Sentinel 7.0.1 Migration Utility

Technical Reference

June 2012

Contents

Sentinel customers upgrading from Sentinel 6.1 Service Pack 2 Hotfix 1 or Sentinel 6.1 Rapid Deployment Service Pack 2 to Sentinel 7.0.1 can leverage existing configuration data, such as user account, plug-in, collector manager, action, and correlation rule configuration data to provide a smooth transition to the new Sentinel technology.

This Technical Reference provides information about migrating configuration data from an existing Sentinel 6.1 Service Pack 2 Hotfix 1 (Sentinel 6.1) or Sentinel 6.1 Rapid Deployment Service Pack 2 (Sentinel 6.1 RD) deployment to a new Sentinel 7.0.1 installation.

Legal Notice

For more information, please contact NetIQ at:

1233 West Loop South, Houston, Texas 77027

U.S.A.

www.netiq.com

Overview

The Migration Utility helps you leverage your Sentinel 6.1 or Sentinel 6.1 environment and the time you have invested in it by migrating configuration data to your Sentinel 7.0.1 environment. Before migrating configuration data, review the changes and enhancements available in Sentinel 7.0.1. Ensure that you understand which data the Migration Utility does and does not migrate to Sentinel 7.0.1.

What's Different in Sentinel 7.0.1?

The Sentinel 7.0.1 release provides improvements in system architecture and performance. The following list highlights significant changes made in the Sentinel 7.0.1 release:

- Enhanced Data Storage
- Changed Windows Support
- Updated Windows Connector
- New Reporting Engine
- Updated Collector Support
- Updated Schema
- New Features and Enhancements

Enhanced Data Storage

This release of Sentinel provides an efficient, file-based event storage tier optimized for long-term archival of events. The new event store provides 10:1 compression, fully supports indexed searches, and speeds up relevant reporting tasks, while still allowing the flexibility to store some or all of your events in a back-end traditional relational database store.

Therefore, a database is no longer required to store Sentinel events. Sentinel 7.0.1 provides the ability to synchronize event data to an enterprise database where you can use a third-party reporting tool to analyze historical data.

Changed Windows Support

This release of Sentinel drops support for installing Sentinel Server components on Windows computers. If you are currently running Sentinel 6.1 on Windows computers, you must re-host the Sentinel Server, Remote Correlation Engines, and Collector Managers on Linux computers. For more information about supported hardware, see the Sentinel 7.0.1 *Installation Guide*.

If you are currently running Sentinel 6.1 RD, you must re-host your Windows Collector Managers on Linux computers and ensure that you have upgraded to the new Windows Connector.

Updated Windows Connector

The latest version of the Windows Connector requires you to install an instance of Windows Event Collection Service (WECS) on a Windows computer in your environment. You must then configure the WECS to communicate with the Windows Event Connector.

New Reporting Engine

This release of Sentinel uses a built-in reporting engine and no longer requires you to host Crystal Reports in your environment.

Updated Collector Support

Sentinel 7.0.1 supports only Collectors written using the JavaScript language and framework, which is significantly more powerful and flexible than the legacy Collector framework. JavaScript Collectors allow for easy handling of multi-line record formats and multi-byte characters, more powerful and extensible string parsing, support for third-party libraries, and significantly higher event rates.

Starting with Sentinel 7.0, Sentinel and Collector Manager installations do not run Legacy Collectors. Updated Collectors are available at the Sentinel Plug-ins Web site (http://support.novell.com/products/sentinel/secure/sentinelplugins.html).

Updated Schema

Sentinel 7.0 has introduced a revised schema that updates and expands on the schema used in Sentinel 6, 6.1, 6.1 RD, and Sentinel Log Manager 1.x. For a detailed list of the schema changes, see "Schema Updates" on page 19.

New Features and Enhancements

Sentinel 7.0.1 includes new features and enhancements, such as anomaly detection, enhanced correlation, and distributed search. For more information about the features and enhancements included in Sentinel 7.0.1, see the Release Notes on the NetIQ Web site (https://www.netiq.com/documentation/sentinel70/).

Information Migrated to Sentinel 7.0.1

The Migration Utility migrates the following configuration data from your Sentinel 6.1 or Sentinel 6.1 RD environment to your Sentinel 7.0.1 environment. Pre-migration considerations are specified in "Preparing to Migrate" on page 7.

- Event Source Management configuration data
- Plug-in configuration data
- Integrator configuration data
- Action configuration data
- Correlation Engine configuration data
- Correlation Rule data
- Dynamic list data
- Asset configuration data
- Vulnerabilities data
- MSSP data
- User account data
- Advisor/Exploit Detection configuration
- Mapping data
- Content configuration data

Information Not Migrated to Sentinel 7.0.1

The Migration Utility does not migrate the following items, and manual steps to retain this information may be required:

- Event data

  Event data is not migrated due to the high cost of system resources required to migrate the large volume of event data an average Sentinel customer has accumulated. Migrating this amount of data can also be time-intensive. Since the value of any data decreases over time, NetIQ Corporation recommends keeping the migrated source system available until access to the event data is no longer needed.

- Event menu configuration

  The Migration Utility does not migrate customization to the Event menu defined using the Event Menu Configuration option.

- Advisor server data

  To prevent unnecessary downtime, Advisor server data is not migrated to your new environment. You can easily download the Advisor feed in your Sentinel 7.0.1 environment using Download Manager. For more information about downloading the Advisor feed, see the Sentinel 7.0.1 *Administration Guide*.

- Patch history

  Due to the architecture changes introduced in Sentinel 7, patch history is not migrated. The patch history is maintained starting with Sentinel 7.

- Legacy Collectors

  Starting with Sentinel 7.0, clean installations of Sentinel and Collector Manager do not run Legacy Collectors. For more information about Collector support, see "Updated Collector Support" on page 3. Updated Collectors are available at the Sentinel Plug-ins Web site (http://support.novell.com/products/sentinel/secure/sentinelplugins.html).

  Plug-in configuration data is migrated so you can easily configure new Collectors.

- Taxonomy

  Taxonomy reference information is automatically available in Sentinel 7.0.1 and does not require migration.

- Filters

  In Sentinel 7.0.1 the filter language used in searches has changed from RuleLG to the Lucene-based query syntax. Filters previously supplied with the product have been updated to the new syntax. You must rewrite any custom filters.

