Security Content Update Release Notes for CCS 11.0

2013-3 Update

Security Content Update 2013-3 Release Notes

Legal Notice

Contents

Chapter 1

What's New

This chapter includes the following topics:

What's new in SCU 2013-3

SCU 2013-3 update includes the following enhancements:

Enhancements for Oracle Real Application Clusters (RAC) configurations on Unix:

- The Listener datasource reports on the listener even if listener.ora file is present at any of the following locations:
  - GRID_HOME
  - ORACLE_HOME
  - ASM_HOME
  - CRS_HOME
  - Global locations such as /etc, /var/opt.
  - Any custom location other than home directories and global location.
- The Listener datasource reports on the listener which is associated with the scoped database, in case listeners for other databases are running.

Note: For listener.ora file that is present at a custom location, you must configure listeners with TCP protocol, for database related data collection and platform-based checks to evaluate correctly. You must ensure that the listener status reports the status of the listener that is running, for data collection to work.

- The checks are modified to skip reporting on the database files (control, data, spfiles) which are configured using Oracle Automatic Storage Management. This prevents the checks from resulting as unknown. The checks now report as 'Not Applicable'.

  Note: This enhancement is applicable for RAC as well as standalone oracle database configurations.

- ASM assets are skipped while importing assets.

About Oracle RAC configurations

You can configure oracle RAC database as asset either with SID_NAME or with SERVICE_NAME. You must configure each node of oracle cluster as an asset, since the current CCS architecture considers each node as individual asset.

- If you configure assets with database name as SID_NAME and database name type as SID, you must ensure that entry of SID_NAME is present in oratab file.
- If you configure assets with database name as SERVICE_NAME and database name type as SERVICE_NAME, you must ensure that database name is present in oratab file.

  Note: All entries from the oratab file are imported by default with database name type as SID. If the oratab file contains database name, it also gets imported as an asset with database name type as SID. Data collection and evaluation does not work on such assets. Hence, you must manually delete such assets.

Enhancements for ESM DB2 Audit Configuration Module on Windows:

The ESM DB2 Audit Configuration Module is enhanced for data collection to work on ESM module from CCS.

Note: You must install the 4.3 release of Symantec Enterprise Security Manager for IBM DB2 databases for data collection to work on ESM DB2 Audit Configuration module from CCS.

Enhancement for Domain Cache Database Performance

For very large domains having multiple large groups, the time taken to build the domain cache is drastically reduced from more than 20 hours to less than 3 hours, thereby improving the domain cache database performance.

The domain cache builder can now be configured to build only the target domain cache and not the trusted domain cache files. This configuration now also ensures that trusted domain cache files are not synchronized to the agent. After this configuration, the domain cache file does not contain the information for user, group, and foreign security principal.

To build the cache file for target domain only, you must do the following configuration in the ConfigurationSettings.xml, located at `<CCS install location>\ Reporting and Analytics\DPS\control\Windows\`:

```
<PlatformSetting>

<Key>CachesToBuild</Key>

<Value><![CDATA[Computer]]></Value>

</PlatformSetting>
```

Note: To build the cache file including the information for user, group, and foreign security principal as well as the trusted domain cache files, you must revert the configuration file changes made to ConfigurationSettings.xml.

Enhancements for CCS Standards

Enhancement for VMware standards

- Earlier, if any check from VM Parameters section of the following standards failed due to incorrect parameter value, the evidence field displayed a custom message along with the name of the invalid parameter.
  - VMware Hardening Guidelines ESXi 4.x
  - VMware Hardening Guidelines ESXi 5.1
  - Security Essential for VMware ESXi 4.x
  - Security Essentials for VMware ESX 4.1 via vCenter

  In the 2013-3 update, the Evidence field shows the current and expected values for the incorrect parameter along with the custom message.

Enhancements for CCS standards for better usability

- The standard, 'VMware Hardening Guidelines for vCenter Servers', is now placed under the VMware folder. The checks in this standard are enhanced to be used for vCenter 5.1

- The name of ESXi standards for the VMware platform is appended with 'via vCenter'. These standards are now placed together under VMware folder.
- The name of ESX standards for the Unix platform is appended with 'via Unix'. These standards are also placed together under VMware folder.

Note: From SCU 2013-3 onwards, the ESX 3.0 and ESX 3.5 standards for UNIX platform have been discontinued. However, data collection on these standards can still be performed using existing target types.

