AUTHORIZED DOCUMENTATION

Reference Guide

Novell®
Sentinel™ Rapid Deployment

6.1

June 15, 2009

www.novell.com

Legal Notices

Novell, Inc.
404 Wyman Street, Suite 500
Waltham, MA 02451
U.S.A.
www.novell.com

Online Documentation: To access the latest online documentation for this and other Novell products, see the Novell Documentation Web page (http://www.novell.com/documentation).

Novell Trademarks

Third-Party Materials

Contents

About This Guide

Sentinel™ is a security information and event management solution that receives information from many sources throughout an enterprise, standardizes it, prioritizes it and presents it to you to make threat, risk and policy related decisions. The Sentinel 6.1 RD User Reference Guide is your reference for the following:

- Collector administrator functions
- Collector and Sentinel meta tags
- Sentinel console user permissions
- Sentinel correlation engine
- Sentinel command line options
- Sentinel server database views

This guide assumes that you are familiar with Network Security, Database Administration and Linux operating system.

This guide discusses about:

- Chapter 1, "Sentinel 6.1 Rapid Deployment Event Fields," on page 11
- Chapter 2, "Sentinel 6.1 Rapid Deployment Control Center User Permissions," on page 25
- Chapter 3, "Sentinel 6.1 Rapid Deployment Correlation Engine RuleLG Language," on page 37
- Chapter 4, "Sentinel 6.1 Rapid Deployment Data Access Service," on page 47
- Chapter 6, "Sentinel 6.1 Rapid Deployment Database Views for PostgreSQL," on page 55
- Appendix A, "Sentinel 6.1 Rapid Deployment Troubleshooting Checklist," on page 121
- Appendix B, "Sentinel 6.1 Rapid Deployment Service Permission Tables," on page 125
- Appendix C, "Sentinel 6.1 Rapid Deployment Log Locations," on page 133

Audience

This documentation is intended for Information Security Professionals.

Feedback

We want to hear your comments and suggestions about this manual and the other documentation included with this product. Please use the User Comments feature at the bottom of each page of the online documentation and enter your comments there.

Additional Documentation

Sentinel technical documentation is broken down into several different volumes. They are:

- *Novell Sentinel 6.1 RD Installation Guide* (http://www.novell.com/documentation/sentinel61rd/s61rd_install/data/index.html)

- *Novell Sentinel 6.1 RD User Guide* (http://www.novell.com/documentation/sentinel61rd/s61rd_user/data/index.html)
- *Novell Sentinel 6.1 RD Reference Guide* (http://www.novell.com/documentation/sentinel61rd/s61rd_reference/data/index.html)
- *Sentinel 6.1 Install Guide* (http://www.novell.com/documentation/sentinel61/pdfdoc/sentinel_61_installation_guide.pdf)
- *Sentinel 6.1 User Guide* (http://www.novell.com/documentation/sentinel61/pdfdoc/sentinel_61_user_guide.pdf)
- *Sentinel 6.1 Reference Guide* (http://www.novell.com/documentation/sentinel61/pdfdoc/sentinel_61_reference_guide.pdf)
- *Sentinel SDK* (http://developer.novell.com/wiki/index.php?title=Develop_to_Sentinel)

  The Sentinel SDK site provides the details about developing collectors (proprietary or JavaScript) and JavaScript correlation actions.

Documentation Conventions

In this documentation, a greater-than symbol (>) is used to separate actions within a step and items within a cross-reference path.

A trademark symbol (®, ™, etc.) denotes a Novell trademark. An asterisk (*) denotes a third-party trademark.

When a single path name can be written with a backslash for some platforms or a forward slash for other platforms, the path name is presented with forward slashes to reflect the Linux* convention. Users of platforms that require a backslash, such as NetWare®, should use backlashes as required by your software.

Contacting Novell

- *Novell Website* (http://www.novell.com)
- *Novell Technical Support* (http://support.novell.com/phone.html?sourceidint=suplnav4_phonesup)
- *Novell Self Support* (http://support.novell.com/support_options.html?sourceidint=suplnav_supportprog)
- *Patch Download Site* (http://download.novell.com/index.jsp)
- *Novell 24x7 Support* (http://www.novell.com/company/contact.html)
- *Sentinel TIDS* (http://support.novell.com/products/sentinel)

Sentinel 6.1 Rapid Deployment Event Fields

1

Every Sentinel event or correlated event has certain fields that are automatically populated (such as Event Time and Event UUID) and other fields that may or may not be populated, depending on the type of event, the collector parsing, and the mapping service configuration. This event data is visible in Active Views, historical queries, and reports. They are stored in the database and can be accessed via the report views. They can also be used in actions available through the right-click event menu, correlation actions, and iTRAC workflow actions.

- Section 1.1, “Event Field Labels and Tags,” on page 11
- Section 1.2, “List of Fields and Representations,” on page 15

1.1 Event Field Labels and Tags

Each field can be referred to by a user-friendly label or a short tag. The user-friendly label is visible throughout the Sentinel Control Center interface, for example:

- Column headers for Active Views, historical event queries, and the Active Browser
- Correlation wizard drop-down menus
- Active View configuration drop-down menus

Each field has a default label, but that label is user-configurable using the Event Configuration option on the Admin tab. For more information, see “Admin” section in *Sentinel 6.1 Rapid Deployment User Guide*. `InitUserName` is the default label to represent the account name of the user who initiated the event, but this can be changed by the administrator. When a user changes the default label, the changes are reflected in most areas of the interface, including any correlation rules, filters, and right-click menu options.

WARNING: Changing the default label for variables other than Customer Variables may cause confusion when working with Novell Technical Services or other parties who are familiar with the default names. In addition, JavaScript Collectors built by Novell refer to the default labels described in this chapter and are not automatically updated to refer to new labels.

Each field also has a short tag name that is always used for internal references to the field and is not user-configurable. This short tag name may not correspond exactly to the default label; Sentinel labels have changed over the years, but the underlying short tags remain the same for backward compatibility. (For example, InitUserName is the default label for the account name of the user who initiated the event. The default label was previously SourceUserName, and the underlying short tag is “sun”.)

NOTE: Many of the default labels were updated for clarity in the Sentinel 6.1 release. Because all filters, actions, and correlation rule definitions are defined using the short tags, even though the label may be visible in the interface, there is no change in functionality due to the label renaming.

Each field is associated with a specific data type, which corresponds to the data type in the database:

- **string:** limited to 255 characters (unless otherwise specified)
- **integer:** 32-bit signed integer
- **UUID:** 36 character (with hyphens) or 32 character (without hyphens) hexadecimal string in the format XXXXXXXX-XXXX-XXXX-XXXX-XXXXXXXXXXXX (For example, -6A5349DA-7CBF-1028-9795-000BCDFFF482)
- **date:** Collector Variable must be set with date as number of milliseconds from January 1, 1970 00:00:00 GMT. When displayed in Sentinel Control Center, meta-tags of type date are displayed in a regular date format.
- **IPv4:** IP address in dotted decimal notation (that is – xxx.xxx.xxx.xxx)

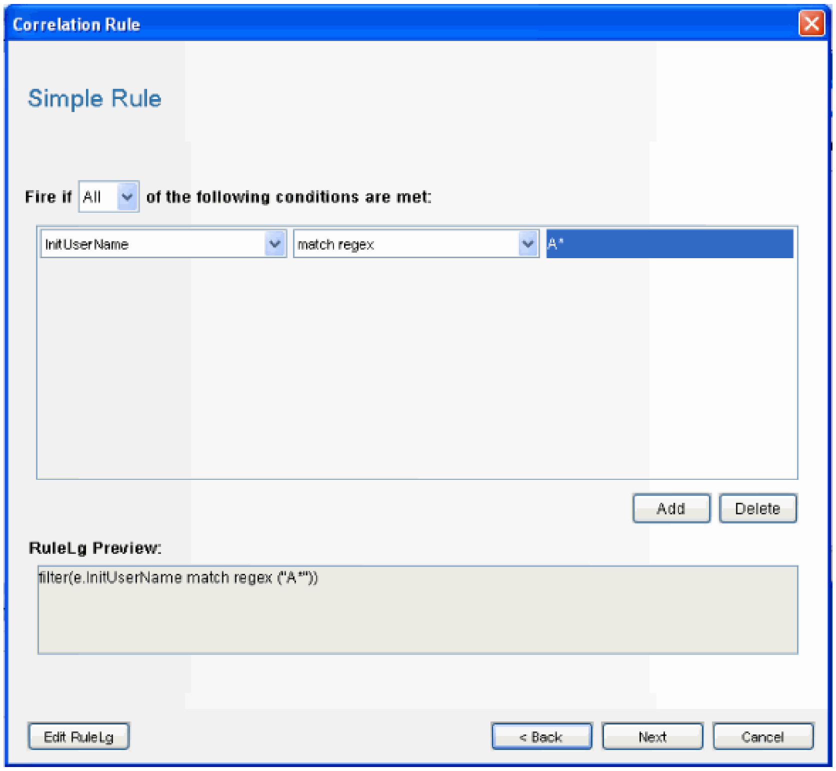
This section has the following information:

- Section 1.1.1, "Free-Form Filters and Correlation Rules," on page 12
- Section 1.1.2, "Actions," on page 13
- Section 1.1.3, "Proprietary Collectors," on page 15
- Section 1.1.4, "JavaScript Collectors," on page 15

1.1.1 Free-Form Filters and Correlation Rules

You can use either the tag or the label when you write free-form language in the Sentinel Control Center. The Sentinel interface shows the user-friendly label.

Figure 1-1 *Correlation Wizard displaying labels in drop-down and free-form language*



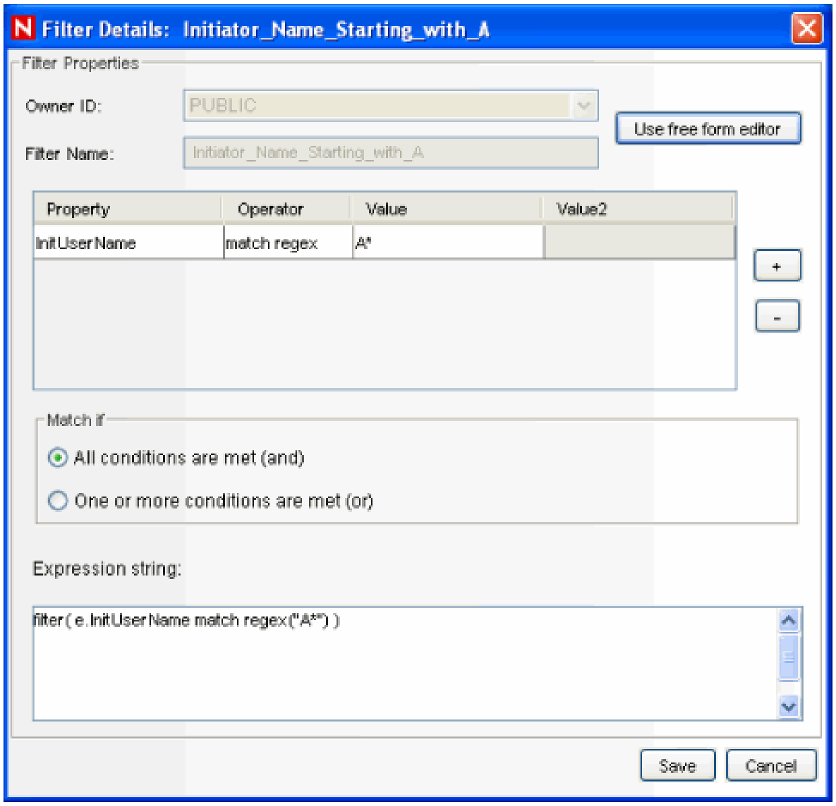
Fire if All of the following conditions are met:

InitUserName | match regex | A*

RuleLg Preview:

```
filter(e.InitUserName match regex ("A*"))
```

Figure 1-2 *Filter Wizard displaying labels in drop-down and free-form language*



Owner ID: PUBLIC

Filter Name: Initiator_Name_Starting_with_A

Property	Operator	Value	Value2
InitUserName	match regex	A*	

Match if

● All conditions are met (and)

○ One or more conditions are met (or)

Expression string:

```
filter( e.InitUserName match regex("A*") )
```

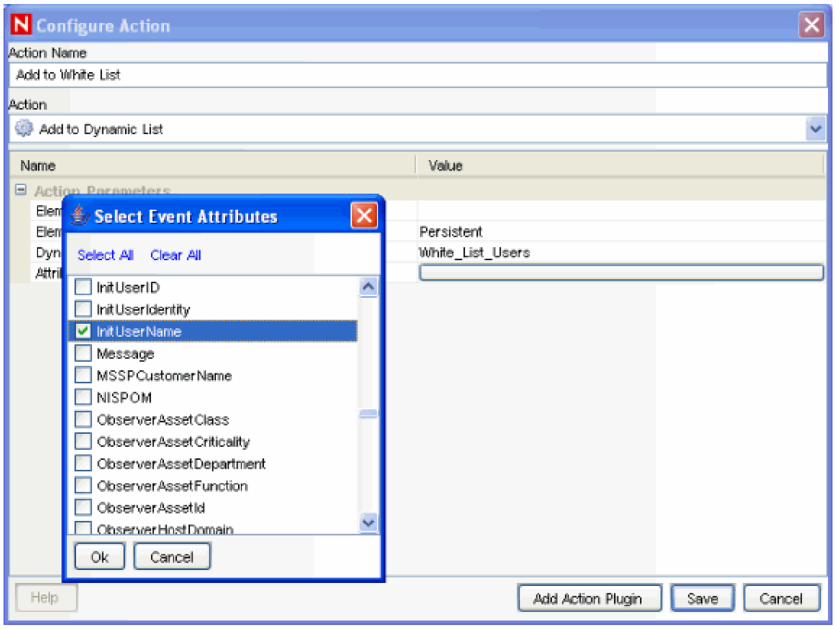
The representation of fields in the free-form RuleLG language is usually prefaced by “e.” for example, “e.InitUserName” or “e.sun” can refer to the Initiator User Name for the incoming or current event. In special cases, “w.” may be used to refer to a field in a past event (for example, “w.InitUserName”). For more information about the RuleLG language, see Chapter 3, “Sentinel 6.1 Rapid Deployment Correlation Engine RuleLG Language,” on page 37.

1.1.2 Actions

Users can use either the tag or the label when they define parameters to be sent to right-click Event Menu actions, correlation actions, and iTRAC workflow actions.

To pass a field value to an action, you may use a checklist that shows the labels or type the parameter name directly into the configuration.

Figure 1-3 *Configuration Action - Select Event Attributes window*



Action Name: Add to White List

Action: Add to Dynamic List

Persistent

White_List_Users

☐ InitUserID
☐ InitUserIdentity
☑ InitUserName
☐ Message
☐ MSSPCustomerName
☐ NISPOM
☐ ObserverAssetClass
☐ ObserverAssetCriticality
☐ ObserverAssetDepartment
☐ ObserverAssetFunction
☐ ObserverAssetId
☐ ObserverHostDomain

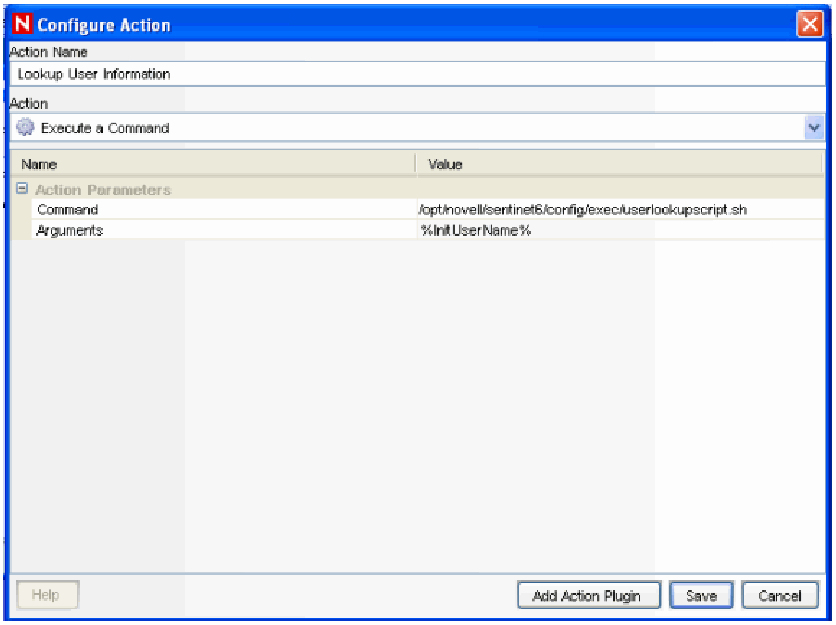
When you type the label or short tag for a field to be used in an action, the name can be enclosed in percent signs (%tag%) or dollar signs (tag). For example:

- %sun% in a correlation action refers to the value of InitUser in the correlated event
- sun in a correlation action refers to the value of InitUser in the current, “trigger” event (the final event that caused the correlation rule to fire)

NOTE: In a right-click menu event operating on a single event, there is no functional difference between %sun% and sun.

For example, to pass the Initiator User Name to a command line action to look up information from a database about that user, you could use %InitUserName% or %sun%. For more information about Actions, see “Actions and Integrators” section in *Sentinel 6.1 Rapid Deployment User Guide*.

Figure 1-4 *Configuration Action window*



Action Name: Lookup User Information

Action: Execute a Command

Name	Value
Action Parameters	
Command	/opt/novell/sentinel6/config/exec/userlookupscript.sh
Arguments	%InitUserName%

1.1.3 Proprietary Collectors

Proprietary Collectors, written in Novell's own language, always use variables based on the short tag to refer to event fields. The short tag name must be prefaced by a letter and underscore, where the letter indicates the data type for the field (i_ for integer, s_ for string).

1.1.4 JavaScript Collectors

JavaScript Collectors usually refer to event fields using an "e." followed by the same user-friendly label set in Event Configuration in the Sentinel Control Center. For a Sentinel system with a default configuration, for example, the Initiator User Name would be referred to as "e.InitUserName" in the JavaScript Collector. There are some exceptions to this general rule. Refer to the Sentinel Collector SDK (http://developer.novell.com/wiki/index.php?title=Develop_to_Sentinel) for more details.

1.2 List of Fields and Representations

The table on the following pages shows the default labels, descriptions and data types for the Sentinel event fields, along with the proper way to refer to the tags in filters, correlation rules, actions, and proprietary collector scripts. Fields that cannot or should not be manipulated in the Collector parsing do not have a Collector variable.

Table 1-1 *Labels and Meta-tags used in Sentinel Control Center and proprietary Collector language*

Default Label	**Filters and Correlation Rules**	**Menu and Correlation Actions**	**Proprietary Collector Language**	**Data Type**	**Description**
DeviceEventTimeString	e.et	%et%	s_ET	string	The normalized date and time of the event, as reported by the sensor.
DeviceEventTime	e.det	%det%		date	The normalized date and time of the event, as reported by the sensor.
SentinelProcessTime	e.spt	%spt%		date	The date and time Sentinel received the event.
BeginTime	e.bgnt	%bgnt%	s_BGNT	date	The date and time the event started occurring (for repeated events).
EndTime	e.endt	%endt%	s_ENDT	date	The date and time the event stopped occurring (for repeated events).
RepeatCount	e.rc	%rc%	s_RC	integer	The number of times the same event occurred if multiple occurrences were consolidated.
EventTime	e.dt	%dt%		date	The normalized date and time of the event, as given by the Collector.
SentinelServiceID	e.src	%src%		UUID	Unique identifier for the Sentinel service which generated this event.
Severity	e.sev	%sev%	i_Severity	integer	The normalized severity of the event (0-5).
Vulnerability	e.vul	%vul%	s_VULN	integer	The vulnerability of the asset identified in this event. Set to 1 if Sentinel detects an exploit against a vulnerable system. Requires Advisor.
Criticality	e.crt	%crt%	s_CRIT	integer	The criticality of the asset identified in this event.
InitIP	e.sip	%sip%	s_SIP	IPv4	IPv4 address of the initiating system.
TargetIP	e.dip	%dip%	s_DIP	IPv4	IPv4 address of the target system.
Collector	e.port	%port%		string	Name of the Collector that generated this event.

Default Label	Filters and Correlation Rules	Menu and Correlation Actions	Proprietary Collector Language	Data Type	Description
CollectorScript	e.agent	%agent%		string	The name of the Collector Script used by the Collector to generate this event.
Resource	e.res	%res%	s_Res	string	Compliance monitoring hierarchy level 1
SubResource	e.sres	%sres%	s_SubRes	string	Subresource name
ObserverHostName	e.sn	%sn%	s_SN	string	Unqualified hostname of the observer (sensor) of the event.
SensorType	e.st	%st%	s_ST	string	The single character designator for the sensor type (N, H, O, V, C, W, A, I).
Protocol	e.prot	%prot%	s_P	string	Protocol used between initiating and target services.
InitHostName	e.shn	%shn%	s_SHN	string	Unqualified hostname of the initiating system.
InitServicePort	e.spint	%spint%	s_SPINT	integer	Port used by service/ application that initiated the connection.
InitServicePortName	e.sp	%sp%	s_SP	string	Name of the initiating service that caused the event.
TargetHostName	e.dhn	%dhn%	s_DHN	string	Unqualified hostname of the target system.
TargetServicePort	e.dpint	%dpint%	s_DPINT	integer	Network port accessed on the target.
TargetServicePortName	e.dp	%dp%	s_DP	string	Name of the target service affected by this event.
InitUserName	e.sun	%sun%	s_SUN	string	Initiating user's account name. Example jdoe during an attempt to su.
TargetUserName	e.dun	%dun%	s_DUN	string	Target user's account name. Example root during a password reset.
FileName	e.fn	%fn%	s_FN	string	The name of the program executed or the file accessed, modified or affected.

Default Label	Filters and Correlation Rules	Menu and Correlation Actions	Proprietary Collector Language	Data Type	Description
ExtendedInformation	e.ei	%ei%	s_EI	string	Stores additional collector-processed information. Values within this variable are separated by semi-colons (;).
ReporterHostName	e.rn	%rn%	s_RN	string	Unqualified hostname of the reporter of the event.
ProductName	e.pn	%pn%	s_PN	string	Indicates the type, vendor and product code name of the sensor from which the event was generated.
Message	e.msg	%msg%	s_BM	string	Free-form message text for the event.
DeviceAttackName	e.rt1	%rt1%	s_RT1	string	Device specific attack name that matches attack name known by Advisor. Used in Exploit Detection.
Rt2	e.rt2	%rt2%	s_RT2	string	Reserved by Novell for expansion.
Ct1 thru Ct2	e.ct1 thru e.ct2	%ct1% thru %ct2%	s_CT1 and s_CT2	string	Reserved for use by customers for customer-specific data.
Rt3	e.rt3	%rt3%		integer	Reserved by Novell for expansion.
Ct3	e.ct3	%ct3%	s_CT3	integer	Reserved for use by customers for customer-specific data.
CorrelatedEventUuids	e.ceu	%ceu%	s_RT3	string	List of event UUIDs associated with th correlated event. Only relevant for correlated events.
CustomerHierarchyId	e.rv1	%rv1%	s_RV1	integer	Used for MSSPs.
ReservedVar2 thru ReservedVar10	e.rv2 thru e.rv10	%rv2% thru %rv10%	s_RV2 thru s_RV10	integer	Reserved by Novell for expansion.
ReservedVar11 thru ReservedVar20	e.rv11 thru e.rv20	%rv11% thru %rv20%	s_RV11 thru s_RV20	date	Reserved by Novell for expansion.

