OpenSCAP 1.2

1.

oscap　　　　　　　　　　　　　. oscap

,

. oscap　[SCAP]　　　　　　　　　　　　　[NIST]

.

NIST　SCAP　　　　　　　　　　　　　. oscap　　　XCCDF　　　　.

. CPE , CCE

OVAL　　　　　　　　　　SCAP　　　　　　　　　　　SCAP

. SCAP　　　　　　　SCAP　　　　　　.

oscap　　　　[OpenSCAP]　　　　　　.
[SCAP Workbench]　　　　.

[scap-security-guide SSG]　　　　　SCAP　　　　　.
SCAP　　　　　　　　　　　　　　(PCI DSS ,
STIG　USGCB)　　　　　　.

XCCDF　　OVAL　　　　　　　SCAP　　　　　　.
XCCDF
. SCAP Workbench　　　　　　.

oscap　　　　　　SCAP　　　　　　　　SCAP
,　　　　　,　　　　　.

SCAP　　　　　,　　　,　　　　　CPE
.

Linux　Windows　　　　　　　oscap
.

2. oscap

.

- A tool (oscap or SCAP Workbench)
- SCAP content (XCCDF, OVAL...)

2.1.

OpenSCAP　　　oscap　　　　(　　　　　　　) Linux
. Fedora　　Red Hat Enterprise Linux　　oscap
yum　　　　　　.

```
# yum install openscap-scanner
```

> ℹ️ openscap-scanner   openscap-utils

  oscap   SCAP   .
                            SSG   .
              .

```
# yum install scap-security-guide
```

SCAP   /usr/share/xml/scap/ssg/content/   .

SCAP   oscap
                  oscap   SCAP 1.2   SCAP   1.1   SCAP 1.0   .
     SCAP   .

oscap,   ,   CPE   OVAL
       .

```
$ oscap -V
```

2.2. SCAP

oscap   SCAP   .   oscap
info   ,   ,   ,   (SCAP
)   (   ).   XCCDF
     SCAP   ,
   .

          target   SCAP   .

```
$ oscap info /usr/share/xml/scap/ssg/content/ssg-rhel7-ds.xml
Document type: Source Data Stream
Imported: 2016-08-10T20:49:16


Stream: scap_org.open-scap_datastream_from_xccdf_ssg-rhel7-xccdf-1.2.xml
Generated: (null)
Version: 1.2
Checklists:
        Ref-Id: scap_org.open-scap_cref_ssg-rhel7-xccdf-1.2.xml
                Status: draft
                Generated: 2016-08-10
                Resolved: true
```

```
             Profiles:
                     xccdf_org.ssgproject.content_profile_standard
                     xccdf_org.ssgproject.content_profile_pci-dss
                     xccdf_org.ssgproject.content_profile_C2S
                     xccdf_org.ssgproject.content_profile_rht-ccp
                     xccdf_org.ssgproject.content_profile_common
                     xccdf_org.ssgproject.content_profile_stig-rhel7-
workstation-upstream
                     xccdf_org.ssgproject.content_profile_stig-rhel7-
server-gui-upstream
                     xccdf_org.ssgproject.content_profile_stig-rhel7-
server-upstream
                     xccdf_org.ssgproject.content_profile_ospp-rhel7-
server
                     xccdf_org.ssgproject.content_profile_nist-cl-il-al
                     xccdf_org.ssgproject.content_profile_cjis-rhel7-
server
             Referenced check files:
                     ssg-rhel7-oval.xml
                             system:
http://oval.mitre.org/XMLSchema/oval-definitions-5
                     ssg-rhel7-ocil.xml
                             system: http://scap.nist.gov/schema/ocil/2
http://www.redhat.com/security/data/oval/Red_Hat_Enterprise_Linux_7.xml
                             system:
http://oval.mitre.org/XMLSchema/oval-definitions-5
Checks:
        Ref-Id: scap_org.open-scap_cref_ssg-rhel7-oval.xml
        Ref-Id: scap_org.open-scap_cref_ssg-rhel7-ocil.xml
        Ref-Id: scap_org.open-scap_cref_output--ssg-rhel7-cpe-oval.xml
        Ref-Id: scap_org.open-scap_cref_output--ssg-rhel7-oval.xml
Dictionaries:
        Ref-Id: scap_org.open-scap_cref_output--ssg-rhel7-cpe-dictionary.xml
```