  The Migration Utility generates a .csv file-based report that lists the various default, user-defined, and global filters in your Sentinel 6.1 or Sentinel 6.1 RD environment. This list enables you to recreate filters as needed in your Sentinel 7.0.1 environment. For more information about writing filters, see the Sentinel 7.0.1 *User Guide*.

- Incidents

  Incident information is dependent on event data, which is not migrated due to the high cost of system resources required and time. Therefore, NetIQ Corporation recommends that you close incidents in the Sentinel 6.1 or Sentinel 6.1 RD environment.

- Custom Incident Categories

  The Migration Utility migrates the association of custom Incident Categories with Action Instances that have a type of `Create Incident`, but these categories are not available for use in Sentinel 7.0.1. You must recreate these custom incident categories in your Sentinel 7.0.1 environment.

- iTrac Workflows

  iTrac workflows are dependent on incident data, which is not migrated due to the high cost of system resources required and time. The Migration Utility does not migrate iTrac workflow instances, workflow definitions, or iTrac roles. Therefore, NetIQ Corporation recommends that you recreate iTrac roles and iTrac workflows based on incidents tracked in your Sentinel 7.0.1 environment prior to migration.

Assessing your Environment

To determine the most efficient and cost-effective method of implementing Sentinel 7.0.1 in your environment, you must first assess your current Sentinel 6.1 or Sentinel 6.1 RD environment. You need to take into account moving Sentinel components on Windows computers to Linux servers, the number of remote Collector Managers, and the volume of events generated. All of these factors can help you decide whether you want to install Sentinel 7.0.1 on existing or new hardware.

Environment Considerations

NetIQ Corporation recommends migrating configuration data, and then migrating Collector Managers and event sources. If you are able to install Sentinel 7.0.1 on new hardware, you can migrate data quickly and you can maintain the original Sentinel 6.1 or Sentinel 6.1 RD system as long as required for access to event and incident data.

Migrating all Sentinel Components to New Hardware

To ensure minimal downtime and to avoid data loss, you can migrate your Sentinel environment to all new hardware. This approach allows you to run your Sentinel 6.1 or Sentinel 6.1 RD environment simultaneously with your new Sentinel 7.0.1 environment.

For example, this deployment scenario assumes a Sentinel 6.1 or Sentinel 6.1 RD server, a Collector Manager on the main Sentinel server (local Collector Manager), two remote Collector Managers, and several Remote Correlation Engines.

After migration, your Sentinel 7.0.1 server, two remote Collector Managers, and several Remote Correlation Engines are installed and running on new hardware.

This scenario is advantageous for organizations that have access to additional hardware and for those who are migrating from a primarily Windows-based environment.

Migrating Sentinel Components to Existing Remote Collector Manager Hardware

To leverage existing hardware, you can migrate your Sentinel server to new hardware while migrating your remote Collector Managers and Remote Correlation Engines to existing hardware. If you want to offload data from your local Sentinel 6.1 or Sentinel 6.1 RD Collector Manager, you can also migrate the local Collector Manager to a remote Collector Manager computer.

For example, this deployment scenario assumes a Sentinel 6.1 or Sentinel 6.1 RD server running a local Collector Manager, two remote Collector Managers, and several Remote Correlation Engines.

After migration, your Sentinel 7.0.1 server is running on new hardware, but your remote Collector Managers and Remote Correlation Engines are running on the existing hardware. Optionally, your local Collector Manager is running on a new remote computer.

The advantage of this approach is the ability to reuse existing hardware. The disadvantage of this approach is increased downtime and potential increased event loss. Migrating to existing hardware requires more planning and post-migration steps than migrating to all new hardware.

Preparing to Migrate

To minimize the amount of post-migration work and help minimize downtime, perform the following tasks as needed for your environment prior to exporting configuration data from your Sentinel 6.1 or Sentinel 6.1 RD installation.

	Category	Task
❑	Hardware	Ensure that the hardware on which you want to install Sentinel 7.0.1 meets the hardware requirements. For more information about Sentinel 7.0.1 hardware requirements and prerequisites, see the *Installation Guide* on the NetIQ Web site (https://www.netiq.com/documentation/sentinel70/).
❑	Collector Manager	Ensure that you have synchronized the date and time of the Collector Manager from which you want to migrate configuration data and that it is in a healthy state.
❑	Plug-ins	Ensure that you have the most current version of the Sentinel Plug-ins installed in your Sentinel 6.1 or Sentinel 6.1 RD environment. For more information about Plug-in versions, see the Sentinel Plug-ins Web site (http://support.novell.com/products/sentinel/secure/sentinelplugins.html).
❑	Integrators	Ensure that there are no duplicate Integrator names in your Sentinel 6.1 or Sentinel 6.1 RD and Sentinel 7.0.1 environments. If there are duplicate instances, rename the duplicate names in either the Sentinel 6.1, Sentinel 6.1 RD, or Sentinel 7.0.1 environment prior to exporting Integrators. If you do not rename duplicate Integrators prior to migration, you can rename the duplicate Integrator in Sentinel 7.0.1 after migration.
❑	Actions	Ensure that there are no duplicate Action names in your Sentinel 6.1 or Sentinel 6.1 RD and Sentinel 7.0.1 environments. If there are duplicate instances, rename the duplicate names in either the Sentinel 6.1, Sentinel 6.1 RD, or Sentinel 7.0.1 environment prior to exporting Actions. If you do not rename duplicate Actions prior to migration, you can rename the duplicate Action in Sentinel 7.0.1 after migration.
		Ensure that there are no duplicate custom scripts associated with Action instances in your Sentinel 6.1 or Sentinel 6.1 RD and Sentinel 7.0.1 environments. If there are duplicate custom scripts, rename the duplicate custom scripts in either the Sentinel 6.1, Sentinel 6.1 RD, or Sentinel 7.0.1 environment prior to exporting Actions. If you do not rename duplicate custom scripts prior to migration, the Migration Utility will create a unique name for the imported custom script.

