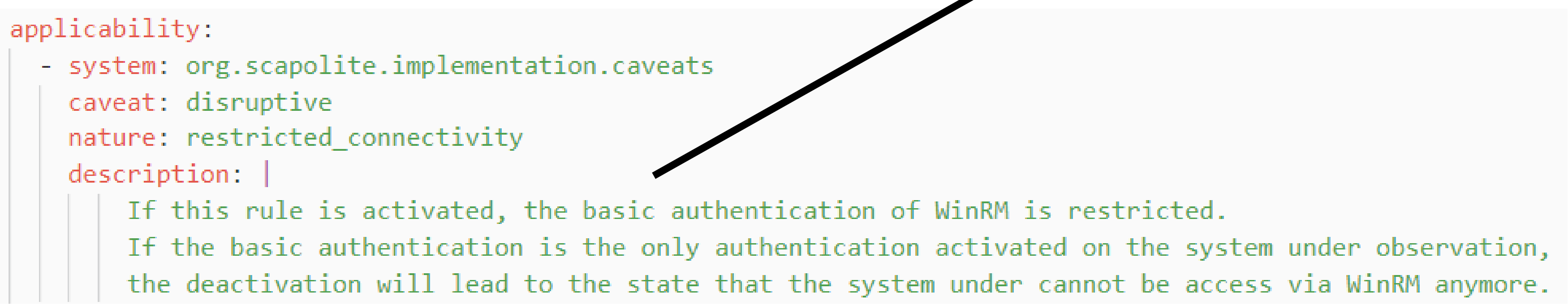
```
applicability:
  - system: com.siemens.cert.acp
    c: '123'
    i: '123'
    a: '123'
```

„Technical“ Applicability

- Distinguishing between different Windows releases
- Caveats: used for displaying information about automations and for manipulating behavior of generated implementation scripts



Rule	**BL968-2931**	Configure 'Allow Basic authentication'	To establish the recommended configuration via GP, set the following UI path to `Disabled`: `Computer Configuration\Policies\Administrative Templates\Windows Components\Windows Remote Management (WinRM)\WinRM Service\Allow Basic authentication` **Impact:** The WinRM service will not accept Basic authentication from a remote client. \\ This is the default configuration.	Primary	GPO UI Path: Computer Configuration\Policies\Administrative Templates\Windows Components\Windows Remote Management (WinRM)\WinRM Service\Allow Basic authentication	Disabled	**CAVEAT: disruptive (restricted connectivity)**	CAVEAT: If this rule is activated, the basic authentication of WinRM is restricted. If the basic authentication is the only authentication activated on the system under observation, the deactivation will lead to the state that the system under cannot be access via WinRM anymore.
				Derived	Registry	config: Computer registry_key: Software\Policies\Microsoft\Windows\WinRM\Service value_name: AllowBasic action: DWORD:0		

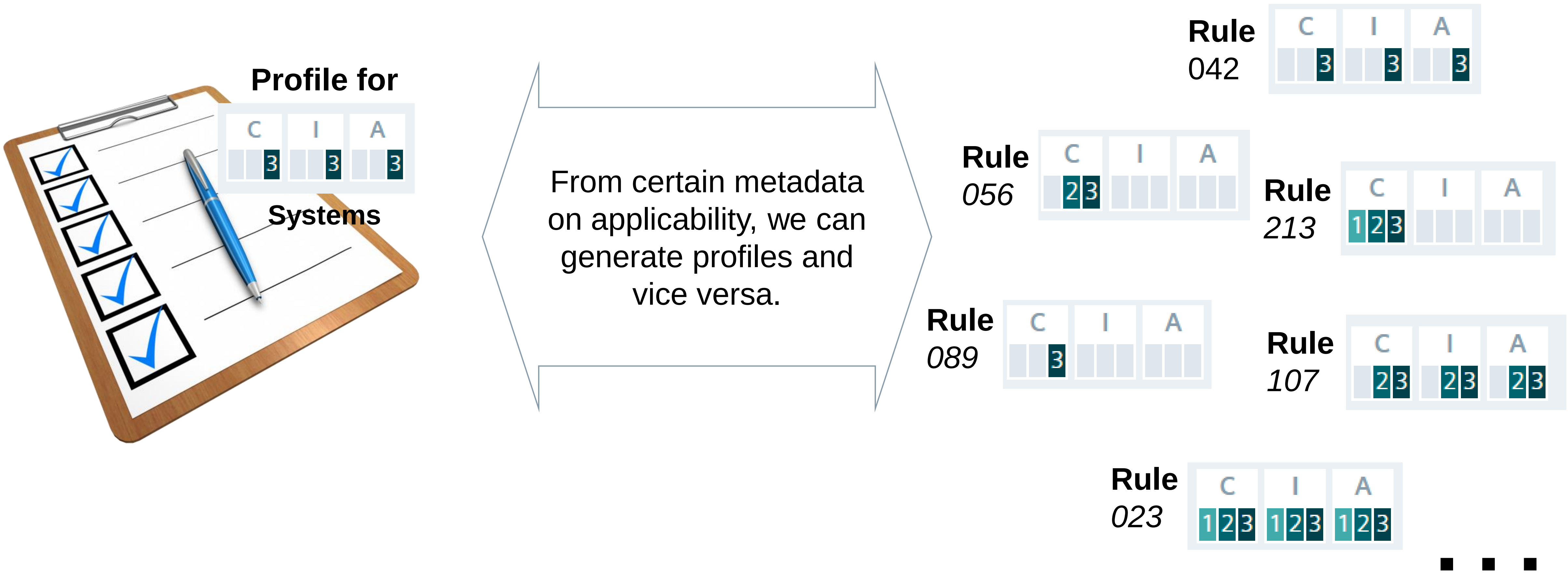


```
applicability:
  - system: org.scapolite.implementation.caveats
    caveat: disruptive
    nature: restricted_connectivity
    description: |
        If this rule is activated, the basic authentication of WinRM is restricted.
        If the basic authentication is the only authentication activated on the system under observation,
        the deactivation will lead to the state that the system under cannot be access via WinRM anymore.
```

Food for thought: Profiles vs. Applicability

SIEMENS
Ingenuity for life

One person‘s applicability metadata (per rule) is another person‘s profile:



Profile for Systems

From certain metadata on applicability, we can generate profiles and vice versa.

Rule 042

Rule *056*

Rule *213*

Rule *089*

Rule *107*

Rule *023*