XCCDF   :

```
$ oscap info /usr/share/xml/scap/ssg/content/ssg-rhel7-xccdf.xml
Document type: XCCDF Checklist
Checklist version: 1.1
Imported: 2016-08-10T20:49:16
Status: draft
Generated: 2016-08-10
Resolved: true
Profiles:
        standard
        pci-dss
        C2S
        rht-ccp
        common
```

```
        stig-rhel7-workstation-upstream
        stig-rhel7-server-gui-upstream
        stig-rhel7-server-upstream
        ospp-rhel7-server
        nist-cl-il-al
        cjis-rhel7-server
Referenced check files:
        ssg-rhel7-oval.xml
                system: http://oval.mitre.org/XMLSchema/oval-definitions-5
        ssg-rhel7-ocil.xml
                system: http://scap.nist.gov/schema/ocil/2
http://www.redhat.com/security/data/oval/Red_Hat_Enterprise_Linux_7.xml
                system: http://oval.mitre.org/XMLSchema/oval-definitions-5
```

Document type：　　　　　　　　　　　　．　　　　　　　　XCCDF, OVAL,　　　　　　　　　W
　　　　　　　　　　　．Checklist version：XCCDF　　　　　　　　　　XCCDF
　　．　　　　　1.1　 1.2　　　．Imported：OpenSCAP
　　．OpenSCAP
　　　　　　　　　　　　　　　．Status：XCCDF　　　　　　　．
accepted, draft, deprecated, incomplete　　　　　．　　　　　　XCCDF
　　．　　XCCDF　　　　　　　　　．Generated date：　　　　／　　　　　　．
　　XCCDF　　W　　　　　　　　XCCDF　　　　　　．Checklists：oscap
xccdf eval　　　　--benchmark-id
　　　　　　　　．　　　　　　　　　　　　　．Profiles：
oscap xccdf eval　　　--profile　　　　　　　ID

(XCCDF   ARF)

oscap info　XCCDF　　　　ARF　　　　　　　　　　　　．
　　　　　　　　　　．

XCCDF　　　　　　　　　　　　　　TestResult　　　　　　．
　　　　　　．

```
<TestResult id="xccdf_org.open-scap_testresult_common" start-
time="2017-01-21T19:16:28" end-time="2017-01-21T19:17:35"
```

ARF　　　　　　　　　　　　TestResult　　　　．　　arf：
report　　　．

```
<arf:reports>
  <arf:report id="xccdf1">
    <arf:content>
      <TestResult xmlns="http://checklists.nist.gov/xccdf/1.2"
id="xccdf_org.open-
scap_testresult_xccdf_org.ssgproject.content_profile_stig-rhel7-server-
```

```
upstream" start-time="2017-01-20T14:30:18" end-time="2017-01-20T14:36:32"
```

HTML   . XCCDF   ARF
HTML   oscap xccdf generate report   .

2.3. OSCAP

oscap   . Oscap   XCCDF
        OVAL   . SCAP
(OVAL   SCAP   )   XML   .
                      .

OVAL

SCAP   OVAL   (OVAL   )   . oscap   OVAL
        OVAL   .   OVAL
    . OVAL   .   OVAL
                      .

        OVAL   .

```
$ oscap oval eval --results oval-results.xml scap-oval.xml
```

        scap-oval.xml   OVAL   oval-results.xml   OVAL   .

        OVAL   .

```
$ oscap oval eval --id oval:rhel:def:1000 --results oval-results.xml scap-
oval.xml
```

        OVAL   oval:rhel:def:1000   scap-oval.xml   OVAL
        oval-results.xml   OVAL   .