	Category	Task
❑	Correlation Engines and Rules	Ensure that there are no duplicate Correlation Rules in your Sentinel 6.1 or Sentinel 6.1 RD and Sentinel 7.0.1 environments. If there are duplicate instances, rename the duplicate Correlation Rules in either the Sentinel 6.1, Sentinel 6.1 RD, or Sentinel 7.0.1 environment prior to exporting Correlation Engines and Rules. If you do not rename duplicate Correlation Rules prior to migration, you can rename the duplicate Rule in Sentinel 7.0.1 after migration.
❑	Dynamic Lists	Ensure that there are no duplicate Dynamic List names in your Sentinel 6.1 or Sentinel 6.1 RD and Sentinel 7.0.1 environments. If there are duplicate instances, rename the duplicate names in either the Sentinel 6.1, Sentinel 6.1 RD, or Sentinel 7.0.1 environment prior to exporting Dynamic Lists. If you do not rename duplicate Dynamic Lists prior to migration, the Migration Utility creates a unique name for the imported instance.
❑	User Accounts	Ensure that there are no user accounts with duplicate names in the Sentinel 7.0.1 environment that are in the active or disabled state. If there are duplicate user accounts in either of these states, the Migration Utility will not migrate user account information for those users. If you want to re-import a user account, you must first modify or delete the account in Sentinel 7.0.1, and then import the user account.
		Ensure that the User role exists in your Sentinel 7.0.1 environment.
		If you use LDAP authentication, manually configure LDAP settings on your Sentinel 7.0.1 computer to enable users to log in to Sentinel as an LDAP user. For more information, see “Configuring LDAP Authentication” in the Sentinel 7.0.1 *Administration Guide*.
❑	Advisor	You need to download and process Advisor feed files to see advisor data post migration.
❑	Ports	On the Sentinel 7.0.1 server, manually modify the Event Source Server port numbers to avoid a duplicate port conflict during the migration process. Sentinel 7.0.1 Event Source Server ports could conflict with ports migrated from the Sentinel 6.1 local Collector Manager or remote Collector Managers.

Exporting Sentinel 6.1 and Sentinel 6.1 RD Configuration Data

Export configuration data from your Sentinel 6.1 or Sentinel 6.1 RD environment by completing the following checklist.

	Checklist
❑	1. Ensure that you have reviewed all tasks in “Preparing to Migrate” on page 7 and have taken any action required for your environment.
❑	2. Log on to the Sentinel 6.1 or Sentinel 6.1 RD Sentinel server with a user account that has permission to run Sentinel services. For example, `esecadm` or `novell` on a Linux server or administrator on a Windows server.
❑	3. Copy the `SentinelMigrationTool.zip` file to your Sentinel 6.1 or Sentinel 6.1 RD Sentinel Server.
❑	4. Extract all files from `SentinelMigrationTool.zip` to the `SentinelMigrationTool` directory.

	Checklist
❑	5. *If you are exporting files from a Windows computer*, run command `export.bat`.
❑	6. *If you are exporting files from a Linux server*, run command `./export.sh`.
❑	7. After the export operation completes, note the name of the export `.zip` file in the Migration Utility directory.

Importing Configuration Data into Sentinel 7.0.1

Import configuration data from your Sentinel 6.1 or Sentinel 6.1 RD environment into your Sentinel 7.0.1 environment by completing the following checklist.

	Checklist
❑	1. Install Sentinel 7.0.1 in your environment. For more information about installing Sentinel 7.0.1, see the Sentinel 7.0.1 *Installation Guide*.
❑	2. *If you are migrating configuration data to all new hardware*, install remote Collector Managers as needed and configure them to communicate with the Sentinel 7.0.1 server. For more information about installing and configuring remote Collector Managers, see the Sentinel 7.0.1 *Installation Guide*.
❑	3. Ensure that Sentinel 7.0.1 is running in your environment.
❑	4. Move the exported `.zip` file created by the Migration Utility to the Sentinel 7 Server. For more information about exporting configuration data, see "Exporting Sentinel 6.1 and Sentinel 6.1 RD Configuration Data" on page 8.
❑	5. *If you are migrating configuration data to all new hardware*, see "Using All New Hardware" on page 10.
❑	6. *If you are migrating configuration data to existing hardware*, see "Reusing Existing Hardware" on page 10.
❑	7. Run the Migration Utility to import Sentinel 6.1 or Sentinel 6.1 RD configuration data. For more information about importing configuration data, see "Using the Migration Utility to Import Configuration Data" on page 12.
❑	8. For configuration changes to take effect, you must restart Sentinel 7 services, remote Collector Managers, and Remote Correlation Engines as root user.
❑	9. Verify the above configurations were migrated properly.

Using All New Hardware

To ensure minimal downtime and to avoid data loss, you can migrate your Sentinel environment to all new hardware.

To import configuration data on all new hardware:

1. Modify all the event sources that were connected to the local Sentinel 6.1 Collector Manager to communicate with the local Sentinel 7.0.1 Collector Manager.
2. Verify that all Collectors configured to communicate with Sentinel 7.0.1 Collector Managers start receiving events.
3. Upgrade Sentinel 6.1 remote Correlation Engine computers to Sentinel 7.0.1.
4. Use the Sentinel 7.0.1 Web console to offload the Correlation Rules deployed on the local Correlation Engine on the Sentinel 7.0.1 server to the remote Correlation Engine as needed.
5. Migrate your remote Collector Managers by performing the following steps:
   a. Note the IP address of the Sentinel 6.1 or Sentinel 6.1 RD remote Collector Manager server.
   b. Change the IP address of the Sentinel 6.1 or Sentinel 6.1 RD remote Collector Manager server.
   c. Assign the IP address from Step **a** to the Sentinel 7.0.1 remote Collector Manager server.
   d. Run the Migration Utility on the Sentinel 7.0.1 server and select the ESM component.
   e. Import the appropriate Sentinel 6.1 or Sentinel 6.1 RD configuration.
   f. Restart the Sentinel 7.0.1 services.
   g. Restart the remote Collector Manager configured above.
   h. Verify that all the Collectors configured to communicate with the Sentinel 7.0.1 remote Collector Managers start receiving events.
   i. Repeat Step **a** through Step **h** for all other remote Collector Managers connected to your Sentinel 6.1 or Sentinel 6.1 RD server.

Reusing Existing Hardware

To leverage existing hardware, you can migrate your Sentinel server to new hardware while migrating your remote Collector Managers and Remote Correlation Engines to existing hardware.