Default Label	Filters and Correlation Rules	Menu and Correlation Actions	Proprietary Collector Language	Data Type	Description
CollectorManagerId	e.rv21	%rv21%	s_RV21	UUID	Unique identifier for the Collector Manager which generated this event.
CollectorId	e.rv22	%rv22%	s_RV22	UUID	Unique identifier for the Collector which generated this event.
ConnectorId	e.rv23	%rv23%	S_RV23	UUID	Unique identifier for the Connector which generated this event.
EventSourceId	e.rv24	%rv24%	S_RV24	UUID	Unique identifier for the Event Source which generated this event.
RawDataRecordId	e.rv25	%rv25%	S_RV25	UUID	Unique identifier for the Raw Data Record associated with this event.
ControlPack	e.rv26	%rv26%	S_RV26	string	Sentinel control categorization level 1 (for Solution Packs).
EventMetricClass	e.rv28	%rv28%	s_RV28	string	Class of the event-dependent numeric value.
InitIPCountry	e.rv29	%rv29%	s_RV29	string	Country where the IPv4 address of the initiating system is located.
TargetIPCountry	e.rv30	%rv30%	s_RV30	string	Country where the IPv4 address of the target system is located.
DeviceName	e.rv31	%rv31%	s_RV31	string	Name of the device generating the event. If this device is supported by Advisor, the name should match the name known by Advisor. Used in Exploit Detection.
DeviceCategory	e.rv32	%rv32%	s_RV32	string	Device category (FW, IDS, AV, OS, DB).
EventContext	e.rv33	%rv33%	s_RV33	string	Event context (threat level).
InitThreatLevel	e.rv34	%rv34%	s_RV34	string	Initiator threat level.
InitUserDomain	e.rv35	%rv35%	s_RV35	string	Domain (namespace) in which the initiating account exists.
DataContext	e.rv36	%rv36%	s_RV36	string	Data context.
InitFunction	e.rv37	%rv37%	s_RV37	string	Initiator function.

Default Label	Filters and Correlation Rules	Menu and Correlation Actions	Proprietary Collector Language	Data Type	Description
InitOperationalContext	e.rv38	%rv38%	s_RV38	string	Initiator operational context.
MSSPCustomerName	e.rv39	%rv39%	s_RV39	string	MSSP customer name.
VendorEventCode	e.rv40	%rv40%	s_RV40	string	Event code reported by device vendor.
TargetHostDomain	e.rv41	%rv41%	s_RV41	string	Domain portion of the target system's fully-qualified hostname.
InitDomain	e.rv42	%rv42%	s_RV42	string	Domain portion of the initiating system's fully-qualified hostname.
ReservedVar43	e.rv43	%rv43%	s_RV43	string	Reserved by Novell for expansion.
TargetThreatLevel	e.rv44	%rv44%	s_RV44	string	Target threat level.
TargetUserDomain	e.rv45	%rv45%	s_RV45	string	Domain (namespace) in which the target account exists..
VirusStatus	e.rv46	%rv46%	s_RV46	string	Virus status.
TargetFunction	e.rv47	%rv47%	s_RV47	string	Target function.
TargetOperationalContext	e.rv48	%rv48%	s_RV48	string	Target operational context.
TaxonomyLevel4	e.rv53	%rv53%	s_RV53	string	Sentinel event code categorization - level 4.
CustomerHierarchyLevel2	e.rv54	%rv54%	s_RV54	string	Customer Hierarchy Level 2 (used by MSSPs).
VirusStatus	e.rv56	%rv56%	s_RV56	string	Virus Status.
InitMacAddress	e.rv57	%rv57%	s_RV57	string	Initiator Mac Address. Part of initiator host asset data.
InitNetworkIdentity	e.rv58	%rv58%	s_RV58	string	Initiator Network Identity. Part of initiator host asset data.
InitAssetFunction	e.rv60	%rv60%	s_RV60	string	Function of the initiating system (fileserver, webserver, etc.).
InitAssetValue	e.rv61	%rv61%	s_RV61	string	Initiator Asset Value. Part of initiator host asset data.
InitAssetCriticality	e.rv62	%rv62%	s_RV62	string	Criticality of the initiating system (0-5).

Default Label	Filters and Correlation Rules	Menu and Correlation Actions	Proprietary Collector Language	Data Type	Description
Variables reserved for future use by Novell	e.rv63 thru e.rv75	%rv63% thru %rv75%	s_RV63 thru s_rv75	string	Variables not currently in use
InitAssetDepartment	e.rv76	%rv76%	s_RV76	string	Department of the initiating system.
InitAssetId	e.rv77	%rv77%	s_RV77	string	Internal asset identifier of the initiator.
Variables reserved for future use by Novell	e.rv78 thru e.rv80	%rv78% thru %rv80%	s_RV78 thru s_rv80	string	Variables not currently in use
TargetAssetClass	e.rv81	%rv81%	s_RV81	string	Class of the target system (desktop, server, etc.).
TargetAssetFunction	e.rv82	%rv82%	s_RV82	string	Function of the target system (fileserver, webserver, etc.).
TargetAssetValue	e.rv83	%rv83%	s_RV83	string	Target Asset Value. Part of target host asset data.
Variables reserved for future use by Novell	e.rv84 thru e.rv97	%rv84% thru %rv97%	s_RV84 thru s_rv97	string	Variables not currently in use.
TargetDepartment	e.rv98	%rv98%	s_RV98	string	Target Department. Part of target host asset data.
TargetAssetId	e.rv99	%rv99%	s_RV99	string	Internal asset identifier of the target.
CustomerHierarchyLevel4	e.rv100	%rv100%	s_RV100	string	Customer Hierarchy Level 4 (used by MSSPs)
Variables reserved for future use by Novell	e.rv101 thru e.rv200	%rv101% thru %rv200%	s_rv101 thru s_rv200	various	Variables not currently in use
CustomerVar1 thru CustomerVar10	e.cv1 thru e.cv10	%cv1% thru %cv10%	s_CV1 thru s_CV10	integer	Number variable reserved for customer use. Stored in database.
CustomerVar11 thru CustomerVar20	e.cv11 thru e.cv20	%cv11% thru %cv20%	s_CV11 thru s_CV20	date	Date variable reserved for customer use. Stored in database.
CustomerVar21 thru CustomerVar89	e.cv21 thru e.cv89	%cv21% thru %cv89%	s_CV21 thru s_CV29	string	String variable reserved for customer use. Stored in database.

Default Label	Filters and Correlation Rules	Menu and Correlation Actions	Proprietary Collector Language	Data Type	Description
SARBOX	e.cv90	%cv90%	s_CV90	string	Set to 1 if the asset is governed by Sarbanes-Oxley.
HIPAA	e.cv91	%cv91%	s_CV91	string	Set to 1 if the asset is governed by the Health Insurance Portability and Accountability Act (HIPAA) regulation.
GLBA	e.cv92	%cv92%	s_CV92	string	Set to 1 if the asset is governed by the Gramm-Leach Bliley Act (GLBA) regulation.
FISMA	e.cv93	%cv93%	s_CV93	string	Set to 1 if the asset is governed by the Federal Information Security Management Act (FISMA) regulation.
NISPOM	e.cv94	%cv94%	s_CV94	string	Set to 1 via an asset map if the target asset is governed by the National Industrial Security Program Operating Manual (NISPOM)
CustomerVar95 thru CustomerVar100	e.cv95 thru e.cv100	%cv95% thru %cv100%	s_CV95 thru s_CV100	string	String variable reserved for customer use. Stored in database.
CustomerVar101 thru CustomerVar110	e.cv101 thru e.cv110	%cv101% thru %cv110%	s_CV101 thru s_CV110	string	Integer variable reserved for customer use. Stored in database.
CustomerVar111 thru CustomerVar120	e.cv111 thru e.cv120	%cv111% thru %cv120%	s_CV111 thru s_CV120	string	Date variable reserved for customer use. Stored in database.
CustomerVar121 thru CustomerVar130	e.cv121 thru e.cv130	%cv121% thru %cv130%	s_CV121 thru s_CV130	string	UUID variable reserved for customer use. Stored in database.
CustomerVar131 thru CustomerVar140	e.cv131 thru e.cv140	%cv131% thru %cv140%	s_CV131 thru s_CV140	string	IPv4 variable reserved for customer use. Stored in database.
CustomerVar141 thru CustomerVar150	e.cv141 thru e.cv150	%cv141% thru %cv150%	s_CV141 thru s_CV150	string	String variable reserved for customer use. Stored in database.
CustomerVar151 thru CustomerVar160	e.cv151 thru e.cv160	%cv151% thru %cv160%	s_CV151 thru s_CV160	string	Integer variable reserved for customer use. Not stored in database.

Default Label	Filters and Correlation Rules	Menu and Correlation Actions	Proprietary Collector Language	Data Type	Description
CustomerVar161 thru CustomerVar170	e.cv161 thru e.cv170	%cv161% thru %cv170%	s_CV161 thru s_CV170	string	Date variable reserved for customer use. Not stored in database.
CustomerVar171 thru CustomerVar180	e.cv171 thru e.cv180	%cv171% thru %cv180%	s_CV171 thru s_CV180	string	UUID variable reserved for customer use. Not stored in database.
CustomerVar181 thru CustomerVar190	e.cv181 thru e.cv190	%cv181% thru %cv190%	s_CV181 thru s_CV190	string	IPv4 variable reserved for customer use. Not stored in database.
CustomerVar191 thru CustomerVar200	e.cv191 thru e.cv200	%cv191% thru %cv200%	s_CV191 thru s_CV200	string	String variable reserved for customer use. Not stored in database.

Sentinel 6.1 Rapid Deployment Control Center User Permissions

2

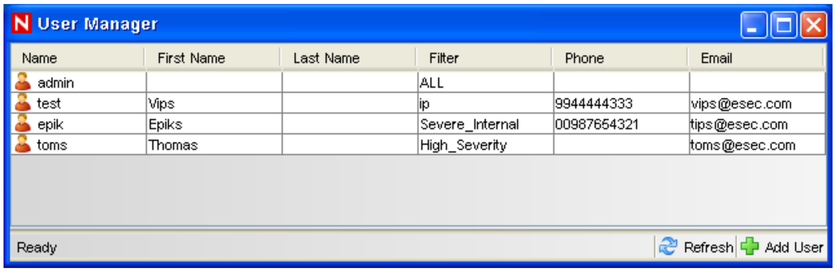
Sentinel™ allows administrators to set user permissions in the Sentinel Control Center at a granular level. The only user created by default is the `admin`, or Sentinel Administrator. All other users are created by the Sentinel Administrator, or someone with similar permissions.

The permissions in the User Manager are grouped into several major categories:

Each of these groups of settings are described in the following sections:

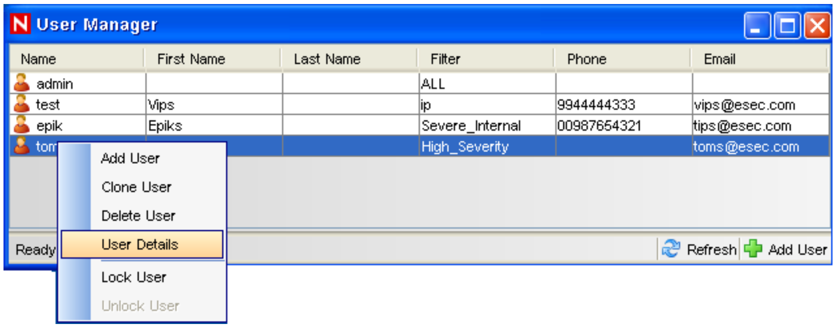
2.1 Changing User Permissions

1. Log into the Sentinel Control Center as a user with the User Management permissions.
2. Click the Admin tab.
3. Select User Configuration from Admin tab. Alternatively, Select User Manager from User Configuration in the Navigator.



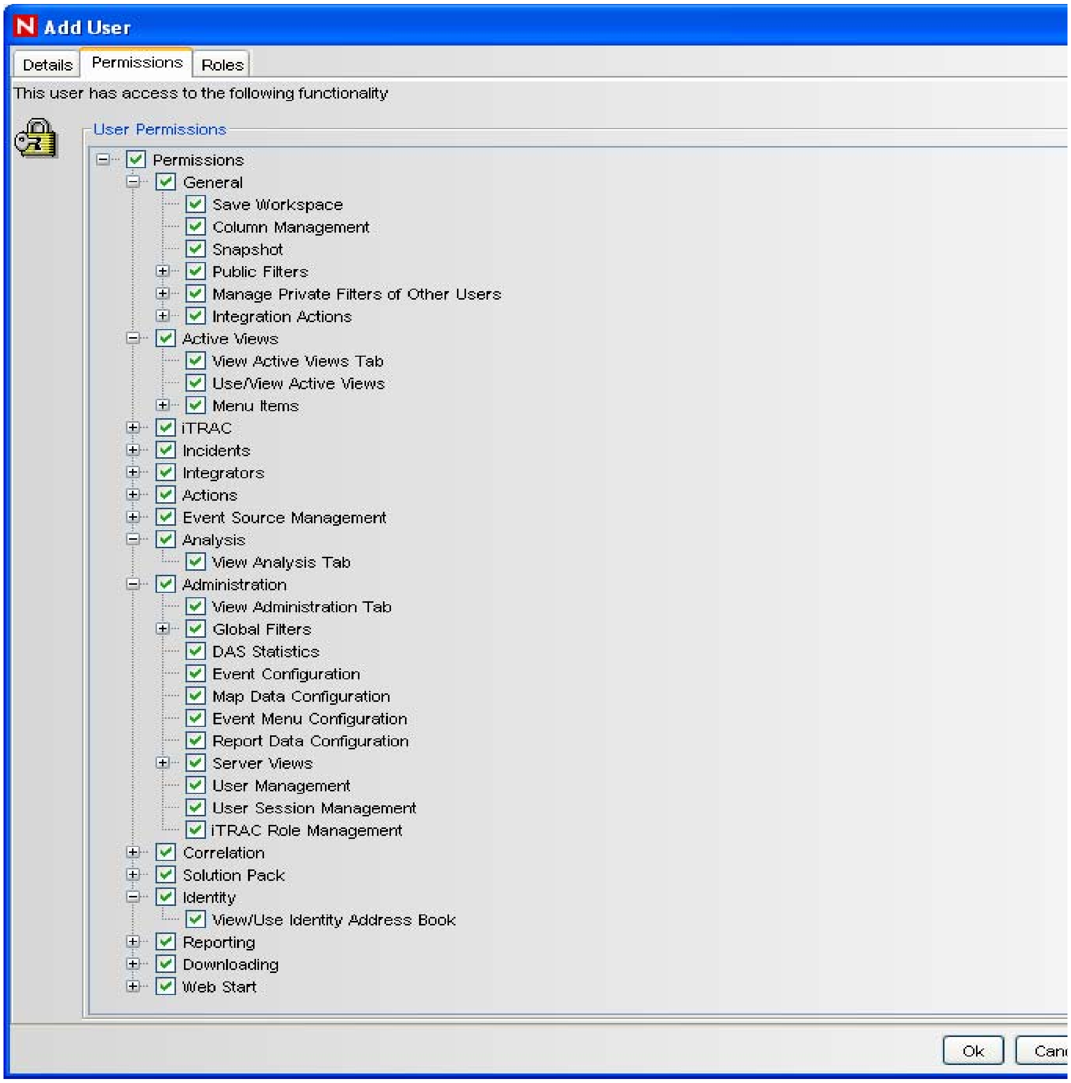
Name	First Name	Last Name	Filter	Phone	Email
admin			ALL		
test	Vips		ip	9944444333	vips@esec.com
epik	Epiks		Severe_Internal	00987654321	tips@esec.com
toms	Thomas		High_Severity		toms@esec.com

4 Right click user and select User Details.



Name	First Name	Last Name	Filter	Phone	Email
admin			ALL		
test	Vips		ip	9944444333	vips@esec.com
epik	Epiks		Severe_Internal	00987654321	tips@esec.com
tom			High_Severity		toms@esec.com

5 Select the *Permissions* tab.



This user has access to the following functionality

User Permissions

- ☑ Permissions
  - ☑ General
    - ☑ Save Workspace
    - ☑ Column Management
    - ☑ Snapshot
    - ☑ Public Filters
    - ☑ Manage Private Filters of Other Users
    - ☑ Integration Actions
  - ☑ Active Views
    - ☑ View Active Views Tab
    - ☑ Use/View Active Views
    - ☑ Menu Items
  - ☑ iTRAC
  - ☑ Incidents
  - ☑ Integrators
  - ☑ Actions
  - ☑ Event Source Management
  - ☑ Analysis
    - ☑ View Analysis Tab
  - ☑ Administration
    - ☑ View Administration Tab
    - ☑ Global Filters
    - ☑ DAS Statistics
    - ☑ Event Configuration
    - ☑ Map Data Configuration
    - ☑ Event Menu Configuration
    - ☑ Report Data Configuration
    - ☑ Server Views
    - ☑ User Management
    - ☑ User Session Management
    - ☑ iTRAC Role Management
  - ☑ Correlation
  - ☑ Solution Pack
  - ☑ Identity
    - ☑ View/Use Identity Address Book
  - ☑ Reporting
  - ☑ Downloading
  - ☑ Web Start

6 Deselect the check boxes for which you want to restrict the user.

7 Click *OK*.

2.2 General

Table 2-1 *Permissions-General*

Permission Name	Description
Save Workspace	Allows user to save preferences. If this permission is unavailable, user will never be prompted to save changes to preferences when logging out or exiting the Sentinel Control Center.
Column Management	Allows user to manage the columns in the Active View tables.
Snapshot	Allows user to take a snapshot of Active View tables.

2.2.1 General – Public Filters

Table 2-2 *Permissions-General-Public Filters*

Permission Name	Description
Create Public Filters	Allows user to create a filter with an owner ID of PUBLIC. If user does not have this permission, then the value PUBLIC will not be listed as one of the owner IDs that user can create a filter for.
Modify Public Filters	Allows user to modify a public filter.
Delete Public Filters	Allows user to delete a public filter.

2.2.2 General – Manage Private Filters of Other Users

Table 2-3 *Permissions-General-Manage Private Filters of Other Users*

Permission Name	Description
Create Private Filters for Other Users	Allows user to create private filters for themselves or for other users.
Modify Private Filters of Other Users	Allows user to modify their own private filters and private filters created by other users.
Delete Private Filters of Other Users	Allows user to delete their own private filters and private filters created by other users.
View/Use Private Filters of Other Users	Allows user to view/use their own private filters and private filters crated by other users.

2.2.3 General – Integration Actions

Table 2-4 *Permissions-General-Integration Actions*

Permission Name	Description
Send to HP Service Desk	Allows user to send events, incident and associated objects to Remedy. (requires the optional Remedy integration component)

2.3 Active Views

Table 2-5 *Permissions-Active Views*

Permission Name	Description
View Active Views Tab	Allows user to see and use the Active Views tab, menu and other related functions associated with the Active Views tab.

Permission Name	**Description**
Use/View Active Views	Allows user to access the Active Views charts.

2.3.1 Active Views – Menu Items

Table 2-6 *Permissions-Active Views-Menu Items*

Permission Name	**Description**
Use Assigned Menu Items	Allows user to use assigned menu items in the Active Views Events table (the right-click menu).
Add to Existing Incident	Allows user to add events to existing incidents using the Active Views Events table (the right-click menu).
Remove from Incident	Allows user to remove events from an existing incident using the Events tab Events table (the right-click menu).
Email Events	Allows user to e-mail events using the Active Views Events table (the right-click menu).
View Advisor Attack Data	Allows user to view the Advisor Attack Data stream.
View Vulnerability	Allows user to view the vulnerabilities present in the Sentinel database

2.4 iTRAC

Table 2-7 *Permissions-iTRAC*

Permission Name	**Description**
View iTRAC Tab	Allows user to see and use the iTRAC tab, menu and other related functions associated with the iTRAC tab.
Activity Management	Allows user to access the Activity Manager.
Manage Work Items Of Users	Gives user administrative control over all workitems, including those assigned to other users.

2.4.1 iTRAC - Template Management

Table 2-8 *Permissions-iTRAC-Template Management*

Permission Name	**Description**
View/Use Template Manager	Allows user to access the Template Manager.
Create/Modify Templates	Allows user to create and modify templates.

2.4.2 iTRAC - Process Management

Table 2-9 *Permissions-iTRAC-Process Management*

Permission Name	Description
View/Use Process Manager	Allows user to access the Process View Manager.
Start/Stop Processes	Allows user to use the Process View Manager.

2.5 Incidents

Table 2-10 *Permissions-Incidents*

Permission Name	Description
View Incidents Tab	Allows user to see and use the Incidents tab, menu and other related functions associated with the View Incidents tab.
Incident Administration	Allows user to modify an incident.
View Incident(s)	Allows user to view/modify the details of an incident. If the user does not have this permission, then the Incident Details window will not be displayed when the user either double-clicks an Incident in the Incident View window or right-clicks the incident or selects the Modify option.
Create Incident(s)	Allows user to create Incidents in the in the Incident View window or by right clicking on the incident and select Modify option. Alternatively you can select Create Incident menu item in the Incidents menu bar and clicking Create Incident option in the tool bar.
Modify Incident(s)	Allows user to modify an incident in the Incident Details window.
Delete Incident(s)	Allows user to delete incidents.
Assign Incident(s)	Allows user to assign an incident in the Modify and Create Incident window.
Email Incidents	Allows user to e-mail Incidents of interest.
Incident Actions	Allows user to view Execute Incident Action menu option in an Incident and to execute actions.
Add Notes	Allows user to add any number notes to an incident.

2.6 Integrators

Table 2-11 *Permissions-Integrators*

Permission Name	Description
View Integrator	Allows user to view Integrators, open Integrator Manager, use update, refresh, help, test buttons and view integrator event details.

Permission Name	Description
Manage Integrator	Allows user to manage (add/modify/delete) the configured Integrators.
Manage Integrator Plugins	Allows user to manage (add/modify/delete) the Integrators plugins.

2.7 Actions

Table 2-12 Permissions-Action Manager

Permission Name	Description
View Actions	Allows user to use Action Manager and view Actions.
Manage Actions	Allows user to add/edit/delete actions of type "Execute Action Plugins"
Manage Action Plugins	Allows user to add/edit/delete Action Plugins.

2.8 Event Source Management

Table 2-13 Permissions-Event Source Management

Permission Name	Description
View Status	Allows user to view the status of ESM components.
View Scratchpad	Allows user to design and configure ESM components.
Configure ESM Components	Allows you to configure ESM components.
Control ESM Components	Allows you to control and manage ESM components.
Manage Plugins	Allows you to manage Collector and Connector Plugins.
View Raw Data	Allows you to view/parse raw data.
Debug Collector	Allows you to debug Collector.

Command and Control consists of:

- start/stop individual ports
- start/stop all ports
- restart hosts
- rename hosts

2.9 Analysis Tab

Table 2-14 Permissions-Analysis Tab

Permission Name	Description
Analysis Tab	Allows user to see and use the View Analysis tab, menu and other related functions associated with the System Overview tab.