SCAP   OVAL
          .

```
$ oscap oval eval --datastream-id ds.xml --oval-id xccdf.xml --results oval-
results.xml scap-ds.xml
```

        ds.xml   , xccdf.xml   OVAL   XCCDF   .
oval-results.xml   OVAL   , scap-ds.xml   SCAP
        .

SCAP   XML   OVAL   XCCDF   .

OVAL   XCCDF   OVAL
.   OVAL
.   .

```
$ oscap xccdf export-oval-variables --profile
united_states_government_configuration_baseline usgcb-rhel5desktop-xccdf.xml
$ oscap oval eval --variables usgcb-rhel5desktop-oval.xml-0.variables-0.xml
--results usgcb-results-oval.xml usgcb-rhel5desktop-oval.xml
```

       united_states_government_configuration_baseline   XCCDF
     , usgcb-rhel5desktop-xccdf.xml   XCCDF   , usgcb-
rhel5desktop-oval.xml   OVAL   usgcb-rhel5desktop-
oval.xml-0.variables-0.xml   XCCDF   , usgcb-
results-oval.xml   OVAL   .

OVAL   "thin"   "full"   .   --
directives <file>   OpenSCAP   .

full   thin   OVAL   :

```
<?xml version="1.0" encoding="UTF-8"?>
<oval_directives xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
xmlns:oval="http://oval.mitre.org/XMLSchema/oval-common-5" xmlns:oval-
res="http://oval.mitre.org/XMLSchema/oval-results-5"
xmlns="http://oval.mitre.org/XMLSchema/oval-directives-5"
xsi:schemaLocation="http://oval.mitre.org/XMLSchema/oval-results-5 oval-
results-schema.xsd http://oval.mitre.org/XMLSchema/oval-common-5 oval-
common-schema.xsd http://oval.mitre.org/XMLSchema/oval-directives-5 oval-
directives-schema.xsd">
  <generator>
    <oval:product_name>OpenSCAP</oval:product_name>
    <oval:schema_version>5.8</oval:schema_version> <!-- make sure the OVAL
version matches your input -->
    <oval:timestamp>2017-02-04T00:00:00</oval:timestamp>
  </generator>
  <directives include_source_definitions="true">
    <oval-res:definition_true reported="true" content="thin"/>
    <oval-res:definition_false reported="true" content="thin"/>
    <oval-res:definition_unknown reported="true" content="thin"/>
    <oval-res:definition_error reported="true" content="thin"/>
    <oval-res:definition_not_evaluated reported="true" content="thin"/>
    <oval-res:definition_not_applicable reported="true" content="thin"/>
  </directives>
</oval_directives>
```

          thin OVAL   .
--without-syschar   .

OVAL　　　　　　　　OVAL　　　　　　　　　　　：

```
$ oscap oval eval --directives directives.xml --without-syschar --results
oval-results.xml oval.xml
```

DataStream　　OVAL　　　　　　　　　　OVAL　　　　　　　　　　：

```
$ oscap oval eval --directives directives.xml --without-syschar --
datastream-id ds.xml --oval-id oval.xml --results oval-results.xml scap-
ds.xml
```

　　　　　　　　　　OVAL　　　　　　　　　　　　　　　. XCCDF
　　　　　　　　.

```
$ oscap info ssg-rhel7-xccdf.xml
Document type: XCCDF Checklist
Checklist version: 1.1
Imported: 2017-01-20T14:20:43
Status: draft
Generated: 2017-01-19
Resolved: true
Profiles:
        standard
        pci-dss
        C2S
        rht-ccp
        common
        stig-rhel7-workstation-upstream
        stig-rhel7-server-gui-upstream
        stig-rhel7-server-upstream
        stig-rhevh-upstream
        ospp-rhel7-server
        nist-cl-il-al
        cjis-rhel7-server
        docker-host
        nist-800-171-cui
Referenced check files:
        ssg-rhel7-oval.xml
                system: http://oval.mitre.org/XMLSchema/oval-definitions-5
        ssg-rhel7-ocil.xml
                system: http://scap.nist.gov/schema/ocil/2
https://www.redhat.com/security/data/oval/com.redhat.rhsa-RHEL7.xml.bz2
                system: http://oval.mitre.org/XMLSchema/oval-definitions-5
```