To import configuration data on existing hardware:

1. ***If you are migrating Sentinel 6.1 or Sentinel 6.1 RD remote Collector Manager data to a Sentinel 7.0.1 remote Collector Manager computer***, perform the following steps:
   a. To help prevent event loss during migration, NetIQ Corporation recommends that you temporarily set up port forwarding for the Event Source Servers configured on the Sentinel 6.1 remote Collector Manager to the Sentinel 7.0.1 local Collector Manager. To temporarily forward events, perform the following steps:
      1.Run the Migration Utility on the Sentinel 7.0.1 server and import the Sentinel 6.1 remote Collector Manager to the Sentinel 7.0.1 local Collector Manager.
      2. Restart the Sentinel 7.0.1 services.

b. On the Sentinel 6.1 or Sentinel 6.1 RD remote Collector Manager, ensure that all events are cleared out of the following directory:

```
/opt/novell/sentinel6/data/plugindata/auditConnectorServer/pageFile/
<ESS_UUID>/<Connector_UUID>
```

c. Stop all services on the Sentinel 6.1 or Sentinel 6.1 RD remote Collector Manager, and then uninstall the remote Collector Manager.

d. Install a Sentinel 7.0.1 remote Collector Manager on the same server retaining the same IP address.

e. Configure the Sentinel 7.0.1 Collector Manager to communicate with the Sentinel 7.0.1 Sentinel server.

f. Run the Migration tool again on the Sentinel 7.0.1 server and import the Sentinel 6.1 or Sentinel 6.1 RD remote Collector Manager.

g. Restart the Sentinel 7.0.1 services.

h. Remove the port forwarding set up in Step **a**.

i. Restart the Sentinel 7.0.1 remote Collector Manager configured in Step **e**.

j. Verify that all the collectors configured to communicate with the Sentinel 7.0.1 remote Collector Manager start receiving events.

k. Repeat Steps **a** through Step **j** for all other remote Collector Managers.

2. ***If you are migrating Sentinel 6.1 or Sentinel 6.1 RD local Collector Manager data to a Sentinel 7.0.1 local Collector Manager***, perform the following steps:

a. To help prevent event loss during migration, NetIQ Corporation recommends that you temporarily set up port forwarding for the Event Source Servers configured on the Sentinel 6.1 remote Collector Manager to the Sentinel 7.0.1 local Collector Manager. To temporarily forward events, perform the following steps:

1.Run the Migration Utility on the Sentinel 7.0.1 server and import the Sentinel 6.1 remote Collector Manager to the Sentinel 7.0.1 local Collector Manager.

2. Restart the Sentinel 7.0.1 services.

b. Modify all the event sources that were connected to the Sentinel 6.1 or Sentinel 6.1 RD local Collector Manager to communicate with the Sentinel 7.0.1 local Collector Manager.

c. Verify that all the collectors configured to communicate with the Sentinel 7.0.1 server and remote Collector Managers start receiving events.

3. ***If you are migrating Sentinel 6.1 or Sentinel 6.1 RD Local Collector Manager data to a Sentinel 7.0.1 remote Collector Manager computer***, perform the following steps:

   a. Install Sentinel 7.0.1 remote Collector Manager and configure it to communicate with the Sentinel 7.0.1 server.

   b. On the Sentinel 6.1 or Sentinel 6.1 RD local Collector Manager, enable client side caching of events for Sentinel Link and Audit Event Source servers by performing the following steps:

      1.Change the port on which your Audit Event Source servers are configured to listen.

      2. Configure the Sentinel Link Integrator to enable `event queuing`.

      By doing this, the clients connected to these Event Source Servers start caching events. Once the connection is re-established for the Audit Event Source server and the Sentinel Link Integrator is reconfigured to use `event forward` mode, the clients will forward these events to the Sentinel 7.0.1 remote Collector Manager.

   c. Verify that all events in the Event Source Server are cleared out of the queue.

   d. Note the IP address of the Sentinel 6.1 or Sentinel 6.1 RD server.

   e. Change the IP address of the Sentinel 6.1 or Sentinel 6.1 RD server.

   f. Assign the IP address noted in Step **d** to the Sentinel 7.0.1 remote Collector Manager.

   g. Run the Migration Utility on the Sentinel 7.0.1 server and select the ESM component.

   h. Import the Sentinel 6.1 or Sentinel 6.1 RD local Collector Manager configuration to the Sentinel 7.0.1 remote Collector Manager.

   i. Restart the Sentinel 7.0.1 server and remote Collector Manager.

   j. Verify that all the Collectors configured to communicate with the Sentinel 7.0.1 server and remote Collector Managers start receiving the events.

4. Upgrade the Sentinel 6.1 Remote Correlation Engine computers to Sentinel 7.0.1.

5. Use the Sentinel 7.0.1 Web console to offload the Correlation Rules deployed on the local Correlation Engine on the Sentinel 7.0.1 server to the Remote Correlation Engine as needed.

Using the Migration Utility to Import Configuration Data

After exporting configuration data from your Sentinel 6.1 or Sentinel 6.1 RD environment, import the configuration data into your Sentinel 7.0.1 environment.

To import configuration data:

1. Log on to the Sentinel 7.0.1 server with a user account that has permission to run Sentinel services. For example, `novell`.

2. Extract the `SentinelMigrationTools.zip` file to the `SentinelMigrationTool` directory.

3. Run the `./import.sh` command.

4. Use the interactive import operation menu to import configuration data. For more information about importing various configuration data types, see the following sections:

   - "Importing Event Source Management Configuration Data" on page 13
   - "Importing Plug-in Configuration Data" on page 13
   - "Importing Action Configuration Data" on page 14

Importing Event Source Management Configuration Data

Before importing Event Source Management configuration data, consider the following:

- ***If your Sentinel 7.0.1 environment contains more than one Collector Manager***, the Migration Utility prompts you to specify to which Collector Manager you want to migrate the Sentinel 6.1 or Sentinel 6.1 RD Collector Manager data. If there is only one Collector Manager, the Migration Utility maps the Collector Manager automatically.
- ***If the Sentinel 6.1 or Sentinel 6.1 RD Collector Manager is configured to communicate with any legacy Collectors that were not replaced with JavaScript Collectors in the Sentinel 7.0.1 environment***, you must update the legacy Collector information in the Collector Manager configuration.
- ***If you import the Event Source Management data to a Sentinel 7.0.1 server that was installed on new hardware***, you must manually configure the File Connector event source file location and configure the clients, such as Syslog, Platform Agent, and SNMP, to communicate with the new server.