New standards

SCU 2013-3 update contains the following new standard:

- **VMware Hardening Guidelines ESXi 5.1 via vCenter**
  The standard contains checks for a set of security baseline configuration parameters. These parameters are recommended for hardening purpose by official VMware Hardening Guidelines ESXi 5.1 which result in a secured posture for the ESX Standalone installations.
- **VMware Hardening Guidelines for vCenter Servers**

Note: This is an existing standard. A new target type - VMware vCenter 4.x and 5.x Servers, has been added to this standard.

New regulatory standards

SCU 2013-3 adds the following new regulatory standard:

- Australian Prudential Regulation Authority (APRA)
  It is the prudential regulator of the Australian financial services industry. It oversees banks, credit unions, building societies, general insurance and reinsurance companies, life insurance, friendly societies, and most members of the superannuation industry.
- ISO/IEC 27001:2013
  ISO 27001 is a technology-neutral, vendor-neutral information security management standard. Of the three parts to IT security governance, ISO 27001 offers the specification – a prescription of the features of an effective information security management system.

New additions in predefined platforms

SCU 2013-3 updates the following predefined platforms:

- Unix
  Updates for the Unix predefined platform are as follows:

Package Datasource	Package datasource is enhanced to support checks from the new CCS standard, 'Comprehensive Standard for AIX'. This standard contains checks that report whether recommended packages are installed on AIX systems. The checks assess patches based on the technology level applied. The checks do not assess patches that are more than two years old and report the minimum technology level that is required to assess such patches.
User Datasource	The field, 'Login: Last Date/Time using su', reports the date and time of last login using su. This support has been added on RHEL. Support for SHA-512 password hashing algorithm for the following fields has been added on agent-based machines: ■ Password: Is Blank? ■ Is Password Weak? The Users data source now reports on users that have password encrypted with SHA-512.

- VMware
  Additions for the VMware predefined platform are as follows:

Target Type	The following new target types are added: ■ VMware ESXi Server 5.x Machines ■ VMware ESXi Server 5.1 Machines
Asset Group	The following new asset group is added: ■ VMware ESXi 5.1 machines The following asset group is updated: ■ VMware ESXi 5.0 machines

- Windows
  Addition for the Windows predefined platform is as follows:

Target Type	The following new target type is added: ■ VMware vCenter 4.x and 5.x Servers

- Oracle
  Addition for the Oracle predefined platform is as follows:

Field	The following field is added to the Listener datasource: ■ Listener Path

Chapter 2

Resolved Issues

This chapter includes the following topics:

Resolved Issues

The 2013-3 Update resolves the following issues for different modules:

- Installation
  - Unable to install ccs.tpk through manual or liveupdate on agent when noexec option is set for /tmp Partition.
    2013 update resolves this issue by changing the extraction path of version verification binary on all UNIX platforms.
- Jobs
  - The asset import job which is scheduled to import ESXi assets through a CSV file, fails.
    2013-2 Update resolves this issue.
  - When the asset import job is executed for Oracle configured databases scoping the UNIX machines, the asset properties of the imported assets are not getting updated.
    2013-3 update resolves this issue by updating the fields with the correct database name and version and operating system version information.
- Data Collection
  - The following checks report incorrect results if '?' or '@' character is used while configuring any initialization parameter on Oracle server because the data collection query is unable to resolve these characters to actual oracle_home and SID name:

- Checks 3.02, 3.03, 3.06, 3.07, 3.09, 3.13 of the standard, 'CIS Oracle 9i and 10g Database Security Benchmark v2.0'
- Checks 3.02, 3.03, 3.06, 3.07, 3.09, 3.11 of the standard, 'CIS Oracle Database Server 11g Security Benchmark v1.0.1'

2013-3 update resolves this issue by enabling the checks to resolve the '?' and '@' character to actual oracle_home and SID name for the scoped asset.

- The ESM Data Collector is unable to handle those DB2 instance connection error messages that do not have database or instance information. Also, these error messages are not being passed to CCS due to which all checks in DB2 standard result as 'PASS' even for those DB2 instances that show connection failure.
  2013-3 update resolves this issue by parsing the database name and instance name in the 'Information' field.

Note: You must install the 4.3 release of Symantec Enterprise Security Manager for IBM DB2 databases for data collection to work on ESM modules from CCS.