2.10 Administration

Table 2-15 Permissions-Administration

Permission Name	Description
View Administration Tab	Allows user to see and use the View Administration tab, menu and other related functions associated with the View Administration tab.
DAS Statistics	Allows user to view DAS activity (DAS binary and query).
Event Configuration	Allows user to rename columns, set mappings from mapping files. This function is associated with Mapping Configuration.
Map Data Configuration	Allows user to add, edit and delete mapping files.
Event Menu Configuration	Allows user to access the Menu Configuration window and add new options that display on the Event menu when you right-click an event.
Report Data Configuration	Allows user to enable or disable summary tables used in aggregation.
User Management	Allows user to add, modify and delete user details
User Session Management	Allows user to view, lock and terminate active users (logins to Sentinel Control Center).
iTRAC Role Management	Allows user to view and use the role manager in the Admin Tab.

2.10.1 Administration – Global Filters

Table 2-16 Permissions-Administration-Global Filters

Permission Name	Description
View/Use Global Filters	Allows user to access the Global Filter Configuration window.
Modify Global Filters	Allows user to modify the global filters configuration. **NOTE:** To access this function, View Global Filters permission must also be assigned.

2.10.2 Administration – Server Views

Table 2-17 *Permissions-Administration-Server Views*

Permission Name	Description
View Servers	Allows user to monitor the status of all processes.
Control Servers	Allows user to start, restart and stop processes.

2.11 Correlation

Table 2-18 *Permissions-Correlation*

Permission Name	Description
View Correlation Tab	Allows user to use the Correlation functions.
View/Use Correlation Rule Manager	Allows user to start or stop the Correlation Rules.
View/Use Correlation Engine Manager	Allows user to deploy/undeploy the Correlation Rules.
View/Use Dynamic Lists	Allows user to Create, use, view, modify the Dynamic Lists.

2.12 Solution Pack

Table 2-19 *TPermissions-Solution Pack*

Permission Name	Description
Solution Designer	Allows user to access Solution Designer.
Solution Manager	Allows user to access Solution Manager.

2.13 Identity

Table 2-20 *Permissions-Action Manager*

Permission Name	Description
View/Use Identity Address Book	Allows user to view and use Identity Browser.

2.14 Reporting

***Table 2-21** Reporting Permissions*

Permission Name	**Description**
Run/View Reports	Allows user for the following: ◆ View the report results and sample reports ◆ Run the reports by using the Run option *Now* in the Reports page of the Web interface. For more information on Running the reports, see "Running Reports" in the *Sentinel 6.1 Rapid Deployment User Guide*. **NOTE:** Users with Run/View permission cannot schedule reports . They cannot use the run options *Daily*, *Once, Weekly*, and *Monthly*. ◆ Delete the report results ◆ Rename the report results ◆ Restart report runs
Manage Reports	Allows user for the following: ◆ Access the reporting features listed under Run/View Reports permission ◆ Schedule report runs. In addition to the the run option *Now*, the user can also run the reports using the run options *Once*, *Daily*, *Weekly*, and *Monthly*. For more information on Running the reports, see "Running Reports" in the *Sentinel 6.1 Rapid Deployment User Guide*. ◆ Upload report definitions ◆ Delete report definitions

2.15 Downloading

***Table 2-22** Downloading Permissions*

Permission Name	Description
Download Client Installers	Allows user for the following: ◆ Download Collector Manager Installer The Collector Manager Installer helps you install the Sentinel Collector Manager on any machine from which you want to forward events. ◆ Download Client Installer The Client Installer helps you install the Sentinel Control Center and Sentinel Data Manager on any client machine.

2.16 Java Webstart

All the authenticated users can web start the Sentinel Control center. With the following new permissions you can restrict users from webstarting Sentinel Data Manager and Solution Designer. For more information on Webstart, refer to "Applications and Installers".

***Table 2-23** Web Start Permissions*

Permission Name	Description
Run SDM Through WebStart	Allows user to run SDM by using the WebStart option in the Sentinel 6.1 Rapid Deployment Web interface.
Run Solution Designer Through WebStart	Allows user to run Solution Designer by using the WebStart option in the Sentinel 6.1 Rapid Deployment Web interface.

Sentinel 6.1 Rapid Deployment Correlation Engine RuleLG Language

3

This section has the following information about Sentinel™ correlation engine Rule LG language.

3.1 Correlation RuleLG Language Overview

The Sentinel Correlation Engine runs rules that are written in the Correlation RuleLg language. Rules are created in the Sentinel Control Center. Users can create rules using a wizard for the following rule types:

- Simple Rule
- Composite Rule
- Aggregate Rule
- Sequence Rule

These rules are converted to the Correlation RuleLg language when the rules are saved. The same rule types, plus even more complex rules, can be created in the Sentinel Control Center using the Custom/Freeform option. To use the Custom/Freeform option, the user must have a good understanding of the Correlation RuleLg language.

RuleLg uses several operations, operators, and event field short tags to define a rule. The Correlation Engine loads the rule definition and uses the rules to evaluate, filter, and store in memory events that meet the criteria specified by the rule. Depending on the rule definition, a correlation rule might fire based on

- the value of one field or multiple fields
- the comparison of an incoming event to past events
- the number of occurrences of similar events within a defined time period
- one or more subrules firing
- one or more subrules firing in a particular order

Each of these constructs is represented by an operation in RuleLg.

3.2 Event Fields

All operations function on event fields, which can be referred to by their labels or by their short tags within the correlation rule language. For a full list of labels and short tags, see Chapter 1, "Sentinel 6.1 Rapid Deployment Event Fields," on page 11. The label or metatag must also be combined with a prefix to designate whether the event field is part of the incoming event or a past event that is stored in memory.

Examples:

```
e.DestinationIP (Destination IP for the current event)
e.dip (Destination IP for the current event)
w.dip (Destination IP for any stored event)
```

WARNING: If you rename the label of a metatag, do not use the original label name when creating a correlation rule.

3.3 Event Operations

Event operations evaluate, compare, and count events. They include the following operations:

- **Filter:** Evaluates the current events to determine whether they can potentially trigger a rule to fire
- **Window:** Compares the current event to past events that have been stored in memory
- **Trigger:** Counts events to determine whether enough events have occurred to trigger a rule

Each operation works on a set of events, receiving a set of events as input and returning a set of events as output. The current event processed by a rule often has a special meaning for the semantic of the language. The current event is always part of the set of events in and out of an operation unless the set is empty. If an input set of an operation is empty, then the operation is not evaluated.

3.3.1 Filter Operation

Filter consists of a Boolean expression that evaluates the current event from the real-time event stream. It compares event attributes to user-specified values using a wide set of operators

The Boolean expression is a composite of comparison and match instructions.

The syntax for filter is:

```
Filter <Boolean expression 1> [NOT|AND|OR <Boolean expression 2] […]
[NOT|AND|OR <Boolean expression n>]
```

Where

```
<Boolean expressions 1…n> are expressions using one or more event field names
and filter operators
```

For example, this rule detects whether the current event has a severity of 4 and the resource event field contains either "FW" or "Comm."

```
filter(e.sev = 4 and (e.res match regex ("FW") or e.res match regex ("Comm")))
```

Boolean Operators

Filter expressions can be combined using the Boolean operators AND, OR and NOT. The filter boolean operator precedence (from highest [top] to lowest [bottom] precedence) is:

Table 3-1 *Boolean Operators*

Operator	Meaning	Operator Type	Associativity
Not	logical not	unary	None
And	logical and	binary	left to right
Or	logical or	binary	left to right

In addition to Boolean operators, filter supports the following operators.

Standard Arithmetic Operators

Standard arithmetic operators can be used to build a condition that compares the value of a Sentinel metatag and a user-specified value (either a numeric value or a string field). The standard arithmetic operators in Sentinel are =, <, >, !=, <=, and >=.

Examples:

```
filter(e.Severity > 3)
filter(e.BeginTime < 1179217665)
filter(e.SourceUserName != “Administrator”)
```

Match Regex Operators

The match regex operator can be used to build a condition where the value of a metatag matches a user-specified regular expression value specified in the rule. This operator is used only for string tags, and the user-specified values for this operator are case-sensitive.

Examples:

```
filter(e.Collector match regex ("IBM"))
filter(e.EventName match regex ("Attack"))
```

Match Subnet Operators

The match subnet operator can be used to build a condition where the value of a metatag maches a user-specified subnet specified in the rule in CIDR notation. This operator is used only for IP address fields.

Example:

```
filter(e.DestinationIP match subnet (10.0.0.1/22))
```

Inlist Operator

The inlist operator is used to perform a lookup on an existing dynamic list of string values, returning true if the value is present in the list. For more information on Dynamic Lists, see “Correlation Tab” in *Sentinel 6.1 Rapid Deployment User Guide*.

For example, this filter expression is used to evaluate whether the Source IP of the current event is present on a dynamic list called MailServerList. If the Source IP is present in this list, the expression evaluates to TRUE.

```
filter(e.sip inlist MailServerList)
```

As another example, this filter expression combines the NOT and the INLIST operator. This expression evaluates to TRUE if the Source IP is not present in the dynamic list called MailServerList.

```
filter(not (e.sip inlist MailServerList))
```

This filter expression is used to evaluate whether the event name of the current event equals “File Access” and the Source User Name is also not present on a dynamic list called AuthorizedUsers. If both conditions are true for the current event, the expression evaluates to TRUE.

```
filter(e.evt="File Access" and not(e.sun inlist AuthorizedUsers))
```

ISNULL Operator

The isnull operator returns true if the metatag value is equal to NULL.

Example:

```
Filter(isnull(e.SIP))
```

Output Sets

- The output of a filter is either the empty set (if the Boolean expression evaluates to false) or a set containing the current event and all of the other events from the incoming set (if the Boolean expression evaluates to true).
- If filter is the last or only operation of a correlation rule, then the output set of the filter is used to construct a correlated event. The trigger events are the filter operation output set of events with the current event first.
- If filter is not the last operation of a correlation rule (that is, filter is followed by a flow operatior), then the output set of a filter is used as the input set to other operations (through the flow operator).

Additional Information

- The filter operator can be used to compare metatag values with other metatag values, for example:

  ```
  e.SourceIP=e.DestinationIP
  ```

3.3.2 Window Operation

Window compares the current event to a set of past events that are stored in a “window.” The events in the window can be all past events for a certain time period, or they can be filtered.

The Boolean expression is a composite of comparison instructions and match instructions with the Boolean operators AND, OR and NOT.

The syntax for window is:

```
Window (<Boolean expression>[, <filter expression>, <evaluation period>)
```

Where

```
<Boolean expression> is an expression comparing a metatag value from the
current event to a metatag value from a past event (or a user-specified
constant)
<filter expression> is optional and specifies filter criteria for the past
events
<evaluation period> specifies the duration for which past events matching the
filter expression are maintained, specified in seconds (s), minutes (m), or
hours (h). If no letter is specified, seconds are assumed.
```

For example, this rule detects whether the current event has a source IP address in the specified subnet (10.0.0.10/22) and matches an event(s) that happened within the past 60 seconds.

```
window(e.sip = w.sip, filter(e.sip match subnet (10.0.0.10/22),60)
```

As another example, this rule is a domino type of rule. An attacker exploits a vulnerable system and uses it as an attack platform.

```
window((e.sip = w.dip AND e.dp = w.dp AND e.evt = w.evt), 1h)
```

This rule identifies a potential security breach after a denial of service attack. The rule fires if the destination of a denial of service attack has a service stopped within 60 seconds of the attack.

```
filter(e.rv51="Service" and e.rv52="Stop" and e.st = "H") flow window (e.sip =
w.dip, filter(e.rv52="Dos"), 60s) flow trigger(1,0))
```

Output Sets

- If any past event evaluates to true with the current event for the simple boolean expression, the output set is the incoming event plus all matching past events.
- If no events in the window match the current event for the simple boolean expression, the output set is empty.
- If a window is the last or only operation of a correlation rule, then the output set of the window is used to construct a correlated event (the correlated events being the window operation output set of events with the current event first).

Additional Information

- You must prepend a metatag name with "e." to specify the current event or with "w." to specify the past events
- All window simple Boolean expressions must include a metatag in the form w.[metatag].
- For more information about valid filter expressions, see Section 3.3.1, "Filter Operation," on page 38.
- Every event coming in to the Correlation Engine that passes this filter is put into the window of past events
- If no filter expression exists, then all events coming into the Correlation Engine are maintained by the window. With extremely high event rates or long durations, this might require a large amount of memory.

- The current event is not placed into the window until after the current event window evaluation is complete
- To minimize memory usage, only the relevant parts of the past events, not all metatag values, are maintained in memory.

3.3.3 Trigger Operation

Trigger is used to specify a number of events for a user-specified duration.

The syntax for trigger is:

```
Trigger (<number of events>, <evaluation period>[, discriminator (<list of
tags>))
```

Where

```
<number of events> is an integer value specifying the number of matching
events that are necessary for the rule to fire
<evaluation period> specifies the duration for which past events matching the
filter expression are maintained, specified in seconds (s), minutes (m), or
hours (h).  If no letter is specified, seconds are assumed.
discriminator is a field to group by
```

For example, this rule detects if 5 events with the same source IP address happen within 10 seconds.

```
trigger(5,10,discriminator(e.sip))
```

Output Sets

- If the specified count is reached within the specified duration, then a set of events containing all of the events maintained by the trigger is output; if not, the empty set is output.
- When receiving a new input set of events, a trigger first discards the outdated events (events that have been maintained for more than the duration) and then inserts the current event. If the number of resulting events is greater than or equal to the specified count, then the trigger outputs a set containing all of the events.
- If a trigger is the last operation (or the only operation) of a correlation rule, then the output set of the trigger is used to construct a correlated event (the correlated events being the trigger operation output set of events with the current event first).
- If a trigger is not the last operation of a correlation rule (that is, it is followed by a flow operator), then the output set of a trigger is used as the input set to other operations (through the flow operator).
- The discriminator (meta-tag list) is a comma-delimited list of meta-tags. A trigger operation keeps different counts for each distinct combination of the discriminator meta-tags.

3.4 Rule Operations

Rule operations work on subrules that have been combined into a compound rule. They include:

- Gate
- Sequence

3.4.1 Gate Operation

The gate operation is used to create a composite rule which is used in identifying complex situations from the occurrence of simple situations.

The composite rule is made up of one or more nested subrules and can be configured to fire if some, any or all of the subrules fire within a specified time window. The subrules can be a simple rule or another composite rule. For more information on Composite Rule, see “Correlation Tab” in *Sentinel 6.1 Rapid Deployment User Guide*.

The syntax for gate is:

```
Gate(<subrule 1 rulelg>, <subrule 2 rulelg>…<subrule n ruleLg>,  <mode>,
<evaluation period>, discriminator(<list of tags>))
```

Where

```
Subrule Rulelgs are the rulelg definitions for 1 to n subrules
mode = all | any | 1 | 2 | … | n, which is the number of subrules that must be
triggered in order for the gate rule to trigger
<evaluation period> specifies the duration for which past events matching the
filter expression are maintained, specified in seconds (s), minutes (m), or
hours (h).  If no letter is specified, seconds are assumed.
discriminator is a field to group by
```

For example, this rule is a typical perimeter security IDS inside/outside rule

```
filter(e.sev > 3) flow gate(filter(e.sn = "in"), filter(e.sn = "out"), all,
60s, discriminator(e.dip, e.evt))
```

3.4.2 Sequence Operation

Sequence rules are similar to gate rules, except that all child rules must fire in time order for the sequenced rule to evaluate to true.

The subrules can be a simple rule or another composite rule.

The syntax for sequence is:

```
Sequence(<subrule 1 rulelg>, <subrule 2 rulelg>…<subrule n ruleLg>,
<evaluation period>, discriminator(<list of tags>))
```

Where

```
Subrule Rulelgs are the rulelg definitions for 1 to n subrules
<evaluation period> is a time period expressed in seconds (s), minutes (m), or
hours (h)
discriminator is a field to group by
```

For example, this rule detects three failed logins by a particular user in 10 minutes followed by a successful login by same user.

```
sequence (filter(e.evt="failed logins") flow trigger(3, 600,
discriminator(e.sun,e.dip)), filter(e.evt="goodlogin"), 600,
discriminator(e.sun, e.dip))
```

3.5 Operators

Operators are used to transition between operations or expressions. The fundamental operators used between operations are:

- Flow operator
- Union operator
- Intersection operator
- Discriminator operator

3.5.1 Flow Operator

The output set of events of the left-hand side operation is the input set of events for the right-hand side operation. Flow is typically used to transition from one correlation operation to the next.

For example:

```
filter(e.sev = 5) flow trigger(3, 60)
```

The output of the filter operation is the input of the trigger operation. The trigger only counts events with severity equal to 5.

3.5.2 Union Operator

The union of the left side operation output set and the right side operation output set. The resulting output set contains events from either the left-hand side operation output set or the right-hand side operation output set without duplicates.

For example:

```
filter(e.sev = 5) union filter(e.sip = 10.0.0.1)
```

is equivalent to

```
filter(e.sev = 5 or e.sip = 10.0.0.1)
```

3.5.3 Intersection Operator

The intersection of the left side operation output set and the right side operation output set. The resulting output set contains events that are common in both the left-hand side operation output set and the right-hand side operation output set without duplicates.

For example:

```
filter(e.sev = 5) intersection filter(e.sip = 10.0.0.1)
```

is equivalent to

```
filter(e.sev = 5 and e.sip = 10.0.0.1)
```

3.5.4 Discriminator Operator

The discriminator operator allows users to group by event fields within other event operations. Discriminator can be used within the trigger, gate, or sequence operations. This is the last operation when executing a condition. The input for this operator will generally be the output of other operations, if any.

For example, this filter expression is used to identify five severity 5 events within 60s that all have the same Source IP. Note that the attribute (SIP in this example) can be any value, even a NULL, but it must be the same for all five events in order for the rule to fire.

```
filter(e.sev=5 ) flow trigger(5, 60s, discriminator(e.sip)
```

3.6 Order of Operators

The operator precedence (from highest (top) to lowest (bottom)) are:

Table 3-2 *Operator Precedence*

Operator	**Meaning**	**Operator Type**	**Associativity**
flow	Output set becomes input set	binary	left to right
intersection	Set intersection (remove duplicates)	binary	left to right
union	Set union (remove duplicates)	binary	left to right

3.7 Differences between Correlation in 5.x and 6.x

There are several new functionalities updated / included in 6.*x* to widen the usage of Correlation to meet user's requirements and for the ease-of-use.

Table 3-3 *Comaprison Table*

Features	**Correlation in Sentinel 5.x**	**Correlation in Sentinel 6.1RD**
Gate Operation	Not available	This is new in 6.*x*
Sequence Operation	Not available	This is new in 6.*x*
Inlist Operator and Dynamic Lists	Not available	These are new in 6.x
Isnull Operator	For metatag values equal to null, Sentinel 5.x supported the following syntax which is replaced by the ISNull operator in Sentinel 6.0 `e.SIP= " "`	This is new in 6.*x*. Uses ISNull operator.
Update Window		This is new in Sentinel 6.*x*

Features	Correlation in Sentinel 5.x	Correlation in Sentinel 6.1RD
SensorType field		Sentinel 6.*x* merges the “C” (Correlated Events) and “W” (watchlist events) SensorTypes. All events generated by the Correlation Engine are now labeled “C” in the SensorType field.
Correlation Actions and Correlation Rules		Correlation Actions and Correlation Rules are decoupled in Sentinel 6.x

Boolean expressions	filter operation supported the Boolean expressions AND and OR.	The window operation supports Boolean expressions
		`OR: window(e.dip=w.dip OR e.sip=w.sip, filter(e.sev>2),60)`
		`AND: window(e.evt=w.evt AND e.sun=w.sun, filter(e.sev>2),60)`

Creating a rule from a PUBLIC filter	GUI Option	Sentinel 6.x doesn't have the GUI option to create a rule from a PUBLIC filter. The filter criteria must be defined in the correlation wizard or language.
Update functionality for rules	Updates to a rule were based on a sliding window based on the trigger time period.	The update functionality for a rule that is triggered more than once is configurable in Sentinel 6.x.The update functionality can be set when the rule is deployed; the rule actions might happen every time the rule is triggered, or they can be set to occur once and then wait for some period of time before the action occurs again. This prevents multiple notifications on a single, ongoing event. The IN, NOT IN, and difference operators are deprecated. Correlation rules using these operators must be modified before running them in Sentinel 6.*x*.
The e.all metatag		The e.all metatag has been deprecated. Correlation rules using this operator should be updated to use specific short tags before running them in Sentinel 6.x.

Sentinel 6.1 Rapid Deployment Data Access Service

4

The Data Access Service (DAS) is Sentinel Server's persistence service and provides a message bus interface to the database. Some of the services it provides are event storage, Historical Query, event drill down, vulnerability, Advisor data retrieval, and configuration manipulation.

- Section 4.1, "DAS Container Files," on page 47

4.1 DAS Container Files

DAS is a collection of services provided by different processes. Each process is a container responsible for different types of database operations. These processes are:

- **DAS Core:** DAS Core is responsible for the following:
  - Performs general Sentinel Service operations including Login and Historical Query.
  - Provides the server-side functionality for Active Views.
  - Calculates event data summaries that are used in reports.
  - Provides the server-side functionality for the Sentinel iTRAC functionality.
  - Provides a command line interface to certain DAS services. Used primarily for third-party integration.
  - Provides the server-side of the SSL proxy connection to Sentinel Server.
- **DAS Binary:** Performs event database insertion.

DAS Proxy is not directly part of the DAS collection of services. It is part of the Communication Server and does not directly connect to the database.

- Section 4.1.1, "Reconfiguring Database Connection Properties," on page 47
- Section 4.1.2, "DAS Logging Properties Configuration Files," on page 48

4.1.1 Reconfiguring Database Connection Properties

The primary settings in these configuration files that can be configured using the dbconfig utility are related to the database connection, including:

- username
- password
- hostname
- port number
- database (database name)

If any of these database connection settings need to be changed, they must be changed in every `das_*.xml` file using the `dbconfig` utility. Using the –a argument, this utility can update all files at the same time (For example, update all files in the <Install_directory>\config or <Install_directory>/config directory). Alternately, using the –n argument, this utility can update a single file's contents if only one file need to be updated. Typically, all files should be updated at the same time.

WARNING: Do not manually edit the database connection properties. Use the `dbconfig` utility to change any database connection values within these files.

To Reconfigure Database Connection Properties:

1. Login to the machine where DAS is installed as the admin user.
2. Go to:

   ```
   <Install_directory>/bin
   ```
3. Run the following command:

   ```
   dbconfig -a <Install_directory>/config [-u username] [-p password] [-h
   hostname] [-t portnum] [-d database] [-s server] [-help] [-version]
   ```

Other settings in the files can be adjusted manually (without using dbconfig):

- maxConnections
- batchSize
- loadSize

Changing these settings might affect database performance and should be done with caution

4.1.2 DAS Logging Properties Configuration Files

The following files are used to configure logging of the DAS process. These files are typically changed when troubleshooting the DAS process.

- `das_core_log.prop`
- `das_binary_log.prop`

They are located in the following locations:

```
<Install_directory>/config
```

These files contain the configuration that determines how the DAS processes will log messages. The most important part of the configuration is the logging levels, which indicate how verbose the log messages should be. The section of the file to configure these settings is:

```
###### Configure the logging levels
# Logging level rules are read from the top down.
# Start with the most general, then get more specific.
#
# Defaults all loggers to INFO (enabled by default)
.level=INFO
#
```

```
# < Set level of specific loggers here >
#
# Turns off all logging (disabled by default)
#.level=OFF
######
```

NOTE: The logger `.level` is a wildcard logger name that refers to all loggers. Setting this logger's level will affect all loggers.