  Due to a time lag during the migration process and between exporting and importing data, the offset value for the Connector may not be current and could cause Sentinel to read events from the beginning of the file. This can result in duplicate events.

For more information about Event Source Management considerations, see "Understanding Event Source Management Components" on page 15.

Importing Plug-in Configuration Data

Before importing Plug-in configuration data, consider the following:

- The Migration Utility imports all JavaScript Collectors found in the Sentinel 6.1 or Sentinel 6.1 RD environment if the same Collector does not exist in the Sentinel 7.0.1 environment.
- When importing Plug-ins to the Sentinel 7.0.1 environment, the Migration Utility imports configuration data for only legacy Collectors that do not have a JavaScript equivalent Collector already installed in the Sentinel 7.0.1 environment. Since the Sentinel 7.0.1 environment does not support legacy Collectors, the configuration information is imported to assist with the configuration of new JavaScript Collectors. This is also true for the legacy Windows Connector (version 6r[1-7]).
- If you import an older version of the Database Connector, you receive the error `The url cannot be null` until you install the latest version of the Database Connector in your Sentinel 7.0.1 environment.

Importing Action Configuration Data

The Migration Utility does not migrate custom scripts saved with the batch (.bat) extension on Sentinel 6.1 Windows computers. Since Sentinel 7.0.1 no longer supports installing Sentinel components on Windows computers, these scripts are not migrated because they are no longer applicable when you install Sentinel on a Linux server.

Importing Correlation Engine and Rule Configuration Data

If your Sentinel 7.0.1 environment contains more than one Correlation Engine, the Migration Utility prompts you to specify to which Correlation Engine you want to migrate the Sentinel 6.1 or Sentinel 6.1 RD correlation rules. If there is only one Correlation Engine, the Migration Utility maps the correlation rules automatically.

NetIQ Corporation recommends that you initially migrate all Sentinel 6.1 or Sentinel 6.1 RD correlation rules to the Sentinel 7.0.1 local Correlation Engine.

Importing Dynamic List Data

If there are duplicate Dynamic List names in Sentinel 6.1 or Sentinel 6.1 RD and Sentinel 7.0.1, the Migration Utility provides a unique name for the imported Map name using the format `<originalname><number>`.

For example, if you have a Dynamic List named `XYZ` in your Sentinel 6.1 environment and a Dynamic List named `XYZ` in your Sentinel 7.0.1 environment, the Migration Utility imports the Dynamic List as `XYZ0_migrated`. If you reimport Dynamic Lists and there is already a Dynamic List named `XYZ0_migrated` in your Sentinel 7.0.1 environment, the Migration Utility increments the number until it creates a unique Dynamic List name. For example, `XYZ1_migrated.`

Importing Vulnerability Data

The Migration Utility migrates vulnerability data, but you can see advisor information and reports for the event if you configure the Advisor, download and process the Advisor feed files, and then use the Tenable Nessus scanner to generate the `exploitDetection.csv` file.

Importing MSSP Data

The Migration Utility migrates MSSP data required for Assets and Vulnerabilities to work properly, so these components are all migrated together. All customer names and their hierarchy information is migrated to Sentinel 7.0.1.

If identical MSSP data, such as customer names, already exist in the Sentinel 7.0.1 environment, the Migration Utility does not migrate the duplicate information.

Importing User Data

Before importing user data, consider the following:

- If you are importing user account information from Sentinel 6.1, the Migration Utility creates the user password file `user_password_mapping.csv` in the directory where you placed the migration scripts. This file contains the user names and passwords for the migrated users. Due to database restrictions, passwords were reset. You can reset these passwords using the provided file or communicate the new passwords to their respective users.
- If you are importing user account information from Sentinel 6.1 RD, existing passwords are retained for users.
- Random passwords are generated for all non-postgres (MSSQL and Oracle) exported users.
- Passwords are not generated for Inactive and LDAP users.

- Windows domain users are not migrated.
- All users are assigned to the User role, by default.
- The Migration Utility does not migrate user account information for user accounts that already exist in the Sentinel 7.0.1 environment.
- Administrator users, such as `esecadm`, are not migrated.

Importing Advisor Data

User-defined advisor instances retain the Sentinel 6.1 or Sentinel 6.1 RD download directory location configuration. You must update this location for each user-defined advisor instance after migration.

Importing Integrator Configuration Data

As part of File Integrator instance migration, the file to which the integrator writes events is not migrated. However, the path of the file is migrated as part of the configuration information. Sentinel may not be able to continue writing to the same location due to permission issues. Ensure that the user account has the appropriate permission or change the location of the file.

Importing Map File Data

If there are duplicate Map names in Sentinel 6.1 or Sentinel 6.1 RD and Sentinel 7.0.1, the Migration Utility provides a unique name for the imported Map name using the format `<originalname><number>`.

For example, if you have a Map named `XYZ` in your Sentinel 6.1 environment and a Map named `XYZ` in your Sentinel 7.0.1 environment, the Migration Utility imports the Map as `XYZ0_migrated`. If you reimport Maps, and there is already a Map named `XYZ0_migrated` in your Sentinel 7.0.1 environment, the Migration Utility increments the number until it creates a unique Map name. For example, `XYZ1_migrated.`

Importing Namespace and Folder Structure Data

The Correlation namespace is no longer available in the Sentinel Control Center. However, if you import the namespace from your Sentinel 6.1 or Sentinel 6.1 RD environment you can view the namespace information using Solution Designer.

The Migration Utility migrates the folder structure for Correlation Rules and Maps but does not migrate the folder structure for Templates and Activities.

Understanding Event Source Management Components

Sentinel supports two types of event sources: pull-based and push-based event sources. For pull-based event sources Sentinel Connectors read the data Sentinel needs from a particular location, such as a file. Push-based event sources provide live and stored data to Sentinel. Push-based event sources are at a higher risk for data loss during migration.

To help minimize data loss during migration, follow the migration instructions for each of the following four supported push-based event sources.

Migrating Audit Event Source Server

To minimize data loss for Audit event sources, perform the following steps.