- Data collection fails for the following standard, if non-system databases are offline.
  - CIS Security Configuration Benchmark for Microsoft SQL Server 2008 R2 Database v1.0.0
    This issue is observed when Security Content Update (SCU) 2013-1 or SCU 2013-2 is applied on Symantec Control Compliance Suite (Reporting & Analytics) v11.0

  2013-3 update resolves this issue. The warnings listed under the Messages tab mention which non-system databases are offline.
- The ExecutionContext.ini file that is used in setting the inclusion or exclusion of commands when using the sudo functionality, was ignored. Hence all the UNIX commands that were sent to the target computers were incorrectly prefixed with the sudo command.
  2013-3 update resolves this issue by considering the ExecutionContext.ini file during data collection and the commands are executed with or without the sudo prefix based on the values in the file.
- Time-out error was displayed for the sudo test command that took more than 40 seconds for data collection on the target computer. This issue occurred because the command time-out threshold was set to 40 seconds by default.

2013-3 update resolves this issue by increasing the command time-out threshold using the CommandOutputTimeOutSeconds configuration option in case the command is expected to take more than 40 seconds to execute.

- Data collection fails for 'Bulletin/APAR install state' field of APAR datasource for agent-less as well as agent-based mode of data collection on AIX machines. This issue is observed only if Product Update (PU 2012-1) or a later version is applied to CCS 11.0 installation.
  2013-3 update resolves this issue.
- The following check from the standard 'Security Essentials for AIX 5.x and 6.1' evaluates all directories of the system and then filters down to the directories that are mentioned in the root's path, resulting in inefficient use of disk space as well as unnecessary consumption of CPU:
  - The PATH attribute of root does not contain group/world-writable directory.

  2013-3 update resolves this issue by getting the data collected only for group/world writable directories mentioned in root's $path.
- The following check from the standard 'Security Essentials for AIX 5.x and 6.1' passes even if world writable/group files exist in the user's home directory:
  - Are write permissions not allowed for group and others on configuration files in the home directories?

  2013-3 update resolves this issue as the check fails in case world writable/group files exist in the user's home directory.
- Few checks from the standard, 'CIS Security Configuration Benchmark for Microsoft SQL Server 2005 v1.1.1' evaluate as unknown for MS SQL Server 2005 which is installed on a Windows work group machine.
  2013-3 update resolves this issue as these checks evaluate correctly.
- SQL data collection using a non-default MSSQL port fails and reports unknown values in the evaluation.
  2013-3 update resolves this issue.
- IIS version field reports incorrect IIS version in case datasource fails to retrieve IIS version.
  2013-3 update resolves this issue by providing the correct IIS version or by showing appropriate error message in case the IIS version field reports incorrect value.
- Data collection on Windows computers significantly slows down when the domain controller for the trusted domains of the target machine domain are unavailable for cache building.

2013-3 update resolves this issue as the retry attempts for the unavailable domain controllers is reduced by maintaining a map of failed domains during cache building.

- If a domain cache file is corrupt and consistent attempts are made to open the cache then the data collection is delayed significantly.
  2013-3 update resolves this issue. If a cache file is corrupt it is auto-deleted and the entire cache for that domain is rebuilt. If the cache cannot be deleted then an error indicating the same is logged.

Chapter 3

Known Issues

This chapter includes the following topics:

Known Issues

The following known issue is observed in 2013-3 Update:

Table 3-1 Known issues

Issue	Description
Default port 1521 is automatically set for all the imported windows oracle assets.	Default port 1521 is automatically set for all the imported windows oracle assets in the asset system. The oracle data collection job fails and shows error message, if oracle database is configured on a different port other than the default port 1521 . Workaround: Manually change the port for data collection to work.

Chapter 4

Files Added or Updated

This chapter includes the following topics:

Files added or updated for SCU 2013-3

The following files are updated in SCU 2013-3:

Note: The version number for all the files is <11.0.10500.1090>

- Symantec.CSM.ESM.Collector.dll
- ESM.Schema.dll
- Symantec.CSM.VMwarePlatformContent.VMwareESXi4x.dll
- Symantec.CSM.UnixPlatformContent.AIXv1.0.1.dll
- Symantec.CSM.OraclePlatformContent.Oracle_v2.dll
- Symantec.CSM.OraclePlatformContent.Oracle11g.dll
- Symantec.CSM.ESM.MessageSchema.xml
- Symantec.CSM.Content.Localization.Resources.dll
- ORCL.Schema.dll
- VMware.Schema.dll
- Windows.Schema.dll
- Symantec.CSM.ESM.Collector.dll
- Symantec.CSM.ESM.Integration.dll

Data Collector file version for SCU 2013-3

The data collector file version of the following platforms for SCU 2013-3 is <11.0.10500.1090>:

- Oracle
- Microsoft SQL Server
- Unix
- Windows
- VMware