The available logging levels are:

- **OFF:** disables all logging
- **SEVERE (highest value):** indication that a component has malfunctioned or there is a loss/ corruption of critical data
- **WARNING:** if an action can cause a component to malfunction in the future or if there is non-critical data loss/corruption
- **INFO:** audit information
- **CONFIG:** for debugging
- **FINE:** for debugging
- **FINER:** for debugging
- **FINEST:** (lowest value) – for debugging
- **ALL:** will log all levels

When one specifies a logging level, all log messages of that level and higher (in the above list) will actually be logged. For example, if one specifies the INFO level, then all INFO, WARNING and SEVERE message will be logged.

NOTE: At 10 second intervals, the logging properties file will be checked to see if any changes have occurred since it was last read. If the file has changed, the LogManagerRefreshService will re-read the logging properties file. Therefore, it is not necessary to restart the processes to begin using the updated logging levels.

Log messages are written to `<`*`Install_Directory`*`>/log` in the following files:

- `das_binary_0.*.log`
- `das_core_0.*.log`

The 0 indicates the unique number to resolve conflicts and the * indicates a generation number to distinguish rotated logs. For example, `das_query0.0.log` is the log with index 0 (latest) file in a rotated set of log files for the DAS Query process.

Log messages are also written to the process's console (standard output). However, since the processes are running as services, users do not have access to the console output. It is possible, however, to capture the console output in the `sentinel0.*.log file`. This is useful, for example, if the process is producing an error that is not printed to the process's own log file. This can be enabled by adding the following line to the `sentinel_log.prop` file:

```
esecurity.base.process.MonitorableProcess.level=FINEST
```

Sentinel 6.1 Rapid Deployment Accounts and Password Changes

5

This section discusses the users that are created or used during Sentinel installation and normal Sentinel operations. These user accounts are used for normal operations of Sentinel, such as event inserts into the Sentinel database.

The administrator might select to occasionally change the passwords for these accounts. To ensure continued normal Sentinel operations, there are special procedures necessary to update the passwords in all necessary locations.

- Section 5.1, "Sentinel Default Users," on page 51
- Section 5.2, "Password Changes," on page 51

5.1 Sentinel Default Users

This section discusses the users that are created by the Sentinel RD installer.

The following operating system user is created:

- **novell:** This user is primarily for system use and does not have a password. To log in as this user, the administrator must set a password for novell or su to novell as root.

The following users are all created as database users in the PostgreSQL Server database.

- **postgres:** This user owns the database and is for system use only. It is not possible to log in as this user.
- **dbauser:** This user owns the Sentinel schema and the password is set during installation. This account should be used to log into the Sentinel Database Manager.
- **admin:** This user is the Sentinel administrator and the password is set during installation. This account should be used to log into the web interface and the Sentinel Control Center in order to create more users.
- **rptuser:** This user is used by the system to run reports. The password set to the same password as the dbauser.
- **appuser:** This user is used by the system for a wide variety of operations. The password is set to the same password as the dbauser.

5.2 Password Changes

Corporate policy might require that passwords be changed on a regular schedule. Passwords can be changed using either the Sentinel Control Center or standard database utilities. After changing a password, some Sentinel components need to be updated to use the new password.

- Section 5.2.1, "Changing Application User Passwords," on page 52
- Section 5.2.2, "Changing Database Passwords," on page 52

5.2.1 Changing Application User Passwords

This procedure can be used to change the password for the Sentinel Administrator account (admin) or any other Sentinel Control Center or Web interface user.

1. Log in to the Sentinel Control Center as the Sentinel Administrator or another user with User Management permissions.

   For more information on logging into the SCC, see "Accessing Novell Sentinel Web Interface" in the *Sentinel 6.1 Rapid Deployment User Guide*.
2. Click *Admin* > *User Configuration*. The User Manager window displays.
3. Double-click admin user account or right-click User Details.
4. Modify the account password and confirm password. Click *OK*.

   No additional updates are needed in the Sentinel system.

5.2.2 Changing Database Passwords

Changing the passwords for system users, such as dbauser, rptuser, or appuser, must be done using standard database utilities; it cannot be done by using the Sentinel Control Center. Some of these passwords are encrypted and stored in configuration files and used in normal Sentinel operations. These configuration files must be updated after the passwords are changed. System user passwords can be updated using standard database utilities.

IMPORTANT: Changing password for the postgre user is not supported in Sentinel 6.1 Rapid Deployment.

- "Updating PostgreSQL Database Password" on page 52
- "Updating Sentinel Configuration Files" on page 53
- "Updating Sentinel Data Manager Connection Properties" on page 53

Updating PostgreSQL Database Password

1. Open the `/opt/novell/sentinel6_rd_x86/3rdparty/postgresql/data/pg_hba.conf` file and add the following line at the top:

   ```
   local all trust
   ```
2. Restart PostgreSQL by using the following command:

   ```
   /opt/novell/sentinel6_rd_x86/bin/sentinel.sh stopdb
   ```

   ```
   /opt/novell/sentinel6_rd_x86/bin/sentinel.sh startdb
   ```
3. Export `/opt/novell/sentinel6_rd_x86/3rdparty/postgresql/lib` directory to LD_LIBRARY_PATH
4. Specify the following command to connect to PostgreSQL with `/opt/novell/sentinel6_rd_x86/3rdparty/postgresql/bin/psql`

   ```
   psql -d SIEM -U dbauser
   ```
5. Specify the following to change the dbauser password:

   ALTER USER <*user name*> WITH PASSWORD '<*new_password*>';

   Replace <*username*> with the user name such as dbuser, appuser, or rptuser.

ALTER USER dbuser WITH PASSWORD '<*new_password*>';

6. Specify any of the following to exit psql:
   - Ctrl-D
   - `\q`
7. Open the pg_hba.conf file and remove the following line:

```
local all trust
```

8. Restart PostgreSQL by using the following command:

```
/opt/novell/sentinel6_rd_x86/bin/sentinel.sh stopdb
/opt/novell/sentinel6_rd_x86/bin/sentinel.sh startdb
```

Updating Sentinel Configuration Files

If the appuser password is changed, several Sentinel configuration files must be updated with an encrypted form of the new password or the system cannot access the database. The dbconfig utility is designed to encrypt the password and add it to the appropriate files.

To update the Sentinel configuration files with a new password:

1. Change the password for the Sentinel DB Administrator User by using dbconfig utility.
2. This utility is used to set the database connection related information in the config file/s under `/opt/novell/sentinel6_rd_x86/config` directory such as username, password, database name, port, hostname.

Updating Sentinel Data Manager Connection Properties

If the dbauser password is changed, the Sentinel Data Manager connection properties must be updated in order for any automated Sentinel Data Manager command line tasks to continue to work (if applicable in your environment). These password change procedures are only necessary if extra Sentinel Data Manager jobs have been created and scheduled or the Sentinel Data Manager command line interface is used.

To update the saved SDM connection settings:

1. Run the following command and use the new dbauser password for the <dbPass> parameter. For more information, see "Sentinel Data Manager" in *Sentinel 6.1 Rapid Deployment User Guide*.

```
sdm -action saveConnection -server <postgresql> -host <hostIp/hostName> -
port <portnum> -database <databaseName/SID> [-driverProps
<propertiesFile>] {-user <dbUser> -password <dbPass>} -connectFile
<filenameToSaveConnection>
```

Sentinel 6.1 Rapid Deployment Database Views for PostgreSQL

6

This section lists the views in the PostgreSQL DB schema for Sentinel™ 6.1 Rapid Deployment. These views provide information for developing your own reports (JasperReports*).

6.1 Views

Below listed are the views available with Sentinel Rapid Deployment.

- Section 6.1.65, “EVT_PRTCL_RPT_V,” on page 96
- Section 6.1.66, “EVT_PRTCL_RPT_V3,” on page 97
- Section 6.1.67, “EVT_RSRC_RPT_V,” on page 97
- Section 6.1.68, “EVT_SEV_SMRY_1_RPT_V,” on page 97
- Section 6.1.69, “EVT_SRC_COLLECTOR_RPT_V,” on page 98
- Section 6.1.70, “EVT_SRC_GRP_RPT_V,” on page 98
- Section 6.1.71, “EVT_SRC_MGR_RPT_V,” on page 99
- Section 6.1.72, “EVT_SRC_OFFSET_RPT_V,” on page 99
- Section 6.1.73, “EVT_SRC_RPT_V,” on page 99
- Section 6.1.74, “EVT_SRC_SMRY_1_RPT_V,” on page 100
- Section 6.1.75, “EVT_SRC_SRVR_RPT_V,” on page 101
- Section 6.1.76, “EVT_TXNMY_RPT_V,” on page 101
- Section 6.1.77, “EVT_USR_RPT_V,” on page 102
- Section 6.1.78, “EVT_XDAS_TXNMY_RPT_V,” on page 102
- Section 6.1.79, “EXTERNAL_DATA_RPT_V,” on page 102
- Section 6.1.80, “HIST_CORRELATED_EVENTS_RPT_V (legacy view),” on page 103
- Section 6.1.81, “HIST_EVENTS_RPT_V (legacy view),” on page 103
- Section 6.1.82, “IMAGES_RPT_V,” on page 103
- Section 6.1.83, “INCIDENTS_ASSETS_RPT_V,” on page 103
- Section 6.1.84, “INCIDENTS_EVENTS_RPT_V,” on page 104
- Section 6.1.85, “INCIDENTS_RPT_V,” on page 104
- Section 6.1.86, “INCIDENTS_VULN_RPT_V,” on page 105
- Section 6.1.87, “L_STAT_RPT_V,” on page 105
- Section 6.1.88, “LOGS_RPT_V,” on page 106
- Section 6.1.89, “MSSP_ASSOCIATIONS_V,” on page 106
- Section 6.1.90, “NETWORK_IDENTITY_RPT_V,” on page 106
- Section 6.1.91, “ORGANIZATION_RPT_V,” on page 107
- Section 6.1.92, “PERSON_RPT_V,” on page 107
- Section 6.1.93, “PHYSICAL_ASSET_RPT_V,” on page 107
- Section 6.1.94, “PRODUCT_RPT_V,” on page 108
- Section 6.1.95, “ROLE_RPT_V,” on page 108
- Section 6.1.96, “RPT_LABELS_RPT_V,” on page 109
- Section 6.1.97, “SENSITIVITY_RPT_V,” on page 109
- Section 6.1.98, “SENTINEL_HOST_RPT_V,” on page 109
- Section 6.1.99, “SENTINEL_PLUGIN_RPT_V,” on page 110
- Section 6.1.100, “SENTINEL_RPT_V,” on page 110
- Section 6.1.101, “STATES_RPT_V,” on page 110
- Section 6.1.102, “UNASSIGNED_INCIDENTS_RPT_V,” on page 111

6.1.1 ACTVY_PARM_RPT_V

View contains information about iTRAC activities.

Column Name	Datatype	Comment
ACTVY_PARM_ID	uuid	Activity parameter identifier
ACTVY_ID	uuid	Activity identifier
PARM_NAME	character varying(255)	Activity Parameter name
PARM_TYP_CD	character varying(1)	Activity parameter type code
DATA_TYP	character varying(50)	Activity parameter data type
DATA_SUBTYP	character varying(50)	Activity parameter data subtype
RQRD_F	boolean	Required flag
PARM_DESC	character varying(255)	Activity parameter description
PARM_VAL	character varying(1000)	Activity parameter value
FORMATTER	character varying(255)	Activity parameter formatter
DATE_CREATED	timestamp with time zone	Date the entry was created
DATE_MODIFIED	timestamp with time zone	Date the entry was modified
CREATED_BY	integer	User who created object
MODIFIED_BY	integer	User who last modified object

6.1.2 ACTVY_REF_PARM_VAL_RPT_V

View contains information about iTRAC activities.

Column Name	Datatype	Comment
ACTVY_ID	uuid	Activity identifier
SEQ_NUM	integer	Sequence number
ACTVY_PARM_ID	uuid	Activity parameter identifier
PARM_VAL	character varying(1000)	Activity parameter value
DATE_CREATED	timestamp with time zone	Date the entry was created
DATE_MODIFIED	timestamp with time zone	Date the entry was modified
CREATED_BY	integer	User who created object
MODIFIED_BY	integer	User who last modified object

6.1.3 ACTVY_REF_RPT_V

View contains information about iTRAC activities.

Column Name	Datatype	Comment
ACTVY_ID	uuid	Activity identifier
SEQ_NUM	integer	Sequence number
REFD_ACTVY_ID	uuid	Referenced activity identifier
DATE_CREATED	timestamp with time zone	Date the entry was created
DATE_MODIFIED	timestamp with time zone	Date the entry was modified
CREATED_BY	integer	User who created object
MODIFIED_BY	integer	User who last modified object

6.1.4 ACTVY_RPT_V

View contains information about iTRAC activities

Column Name	Datatype	Comment
ACTVY_ID	uuid	Activity identifier
ACTVY_NAME	character varying(255)	Activity name
ACTVY_TYP_CD	character varying(1)	Activity type code
ACCESS_LVL	character varying(50)	Access level
EXEC_LOC	character varying(50)	Execution location
ACTVY_DESC	character varying(255)	Activity description

Column Name	Datatype	Comment
PROCESSOR	character varying(255)	Processor
INPUT_FORMATTER	character varying(255)	Input formatter
OUTPUT_FORMATTER	character varying(255)	Output formatter
APP_NAME	character varying(25)	Application name
DATE_CREATED	timestamp with time zone	Date the entry was created
DATE_MODIFIED	timestamp with time zone	Date the entry was modified
CREATED_BY	integer	User who created object
MODIFIED_BY	integer	User who last modified object

6.1.5 ADV_ATTACK_MAP_RPT_V

View references ADV_ATTACK_MAP table that stores Advisor map information.

Column Name	Datatype	Comment
ATTACK_KEY	integer	ID used to reference the attack entry
SERVICE_PACK_ID	integer	ID used to reference the attack entry
ATTACK_NAME	character varying(256)	Name of the Attack
ATTACK_CODE	character varying(256)	Attack code
DATE_PUBLISHED	timestamp with time zone	Date the attack has been published
DATE_UPDATED	timestamp with time zone	Date the attack has been uptimestamp with time zoned
DATE_CREATED	timestamp with time zone	Date the entry was created
DATE_MODIFIED	timestamp with time zone	Date the entry was modified
CREATED_BY	integer	User who created object
MODIFIED_BY	integer	User who last modified object

6.1.6 ADV_ATTACK_PLUGIN_RPT_V

View references ADV_ATTACK_PLUGIN table that stores Advisor plug-in information.

Column Name	Datatype	Comment
PLUGIN_KEY	integer	ID used to reference the vulnerability entry
SERVICE_PACK_ID	integer	ID of the vulnerability
PLUGIN_ID	character varying(256)	ID used to reference the vulnerability entry
PLUGIN_NAME	character varying(256)	Name of the vulnerability
DATE_PUBLISHED	timestamp with time zone	Date the vulnerability has been published

Column Name	Datatype	Comment
DATE_UPDATED	timestamp with time zone	Date the vulnerability has been uptimestamp with time zoned
DATE_CREATED	timestamp with time zone	Date the entry was created
DATE_MODIFIED	timestamp with time zone	Date the entry was modified
CREATED_BY	integer	User who created object
MODIFIED_BY	integer	User who last modified object

6.1.7 ADV_ATTACK_RPT_V

View references ADV_ATTACK table that stores Advisor attack information.

Column Name	Datatype	Comment
ATTACK_ID	integer	ID to identify the attack
TRUSECURE_ATTACK_NAME	character varying(512)	Name of the attack
FEED_DATE_CREATED	timestamp with time zone	Date when the feed first have the information on this attack
FEED_DATE_UPDATED	timestamp with time zone	Last timestamp with time zone when the information on this attack has been uptimestamp with time zoned
ATTACK_CATEGORY	character varying(256)	Category of the attack
URGENCY_ID	integer	The urgency associated with this attack
SEVERITY_ID	integer	Severity associated with this attack
LOCAL	integer	Indicates if this attack was executed locally
REMOTE	integer	Indicates if this attack was executed from remote
DESCRIPTION	text	Impact of the attack
SCENARIO	text	Safeguards that could be followed to avert the attack
IMPACT	text	Patches for the product to fix the vulnerability exploited by the attack
SAFEGUARDS	text	False Positives associated with this attack
PATCHES	text	Date the information on this attack was published
FALSE_POSITIVES	text	Date the information on this attack was uptimestamp with time zoned
DATE_PUBLISHED	timestamp with time zone	ID to identify the attack

Column Name	Datatype	Comment
DATE_UPDATED	timestamp with time zone	Name of the attack
DATE_CREATED	timestamp with time zone	Date the entry was created
DATE_MODIFIED	timestamp with time zone	Date the entry was modified
CREATED_BY	integer	By user ID
MODIFIED_BY	integer	By user ID

6.1.8 ADV_ATTACK_SIGNATURES

Column Name	Datatype	Comment
ATTACK_KEY	integer	Attack ID
ATTACK_SCANNER_NAME	character varying(128)	Name of the attack scanner or intrusion detection system
ATTACK_NAME	character varying(256)	Name of the attack
ATTACK_ID	character varying(256)	ID of the attack

6.1.9 ADV_FEED_RPT_V

View references ADV_FEED table that stores Advisor feed information, such as feed name and timestamp with time zone.

Column Name	Datatype	Comment
FEED_NAME	character varying(128)	Name of feed
FEED_FILE	character varying(256)	File name that contains the feed data
BEGIN_DATE	timestamp with time zone	The timestamp with time zone from which this feed file carries the advisor information
END_DATE	timestamp with time zone	The timestamp with time zone until which this feed file carries the advisor information
FEED_INSERT	integer	Number of rows inserted into the advisor schema by this feed file
FEED_UPDATE	integer	Number of rows uptimestamp with time zoned into the advisor schema by this feed file
FEED_EXPIRE	integer	Number of rows deleted into the advisor schema by this feed file

6.1.10 ADV_MASTER_RPT_V

Column Name	Datatype	Comment
MASTER_ID	integer	ID that associates PLUGIN_KEY, ATTACK_KEY and VULN_KB_ID
PLUGIN_KEY	integer	ID to reference the ADV_ATTACK_PLUGIN_V
ATTACK_KEY	integer	ID to reference the ADV_ATTACK_MAP_V
VULN_KB_ID	integer	ID to reference the VULN_KB_ID_V
DATE_PUBLISHED	timestamp with time zone	Date the entry was published
DATE_UPDATED	timestamp with time zone	Date the entry was uptimestamp with time zoned
BEGIN_EFFECTIVE_DATE	timestamp with time zone	Date from which the entry is valid
END_EFFECTIVE_DATE	timestamp with time zone	Date until which the entry is valid
DATE_CREATED	timestamp with time zone	Date the entry was created
DATE_MODIFIED	timestamp with time zone	Date the entry was modified
CREATED_BY	integer	User who created object
MODIFIED_BY	integer	User who last modified object

6.1.11 ADV_PRODUCT_RPT_V

View references ADV_PRODUCT table that stores Advisor product information such as vendor and product ID.

Column Name	Datatype	Comment
PRODUCT_ID	integer	ID of the product
VENDOR_ID	integer	ID of the vendor
PRODUCT_CATEGORY_ID	integer	ID of the Product Category
PRODUCT_CATEGORY_NAME	character varying(128)	Product Category Name
PRODUCT_TYPE_ID	integer	ID of the product type
PRODUCT_TYPE_NAME	character varying(256)	Name of the Product Type
PRODUCT_NAME	character varying(128)	Product Name
PRODUCT_DESCRIPTION	character varying(512)	Product Descritpion
FEED_DATE_CREATED	timestamp with time zone	Date of the Feed that carried information on this product

Column Name	Datatype	Comment
FEED_DATE_UPDATED	timestamp with time zone	Date of the Feed that uptimestamp with time zoned information on this product
ACTIVE_FLAG	integer	Reserved for future use
DATE_CREATED	timestamp with time zone	Date the entry was created
DATE_MODIFIED	timestamp with time zone	Date the entry was modified
CREATED_BY	integer	User who created object
MODIFIED_BY	integer	User who last modified object

6.1.12 ADV_PRODUCT_SERVICE_PACK_RPT_V

View references ADV_PRODUCT_SERVICE _PACK table that stores Advisor service pack information, such as service pack name, version ID and timestamp with time zone.

Column Name	Datatype	Comment
SERVICE_PACK_ID	integer	Service Pack ID
VERSION_ID	integer	Version ID
SERVICE_PACK_NAME	character varying(32)	Name of the Service Pack
FEED_DATE_CREATED	timestamp with time zone	Date of the Feed that carried information on this product
FEED_DATE_UPDATED	timestamp with time zone	Date of the Feed that uptimestamp with time zoned information on this product
ACTIVE_FLAG	integer	Reserved for future use
BEGIN_EFFECTIVE_DATE	timestamp with time zone	Date from which the entry is valid
END_EFFECTIVE_DATE	timestamp with time zone	Date until which the entry is valid
DATE_CREATED	timestamp with time zone	Date the entry was created
DATE_MODIFIED	timestamp with time zone	Date the entry was modified
CREATED_BY	integer	User who created object
MODIFIED_BY	integer	User who last modified object

6.1.13 ADV_PRODUCT_VERSION_RPT_V

View references ADV_PRODUCT_VERSION table that stores Advisor product version information, such as version name, product and version ID.

Column Name	Datatype	Comment
VERSION_ID	integer	Version ID

Column Name	Datatype	Comment
PRODUCT_ID	integer	Product ID
VERSION_NAME	character varying(128)	Version Name of the product
FEED_DATE_CREATED	timestamp with time zone	Date of the feed that carried the information on the entry
FEED_DATE_UPDATED	timestamp with time zone	Date of the feed that carried the uptimestamp with time zone on the entry
ACTIVE_FLAG	integer	Reserved for future use
DATE_CREATED	timestamp with time zone	Date the entry was created
DATE_MODIFIED	timestamp with time zone	Date the entry was modified
CREATED_BY	integer	User who created object
MODIFIED_BY	integer	User who last modified object

6.1.14 ADV_VENDOR_RPT_V

View references ADV_VENDOR table that stores Advisor address information.