To migrate Audit event source data on existing hardware:

1. Export Sentinel 6.1 or Sentinel 6.1 RD configuration data using the Migration Utility. For more information about exporting configuration data, see "Exporting Sentinel 6.1 and Sentinel 6.1 RD Configuration Data" on page 8.
2. Change the port number of the Event Source Server. Changing the Event Source Server port number breaks the communication with the Platform Agent, causing the Platform Agent to cache events.
3. Ensure that all cached events in the Event Source Server are cleared out of Sentinel 6.1 or Sentinel 6.1 RD.
4. Uninstall the Sentinel 6.1 remote Collector Manager and install the Sentinel 7.0.1 remote Collector Manager on the same computer.
5. Import your Sentinel 6.1 or Sentinel 6.1 RD configuration data on your Sentinel 7.0.1 remote Collector Manager. For more information about importing configuration data, see "Importing Configuration Data into Sentinel 7.0.1" on page 9.

The Platform Agent forwards events to the Sentinel 7.0.1 Event Source Server once it is running. After the Sentinel 7.0.1 remote Collector Manager establishes a connection with the Sentinel server, all events are forwarded.

Migrating Syslog Event Source Server

To minimize data loss for Syslog event sources, perform the following steps.

To migrate Syslog event source data:

1. Install Sentinel 7.0.1 on new hardware.
2. Ensure that there is one Sentinel 7.0.1 Syslog Event Source Server in the local Collector Manager.
3. Export Sentinel 6.1 or Sentinel 6.1 RD configuration data using the Migration Utility. For more information about exporting configuration data, see "Exporting Sentinel 6.1 and Sentinel 6.1 RD Configuration Data" on page 8.
4. On the Sentinel 6.1 remote Collector Manager computer, create an IP table rule to forward all events from the Syslog port to the Sentinel 7.0.1 Syslog Event Source Server.
5. Uninstall the Sentinel 6.1 remote Collector Manager from the server and install the Sentinel 7.0.1 remote Collector Manager on the same hardware.
6. Import your Sentinel 6.1 or Sentinel 6.1 RD configuration data on your Sentinel 7.0.1 remote Collector Manager. For more information about importing configuration data, see "Importing Configuration Data into Sentinel 7.0.1" on page 9.
7. Once the remote Collector Manager establishes a connection with Sentinel 7.0.1 and all services are running, remove the IP rule to redirect events to the Sentinel 7.0.1 Syslog Event Source Server.
8. Ensure that all auto- and user-configured Syslog files in the Sentinel 7.0.1 local Collector Manager created in Step 4 are removed.

Migrating SNMP Event Source Server

To minimize data loss for SNMP event sources, perform the following steps.

To migrate SNMP event source data:

1. Install Sentinel 7.0.1 on new hardware.
2. Export Sentinel 6.1 or Sentinel 6.1 RD configuration data using the Migration Utility. For more information about exporting configuration data, see "Exporting Sentinel 6.1 and Sentinel 6.1 RD Configuration Data" on page 8.
3. Import your Sentinel 6.1 or Sentinel 6.1 RD configuration data on your Sentinel 7.0.1 local Collector Manager. For more information about importing configuration data, see "Importing Configuration Data into Sentinel 7.0.1" on page 9.
4. On the Sentinel 6.1 remote Collector Manager computer, create an IP table rule to forward all events from the SNMP Event Source Server to the Sentinel 7.0.1 SNMP Event Source Server.
5. Uninstall the Sentinel 6.1 remote Collector Manager from the server and install the Sentinel 7.0.1 remote Collector Manager on the same hardware.
6. Import your Sentinel 6.1 or Sentinel 6.1 RD configuration data on your Sentinel 7.0.1 remote Collector Manager. For more information about importing configuration data, see "Importing Configuration Data into Sentinel 7.0.1" on page 9.
7. Once the remote Collector Manager establishes a connection with Sentinel 7.0.1 and all services are running, remove the IP rule to redirect events to the Sentinel 7.0.1 SNMP Event Source Server.
8. Ensure that all auto- and user-configured SNMP files in the Sentinel 7.0.1 local Collector Manager created in Step 4 are removed.

Migrating Sentinel Link Server

To minimize data loss for Sentinel Link, perform the following steps.

To migrate Sentinel Link data using the Sentinel Link integrator Queue feature:

1. On the Sentinel 6.1 or Sentinel 6.1 RD server, launch the Integrator Manager.
2. Change the integrator mode to `Queuing`.
3. Uninstall the Sentinel 6.1 remote Collector Manager from the server and install the Sentinel 7.0.1 remote Collector Manager on the same hardware.
4. Import your Sentinel 6.1 or Sentinel 6.1 RD configuration data on your Sentinel 7.0.1 remote Collector Manager. For more information about importing configuration data, see "Importing Configuration Data into Sentinel 7.0.1" on page 9.
5. Once the remote Collector Manager establishes a connection with Sentinel 7.0.1 and all services are running, change the integrator mode back to `Send immediate` under Event Forwarding.

Finalizing Migration

Use the following checklist to ensure you have migrated the configuration data from your Sentinel 6.1 or Sentinel 6.1 RD environment into your Sentinel 7.0.1 environment.

	Checklist
❑	1. Compare the export and import summary .csv files to ensure you have completed the migration of your Sentinel 6.1 or Sentinel 6.1 RD environment. These files are located in the migration home directory. For example, the export summary is located in the following location: `<Directory of Sentinel user permission>/<SentinelMigrationTool-7.0-121>/sentinel6-Sles10Sp264WithDB-export/Sentinel_6_Sles10Sp264WithDB_Export_Summary_060712213917.csv`
❑	2. Rename any missed duplicate Integrators, Actions, or Correlation Rules.
❑	3. If you are importing user account information from Sentinel 6.1, the Migration Utility creates the user password file `user_password_mapping.csv` in the directory where you placed the migration scripts. This file contains the user names and passwords for the migrated users. Due to database restrictions, passwords were reset. You can reset these passwords using the provided file or communicate the new passwords to their respective users.
❑	4. Download the Advisor feed in your Sentinel 7.0.1 environment using Download Manager. For more information about downloading the Advisor feed, see the Sentinel 7.0.1 *Administration Guide*.
❑	5. Use the.csv file-based report provided by the Migration Utility to recreate the default, user-defined, and global filters. For more information about writing filters, see the Sentinel 7.0.1 *User Guide*.
❑	6. Restart Asset File event sources configured with the Generic Asset Collector. Restarting these event sources synchronizes asset information for assets that were not part of the migration.
❑	7. Recreate custom Incident Categories in your Sentinel 7.0.1 environment. The Migration Utility migrates the association of custom Incident Categories with Action Instances that have a type of `Create Incident`, but these categories are not available for use in Sentinel 7.0.1.
❑	8. If you are running a non-English Sentinel installation, you must reassociate Incident Category names with Action Instances that have the type `Create Incident` using the Sentinel Control Center.
❑	9. Recreate iTrac workflows based on incidents tracked in your Sentinel 7.0.1 environment. For more information about iTrac workflows, see the Sentinel 7.0.1 *User Guide*.
❑	10. Reassign users to iTrac roles as appropriate.
❑	11. Update the download directory location for all user-defined Advisor instances.
❑	12. Verify that all the Collectors configured to communicate with the Sentinel 7.0.1 server and remote Collector Managers start receiving the events.
❑	13. Ensure that pull-based Connectors, such as the File Connector, are configured to read from the correct location. For example, if the Collector Manager is on new hardware, the local file from which the File Connector reads is in a new location.