　　　　　　　　　　　　　　　　　　.　　　　　　ssg-rhel7-oval.xml
　　　　　　.　　　　　　　　　　　　　　　.

oscap info   . Source DataStream
        OVAL   .   oscap ds sds-split
OVAL   .

```
$ oscap ds sds-split ssg-rhel7-ds.xml extracted/
$ ls -1 extracted/
scap_org.open-scap_cref_output--ssg-rhel7-cpe-dictionary.xml
scap_org.open-scap_cref_ssg-rhel7-xccdf-1.2.xml
ssg-rhel7-cpe-oval.xml
ssg-rhel7-ocil.xml
ssg-rhel7-oval.xml
```

                                                    OVAL   XCCDF
        .   DataStream   Source
DataStream   Result DataStream   XCCDF   OVAL   .

XCCDF

XCCDF   oscap   XCCDF   , OVAL   CPE   .
                                  XCCDF   .
        XCCDF   . XCCDF   XCCDF
                              .   CVE   CCE   .
   XCCDF   .

```
Title    Verify permissions on 'group' file
Rule     usgcb-rhel5desktop-rule-2.2.3.1.j
Ident    CCE-3967-7
Result   pass
```

CPE dictionary   .
                          XCCDF   .

        XCCDF   .

XCCDF   .

```
$ oscap xccdf eval --profile Desktop --results xccdf-results.xml --cpe cpe-
dictionary.xml scap-xccdf.xml
```

scap-xccdf.xml   XCCDF   , Desktop   XCCDF   xccdf-
results.xml   , cpe-dictionary.xml   CPE dictionary   .

            --rule   .

```
$ oscap xccdf eval --profile Desktop --rule
ensure_gpgcheck_globally_activated  --results xccdf-results.xml --cpe cpe-
dictionary.xml scap-xccdf.xml
```

        ensure_gpgcheck_globally_activated

.

Source DataStream

. Source DataStream

                oscap xccdf eval   .

SCAP DataStream   DataStream   XCCDF
            .

```
$ oscap xccdf eval --datastream-id ds.xml --xccdf-id xccdf.xml --results
xccdf-results.xml scap-ds.xml
```

      scap-ds.xml   SCAP   , ds.xml
      , xccdf.xml   XCCDF   component-ref   ID   xccdf-
results.xml   .

> --datastream-id
> . --xccdf-id   checklists   .
>   checklists   DataStream   . checklists
>   .

(,   ) SCAP DataStream   DataStream   XCCDF
            .

```
$ oscap xccdf eval --benchmark-id benchmark_id --results xccdf-results.xml
scap-ds.xml
```

      scap-ds.xml   SCAP   , benchmark_id
        xccdf:Benchmark   id   . xccdf-results.xml
            .

Result DataStream (ARF)

            --results   XCCDF   . Result
DataStream (ARF - Asset Reporting Format   ) XML   --results-arf
            .

```
$ oscap xccdf eval --benchmark-id benchmark_id --results-arf arf-results.xml
scap-ds.xml
```

Result STIG Viewer

XCCDF   DISA STIG Viewer   Rule ID   DISA
      --stig-viewer   DISA STIG Viewer   XCCDF
                  .

```
$ oscap xccdf eval --profile stig-rhel7-disa --stig-viewer results-stig.xml
ssg-rhel7-ds.xml
```

    XCCDF   STIG   ID   href
http://iase.disa.mil/stigs/Pages/stig-viewing-guidance.aspx   .

  :

```
<Rule id="rpm_verify_permissions">
  ...
  <reference
href="http://iase.disa.mil/stigs/Pages/stig-viewing-guidance.aspx">SV-86473r
2_rule</reference>
  ...
</Rule>
```

DISA STIG Viewer   .

2.4. Remediate System   (   )

OpenSCAP   .
      XCCDF   . scap-security-guide
    .

                        .