Column Name	Datatype	Comment
VENDOR_ID	integer	ID of the vendor
VENDOR_NAME	character varying(128)	Name of the vendor
CONTACT_PERSON	character varying(128)	Contains the contact person name for the vendor
ADDRESS_LINE_1	character varying(128)	Address of the vendor
ADDRESS_LINE_2	character varying(128)	Address of the vendor
ADDRESS_LINE_3	character varying(128)	Address of the vendor
ADDRESS_LINE_4	character varying(128)	Address of the vendor
CITY	character varying(128)	City of the vendor
STATE	character varying(128)	State of the vendor
COUNTRY	character varying(128)	Country of the vendor
ZIP_CODE	character varying(128)	Zip code of the vendor
URL	character varying(256)	Web URL of the vendor
PHONE	character varying(32)	Contact number of the vendor
FAX	character varying(32)	Fax number of the vendor
EMAIL	character varying(128)	Email of the vendor
PAGER	character varying(32)	Pager of the vendor
FEED_DATE_CREATED	timestamp with time zone	Date of the feed that carried the information on the entry

Column Name	Datatype	Comment
FEED_DATE_UPDATED	timestamp with time zone	Date of the feed that carried the uptimestamp with time zone on the entry
ACTIVE_FLAG	integer	Reserved for future use
DATE_CREATED	timestamp with time zone	Date the entry was created
DATE_MODIFIED	timestamp with time zone	Date the entry was modified
CREATED_BY	integer	User who created object
MODIFIED_BY	integer	User who last modified object

6.1.15 ADV_VULN_KB_RPT_V

Column Name	Datatype	Comment
VULN_KB_ID	integer	Knowledge base ID mapping CVE_ID, OSVDB_ID, BUGTRAQ_ID
CVE_ID	character varying(10)	CVE ID for the related vulnerability
OSVDB_ID	integer	OSVDB ID for the related vulnerability
BUGTRAQ_ID	integer	Bugtraq id for the related vulnerability
DATE_PUBLISHED	timestamp with time zone	Date the entry was published
DATE_UPDATED	timestamp with time zone	Date the entry was uptimestamp with time zoned
DATE_CREATED	timestamp with time zone	Date the entry was created
DATE_MODIFIED	timestamp with time zone	Date the entry was modified
CREATED_BY	integer	User who created object
MODIFIED_BY	integer	User who last modified object

6.1.16 ADV_VULN_PRODUCT_RPT_V

View references ADV_VULN_PRODUCT table that stores Advisor vulnerability attack ID and service pack ID.

Column Name	Datatype	Comment
SERVICE_PACK_ID	integer	Contains the service pack id
ATTACK_ID	integer	Contains the attack id
DATE_CREATED	timestamp with time zone	Date the entry was created
DATE_MODIFIED	timestamp with time zone	Date the entry was modified

Column Name	Datatype	Comment
CREATED_BY	integer	User who created object
MODIFIED_BY	integer	User who last modified object

6.1.17 ADV_VULN_SIGNATURES

Column Name	Datatype	Comment
VULN_KEY	integer	Vulnerability key
VULN_SCANNER_NAME	character varying(128)	Vulnerability scanner name
VULN_NAME	character varying(256)	Vulnerability name
VULN_ID	character varying(256)	Vulnerability ID

6.1.18 ANNOTATIONS_RPT_V

View references ANNOTATIONS table that stores documentation or notes that can be associated with objects in the SentinelRD system such as cases and incidents.

Column Name	Datatype	Comment
ANN_ID	integer	Annotation identfier - sequence number.
TEXT	character varying(4000)	Documentation or notes.
DATE_CREATED	timestamp with time zone	Date the entry was created
DATE_MODIFIED	timestamp with time zone	Date the entry was modified
MODIFIED_BY	integer	User who last modified object
CREATED_BY	integer	User who created object
ACTION	character varying(255)	Action

6.1.19 ASSET_CATEGORY_RPT_V

View references ASSET_CTGRY table that stores information about asset categories

Column Name	Datatype	Comment
ASSET_CATEGORY_ID	bigint	Asset category identifier
ASSET_CATEGORY_NAME	character varying(100)	Asset category name
DATE_CREATED	timestamp with time zone	Date the entry was created
DATE_MODIFIED	timestamp with time zone	Date the entry was modified
CREATED_BY	integer	User who created object
MODIFIED_BY	integer	User who last modified object

6.1.20 ASSET_HOSTNAME_RPT_V

View references ASSET_HOSTNAME table that stores information about alternate host names for assets.

Column Name	Datatype	Comment
ASSET_HOSTNAME_ID	uuid	Asset alternate hostname identifier
PHYSICAL_ASSET_ID	uuid	Physical asset identifier
HOST_NAME	character varying(255)	Host name
CUST_ID	bigint	Customer identifier
DATE_CREATED	timestamp with time zone	Date the entry was created
DATE_MODIFIED	timestamp with time zone	Date the entry was modified
CREATED_BY	integer	User who created object
MODIFIED_BY	integer	User who last modified object

6.1.21 ASSET_IP_RPT_V

View references ASSET_IP table that stores information about alternate IP addresses for assets.

Column Name	Datatype	Comment
ASSET_IP_ID	uuid	Asset alternate IP identifier
PHYSICAL_ASSET_ID	uuid	Physical asset identifier
IP_ADDRESS	integer	Asset IP address
CUST_ID	bigint	Customer identifier
DATE_CREATED	timestamp with time zone	Date the entry was created
DATE_MODIFIED	timestamp with time zone	Date the entry was modified
CREATED_BY	integer	User who created object
MODIFIED_BY	integer	User who last modified object

6.1.22 ASSET_LOCATION_RPT_V

View references ASSET_LOC table that stores information about asset locations.

Column Name	Datatype	Comment
LOCATION_ID	bigint	Location identifier
CUST_ID	bigint	Customer identifier
BUILDING_NAME	character varying(255)	Building name
ADDRESS_LINE_1	character varying(255)	Address line 1

Column Name	Datatype	Comment
ADDRESS_LINE_2	character varying(255)	Address line 2
CITY	character varying(100)	City
STATE	character varying(100)	State
COUNTRY	character varying(100)	Country
ZIP_CODE	character varying(50)	Zip code
DATE_CREATED	timestamp with time zone	Date the entry was created
DATE_MODIFIED	timestamp with time zone	Date the entry was modified
CREATED_BY	integer	User who created object
MODIFIED_BY	integer	User who last modified object

6.1.23 ASSET_RPT_V

View references ASSET table that stores information about the physical and soft assets.

Column Name	Datatype	Comment
ASSET_ID	uuid	Asset identifier
CUST_ID	bigint	Customer identifier
ASSET_NAME	character varying(255)	Asset name
PHYSICAL_ASSET_ID	uuid	Physical asset identifier
PRODUCT_ID	bigint	Product identifier
ASSET_CATEGORY_ID	bigint	Asset category identifier
ENVIRONMENT_IDENTITY_CD	bigint	Environment identify code
PHYSICAL_ASSET_IND	boolean	Physical asset indicator
ASSET_VALUE_CODE	bigint	Asset value code
CRITICALITY_ID	bigint	Asset criticality code
SENSITIVITY_ID	bigint	Asset sensitivity code
DATE_CREATED	timestamp with time zone	Date the entry was created
DATE_MODIFIED	timestamp with time zone	Date the entry was modified
CREATED_BY	integer	User who created object
MODIFIED_BY	integer	User who last modified object

6.1.24 ASSET_VALUE_RPT_V

View references ASSET_VAL_LKUP table that stores information about the asset value.

Column Name	Datatype	Comment
ASSET_VALUE_ID	bigint	Asset value code
ASSET_VALUE_NAME	character varying(50)	Asset value name
DATE_CREATED	timestamp with time zone	Date the entry was created
DATE_MODIFIED	timestamp with time zone	Date the entry was modified
CREATED_BY	integer	User who created object
MODIFIED_BY	integer	User who last modified object

6.1.25 ASSET_X_ENTITY_X_ROLE_RPT_V

View references ASSET_X_ENTITY_X_ROLE table that associates a person or an organization to an asset.

Column Name	Datatype	Comment
PERSON_ID	uuid	Person identifier
ORGANIZATION_ID	uuid	Organization identifier
ROLE_CODE	character varying(5)	Role code
ASSET_ID	uuid	Asset identifier
ENTITY_TYPE_CODE	character varying(5)	Entity type code
PERSON_ROLE_SEQUENCE	integer	Order of persons under a particular role
DATE_CREATED	timestamp with time zone	Date the entry was created
DATE_MODIFIED	timestamp with time zone	Date the entry was modified
CREATED_BY	integer	User who created object
MODIFIED_BY	integer	User who last modified object

6.1.26 ASSOCIATIONS_RPT_V

View references ASSOCIATIONS table that associates users to incidents, incidents to annotations and so on.

Column Name	Datatype	Comment
TABLE1	character varying(64)	Table name 1. For example, incidents
ID1	integer	ID1. For example, incident ID.
TABLE2	character varying(64)	Table name 2. For example, users.
ID2	integer	ID2. For example, user ID.
DATE_CREATED	timestamp with time zone	Date the entry was created

Column Name	Datatype	Comment
DATE_MODIFIED	timestamp with time zone	Date the entry was modified
CREATED_BY	integer	User who created object
MODIFIED_BY	integer	User who last modified object

6.1.27 ATTACHMENTS_RPT_V

View references ATTACHMENTS table that stores attachment data.

Column Name	Datatype	Comment
ATTACHMENT_ID	integer	Attachment identifier
NAME	character varying(255)	Attachment name
SOURCE_REFERENCE	character varying(64)	Source reference
TYPE	character varying(32)	Attachment type
SUB_TYPE	character varying(32)	Attachment subtype
FILE_EXTENSION	character varying(32)	File extension
ATTACHMENT_DESCRIPTION	character varying(255)	Attachment description
DATA	text	Attachment data
DATE_CREATED	timestamp with time zone	Date the entry was created
DATE_MODIFIED	timestamp with time zone	Date the entry was modified
CREATED_BY	integer	User who created object
MODIFIED_BY	integer	User who last modified object

6.1.28 AUDIT_RECORD_RPT_V

View references AUDIT_RECORD table that stores SentinelRD internal audit data.

Column Name	Datatype	Comment
AUDIT_ID	uuid	Audit record identifier
AUDIT_TYPE	character varying(255)	Audit type
SRC	character varying(255)	Audit source
SENDER_HOSTNAME	character varying(255)	Sender hostname
SENDER_HOST_IP	character varying(255)	Sender host IP
SENDER_CONTAINER	character varying(255)	Sender container name
SENDER_ID	character varying(255)	Sender Identifier
CLIENT	character varying(255)	Client application that requested audit

Column Name	Datatype	Comment
EVT_NAME	character varying(255)	Event name
RES	character varying(255)	Event resource
SRES	character varying(255)	Event sub-resource
MSG	character varying(500)	Event message
CREATED_BY	integer	User who created object
MODIFIED_BY	integer	User who last modified object
DATE_CREATED	timestamp with time zone	Date the entry was created
DATE_MODIFIED	timestamp with time zone	Date the entry was modified

6.1.29 CONFIGS_RPT_V

View references CONFIGS table that stores general configuration information of the application.

Column Name	Datatype	Comment
USR_ID	character varying(32)	User name
APPLICATION	character varying(255)	Application identifier
UNIT	character varying(64)	Application unit
VALUE	character varying(255)	Text value if any
DATA	text	XML data
DATE_CREATED	timestamp with time zone	Date the entry was created
DATE_MODIFIED	timestamp with time zone	Date the entry was modified
CREATED_BY	integer	User who created object
MODIFIED_BY	integer	User who last modified object

6.1.30 CONTACTS_RPT_V

View references CONTACTS table that stores contact information.

Column Name	Datatype	Comment
CNT_ID	integer	Contact ID - Sequence number
FIRST_NAME	character varying(20)	Contact first name
LAST_NAME	character varying(30)	Contact last name
TITLE	character varying(128)	Contact title
DEPARTMENT	character varying(128)	Department
PHONE	character varying(64)	Contact phone

Column Name	Datatype	Comment
EMAIL	character varying(255)	Contact email
PAGER	character varying(64)	Contact pager
CELL	character varying(64)	Contact cell phone
DATE_CREATED	timestamp with time zone	Date the entry was created
DATE_MODIFIED	timestamp with time zone	Date the entry was modified
CREATED_BY	integer	User who created object
MODIFIED_BY	integer	User who last modified object

6.1.31 CORRELATED_EVENTS_RPT_V (legacy view)

This view is provided for backward compatibility. New reports should use CORRELATED_EVENTS_RPT_V1.

6.1.32 CORRELATED_EVENTS_RPT_V1

View contains current and historical correlated events (correlated events imported from archives).

Column Name	Datatype	Comment
PARENT_EVT_ID	uuid	Event Universal Unique Identifier (UUID) of parent event
CHILD_EVT_ID	uuid	Event Universal Unique Identifier (UUID) of child event
PARENT_EVT_TIME	timestamp with time zone	Parent event time
CHILD_EVT_TIME	timestamp with time zone	Child event time
DATE_CREATED	timestamp with time zone	Date the entry was created
DATE_MODIFIED	timestamp with time zone	Date the entry was modified
CREATED_BY	integer	User who created object
MODIFIED_BY	integer	User who last modified object

6.1.33 CRITICALITY_RPT_V

View references CRIT_LKUP table that contains information about asset criticality.

Column Name	Datatype	Comment
CRITICALITY_ID	bigint	Asset criticality code
CRITICALITY_NAME	character varying(50)	Asset criticality name

Column Name	Datatype	Comment
DATE_CREATED	timestamp with time zone	Date the entry was created
DATE_MODIFIED	timestamp with time zone	Date the entry was modified
CREATED_BY	integer	User who created object
MODIFIED_BY	integer	User who last modified object

6.1.34 CUST_HIERARCHY_V

View references CUST_HIERARCHY table that stores information about MSSP customer hierarchy.

Column Name	Datatype	Comment
CUST_HIERARCHY_ID	bigint	Customer hierarchy ID
CUST_NAME	character varying(255)	Customer
CUST_HIERARCHY_LVL1	character varying(255)	Customer hierarchy level 1
CUST_HIERARCHY_LVL2	character varying(255)	Customer hierarchy level 2
CUST_HIERARCHY_LVL3	character varying(255)	Customer hierarchy level 3
CUST_HIERARCHY_LVL4	character varying(255)	Customer hierarchy level 4
DATE_CREATED	timestamp with time zone	Date the entry was created
DATE_MODIFIED	timestamp with time zone	Date the entry was modified
CREATED_BY	integer	User who created object
MODIFIED_BY	integer	User who last modified object

6.1.35 CUST_RPT_V

View references CUST table that stores customer information for MSSPs.

Column Name	Datatype	Comment
CUST_ID	bigint	Customer identifier
CUSTOMER_NAME	character varying(255)	Customer name
DATE_CREATED	timestamp with time zone	Date the entry was created
DATE_MODIFIED	timestamp with time zone	Date the entry was modified
CREATED_BY	integer	User who created object
MODIFIED_BY	integer	User who last modified object

6.1.36 ENTITY_TYPE_RPT_V

View references ENTITY_TYP table that stores information about entity types (person, organization).

Column Name	Datatype	Comment
ENTITY_TYPE_CODE	character varying(5)	Entity type code
ENTITY_TYPE_NAME	character varying(50)	Entity type name
DATE_CREATED	timestamp with time zone	Date the entry was created
DATE_MODIFIED	timestamp with time zone	Date the entry was modified
CREATED_BY	integer	User who created object
MODIFIED_BY	integer	User who last modified object

6.1.37 ENV_IDENTITY_RPT_V

View references ENV_IDENTITY_LKUP table that stores information about asset environment identity.

Column Name	Datatype	Comment
ENVIRONMENT_IDENTITY_ID	bigint	Environment identity code
ENV_IDENTITY_NAME	character varying(255)	Environment identity name
DATE_CREATED	timestamp with time zone	Date the entry was created
DATE_MODIFIED	timestamp with time zone	Date the entry was modified
CREATED_BY	integer	User who created object
MODIFIED_BY	integer	User who last modified object

6.1.38 ESEC_CONTENT_GRP_CONTENT_RPT_V

View contains information about Solution Packs.

Column Name	Datatype	Comment
CONTENT_GRP_ID	uuid	Content group identifier
CONTENT_ID	character varying(255)	Content identifier
CONTENT_TYP	character varying(100)	Content type
CONTENT_HASH	character varying(255)	Content hash
DATE_CREATED	timestamp with time zone	Date the entry was created
DATE_MODIFIED	timestamp with time zone	Date the entry was modified
CREATED_BY	integer	User who created object

Column Name	Datatype	Comment
MODIFIED_BY	integer	User who last modified object

6.1.39 ESEC_CONTENT_GRP_RPT_V

View contains information about Solution Packs.

Column Name	Datatype	Comment
CONTENT_GRP_ID	uuid	Content group identifier
CONTENT_GRP_NAME	character varying(255)	Content group name
CONTENT_GRP_DESC	text	Content group description
CTRL_ID	uuid	Control identifier
CONTENT_EXTERNAL_ID	character varying(255)	Content external identifier
DATE_CREATED	timestamp with time zone	Date the entry was created
DATE_MODIFIED	timestamp with time zone	Date the entry was modified
CREATED_BY	integer	User who created object
MODIFIED_BY	integer	User who last modified object

6.1.40 ESEC_CONTENT_PACK_RPT_V

View contains information about Solution Packs.

Column Name	Datatype	Comment
CONTENT_PACK_ID	uuid	Content pack identifier
CONTENT_PACK_DESC	text	Content pack description
CONTENT_PACK_NAME	character varying(255)	Content pack name
CONTENT_EXTERNAL_ID	character varying(255)	Content external identifier
DATE_MODIFIED	timestamp with time zone	Date the entry was modified
DATE_CREATED	timestamp with time zone	Date the entry was created
CREATED_BY	integer	User who created object
MODIFIED_BY	integer	User who last modified object

6.1.41 ESEC_CONTENT_RPT_V

View contains information about Solution Packs.

Column Name	Datatype	Comment
CONTENT_ID	character varying(255)	Content identifier

Column Name	Datatype	Comment
CONTENT_NAME	character varying(255)	Content name
CONTENT_DESC	text	Content description
CONTENT_STATE	integer	Content state
CONTENT_TYP	character varying(100)	Content type
CONTENT_CONTEXT	text	Content context
CONTENT_HASH	character varying(255)	Content hash
DATE_CREATED	timestamp with time zone	Date the entry was created
DATE_MODIFIED	timestamp with time zone	Date the entry was modified
MODIFIED_BY	integer	User who last modified object
CREATED_BY	integer	User who created object

6.1.42 ESEC_CTRL_CTGRY_RPT_V

View contains information about Solution Packs.

Column Name	Datatype	Comment
CTRL_CTGRY_ID	uuid	Control category identifier
CTRL_CTGRY_DESC	text	Control category description
CTRL_CTGRY_NAME	character varying(255)	Control category name
CONTENT_PACK_ID	uuid	Content pack identifier
CONTENT_EXTERNAL_ID	character varying(255)	Content external identifier
DATE_CREATED	timestamp with time zone	Date the entry was created
DATE_MODIFIED	timestamp with time zone	Date the entry was modified
CREATED_BY	integer	User who created object
MODIFIED_BY	integer	User who last modified object

6.1.43 ESEC_CTRL_RPT_V

View contains information about Solution Packs.

Column Name	Datatype	Comment
CTRL_ID	uuid	Control identifier
CTRL_NAME	character varying(255)	Control name
CTRL_DESC	text	Control description
CTRL_STATE	integer	Control state

Column Name	Datatype	Comment
CTRL_NOTES	text	Control notes
CTRL_CTGRY_ID	uuid	Control category identifier
CONTENT_EXTERNAL_ID	character varying(255)	Content external identifier
DATE_CREATED	timestamp with time zone	Date the entry was created
DATE_MODIFIED	timestamp with time zone	Date the entry was modified
CREATED_BY	integer	User who created object
MODIFIED_BY	integer	User who last modified object

6.1.44 ESEC_DISPLAY_RPT_V

View references ESEC_DISPLAY table that stores displayable properties of objects. Currently used in renaming meta-tags. Used with Event Configuration (Business Relevance).

Column Name	Datatype	Comment
DISPLAY_OBJECT	character varying(32)	The parent object of the property
TAG	character varying(32)	The native tag name of the property
LABEL	character varying(32)	The display string of tag.
POSITION	integer	Position of tag within display.
WIDTH	integer	The column width
ALIGNMENT	integer	The horizontal alignment
FORMAT	integer	The enumerated formatter for displaying the property
ENABLED	boolean	Indicates if the tag is shown.
TYPE	integer	Indicates datatype of tag. 1 = string 2 = ulong 3 = timestamp with time zone 4 = uuid 5 = ipv4
DESCRIPTION	character varying(255)	Textual description of the tag
DATE_CREATED	timestamp with time zone	Date the entry was created
DATE_MODIFIED	timestamp with time zone	Date the entry was modified
CREATED_BY	integer	User who created object
MODIFIED_BY	integer	User who last modified object
REF_CONFIG	character varying(4000)	Referential data configuration

6.1.45 ESEC_PORT_REFERENCE_RPT_V

View references ESEC_PORT_REFERENCE table that stores industry standard assigned port numbers.

Column Name	Datatype	Comment
PORT_NUMBER	integer	Per http://www.iana.org/assignments/port-numbers (http://www.iana.org/assignments/port-numbers), the numerical representation of the port. This port number is typically associated with the Transport Protocol level in the TCP/IP stack.
PROTOCOL_NUMBER	integer	Per http://www.iana.org/assignments/protocol-numbers (http://www.iana.org/assignments/protocol-numbers), the numerical identifiers used to represent protocols that are encapsulated in an IP packet.
PORT_KEYWORD	character varying(64)	Per http://www.iana.org/assignments/port-numbers (http://www.iana.org/assignments/port-numbers), the keyword representation of the port.
PORT_DESCRIPTION	character varying(512)	Port description
DATE_CREATED	timestamp with time zone	Date the entry was created
DATE_MODIFIED	timestamp with time zone	Date the entry was modified
CREATED_BY	integer	User who created object
MODIFIED_BY	integer	User who last modified object

6.1.46 ESEC_PROTOCOL_REFERENCE_RPT_V

View references ESEC_PROTOCOL_REFERENCE table that stores industry standard assigned protocol numbers.

Column Name	Datatype	Comment
PROTOCOL_NUMBER	integer	Per http://www.iana.org/assignments/protocol-numbers (http://www.iana.org/assignments/protocol-numbers), the numerical identifiers used to represent protocols that are encapsulated in an IP packet.
PROTOCOL_KEYWORD	character varying(64)	Per http://www.iana.org/assignments/protocol-numbers (http://www.iana.org/assignments/protocol-numbers), the keyword used to represent protocols that are encapsulated in an IP packet.
PROTOCOL_DESCRIPTION	character varying(512)	IP packet protocol description
DATE_CREATED	timestamp with time zone	Date the entry was created

Column Name	Datatype	Comment
DATE_MODIFIED	timestamp with time zone	Date the entry was modified
CREATED_BY	integer	User who created object
MODIFIED_BY	integer	User who last modified object

6.1.47 ESEC_SEQUENCE_RPT_V

View references ESEC_SEQUENCE table that's used to generate primary key sequence numbers for SentinelRD tables.

Column Name	Datatype	Comment
TABLE_NAME	character varying(32)	Name of the table.
COLUMN_NAME	character varying(255)	Name of the column
SEED	integer	Current value of primary key field
DATE_CREATED	timestamp with time zone	Date the entry was created
DATE_MODIFIED	timestamp with time zone	Date the entry was modified
CREATED_BY	integer	User who created object
MODIFIED_BY	integer	User who last modified object

6.1.48 ESEC_UUID_UUID_ASSOC_RPT_V

Contains information about object relationships. Used internally by SentinelRD and not for reporting purposes.

Column Name	Datatype	Comment
OBJECT1	character varying(64)	Object 1
ID1	uuid	UUID for object 1
OBJECT2	character varying(64)	Object 2
ID2	uuid	UUID for object 2
DATE_CREATED	timestamp with time zone	Date the entry was created
DATE_MODIFIED	timestamp with time zone	Date the entry was modified
CREATED_BY	integer	User who created object
MODIFIED_BY	integer	User who last modified object

6.1.49 EVENTS_ALL_RPT_V (legacy view)

This view is provided for backward compatibility. View contains current and historical events (events imported from archives).

6.1.50 EVENTS_ALL_RPT_V1 (legacy view)

This view is provided for backward compatibility. New reports should use EVENTS_RPT_V2. View contains current events.