Schema Updates

Sentinel uses a standard event schema, or field structure, into which it places the parsed and normalized event data from event sources. Sentinel uses this schema to make searching for and processing specific events more efficient. Over time, this schema has evolved to support new event source types and new metadata enrichment. Sentinel 7 introduced a revised schema that updates and expands on the schema used in Sentinel 6, Sentinel 6.1, Sentinel 6.1 RD, and Sentinel Log Manager 1.x.

In some rare cases fields are deprecated, either because new fields express the same information in a better way, or because the fields became overloaded and were being used for too many different purposes.

The tables below describe the updates found in the Sentinel 7.x event schema.

New Fields

The following fields were added in Sentinel 7..

Field Label	Tag Name	Description
InitiatorEmail	iemail	The user's primary e-mail address from the identity associated with the account (provided by the Identity mapping).
InitiatorUserPrivilegeLevel	iup	The local privilege level of the initiating user (or effective user, if set), based on event source conventions. For example, the 'root' user on UNIX or Linux and the 'Administrator' on Windows would have elevated privileges.
InitiatorUserWorkforceID	iwfid	The user's workforce ID from the identity associated with the account (provided by the Identity mapping).
ObserverHostCountry	obscountry	The country where the IP address of the observing host is located (provided by the Country mapping).
ObserverHostLatitude	obslat	The geographic latitude of the observing IP, usually provided by an online database of ISP location data (provided by the Country mapping).
ObserverHostLongitude	obslong	The geographic longitude of the observing IP, usually provided by an online database of ISP location data (provided by the Country mapping).
ObserverMAC	obsmac	The MAC address of the observing host.
ObserverServiceName	obssvcname	The name of the service that observed and reported the activity.
ObserverTZ	estz	The local time zone of the event source in any of the formats supported by the java TimeZone.getTimeZone() method. Preferably, it should be in the long "America/Los_Angeles" type format because it is the least ambiguous.
ObserverTZDayInMonth	estzdim	The event time day in the month at the local time zone of the event source. This can be used to run bi-monthly reports (for example, paycheck intervals). This value is based on the EventTime field (1 .. 31).
ObserverTZDayInWeek	estzdiw	The event time day in the week at the local time zone of the event source. This can be used to run "work day" reports. This value is based on the EventTime field (1=Sunday. 7=Saturday).

Field Label	Tag Name	Description
ObserverTZDayInYear	estzdiy	The event time day in the year at the local time zone of the event source. This can be used to run queries to find events spanning a large portion of the year (for example, first half of the year versus. second half of the year). This value is based on the EventTime field (1=Jan 1 .. 365/ 366=Dec 31/Dec 31 on leap years).
ObserverTZHour	estzhour	The event time hour in the day at the local time zone of the event source. This can be used to run "work hours" reports. This value is based on the EventTime field (0 .. 23).
ObserverTZMinute	estzmin	The event time hour in the day at the local time zone of the event source. This can be used to run "work hours" reports. This value is based on the EventTime field (0 .. 59).
ObserverTZMonth	estzmonth	The event time month in the year at the local time zone of the event source. This can be used to run quarterly reports. This value is based on the EventTime field (0=January .. 11=December).
PolicyID	polid	The name or ID of the third-party policy that was applied to cause the event to occur. For example, the ID of a firewall policy that blocks network traffic.
ReporterMAC	repmac	The MAC address of the reporting host.
SessionID	sessid	An identifier used by one service to identify a request, session, or transaction that was initiated by another service. This can be used to associate events from the called service with the initiating service's request.
SourceHostLatitude	srclat	The geographic latitude of the source IP, usually provided by an online database of ISP location data (provided by the Country mapping).
SourceHostLongitude	srclong	The geographic longitude of the source IP, usually provided by an online database of ISP location data (provided by the Country mapping).
SourceMAC	smac	The MAC address of the source host.
SourceTranslatedIP	sxip	The translated IP address (for example, by NAT) of the source host provided by the event source.
SourceTranslatedMAC	sxmac	The translated MAC address of the source host provided by the event source.
SourceTranslatedPort	sxport	The translated port (for example, by PAT) used by the service or application that initiated the connection provided by the event source.
TargetAttributeName	attr	The name of the affected attribute of the primary target.
TargetDataNamespace	tdspace	The name of the top-level namespace container (for example, volume or tree) where the TargetDataName and TargetDataContainer exist.

Field Label	Tag Name	Description
TargetDataSensitivity	tds	The local sensitivity level of the target data object, based on how the event source uses the data in the object. For example, /etc/passwd and /etc/shadow on Unix or Linux and SYS/SYSTEM on Oracle would have elevated sensitivity. This would be set by the Collector based on known sensitive files for the source. Note that this indicates the sensitivity based on how the event source natively uses the data object. If users choose to store sensitive data in other files, such files will not be detected solely from the use of this field.
TargetEmail	temail	The user's primary email address from the identity associated with the account (provided by the Identity mapping).
TargetHostLatitude	dlat	The geographic latitude of the target IP, usually provided by an online database of ISP location data (provided by the Country mapping).
TargetHostLongitude	dlong	The geographic longitude of the target IP, usually provided by an online database of ISP location data (provided by the Country mapping).
TargetMAC	dmac	The MAC address of the target host.
TargetNewResourceContainer	dnewcont	The name of the container where the TargetNewResourceName exists. This is a full path to the resource (not including the top-level namespace).
TargetNewResourceName	dnewname	The new name assigned to a resource (such as a user account, group, file, or table) that was renamed or copied, or the name of a child resource added as a member of a trust relationship (for example, a group being added to another group). The type of resource should be specified in the TargetNewResourceType field if this field is used.
TargetNewResourceNamespace	dnewspace	The name of the top-level namespace container (for example, volume or tree) where the TargetNewResourceName and TargetNewResourceContainer exist.
TargetNewResourceType	dnewtype	The type of resource affected when a rename or copy is performed (User, Trust, Host, Service, or Data).
TargetTranslatedIP	dxip	The translated IP address (for example, by NAT) of the target host.
TargetTranslatedMAC	dxmac	The translated MAC address of the target host.
TargetTranslatedPort	dxport	The translated port (for example, by PAT) used by the service or application that was the target of the connection.
TargetUserWorkforceID	twfid	The user's workforce ID from the identity associated with the account (provided by the Identity mapping).
VendorOutcomeCode	voc	A third-party outcome or result code that is assigned to the event by the event source vendor.