  - oscap   XCCDF   .
  -             OVAL   .   .
  - oscap   .
  -                        oscap   rule-result   .
          .
  - oscap
      OVAL   .   OVAL
                                        .
  -                            XCCDF   .   TestResult   .

TestResult . TestResult
TestResult .

oscap online, offline review .

Online Remediation ( )

. .

--remediate . , `scap-security-guide` .

```
$ oscap xccdf eval --remediate --profile
xccdf_org.ssgproject.content_profile_rht-ccp --results scan-xccdf-
results.xml /usr/share/xml/scap/ssg/content/ssg-rhel7-ds.xml
```

. .
. . ,
.

Offline Remediation ( )

.

XCCDF TestResult .

oscap .
.
TestResult . TestResult - .
.

`scap-security-guide` .

```
$ oscap xccdf eval --profile xccdf_org.ssgproject.content_profile_rht-ccp --
results scan-xccdf-results.xml /usr/share/xml/scap/ssg/content/ssg-rhel7-
ds.xml

$ oscap xccdf remediate --results scan-xccdf-results.xml scan-xccdf-
results.xml
```

Remediation Review

.
.
.

```
$ oscap xccdf generate fix --template urn:xccdf:fix:script:sh --profile
xccdf_org.ssgproject.content_profile_rht-ccp --output my-remediation-
script.sh /usr/share/xml/scap/ssg/content/ssg-rhel7-ds.xml
```

2.5. Check Engines

XCCDF   OVAL   .   OVAL

    .   OVAL   OVAL   .

                            . --
`oval-results`   .

        (: SCE   )   .

OpenSCAP   .

             ,   .

      XCCDF   .

```
$ oscap xccdf eval sds-datastream.xml

Title   Check group file contents
Rule    xccdf_org.example_rule_system_authcontent-group
Result  notchecked

Title   Check password file contents
Rule    xccdf_org.example_rule_system_authcontent-passwd
Result  notchecked

Title   Check shadow file contents
Rule    xccdf_org.example_rule_system_authcontent-shadow
Result  notchecked

...
```

                                    . `notchecked`
                .

CVE, CCE, CPE

   XCCDF   `xccdf:ident`   .
CVE, CCE, CPE   .

      `oscap`   .   :

```
Title   Ensure Repodata Signature Checking is Not Disabled For Any Repos
Rule    rule-2.1.2.3.6.a
Result  pass
```

```
Title    Verify user who owns 'shadow' file
Rule     rule-2.2.3.1.a
Ident    CCE-3918-0
Result   pass

Title    Verify group who owns 'shadow' file
Rule     rule-2.2.3.1.b
Ident    CCE-3988-3
Result   pass
```

(   )   .

HTML   .   CVE   NVD
                                    (   ). OpenSCAP
                      .

   ID   Result Datastream   .
   --results-arf   .


```
$ oscap xccdf eval --profile xccdf_org.ssgproject.content_profile_common --
fetch-remote-resources --results-arf results.xml
/usr/share/xml/scap/ssg/content/ssg-rhel6-ds.xml
```


                results.xml   <rule-result>   .


```
<rule-result idref="xccdf_org.ssgproject.content_rule_partition_for_tmp"
time="2017-01-20T14:30:18" severity="low" weight="1.000000">
  <result>pass</result>
  <ident system="https://nvd.nist.gov/cce/index.cfm">CCE-27173-4</ident>
  <check system="http://oval.mitre.org/XMLSchema/oval-definitions-5">
    <check-content-ref name="oval:ssg-partition_for_tmp:def:1"
href="#oval0"/>
  </check>
</rule-result>
```


OpenSCAP 1.2.9   HTML   Group-By
              .

HTML   . HTML
(: CCE-27173-4)   .
XCCDF ID   .
                      .   SCAP   .
     HTML   .

            (: CCE   NIST 800-53   )
                  HTML   CCE ID   . NIST SP 800-53 ID
            CCE ID   NIST 800-53 ID   .

CCE

OpenSCAP   CCE   .
                                     CCE   ,
                    .