6.1.51 EVENTS_ALL_V (legacy view)

This view is provided for backward compatibility. New reports should use EVENTS_RPT_V2. View contains current events.

6.1.52 EVENTS_RPT_V (legacy view)

This view is provided for backward compatibility. New reports should use EVENTS_RPT_V2. View contains current and historical events.

6.1.53 EVENTS_RPT_V1 (legacy view)

This view is provided for backward compatibility. New reports should use EVENT_ALL_RPT_V. View contains current events.

6.1.54 EVENTS_RPT_V2

EVENTS_RPT_V2 is included for legacy reports but has been replaced in SentinelRD with EVENTS_RPT_V3.

Column Name	Datatype	Comment
EVENT_ID	uuid	Event identifier
RESOURCE_NAME	character varying(255)	Resource name
SUB_RESOURCE	character varying(255)	Subresource name
SEVERITY	integer	Event severity
EVENT_PARSE_TIME	timestamp with time zone	Event time
EVENT_DATETIME	timestamp with time zone	Event time
EVENT_DEVICE_TIME	timestamp with time zone	Event device time
SENTINEL_PROCESS_TIME	timestamp with time zone	SentinelRD process time
BEGIN_TIME	timestamp with time zone	Events begin time
END_TIME	timestamp with time zone	Events end time
REPEAT_COUNT	integer	Events repeat count
DESTINATION_PORT_INT	integer	Destination port (integer)
SOURCE_PORT_INT	integer	Source port (integer)
BASE_MESSAGE	character varying(4000)	Base message
EVENT_NAME	character varying(255)	Name of the event as reported by the sensor

Column Name	Datatype	Comment
EVENT_TIME	character varying(255)	Event time as reported by the sensor
CUST_ID	bigint	Customer identifier
SOURCE_ASSET_ID	bigint	Source asset identifier
DESTINATION_ASSET_ID	bigint	Destination asset identifier
AGENT_ID	bigint	Collector identifier
PROTOCOL_ID	bigint	Protocol identifier
ARCHIVE_ID	bigint	Archive identifier
SOURCE_IP	integer	Source IP address in numeric format
SOURCE_IP_DOTTED	character varying	Source IP in dotted format
SOURCE_HOST_NAME	character varying(255)	Source host name
SOURCE_PORT	character varying(32)	Source port
DESTINATION_IP	integer	Destination IP address in numeric format
DESTINATION_IP_DOTTED	character varying	Destination in dotted format
DESTINATION_HOST_NAME	character varying(255)	Destination host name
DESTINATION_PORT	character varying(32)	Destination port
SOURCE_USER_NAME	character varying(255)	Source user name
DESTINATION_USER_NAME	character varying(255)	Destination user name
FILE_NAME	character varying(1000)	File name
EXTENDED_INFO	character varying(1000)	Extened information
CUSTOM_TAG_1	character varying(255)	Customer Tag 1
CUSTOM_TAG 2	character varying(255)	Customer Tag 2
CUSTOM_TAG 3	integer	Customer Tag 3
RESERVED_TAG_1	character varying(255)	Reserved Tag 1
		Reserved for future use by Novell. This field is used for Advisor information concerning attack descriptions.
RESERVED_TAG_2	character varying(255)	Reserved for future use by Novell. Use of this field for any other purpose might result in data being overwritten by future functionality.
RESERVED_TAG_3	integer	Reserved for future use by Novell. Use of this field for any other purpose might result in data being overwritten by future functionality.
VULNERABILITY_RATING	integer	Vulnerability rating

Column Name	Datatype	Comment
CRITICALITY_RATING	integer	Criticality rating
DATE_CREATED	timestamp with time zone	Date the entry was created
DATE_MODIFIED	timestamp with time zone	Date the entry was modified
CREATED_BY	integer	User who created object
MODIFIED_BY	integer	User who last modified object
RV01 - 10	integer	Reserved Value 1 - 10 Reserved for future use by Novell. Use of this field for any other purpose might result in data being overwritten by future functionality.
RV11 - 20	timestamp with time zone	Reserved Value 11 - 20 Reserved for future use by Novell. Use of this field for any other purpose might result in data being overwritten by future functionality.
RV21 - 25	uuid	Reserved Value 21 - 25 Reserved for future use by Novell to store UUIDs. Use of this field for any other purpose might result in data being overwritten by future functionality.
RV26 - 31	character varying(255)	Reserved Value 26 - 31 Reserved for future use by Novell. Use of this field for any other purpose might result in data being overwritten by future functionality.
RV33	character varying(255)	Reserved Value 33 Reserved for EventContex Use of this field for any other purpose might result in data being overwritten by future functionality.
RV34	character varying(255)	Reserved Value 34 Reserved for SourceThreatLevel Use of this field for any other purpose might result in data being overwritten by future functionality.
RV35	character varying(255)	Reserved Value 35 Reserved for SourceUserContext. Use of this field for any other purpose might result in data being overwritten by future functionality.

Column Name	Datatype	Comment
RV36	character varying(255)	Reserved Value 36 Reserved for DataContext. Use of this field for any other purpose might result in data being overwritten by future functionality.
RV37	character varying(255)	Reserved Value 37 Reserved for SourceFunction. Use of this field for any other purpose might result in data being overwritten by future functionality.
RV38	character varying(255)	Reserved Value 38 Reserved for SourceOperationalContext. Use of this field for any other purpose might result in data being overwritten by future functionality.
RV40 - 43	character varying(255)	Reserved Value 40 - 43 Reserved for future use by Novell. Use of this field for any other purpose might result in data being overwritten by future functionality.
RV44	character varying(255)	Reserved Value 44 Reserved for DestinationThreatLevel. Use of this field for any other purpose might result in data being overwritten by future functionality.
RV45	character varying(255)	Reserved Value 45 Reserved for DestinationUserContext. Use of this field for any other purpose might result in data being overwritten by future functionality.
RV46	character varying(255)	Reserved Value 46 Reserved for VirusStatus. Use of this field for any other purpose might result in data being overwritten by future functionality.

Column Name	Datatype	Comment
RV47	character varying(255)	Reserved Value 47 Reserved for future use by Novell. Use of this field for any other purpose might result in data being overwritten by future functionality.
RV48	character varying(255)	Reserved Value 48 Reserved for DestinationOperationalContext. Use of this field for any other purpose might result in data being overwritten by future functionality.
RV49	character varying(255)	Reserved Value 49 Reserved for future use by Novell. Use of this field for any other purpose might result in data being overwritten by future functionality.
TAXONOMY_ID	bigint	Taxonomy identifier
REFERENCE_ID_01 - 20	bigint	Reserved for future use by Novell. Use of this field for any other purpose might result in data being overwritten by future functionality.
CV01 - 10	integer	Custom Value 1 - 10 Reserved for use by Customer, typically for association of Business relevant data.
CV11 - 20	timestamp with time zone	Custom Value 11 - 20 Reserved for use by Customer, typically for association of Business relevant data.
CV21 - 29	character varying(255)	Custom Value 21 – 29 Reserved for use by Customer, typically for association of Business relevant data.
CV30 - 34	character varying(4000)	Custom Value 30 – 34 Reserved for use by Customer, typically for association of Business relevant data.
CV35 – 100	character varying(255)	Custom Value 35 – 100 Reserved for use by Customer, typically for association of Business relevant data.

6.1.55 EVENTS_RPT_V3

This is the primary reporting view for SentinelRD. This view contains current event and historical events.

Column Name	Datatype	Comment
EVENT_ID	uuid	Event identifier
RESOURCE_NAME	character varying(255)	Resource name
SUB_RESOURCE	character varying(255)	Subresource name
SEVERITY	integer	Event severity
EVENT_PARSE_TIME	timestamp with time zone	Event time
EVENT_DATETIME	timestamp with time zone	Event date time
EVENT_DEVICE_TIME	timestamp with time zone	Event device time
SENTINEL_PROCESS_TIME	timestamp with time zone	SentinelRD process time
BEGIN_TIME	timestamp with time zone	Events begin time
END_TIME	timestamp with time zone	Events end time
REPEAT_COUNT	integer	Repeat count
TARGET_SERVICE_PORT	integer	Target service port
INIT_SERVICE_PORT	integer	Service port
BASE_MESSAGE	character varying(4000)	Base message
EVENT_NAME	character varying(255)	Event name
EVENT_TIME	character varying(255)	Event time
CUST_ID	bigint	Customer identifier
INIT_ASSET_ID	bigint	Initiator asset identifier
TARGET_ASSET_ID	bigint	Target asset identifier
AGENT_ID	bigint	Agent identifier
PROTOCOL_ID	bigint	Protocol identifier
ARCHIVE_ID	bigint	Archive id
INIT_IP	integer	IP
INIT_IP_DOTTED	character varying	IP dotted
INIT_HOST_NAME	character varying(255)	Host name
INIT_SERVICE_PORT_NAME	character varying(32)	Service port name
TARGET_IP	integer	Target IP
TARGET_IP_DOTTED	character varying	Dotted Target IP
TARGET_HOST_NAME	character varying(255)	Target host name

Column Name	**Datatype**	**Comment**
TARGET_SERVICE_PORT_NAME	character varying(32)	Target service port name
INIT_USER_NAME	character varying(255)	User name
TARGET_USER_NAME	character varying(255)	Target user name
FILE_NAME	character varying(1000)	File name
EXTENDED_INFO	character varying(1000)	Extended info
INIT_USER_ID	character varying(255)	Initiator user ID
INIT_USER_IDENTITY	uuid	Initiator user identity
TARGET_USER_ID	character varying(255)	Target user ID
TARGET_USER_IDENTITY	uuid	Target user identity
EFFECTIVE_USER_NAME	character varying(255)	Effective user name
EFFECTIVE_USER_ID	character varying(255)	Effective user ID
EFFECTIVE_USER_DOMAIN	character varying(255)	Effective user domain
TARGET_TRUST_NAME	character varying(255)	Target trust name
TARGET_TRUST_ID	character varying(255)	Target trust ID
TARGET_TRUST_DOMAIN	character varying(255)	Target trust domain
OBSERVER_IP	integer	Observer IP address in numeric format.
OBSERVER_IP_DOTTED	character varying	Observer IP
REPORTER_IP	integer	Reporter IP address in numeric format.
REPORTER_IP_DOTTED	character varying	Reporter ID
OBSERVER_HOST_DOMAIN	character varying(255)	Observer host domain
REPORTER_HOST_DOMAIN	character varying(255)	Reporter host domain
OBSERVER_ASSET_ID	bigint	Observer asset identifier
REPORTER_ASSET_ID	bigint	Reporter asset identifier
INIT_SERVICE_COMP	character varying(255)	Initiator service component
TARGET_SERVICE_COMP	character varying(255)	Target service component
EVENT_GROUP_ID	character varying(255)	Event group id
CUSTOM_TAG_1	character varying(255)	Customer Tag 1
CUSTOM_TAG_2	character varying(255)	Customer Tag 2
CUSTOM_TAG_3	integer	Customer Tag 3
RESERVED_TAG_1	character varying(255)	Reserved Tag 1
RESERVED_TAG_2	character varying(255)	Reserved Tag 2

Column Name	Datatype	Comment
RESERVED_TAG_3	integer	Reserved Tag 3
VULNERABILITY_RATING	integer	Vulnerability rating
CRITICALITY_RATING	integer	Criticality rating
DATE_CREATED	timestamp with time zone	Date the entry was created
DATE_MODIFIED	timestamp with time zone	Date the entry was modified
CREATED_BY	integer	User who created object
MODIFIED_BY	integer	User who last modified object
RV01	integer	Reserved Value 1 Reserved for future use by Novell. Use of this field for any other purpose might result in data being overwritten by future functionality.
EVENT_METRIC	integer	Event metric
DATA_TAG_ID	integer	Data tag ID
RV04-RV10	integer	Reserved Value 04 - 10 Reserved for future use by Novell. Use of this field for any other purpose might result in data being overwritten by future functionality.
RV11-RV20	timestamp with time zone	Reserved Value 11 - 20 Reserved for future use by Novell. Use of this field for any other purpose might result in data being overwritten by future functionality.
RV21- RV25	uuid	Reserved Value 21 - 25 Reserved for future use by Novell. Use of this field for any other purpose might result in data being overwritten by future functionality.
RV26- RV27	character varying(255)	Reserved Value 26 - 27 Reserved for future use by Novell. Use of this field for any other purpose might result in data being overwritten by future functionality.
EVENT_METRIC_CLASS	character varying(255)	Event metric class
INIT_IP_COUNTRY	character varying(255)	IP country
TARGET_IP_COUNTRY	character varying(255)	Target IP country
RV31	character varying(255)	Reserved Value 31
RV33	character varying(255)	Reserved Value 33

Column Name	Datatype	Comment
INIT_THREAT_LEVEL	character varying(255)	Initiator treat level
INIT_USER_DOMAIN	character varying(255)	Initiator user domain
RV36	character varying(255)	Reserved Value 36
INIT_FUNCTION	character varying(255)	Initiator function
INIT_OPERATIONAL_CONTEXT	character varying(255)	Initiator operational context
RV40	character varying(255)	Reserved Value 40
TARGET_HOST_DOMAIN	character varying(255)	Target host domain
INIT_HOST_DOMAIN	character varying(255)	Host domain
RV43	character varying(255)	Reserved Value 43
TARGET_THREAT_LEVEL	character varying(255)	Target threat level
TARGET_USER_DOMAIN	character varying(255)	Target user domain
RV46	character varying(255)	Reserved Value 46
TARGET_FUNCTION	character varying(255)	Target function
TARGET_OPERATIONAL_CONEXT	character varying(255)	Target operational context
RV49	character varying(255)	Reserved Value 49
TAXONOMY_ID	bigint	Taxonomy identifier
XDAS_TAXONOMY_ID	bigint	XDAS taxonomy identifier
REFERENCE_ID_01-REFERENCE_ID_20	bigint	Reference ID 01-20
CV01-CV10	integer	Custom Value 01 - 10 Reserved for use by Customer, typically for association of Business relevant data.
CV11-CV20	timestamp with time zone	Custom Value 11 - 20 Reserved for use by Customer, typically for association of Business relevant data.
CV21- CV29	character varying(255)	Custom Value 21 - 29 Reserved for use by Customer, typically for association of Business relevant data.
CV30- CV34	character varying(4000)	Custom Value 30 - 34 Reserved for use by Customer, typically for association of Business relevant data.

Column Name	Datatype	Comment
CV35- CV100	character varying(255)	Custom Value 35 - 100 Reserved for use by Customer, typically for association of Business relevant data.
CUSTOMER_VAR_101- CUSTOMER_VAR_110	integer	Customer variable 101 - 110
CUSTOMER_VAR_111- CUSTOMER_VAR_120	timestamp with time zone	Customer variable 111 - 120
CUSTOMER_VAR_121- CUSTOMER_VAR_130	uuid	Customer variable 121 - 130
CUSTOMER_VAR_131- CUSTOMER_VAR_140	integer	Customer variable 131 - 140
CUSTOMER_VAR_131_DOTTED- CUSTOMER_VAR_140_DOTTED	character varying	Customer variable 131 - 140 Dotted
CUSTOMER_VAR_141- CUSTOMER_VAR_150	character varying(255)	Customer variable 141 - 150

6.1.56 EVT_AGENT_RPT_V

View references EVT_AGENT table that stores information about Collectors.

Column Name	Datatype	Comment
AGENT_ID	bigint	Collector identifier
CUST_ID	bigint	Customer identifier
AGENT	character varying(64)	Collector name
PORT	character varying(64)	Collector port
REPORT_NAME	character varying(255)	Reporter name
PRODUCT_NAME	character varying(255)	Product name
SENSOR_NAME	character varying(255)	Sensor name
SENSOR_TYPE	character varying(5)	Sensor type: H - host-based N - network-based V - virus O – other
DEVICE_CATEGORY	character varying(255)	Device category
SOURCE_UUID	uuid	Source component Universal Unique Identifier (UUID)
DATE_CREATED	timestamp with time zone	Date the entry was created

Column Name	Datatype	Comment
DATE_MODIFIED	timestamp with time zone	Date the entry was modified
CREATED_BY	integer	User who created object
MODIFIED_BY	integer	User who last modified object

6.1.57 EVT_AGENT_RPT_V3

View references EVT_AGENT table that stores information about Collectors. The column names in this view reflects the name change of Sensor to Observer. This view is designed for use in SentinelRD.

Column Name	Datatype	Comment
AGENT_ID	bigint	Collector identifier
CUST_ID	bigint	Customer identifier
AGENT	character varying(64)	Collector
PORT	character varying(64)	Port
REPORTER_HOST_NAME	character varying(255)	Reporter host name
PRODUCT_NAME	character varying(255)	Product name
OBSERVER_HOST_NAME	character varying(255)	Observer host name
SENSOR_TYPE	character varying(5)	Sensor type: H - host-based N - network-based V - virus O - other
DEVICE_CATEGORY	character varying(255)	Device category
SOURCE_UUID	uuid	Source component Universal Unique Identifier (UUID)
DATE_CREATED	timestamp with time zone	Date the entry was created
DATE_MODIFIED	timestamp with time zone	Date the entry was modified
CREATED_BY	integer	User who created object
MODIFIED_BY	integer	User who last modified object

6.1.58 EVT_ASSET_RPT_V

View references EVT_ASSET table that stores asset information.

Column Name	Datatype	Comment
EVENT_ASSET_ID	bigint	Event asset identifier
CUST_ID	bigint	Customer identifier
ASSET_NAME	character varying(255)	Asset name
PHYSICAL_ASSET_NAME	character varying(255)	Physical asset name
REFERENCE_ASSET_ID	character varying(100)	Reference asset identifier, links to source asset management system.
MAC_ADDRESS	character varying(100)	MAC address
RACK_NUMBER	character varying(50)	Rack number
ROOM_NAME	character varying(100)	Room name
BUILDING_NAME	character varying(255)	Building name
CITY	character varying(100)	City
STATE	character varying(100)	State
COUNTRY	character varying(100)	Country
ZIP_CODE	character varying(50)	Zip code
ASSET_CATEGORY_NAME	character varying(100)	Asset category name
NETWORK_IDENTITY_NAME	character varying(255)	Asset network identity name
ENVIRONMENT_IDENTITY_NAME	character varying(255)	Environment name
ASSET_VALUE_NAME	character varying(50)	Asset value name
CRITICALITY_NAME	character varying(50)	Asset criticality name
SENSITIVITY_NAME	character varying(50)	Asset sensitivity name
CONTACT_NAME_1	character varying(255)	Name of contact person/ organization 1
CONTACT_NAME_2	character varying(255)	Name of contact person/ organization 2
ORGANIZATION_NAME_1	character varying(100)	Asset owner organization level 1
ORGANIZATION_NAME_2	character varying(100)	Asset owner organization level 2
ORGANIZATION_NAME_3	character varying(100)	Asset owner organization level 3
ORGANIZATION_NAME_4	character varying(100)	Asset owner organization level 4
DATE_CREATED	timestamp with time zone	Date the entry was created
DATE_MODIFIED	timestamp with time zone	Date the entry was modified
CREATED_BY	integer	User who created object
MODIFIED_BY	integer	User who last modified object

6.1.59 EVT_ASSET_RPT_V3

View references EVT_ASSET table that stores asset information. This view is designed for SentinelRD.

Column Name	Datatype	Comment
ASSET_CRITICALITY	character varying(50)	Asset criticality
ASSET_CLASS	character varying(100)	Asset class
ASSET_FUNCTION	character varying(255)	Asset function
ASSET_DEPARTMENT	character varying(100)	Asset department
DATE_CREATED	timestamp with time zone	Date the entry was created
DATE_MODIFIED	timestamp with time zone	Date the entry was modified
CREATED_BY	integer	User who created object
MODIFIED_BY	integer	User who last modified object
EVENT_ASSET_ID	bigint	Event asset identifier
CUST_ID	bigint	Customer identifier
ASSET_NAME	character varying(255)	Asset name
PHYSICAL_ASSET_NAME	character varying(255)	Physical asset name
REFERENCE_ASSET_ID	character varying(100)	Reference asset identifier, links to source asset management system.
MAC_ADDRESS	character varying(100)	MAC address
RACK_NUMBER	character varying(50)	Rack number
ROOM_NAME	character varying(100)	Room name
BUILDING_NAME	character varying(255)	Building name
CITY	character varying(100)	City
STATE	character varying(100)	State
COUNTRY	character varying(100)	Country
ZIP_CODE	character varying(50)	Zip code
NETWORK_IDENTITY_NAME	character varying(255)	Asset network identity name
ASSET_VALUE_NAME	character varying(50)	Asset value name
SENSITIVITY_NAME	character varying(50)	Asset sensitivity name
CONTACT_NAME_1	character varying(255)	Name of contact person/organization 1
CONTACT_NAME_2	character varying(255)	Name of contact person/organization 2
ORGANIZATION_NAME_1	character varying(100)	Asset owner organization level 1
ORGANIZATION_NAME_2	character varying(100)	Asset owner organization level 2
ORGANIZATION_NAME_3	character varying(100)	Asset owner organization level 3

6.1.60 EVT_DEST_EVT_NAME_SMRY_1_RPT_V

View summarizes event count by destination, taxonomy, event name, severity and event time.

Column Name	Datatype	Comment
DESTINATION_IP	integer	Destination IP address
DESTINATION_EVENT_ASSET_ID	bigint	Event asset identifier
TAXONOMY_ID	bigint	Taxonomy identifier
EVENT_NAME_ID	bigint	Event name identifier
SEVERITY	integer	Event severity
CUST_ID	bigint	Customer identifier
EVENT_TIME	timestamp with time zone	Event time
XDAS_TAXONOMY_ID	bigint	Taxonomy identifier
EVENT_COUNT	integer	Event count
DATE_CREATED	timestamp with time zone	Date the entry was created
DATE_MODIFIED	timestamp with time zone	Date the entry was modified
CREATED_BY	integer	User who created object
MODIFIED_BY	integer	User who last modified object
DESTINATION_HOST_NAME	character varying(255)	Destination host name.

6.1.61 EVT_DEST_SMRY_1_RPT_V

View contains event destination summary information.

Column Name	Datatype	Comment
DESTINATION_IP	integer	Destination IP address
DESTINATION_EVENT_ASSET_ID	bigint	Event asset identifier
DESTINATION_PORT	character varying(32)	Destination port
DESTINATION_USER_ID	bigint	Destination user identifier
TAXONOMY_ID	bigint	Taxonomy identifier
EVENT_NAME_ID	bigint	Event name identifier
RESOURCE_ID	bigint	Resource identifier
AGENT_ID	bigint	Collector identifier
PROTOCOL_ID	bigint	Protocol identifier
SEVERITY	integer	Event severity
CUST_ID	bigint	Customer identifier

Column Name	Datatype	Comment
EVENT_TIME	timestamp with time zone	Event time
XDAS_TAXONOMY_ID	bigint	XDAS Taxonomy identifier
TARGET_USER_IDENTITY	uuid	User ID
EVENT_COUNT	integer	Event count
DATE_CREATED	timestamp with time zone	Date the entry was created
DATE_MODIFIED	timestamp with time zone	Date the entry was modified
CREATED_BY	integer	User who created object
MODIFIED_BY	integer	User who last modified object
DESTINATION_HOST_NAME	character varying(255)	Destination host name

6.1.62 EVT_DEST_TXNMY_SMRY_1_RPT_V

View summarizes event count by destination, taxonomy, severity and event time.