Renamed Fields

Some existing fields are renamed in Sentinel 7 and the descriptions of what data should be placed in each field have been updated.

Old Label	Tag Name	New Label	Notes
Init...		Initiator...	Initiator fields have been unabbreviated for clarity.
Device/Sensor...		Observer...	Fields related to the Observer formerly called “Device” or “Sensor” have been renamed to “Observer” for consistency.
...Asset...		...Host...	Host-related fields have been renamed to make it clearer that they are for hosts, not generic assets.
InitIP/Port		SourceIP/Port	Although technically the Initiator, fields related to network traffic have been renamed to conform to common usage.
Customer...		Tenant...	The MSSP Customer-related fields have been renamed to the more accurate “Tenant.”
Collector	port	CollectorNodeName	Renamed to clarify that this is the name assigned to the Collector node in ESM.
CollectorScript or CollectorPlugin	agent	CollectorPluginName	Renamed to clarify that this is the name, not an ID.
DeviceAttackName	rt1	IDSAttackName	The attack name provided by the event source. This name is compared to Advisor's attack database for Exploit Detection.
DeviceName	rv31	IDSName	The canonical name of the IDS/IPS engine assigned to a particular IDS/IPS product. This is used for matching against Advisor data.
ObserverChannel	rv150	ObserverServiceComponent	The name of the component (module, channel, or facility) within the service that detected and reported the activity.
ReservedVar192	rv192	RetentionPolicyName	This field now holds the name of the retention policy that applies to this event. This field is added to the event when viewing search results, and is not persisted in the event store.
ReservedVar172	rv172	SearchTargetID	This field now holds the ID of the Sentinel system that returned this event as part of a distributed search.
LinkEventID	rv121	SentinelID	The ID of the Sentinel system which first collected or generated a particular event.
	rv28	SentinelMetricFormat	The format of the value contained in SentinelMetricValue (such as Count or Percentage).
EventMetric	rv2	SentinelMetricValue	The numeric value associated with a metric event reported by Sentinel.
Rt2	rt2	SentinelProcessingComponent	The name of the internal Sentinel component which processed this event.

Old Label	Tag Name	New Label	Notes
ReservedVar123	rv123	SentinelProcessingComponentID	The ID of the internal Sentinel component that processed this event.
SubResource	sres	SentinelServiceComponent	The name of the component within the Sentinel service that processed or generated this event.
ReservedVar124	rv124	SentinelServiceComponentID	The ID of the component within the Sentinel service that processed or generated this event.
Resource	res	SentinelServiceName	The name of the Sentinel service that processed or generated this event.
ReservedVar141	rv141	TargetAttributeOriginalValue	The data that was originally in the affected attribute stated in TargetAttributeName, if available. Large datasets will be truncated to the size of this field.
DataValue	rv43	TargetAttributeValue	The actual data that was placed in the affected attribute stated in TargetAttributeName. Large datasets will be truncated to the size of this field.
EventGroupID	evtgrpid	TransactionID	An identifier used by a single service to indicate that several events are part of the same transaction.

Generic Usage Fields

The ReservedVar fields that have reverted to generic usage should not be used by any existing Collector, and should not be used by customers. The CustomerVar fields that have reverted to generic usage can now be used by any customer for local customization.

The fields TaxonomyLevel1-4 and Criticality are also now deprecated, and should not be used. The Taxonomy fields have been superseded by the XDAS-based taxonomy, and the Criticality field has been replaced with Target-specific fields.

Old Label	Tag Name	New Label	Notes
DataTagId	rv3	ReservedVar3	Never defined.
ControlPack	rv26	ReservedVar26	Superseded by Solution Packs.
ControlMonitor	rv27	ReservedVar27	Superseded by Solution Packs.
EventContext	rv33	ReservedVar33	Never defined.
SourceThreatLevel	rv34	ReservedVar34	Never defined.
SourceFunction	rv37	ReservedVar37	Never defined.
SourceOperationalContext	rv38	ReservedVar38	Never defined.
DestinationThreatLevel	rv44	ReservedVar44	Never defined.
VirusStatus	rv46	ReservedVar46	Never defined.
DestinationFunction	rv47	ReservedVar47	Never defined.
DestinationOperationalContext	rv48	ReservedVar48	Never defined.
SourceUserFullName	rv56	ReservedVar56	Superseded by InitiatorUserFullName (iufname).
SourceMacAddress	rv57	ReservedVar57	Superseded by SourceMAC (smac).

Old Label	Tag Name	New Label	Notes
SourceNetworkIdentity	rv58	ReservedVar58	Never defined.
SourceUserIdentity	cv23	CustomerVar23	Superseded by InitiatorUserIdentityID (iuident).
DestinationUserIdentity	cv24	CustomerVar24	Superseded by TargetUserIdentityID (tuident).
SARBOX	cv90	CustomerVar90	Superseded by tagging.
HIPAA	cv91	CustomerVar91	Superseded by tagging.
GLBA	cv92	CustomerVar92	Superseded by tagging.
FISMA	cv93	CustomerVar93	Superseded by tagging.
NISPOM	cv94	CustomerVar94	Superseded by tagging.
SIPCountry	cv95	CustomerVar95	Superseded by SourceHostCountry (rv29).
DIPCountry	cv96	CustomerVar96	Superseded by TargetHostCountry (rv30).