Column Name	Datatype	Comment
DESTINATION_IP	integer	Destination IP address
DESTINATION_EVENT_ASSET_ID	bigint	Event asset identifier
TAXONOMY_ID	bigint	Taxonomy identifier
SEVERITY	integer	Event severity
CUST_ID	bigint	Customer identifier
EVENT_TIME	timestamp with time zone	Event time
XDAS_TAXONOMY_ID	bigint	XDAS taxonomy identifier
EVENT_COUNT	integer	Event count
DATE_CREATED	timestamp with time zone	Date the entry was created
DATE_MODIFIED	timestamp with time zone	Date the entry was modified
CREATED_BY	integer	User who created object
MODIFIED_BY	integer	User who last modified object
DESTINATION_HOST_NAME	character varying(255)	Destination host name

6.1.63 EVT_NAME_RPT_V

View references EVT_NAME table that stores event name information.

Column Name	Datatype	Comment
EVENT_NAME_ID	bigint	Event name identifier
EVENT_NAME	character varying(255)	Event name
DATE_CREATED	timestamp with time zone	Date the entry was created
DATE_MODIFIED	timestamp with time zone	Date the entry was modified
CREATED_BY	integer	User who created object
MODIFIED_BY	integer	User who last modified object

6.1.64 EVT_PORT_SMRY_1_RPT_V

View summarizes event count by destination port, severity and event time.

Column Name	Datatype	Comment
DESTINATION_PORT	character varying(32)	Destination port
SEVERITY	integer	Event severity
CUST_ID	bigint	Customer identifier
EVENT_TIME	timestamp with time zone	Event time
EVENT_COUNT	integer	Event count
DATE_CREATED	timestamp with time zone	Date the entry was created
DATE_MODIFIED	timestamp with time zone	Date the entry was modified
CREATED_BY	integer	User who created object
MODIFIED_BY	integer	User who last modified object

6.1.65 EVT_PRTCL_RPT_V

View references EVT_PRTCL table that stores event protocol information.

Column Name	Datatype	Comment
PROTOCOL_ID	bigint	Protocol identifier
PROTOCOL_NAME	character varying(255)	Protocol name
DATE_CREATED	timestamp with time zone	Date the entry was created
DATE_MODIFIED	timestamp with time zone	Date the entry was modified
CREATED_BY	integer	User who created object
MODIFIED_BY	integer	User who last modified object

6.1.66 EVT_PRTCL_RPT_V3

View references EVT_PRTCL table that stores event protocol information.

Column Name	Datatype	Comment
PROTOCOL_ID	bigint	Protocol identifier
PROTOCOL	character varying(255)	Protocol name
DATE_CREATED	timestamp with time zone	Date the entry was created
DATE_MODIFIED	timestamp with time zone	Date the entry was modified
CREATED_BY	integer	User who created object
MODIFIED_BY	integer	User who last modified object

6.1.67 EVT_RSRC_RPT_V

View references EVT_RSRC table that stores event resource information.

Column Name	Datatype	Comment
RESOURCE_ID	bigint	Resource identifier
CUST_ID	bigint	Customer Identifier
RESOURCE_NAME	character varying(255)	Resource name
SUB_RESOURCE_NAME	character varying(255)	Subresource name
DATE_CREATED	timestamp with time zone	Date the entry was created
DATE_MODIFIED	timestamp with time zone	Date the entry was modified
CREATED_BY	integer	User who created object
MODIFIED_BY	integer	User who last modified object

6.1.68 EVT_SEV_SMRY_1_RPT_V

View summarizes event count by severity and event time.

Column Name	Datatype	Comment
SEVERITY	integer	Event severity
CUST_ID	bigint	Customer identifier
EVENT_TIME	timestamp with time zone	Event time
EVENT_COUNT	integer	Event count
DATE_CREATED	timestamp with time zone	Date the entry was created
DATE_MODIFIED	timestamp with time zone	Date the entry was modified
CREATED_BY	integer	User who created object

Column Name	Datatype	Comment
MODIFIED_BY	integer	User who last modified object

6.1.69 EVT_SRC_COLLECTOR_RPT_V

View contains information about the Event Source Management configuration.

Column Name	Datatype	Comment
EVT_SRC_COLLECTOR_ID	uuid	Event source collector identifier
SENTINEL_PLUGIN_ID	uuid	SentinelRD plugin identifier
EVT_SRC_MGR_ID	uuid	Event source manager identifier
EVT_SRC_COLLECTOR_NAME	character varying(255)	Event source collector name
STATE_IND	boolean	State indicator
EVT_SRC_COLLECTOR_PROPS	text	Event source collector prop
MAP_FILTER	text	Map filter
CREATED_BY	integer	User who created object
MODIFIED_BY	integer	User who last modified object
DATE_CREATED	timestamp with time zone	Date the entry was created
DATE_MODIFIED	timestamp with time zone	Date the entry was modified

6.1.70 EVT_SRC_GRP_RPT_V

View contains information about the Event Source Management configuration.

Column Name	Datatype	Comment
EVT_SRC_GRP_ID	uuid	Event source group identifier
EVT_SRC_COLLECTOR_ID	uuid	Event source collector identifier
SENTINEL_PLUGIN_ID	uuid	SentinelRD plugin identifier
EVT_SRC_SRVR_ID	uuid	Event source server identifier
EVT_SRC_GRP_NAME	character varying(255)	Event source group name
STATE_IND	boolean	State indicator
MAP_FILTER	text	Map filter
EVT_SRC_DEFAULT_CONFIG	text	Event source default configuration
CREATED_BY	integer	User who created object
MODIFIED_BY	integer	User who last modified object
DATE_CREATED	timestamp with time zone	Date the entry was created

Column Name	Datatype	Comment
DATE_MODIFIED	timestamp with time zone	Date the entry was modified

6.1.71 EVT_SRC_MGR_RPT_V

View contains information about the Event Source Management configuration.

Column Name	Datatype	Comment
EVT_SRC_MGR_ID	uuid	Event source manager identifier
SENTINEL_ID	uuid	SentinelRD identifier
SENTINEL_HOST_ID	uuid	SentinelRD host identifier
EVT_SRC_MGR_NAME	character varying(255)	Event source manager name
STATE_IND	boolean	State indicator
EVT_SRC_MGR_CONFIG	text	Event source manager configu
CREATED_BY	integer	User who created object
MODIFIED_BY	integer	User who last modified object
DATE_CREATED	timestamp with time zone	Date the entry was created
DATE_MODIFIED	timestamp with time zone	Date the entry was modified

6.1.72 EVT_SRC_OFFSET_RPT_V

View contains information about the Event Source Management configuration.

Column Name	Datatype	Comment
EVT_SRC_ID	uuid	Event source identifier
OFFSET_VAL	text	Offset value
OFFSET_TIMESTAMP	timestamp with time zone	Offset timestamp
CREATED_BY	integer	User who created object
MODIFIED_BY	integer	User who last modified object
DATE_CREATED	timestamp with time zone	Date the entry was created
DATE_MODIFIED	timestamp with time zone	Date the entry was modified

6.1.73 EVT_SRC_RPT_V

View contains information about the Event Source Management configuration.

Column Name	Datatype	Comment
EVT_SRC_ID	uuid	Event source identifier

Column Name	Datatype	Comment
EVT_SRC_NAME	character varying(255)	Event source name
EVT_SRC_GRP_ID	uuid	Event source group identifier
STATE_IND	boolean	State indicator
MAP_FILTER	text	Map filter
EVT_SRC_CONFIG	text	Event source config
CREATED_BY	integer	User who created object
MODIFIED_BY	integer	User who last modified object
DATE_CREATED	timestamp with time zone	Date the entry was created
DATE_MODIFIED	timestamp with time zone	Date the entry was modified

6.1.74 EVT_SRC_SMRY_1_RPT_V

View contains event source and destination summary information.

Column Name	Datatype	Comment
SOURCE_IP	integer	Source IP address
SOURCE_EVENT_ASSET_ID	bigint	Source event asset identifier
SOURCE_PORT	character varying(32)	Source port
SOURCE_USER_ID	bigint	Source user identifier
TAXONOMY_ID	bigint	Taxonomy identifier
EVENT_NAME_ID	bigint	Event name identifier
RESOURCE_ID	bigint	Resource identifier
AGENT_ID	bigint	Collector identifier
PROTOCOL_ID	bigint	Protocol identifier
SEVERITY	integer	Event severity
CUST_ID	bigint	Customer identifier
EVENT_TIME	timestamp with time zone	Event time
XDAS_TAXONOMY_ID	bigint	XDAS taxonomy identifier
INIT_USER_IDENTITY	uuid	User identity
EVENT_COUNT	integer	Event count
DATE_CREATED	timestamp with time zone	Date the entry was created
DATE_MODIFIED	timestamp with time zone	Date the entry was modified
CREATED_BY	integer	User who created object
MODIFIED_BY	integer	User who last modified object

Column Name	Datatype	Comment
SOURCE_HOST_NAME	character varying(255)	Source host name

6.1.75 EVT_SRC_SRVR_RPT_V

View contains information about the Event Source Management configuration.

Column Name	Datatype	Comment
EVT_SRC_SRVR_ID	uuid	Event source server identifier
EVT_SRC_SRVR_NAME	character varying(255)	Event source server name
EVT_SRC_MGR_ID	uuid	Event source manager identifier
SENTINEL_PLUGIN_ID	uuid	SentinelRD plugin identifier
STATE_IND	boolean	State indicator
EVT_SRC_SRVR_CONFIG	text	Event source server configuration
CREATED_BY	integer	User who created object
MODIFIED_BY	integer	User who last modified object
DATE_CREATED	timestamp with time zone	Date the entry was created
DATE_MODIFIED	timestamp with time zone	Date the entry was modified

6.1.76 EVT_TXNMY_RPT_V

View references EVT_TXNMY table that stores event taxonomy information.

Column Name	Datatype	Comment
TAXONOMY_ID	bigint	Taxonomy identifier
TAXONOMY_LEVEL_1	character varying(100)	Taxonomy level 1
TAXONOMY_LEVEL_2	character varying(100)	Taxonomy level 2
TAXONOMY_LEVEL_3	character varying(100)	Taxonomy level 3
TAXONOMY_LEVEL_4	character varying(100)	Taxonomy level 4
DEVICE_CATEGORY	character varying(255)	Device category
DATE_CREATED	timestamp with time zone	Date the entry was created
DATE_MODIFIED	timestamp with time zone	Date the entry was modified
CREATED_BY	integer	User who created object
MODIFIED_BY	integer	User who last modified object

6.1.77 EVT_USR_RPT_V

View references EVT_USR table that stores event user information.

Column Name	Datatype	Comment
USER_ID	bigint	User identifier
USER_NAME	character varying(255)	User name
USER_DOMAIN	character varying(255)	User domain
CUST_ID	bigint	Customer identifier
DATE_CREATED	timestamp with time zone	Date the entry was created
DATE_MODIFIED	timestamp with time zone	Date the entry was modified
CREATED_BY	integer	User who created object
MODIFIED_BY	integer	User who last modified object

6.1.78 EVT_XDAS_TXNMY_RPT_V

Column Name	Datatype	Comment
XDAS_TAXONOMY_NAME	character varying(255)	XDAS taxonomy name
XDAS_OUTCOME_NAME	character varying(255)	XDAS outcome name
XDAS_REGISTRY	integer	XDAS registry
XDAS_PROVIDER	integer	XDAS provider
XDAS_CLASS	integer	XDAS class
XDAS_IDENTIFIER	integer	XDAS identifier
XDAS_OUTCOME	integer	XDAS outcome
XDAS_DETAIL	integer	XDAS detail
XDAS_TAXONOMY_ID	bigint	XDAS taxonomy identifier
DATE_CREATED	timestamp with time zone	Date the entry was created
DATE_MODIFIED	timestamp with time zone	Date the entry was modified
CREATED_BY	integer	User who created object
MODIFIED_BY	integer	User who last modified object

6.1.79 EXTERNAL_DATA_RPT_V

View references EXTERNAL_DATA table that stores external data.

Column Name	Datatype	Comment
EXTERNAL_DATA_ID	integer	External data identifier
SOURCE_NAME	character varying(50)	Source name
SOURCE_DATA_ID	character varying(255)	Source data identifier
EXTERNAL_DATA	text	External data
EXTERNAL_DATA_TYPE	character varying(10)	External data type
DATE_CREATED	timestamp with time zone	Date the entry was created
DATE_MODIFIED	timestamp with time zone	Date the entry was modified
CREATED_BY	integer	User who created object
MODIFIED_BY	integer	User who last modified object

6.1.80 HIST_CORRELATED_EVENTS_RPT_V (legacy view)

This view is provided for backward compatibility. New report should use CORRELATED_EVENTS_RPT_V1 instead.

6.1.81 HIST_EVENTS_RPT_V (legacy view)

This view is provided for backward compatibility. SentinelRD reports should use EVENTS_RPT_V2 instead. SentineRD reports should use EVENTS_RPT_V3 instead.

6.1.82 IMAGES_RPT_V

View references IMAGES table that stores system overview image information.

Column Name	Datatype	Comment
NAME	character varying(128)	Image name
TYPE	character varying(64)	Image type
DATA	text	Image data
DATE_CREATED	timestamp with time zone	Date the entry was created
DATE_MODIFIED	timestamp with time zone	Date the entry was modified
CREATED_BY	integer	User who created object
MODIFIED_BY	integer	User who last modified object

6.1.83 INCIDENTS_ASSETS_RPT_V

View references INCIDENTS_ASSETS table that stores information about the assets that makeup incidents created in the SentinelRD Console.

Column Name	Datatype	Comment
INC_ID	integer	Incident identifier – sequence number
ASSET_ID	uuid	Asset Universal Unique Identifier (UUID)
DATE_CREATED	timestamp with time zone	Date the entry was created
DATE_MODIFIED	timestamp with time zone	Date the entry was modified
CREATED_BY	integer	User who created object
MODIFIED_BY	integer	User who last modified object

6.1.84 INCIDENTS_EVENTS_RPT_V

View references INCIDENTS_EVENTS table that stores information about the events that makeup incidents created in the SentinelRD Console.

Column Name	Datatype	Comment
INC_ID	integer	Incident identifier – sequence number
EVT_ID	uuid	Event Universal Unique Identifier (UUID)
EVT_TIME	timestamp with time zone	Event time
DATE_CREATED	timestamp with time zone	Date the entry was created
DATE_MODIFIED	timestamp with time zone	Date the entry was modified
CREATED_BY	integer	User who created object
MODIFIED_BY	integer	User who last modified object

6.1.85 INCIDENTS_RPT_V

View references INCIDENTS table that stores information describing the details of incidents created in the SentinelRD Console.

Column Name	Datatype	Comment
INC_ID	integer	Incident identifier – sequence number
NAME	character varying(255)	Incident name
SEVERITY	integer	Incident severity
STT_ID	integer	Incident State ID
SEVERITY_RATING	character varying(32)	Average of all the event severities that comprise an incident.
VULNERABILITY_RATING	character varying(32)	Reserved for future use by Novell. Use of this field for any other purpose might result in data being overwritten by future functionality.

Column Name	Datatype	Comment
CRITICALITY_RATING	character varying(32)	Reserved for future use by Novell. Use of this field for any other purpose might result in data being overwritten by future functionality.
DATE_CREATED	timestamp with time zone	Date the entry was created
DATE_MODIFIED	timestamp with time zone	Date the entry was modified
CREATED_BY	integer	User who created object
MODIFIED_BY	integer	User who last modified object
INC_DESC	character varying(4000)	Incident description
INC_CAT	character varying(255)	Incident category
INC_PRIORITY	integer	Incident priority
INC_RES	character varying(4000)	Incident resolution

6.1.86 INCIDENTS_VULN_RPT_V

View references INCIDENTS_VULN table that stores information about the vulnerabilities that makeup incidents created in the SentinelRD Console.

Column Name	Datatype	Comment
INC_ID	integer	Incident identifier – sequence number
VULN_ID	uuid	Vulnerability Universal Unique Identifier (UUID)
DATE_CREATED	timestamp with time zone	Date the entry was created
DATE_MODIFIED	timestamp with time zone	Date the entry was modified
CREATED_BY	integer	User who created object
MODIFIED_BY	integer	User who last modified object

6.1.87 L_STAT_RPT_V

View references L_STAT table that stores statistical information.

Column Name	Datatype	Comment
RES_NAME	character varying(32)	Resource name
STATS_NAME	character varying(32)	Statistic name
STATS_VALUE	character varying(32)	Value of the statistic
OPEN_TOT_SECS	numeric	Number of seconds since 1970.

6.1.88 LOGS_RPT_V

View references LOGS_RPT table that stores logging information.

Column Name	Datatype	Comment
LOG_ID	integer	Sequence number
TIME	timestamp with time zone	Date of Log
MODULE	character varying(64)	Module log is for
TEXT	character varying(4000)	Log text

6.1.89 MSSP_ASSOCIATIONS_V

View references MSSP_ASSOCIATIONS table that associates an number key in one table to a UUID in another table.

Column Name	Datatype	Comment
TABLE1	character varying(64)	Table name 1
ID1	bigint	ID1
TABLE2	character varying(64)	Table name 2
ID2	uuid	ID2
DATE_CREATED	timestamp with time zone	Date the entry was created
DATE_MODIFIED	timestamp with time zone	Date the entry was modified
CREATED_BY	integer	User who created object
MODIFIED_BY	integer	User who last modified object

6.1.90 NETWORK_IDENTITY_RPT_V

View references NETWORK_IDENTITY_LKUP table that stores asset network identity information.

Column Name	Datatype	Comment
NETWORK_IDENTITY_ID	bigint	Network identity code
NETWORK_IDENTITY_NAME	character varying(255)	Network identify name
DATE_CREATED	timestamp with time zone	Date the entry was created
DATE_MODIFIED	timestamp with time zone	Date the entry was modified
CREATED_BY	integer	User who created object
MODIFIED_BY	integer	User who last modified object

6.1.91 ORGANIZATION_RPT_V

View references ORGANIZATION table that stores organization (asset) information.

Column Name	Datatype	Comment
ORGANIZATION_ID	uuid	Organization identifier
ORGANIZATION_NAME	character varying(100)	Organization name
CUST_ID	bigint	Customer identifier
DATE_CREATED	timestamp with time zone	Date the entry was created
DATE_MODIFIED	timestamp with time zone	Date the entry was modified
CREATED_BY	integer	User who created object
MODIFIED_BY	integer	User who last modified object

6.1.92 PERSON_RPT_V

View references PERSION table that stores personal (asset) information.

Column Name	Datatype	Comment
PERSON_ID	uuid	Person identifier
FIRST_NAME	character varying(255)	First name
LAST_NAME	character varying(255)	Last name
CUST_ID	bigint	Customer identifier
PHONE_NUMBER	character varying(50)	Phone number
EMAIL_ADDRESS	character varying(255)	Email address
DATE_CREATED	timestamp with time zone	Date the entry was created
DATE_MODIFIED	timestamp with time zone	Date the entry was modified
CREATED_BY	integer	User who created object
MODIFIED_BY	integer	User who last modified object

6.1.93 PHYSICAL_ASSET_RPT_V

View references PHYSICAL_ASSET table that stores physical asset information.

Column Name	Datatype	Comment
PHYSICAL_ASSET_ID	uuid	Physical asset identifier
CUST_ID	bigint	Customer identifier
HOST_NAME	character varying(255)	Host name
IP_ADDRESS	integer	IP address

Column Name	Datatype	Comment
LOCATION_ID	bigint	Location identifier
NETWORK_IDENTITY_ID	bigint	Network identity code
MAC_ADDRESS	character varying(100)	MAC address
RACK_NUMBER	character varying(50)	Rack number
ROOM_NAME	character varying(100)	Room name
DATE_CREATED	timestamp with time zone	Date the entry was created
DATE_MODIFIED	timestamp with time zone	Date the entry was modified
CREATED_BY	integer	User who created object
MODIFIED_BY	integer	User who last modified object

6.1.94 PRODUCT_RPT_V

View references PRDT table that stores asset product information.

Column Name	Datatype	Comment
PRODUCT_ID	bigint	Product identifier
PRODUCT_NAME	character varying(255)	Product name
PRODUCT_VERSION	character varying(100)	Product version
VENDOR_ID	bigint	Vendor identifier
DATE_CREATED	timestamp with time zone	Date the entry was created
DATE_MODIFIED	timestamp with time zone	Date the entry was modified
CREATED_BY	integer	User who created object
MODIFIED_BY	integer	User who last modified object

6.1.95 ROLE_RPT_V

View references ROLE_LKUP table that stores user role (asset) information.

Column Name	Datatype	Comment
ROLE_CODE	character varying(5)	Role code
ROLE_NAME	character varying(255)	Role name
DATE_CREATED	timestamp with time zone	Date the entry was created
DATE_MODIFIED	timestamp with time zone	Date the entry was modified
CREATED_BY	integer	User who created object
MODIFIED_BY	integer	User who last modified object

6.1.96 RPT_LABELS_RPT_V

View contains report label translations.

Column Name	Datatype	Comment
RPT_NAME	character varying(100)	Report name
LABEL_1 - 35	character varying(2000)	Translated report labels

6.1.97 SENSITIVITY_RPT_V

View references SENSITIVITY_LKUP table that stores asset sensitivity information.

Column Name	Datatype	Comment
SENSITIVITY_ID	bigint	Asset sensitivity code
SENSITIVITY_NAME	character varying(50)	Asset sensitivity name
DATE_CREATED	timestamp with time zone	Date the entry was created
DATE_MODIFIED	timestamp with time zone	Date the entry was modified
CREATED_BY	integer	User who created object
MODIFIED_BY	integer	User who last modified object

6.1.98 SENTINEL_HOST_RPT_V

View contains data used internally by SentinelRD.

Column Name	Datatype	Comment
SENTINEL_HOST_ID	uuid	SentinelRD host identifier
SENTINEL_ID	uuid	SentinelRD identifier
SENTINEL_HOST_NAME	character varying(255)	SentinelRD host name
HOST_NAME	character varying(255)	Host name
IP_ADDR	character varying(255)	Host IP address
HOST_OS	character varying(255)	Host operating system
HOST_OS_VERSION	character varying(255)	Host operating system version
MODIFIED_BY	integer	User who last modified object
CREATED_BY	integer	User who created object
DATE_CREATED	timestamp with time zone	Date the entry was created
DATE_MODIFIED	timestamp with time zone	Date the entry was modified

6.1.99 SENTINEL_PLUGIN_RPT_V

View contains data used internally by SentinelRD.

Column Name	Datatype	Comment
SENTINEL_PLUGIN_ID	uuid	SentinelRD plugin identifier
SENTINEL_PLUGIN_NAME	character varying(255)	SentinelRD plugin name
SENTINEL_PLUGIN_TYPE	character varying(255)	SentinelRD plugin type
FILE_NAME	character varying(512)	File name
CONTENT_PKG	text	Content package
FILE_HASH	character varying(255)	File hash
AUX_FILE_NAME	character varying(512)	Auxilary file name
CREATED_BY	integer	User who created object
MODIFIED_BY	integer	User who last modified object
DATE_CREATED	timestamp with time zone	Date the entry was created
DATE_MODIFIED	timestamp with time zone	Date the entry was modified

6.1.100 SENTINEL_RPT_V

View contains data used internally by SentinelRD.

Column Name	Datatype	Comment
SENTINEL_ID	uuid	SentinelRD identifier
SENTINEL_NAME	character varying(255)	SentinelRD name
ONLINE_IND	boolean	Online indicator
STATE_IND	boolean	State indicator
SENTINEL_CONFIG	text	SentinelRD configuration
CREATED_BY	integer	User who created object
MODIFIED_BY	integer	User who last modified object
DATE_CREATED	timestamp with time zone	Date the entry was created
DATE_MODIFIED	timestamp with time zone	Date the entry was modified

6.1.101 STATES_RPT_V

View references STATES table that stores definitions of states defined by applications or context.

Column Name	Datatype	Comment
STT_ID	integer	State ID – sequence number
CONTEXT	character varying(64)	Context of the state. That is case, incident, user.
NAME	character varying(64)	Name of the state.
TERMINAL_FLAG	character varying(1)	Indicates if state of incident is resolved.
DATE_CREATED	timestamp with time zone	Date the entry was created
DATE_MODIFIED	timestamp with time zone	Date the entry was modified
MODIFIED_BY	integer	User who last modified object
CREATED_BY	integer	User who created object

6.1.102 UNASSIGNED_INCIDENTS_RPT_V

View references CASES and INCIDENTS tables to report on unassigned cases.

Name	Datatype	Comment
INC_ID	integer	Incident identifier
NAME	character varying(255)	Name
SEVERITY	integer	Severity
STT_ID	integer	identifier
SEVERITY_RATING	character varying(32)	Severity rating
VULNERABILITY_RATING	character varying(32)	Vulnerability rating
CRITICALITY_RATING	character varying(32)	Criticality rating
DATE_CREATED	timestamp with time zone	Date the entry was created
DATE_MODIFIED	timestamp with time zone	Date the entry was modified
CREATED_BY	integer	User who created object
MODIFIED_BY	integer	User who last modified object
INC_DESC	character varying(4000)	Incident description
INC_CAT	character varying(255)	Incident category
INC_PRIORITY	integer	Incident priority
INC_RES	character varying(4000)	Incident registry

6.1.103 USERS_RPT_V

View references USERS table that lists all users of the application. The users will also be created as database users to accommotimestamp with time zone 3rd party reporting tools.

Column Name	Datatype	Comment
USR_ID	integer	User identifier – Sequence number
NAME	character varying(64)	Short, unique user name used as a login
CNT_ID	integer	Contact ID – Sequence number
STT_ID	integer	State ID. Status is either active or inactive.
DESCRIPTION	character varying(512)	Comments
DATE_CREATED	timestamp with time zone	Date the entry was created
DATE_MODIFIED	timestamp with time zone	Date the entry was modified
CREATED_BY	integer	User who created object
MODIFIED_BY	integer	User who last modified object
PERMISSIONS	character varying(4000)	Permissions currently assigned to the SentinelRD user
FILTER	character varying(128)	Current security filter assigned to the SentinelRD user
UPPER_NAME	character varying(64)	User name in upper case
DOMAIN_AUTH_IND	boolean	Domain authentication indication

6.1.104 USR_ACCOUNT_RPT_V

View contains user account information from an identity management system.

Column Name	Datatype	Comment
ACCOUNT_ID	bigint	Account identifier
USER_NAME	character varying(255)	User name
USER_DOMAIN	character varying(255)	User domain
CUST_ID	bigint	Customer identifier
BEGIN_EFFECTIVE_DATE	timestamp with time zone	Begin effective timestamp with time zone
END_EFFECTIVE_DATE	timestamp with time zone	End effective timestamp with time zone
CURRENT_F	boolean	Current flag
USER_STATUS	character varying(50)	User status
IDENTITY_GUID	uuid	Identity identifier
SOURCE_USER_ID	character varying(100)	User ID on source system
DATE_CREATED	timestamp with time zone	Date the entry was created
DATE_MODIFIED	timestamp with time zone	Date the entry was modified
CREATED_BY	integer	User who created object

Column Name	Datatype	Comment
MODIFIED_BY	integer	User who last modified object

6.1.105 USR_IDENTITY_EXT_ATTR_RPT_V

View contains extended attributes information from an identity management system, including name value pairs in the ATTRIBUTE_NAME and ATTRIBUTE_VALUE columns.

Column Name	Datatype	Comment
IDENTITY_GUID	uuid	Identity identifier
ATTRIBUTE_NAME	character varying(255)	Attribute name
ATTRIBUTE_VALUE	character varying(1024)	Attribute value

6.1.106 USR_IDENTITY_RPT_V

View contains user identity information from an identity management system.

Column Name	Datatype	Comment
IDENTITY_GUID	uuid	Identity identifier
DN	character varying(255)	Distinguished name
CUST_ID	bigint	Customer identifier
SRC_IDENTITY_ID	character varying(100)	Source identity identifier
WFID	character varying(100)	Workforce identifier
FIRST_NAME	character varying(255)	First name
LAST_NAME	character varying(255)	Last name
FULL_NAME	character varying(255)	Full name
JOB_TITLE	character varying(255)	Job title
DEPARTMENT_NAME	character varying(100)	Department name
OFFICE_LOC_CD	character varying(100)	Office location code
PRIMARY_EMAIL	character varying(255)	Primary email address
PRIMARY_PHONE	character varying(100)	Primary phone number
VAULT_NAME	character varying(100)	Identity vault name
MGR_GUID	uuid	Manager identity identifier
PHOTO	text	Photo
DATE_CREATED	timestamp with time zone	Date the entry was created
DATE_MODIFIED	timestamp with time zone	Date the entry was modified
CREATED_BY	integer	User who created object

Column Name	Datatype	Comment
MODIFIED_BY	integer	User who last modified object

6.1.107 VENDOR_RPT_V

View references VNDR table that stores information about asset product vendors.

Column Name	Datatype	Comment
VENDOR_ID	bigint	Vendor identifier
VENDOR_NAME	character varying(255)	Vendor name
DATE_CREATED	timestamp with time zone	Date the entry was created
DATE_MODIFIED	timestamp with time zone	Date the entry was modified
CREATED_BY	integer	User who created object
MODIFIED_BY	integer	User who last modified object

6.1.108 VULN_CALC_SEVERITY_RPT_V

View references VULN_RSRC and VULN to calculate eSecurity vulnerability severity rating base on current vulnerabilities.

Column Name	Datatype	Comment
RSRC_ID	uuid	Resource identifier
IP	text	IP
HOST_NAME	text	Host name
CRITICALITY	integer	Asset criticality code
ASSIGNED_VULN_SEVERITY	integer	Assigned vulnerability severity
VULN_COUNT	bigint	Vulnerability Count
CALC_SEVERITY	numeric	Calculated severity

6.1.109 VULN_CODE_RPT_V

View references VULN_CODE table that stores industry assigned vulnerability codes such as Mitre's CVEs and CANs.

Column Name	Datatype	Comment
VULN_CODE_ID	uuid	Vulnerability code identifier
VULN_ID	uuid	Vulnerability identifier
VULN_CODE_TYPE	character varying(64)	Vulnerability code type

Column Name	Datatype	Comment
VULN_CODE_VALUE	character varying(255)	Vulnerability code value
URL	character varying(512)	Web URL
DATE_CREATED	timestamp with time zone	Date the entry was created
DATE_MODIFIED	timestamp with time zone	Date the entry was modified
CREATED_BY	integer	User who created object
MODIFIED_BY	integer	User who last modified object

6.1.110 VULN_INFO_RPT_V

View references VULN_INFO table that stores additional information reported during a scan.

Column Name	Datatype	Comment
VULN_INFO_ID	uuid	Vulnerability info identifier
VULN_ID	uuid	Vulnerability identifier
VULN_INFO_TYPE	character varying(36)	Vulnerability info type
VULN_INFO_VALUE	character varying(2000)	Vulnerability info value
DATE_CREATED	timestamp with time zone	Date the entry was created
DATE_MODIFIED	timestamp with time zone	Date the entry was modified
CREATED_BY	integer	User who created object
MODIFIED_BY	integer	User who last modified object

6.1.111 VULN_RPT_V

View references VULN table that stores information of scanned system. Each scanner will have its own entry for each system.

Column Name	Datatype	Comment
VULN_ID	uuid	Vulnerability identifier
RSRC_ID	uuid	Resource identifier
PORT_NAME	character varying(64)	Port Name
PORT_NUMBER	integer	Port Number
NETWORK_PROTOCOL	integer	Network Protocol
APPLICATION_PROTOCOL	character varying(64)	Application Protocol
ASSIGNED_VULN_SEVERITY	integer	Assigned vulnerability severity
COMPUTED_VULN_SEVERITY	integer	Computed vulnerability severity
VULN_DESCRIPTION	text	Vulnerability description

Column Name	Datatype	Comment
VULN_SOLUTION	text	Vulnerability solution
VULN_SUMMARY	character varying(1000)	Vulnerability summary
BEGIN_EFFECTIVE_DATE	timestamp with time zone	Date from which the entry is valid
END_EFFECTIVE_DATE	timestamp with time zone	Date until which the entry is valid
DETECTED_OS	character varying(64)	Operating system of scanned machine
DETECTED_OS_VERSION	character varying(64)	Operating system version of scanned machine
SCANNED_APP	character varying(64)	Scanned application
SCANNED_APP_VERSION	character varying(64)	Scanned application version
VULN_USER_NAME	character varying(64)	Username used by scanner
VULN_USER_DOMAIN	character varying(64)	Domain of user used by scanned
VULN_TAXONOMY	character varying(1000)	Vulnerability taxonomy
SCANNER_CLASSIFICATION	character varying(255)	Scanner classification
VULN_NAME	character varying(300)	Vulnerability name
VULN_MODULE	character varying(64)	Vulnerability module
DATE_CREATED	timestamp with time zone	Date the entry was created
DATE_MODIFIED	timestamp with time zone	Date the entry was modified
CREATED_BY	integer	User who created object
MODIFIED_BY	integer	User who last modified object

6.1.112 VULN_RSRC_RPT_V

View references VULN_RSRC table that stores each resource scanned for a particular scan.

Column Name	Datatype	Comment
RSRC_ID	uuid	Resource identifier
SCANNER_ID	uuid	Scanner identifier
IP	character varying(32)	IP Address
HOST_NAME	character varying(255)	Host name
LOCATION	character varying(128)	Location
DEPARTMENT	character varying(128)	Department
BUSINESS_SYSTEM	character varying(128)	Business System
OPERATIONAL_ENVIRONMENT	character varying(64)	Operational environment
CRITICALITY	integer	Criticality

Column Name	Datatype	Comment
REGULATION	character varying(128)	Regulation
REGULATION_RATING	character varying(64)	Regulation rating
DATE_CREATED	timestamp with time zone	Date the entry was created
DATE_MODIFIED	timestamp with time zone	Date the entry was modified
CREATED_BY	integer	User who created object
MODIFIED_BY	integer	User who last modified object

6.1.113 VULN_RSRC_SCAN_RPT_V

View references VULN_RSRC_SCAN table that stores each resource scanned for a particular scan.

Column Name	Datatype	Comment
RSRC_ID	uuid	Resource identifier
SCAN_ID	uuid	Vulnerability scan identifier
DATE_CREATED	timestamp with time zone	Date the entry was created
DATE_MODIFIED	timestamp with time zone	Date the entry was modified
CREATED_BY	integer	User who created object
MODIFIED_BY	integer	User who last modified object

6.1.114 VULN_SCAN_RPT_V

View references table that stores information pertaining to scans.

Column Name	Datatype	Comment
SCAN_ID	uuid	Vulnerability scan identifier
SCANNER_ID	uuid	Vulnerability scanner identifier
SCAN_TYPE	character varying(10)	Vulnerability scan type
SCAN_START_DATE	timestamp with time zone	Scan start timestamp with time zone
SCAN_END_DATE	timestamp with time zone	Scan start timestamp with time zone
CONSOLIDATION_SERVER	character varying(64)	Consolidation server
LOAD_STATUS	character varying(64)	Load status
DATE_CREATED	timestamp with time zone	Date the entry was created
DATE_MODIFIED	timestamp with time zone	Date the entry was modified
CREATED_BY	integer	User who created object
MODIFIED_BY	integer	User who last modified object

6.1.115 VULN_SCAN_VULN_RPT_V

View references VULN_SCAN_VULN table that stores vulnerabilities detected during scans.

Column Name	Datatype	Comment
SCAN_ID	uuid	Vulnerability scan identifier
VULN_ID	uuid	Vulnerability identifier
DATE_CREATED	timestamp with time zone	Date the entry was created
DATE_MODIFIED	timestamp with time zone	Date the entry was modified
CREATED_BY	integer	User who created object
MODIFIED_BY	integer	User who last modified object

6.1.116 VULN_SCANNER_RPT_V

View references VULN_SCANNER table that stores information about vulnerability scanners.

Column Name	Datatype	Comment
SCANNER_ID	uuid	Vulnerability scanner identifier
PRODUCT_NAME	character varying(100)	Product Name
PRODUCT_VERSION	character varying(64)	Product Version
SCANNER_TYPE	character varying(64)	Vulnerability Scanner Type
VENDOR	character varying(100)	Vendor
SCANNER_INSTANCE	character varying(64)	Scanner Instance
DATE_CREATED	timestamp with time zone	Date the entry was created
DATE_MODIFIED	timestamp with time zone	Date the entry was modified
CREATED_BY	integer	User who created object
MODIFIED_BY	integer	User who last modified object

6.1.117 WORKFLOW_DEF_RPT_V

Column Name	Datatype	Comment
PKG_NAME	character varying(255)	Package name
PKG_DATA	text	Package data
DATE_CREATED	timestamp with time zone	Date the entry was created
DATE_MODIFIED	timestamp with time zone	Date the entry was modified
CREATED_BY	integer	User who created object

Column Name	Datatype	Comment
MODIFIED_BY	integer	User who last modified object

6.1.118 WORKFLOW_INFO_RPT_V

Column Name	Datatype	Comment
INFO_ID	bigint	Info identifier
PROCESS_DEF_ID	character varying(100)	Process definition identifier
PROCESS_INSTANCE_ID	character varying(150)	Process instance identifier
DATE_CREATED	timestamp with time zone	Date the entry was created
DATE_MODIFIED	timestamp with time zone	Date the entry was modified
CREATED_BY	integer	User who created object
MODIFIED_BY	integer	User who last modified object

6.2 Deprecated Views

The following legacy views are no longer created in the SentinelRD 6 database:

- ADV_ALERT_CVE_RPT_V
- ADV_ALERT_PRODUCT_RPT_V
- ADV_ALERT_RPT_V
- ADV_ATTACK_ALERT_RPT_V
- ADV_ATTACK_CVE_RPT_V
- ADV_CREDIBILITY_RPT_V
- ADV_SEVERITY_RPT_V
- ADV_SUBALERT_RPT_V
- ADV_URGENCY_RPT_V

A

Sentinel 6.1 Rapid Deployment Troubleshooting Checklist

This checklist is provided to aid in diagnosing a problem. By filling in this checklist, you can solve common issues or reduce the amount of time needed to solve more complex issues.

Table A-1 *Checklist*

Checklist Item	Example
Novell Version	V6.1 Rapid Deployment
Novell Platform and OS Version	SUSE Linux Enterprise Server 10 SP2 or later
Database Platform and OS Version	PostgreSQL 8.3
Sentinel Server Hardware Configuration	◆ **Processor:** 4 CPU @ 3 GHz ◆ **Memory:** 5 GB RAM ◆ Other
Database Storage Configuration (NAS, SAN, Local and so on.)	Local with offsite backup
Reporting Engine and Configuration	Jasper Report Engine

NOTE: Depending upon how your Sentinel system is configured, you might need to expand the above table. For instance additional information might be needed for Advisor, Sentinel Control Center, and Collector Manager.

1. Check the Novell Customer Center (http://support.novell.com/phone.html?sourceidint=suplnav4_phonesup) for your particular issue:
   - Is this a known issue with a work-around?
   - Is this issue fixed in the latest patch release or hot-fix?
   - Is this issue currently scheduled to be fixed in a future release?
2. Determine the nature of the problem.
   - Can it be reproduced? Can the steps to reproduce the problem be enumerated?
   - What user action, if any, will cause the problem?
   - Is the issue periodic in nature?
3. Determine the severity of this problem.
   - Is the system still useable?

4 Understand the environment and systems involved.
   - What platforms and product versions are involved?
   - Are there any non-standard or custom components involved?
   - Is it a high event rate environment?
   - What is the rate of events being collected?
   - What is the event rate of insertion into the database?
   - How many concurrent users are there?
   - Is correlation used? How many rules are deployed?

   Collect configuration files, log files and system information from appropriate subdirectories in `<Install_Directory>`. Assemble this information for possible future knowledge transfer.

5 Check the health of the system.
   - Can you log into the Sentinel Control Center?
   - Are events being generated and inserted into the database?
   - Can events be seen on the Sentinel Control Center?
   - Can events be retrieved from the database using quick query?
   - Check the RAM usage, disk space, process activity, CPU usage and network connectivity of the hosts involved.
   - Verify all expected Sentinel processes are running. Use the command `ps -ef|grep novell` can be used.
   - Check for any core dumps in any of the sub-directories of `<Install_Directory>`. Find out which process core dumped.

     ```
     cd <Install_Directory>
     find . -name core -print
     ```

   - Make sure the ActiveMQ broker is running. Connectivity can be verified using the ActiveMQ management console. Check that the various connections are active from Novell processes. Make sure that a lock file is not preventing ActiveMQ from starting. Optionally telnet to that server on the port, telnet sentinel.company.com 61616.
   - Check whether the wrapper service is running on the server. (`ps -ef | grep wrapper`)
   - Are any errors visible in the Servers View of the Sentinel Control Center? Are any errors visible in the Event Source Management Live View in the Sentinel Control Center? What is the OS resource consumption on the Collector Managers?

6 Is there a problem with the Database?
   - Using Pgadmin*, can you log into the database?
   - Does the database allow a Pgadmin login using the Novell dbauser account into the SIEM schema?
   - Does querying on one of the table succeed?
   - Does a select statement on a database table succeed?
   - Check the JDBC drivers, their locations and class path settings.
   - Is the database being maintained by an administrator? By anyone?
   - Has the database been modified by that administrator?

- Is SDM being used to maintain the partitions and archive/delete the partitions to make more room in the database?
- Using SDM what is the current partition? Is it P_MAX?

7. Inspect whether the product environment settings are correct.
   - Verify the sanity of User login shell scripts, environment variables, configurations, java home settings.
   - Are the environment variable set to run the correct jvm?
   - Verify the proper permissions on the folders for the installed product.
   - Check if any cron jobs are setup causing interference with our product's functionality.
   - If the product is installed on NFS mounts, check the sanity of NFS mounts & NFS/NIS services.
8. Is there a possible memory leak?
   - Obtain the statistics on how fast the memory is being consumed and by which process.
   - Gather the metrics of the events throughput per Collector.
   - Run the prstat command on Solaris. This will give the process runtime statistics.
   - In Windows you can check the process size and handle count in task manager.

This issue, if not resolved, is now ready for escalation. Possible results of escalation are:

- Configuration file changes
- Hot fixes or patches to your system
- Enhancement request
- Temporary workaround.

Sentinel 6.1 Rapid Deployment Service Permission Tables

B

The purpose of this document is to describe in detail various Sentinel™ Services and the Permissions they require for their functioning.

B.1 Advisor

Table B-1 *Table C-1: Advisor*

Sentinel Component	Sentinel Service	Sentinel Process	Function summary	Permission's required	Permission Explanation
Advisor	Sentinel	java	Download and processes Advisor attack data.	Network access Internet access over port 443 (optional) File read access to: ◆ `<Install_Directory>/config` ◆ `<Install_Directory>/lib` ◆ `<Install_Directory>/jre` File write access to: ◆ `<Install_Directory>/data` ◆ `<Install_Directory>/log`	It connects to the database to read and insert data. It communicates over the network with ActiveMQ to notify other processes it is down processing a feed. It reads local configuration files and uses the java executable. It writes log files as well as caches data in the local file system.

B.2 Collector Manager

Table B-2 *Collector Manager*

Sentinel Component	**Sentinel Service**	**Sentinel Process**	**Function summary**	**Permissions required**	**Permission Explanation**
Collector Manager	Sentinel	java agentengine (child process)	Manages Connectors and Collectors. It spawns off an agentengine process for each Collector it manages. Collector Manager also publishes system status messages, performs global filtering of events, and performs referential mappings. The agentengine process runs as an interpreter for Collector scripts, which normalize unprocessed (raw) events from security devices and systems producing event, vulnerability, and asset data that Sentinel can analyze and store in its database.	Network access (both outgoing access and local access to bind to ports greater than 1024) File read access to: ◆ `<Install_Directory>/config` ◆ `<Install_Directory>/lib` ◆ `<Install_Directory>/jre` File write access to: ◆ `<Install_Directory>/data` ◆ `<Install_Directory>/log` **NOTE:** Additionally, will need access to other resources depending which Connectors it is configured to run and which Event Sources it connecting to. Please refer to the individual Connector documentation for any additional permission requirements.	It communicates with ActiveMQ for configuration, event processing, and mapping data. It reads local configuration files and uses the java executable. It writes log files as well as caches data in the local file system.

B.3 Correlation Engine

Table B-3 *Correlation Engine*

Sentinel Component	Sentinel Service	Sentinel Process	Function summary	Permission's required	Permission Explanation
Correlation Engine	Sentinel	java	Receives events from the Collector Manager and publishes correlated events based on user-defined correlation rules.	Network access File read access to: ◆ `<Install_Directory>/config` ◆ `<Install_Directory>/lib` ◆ `<Install_Directory>/jre` File write access to: ◆ `<Install_Directory>/data` ◆ `<Install_Directory>/log`	It communicates over the network with ActiveMQ for configuration, event processing, and correlated event generation. It reads local configuration files and uses the java executable. It writes log files as well as caches data in the local file system.

B.4 Data Access Server (DAS)

Table B-4 *DATA Access Server (DAS)*

Sentinel Component	Sentinel Service	Sentinel Process	Function summary	Permission's required	Permission Explanation
DAS	Sentinel	java (das_binary) java (das_core)	Responsible for event insertion. Provides the following: ◆ General database access services, map data server, exploit detection data generation, Sentinel user login, and other general services. ◆ Data that drives the Active View charts. ◆ Services to use and manage iTRAC workflow processes ◆ Summaries event data into summary database tables, primarily for use by reports.	Network access Database Access File read access to: ◆ `<Install_Directory>/config` ◆ `<Install_Directory>/lib` ◆ `<Install_Directory>/jre` File write access to: ◆ `<Install_Directory>/data` ◆ `<Install_Directory>/log`	It connects to the database to read and insert data. It communicates over the network with ActiveMQ for configuration and event processing and other general data processing. It reads local configuration files and uses the java executable. It writes log files as well as caches data in the local file system.

B.5 Sentinel Communication Server

Table B-5 *Sentinel Communication Server*

Sentinel Component	**Sentinel Service**	**Sentinel Process**	**Function summary**	**Permission's required**	**Permission Explanation**
Communication Server (ActiveMQ / MOM)	Sentinel	java (ActiveMQ)	ActiveMQ: A Message Oriented Middleware (MOM). The ActiveMQ component provides a Java Message Service (JMS) framework for inter-process communication. Processes communicate through a broker, which is responsible for routing and buffering messages.	Network access (binds to port greater than 1024) File read access to: ◆ `<Install_Directory>/jre` File write access to: ◆ `<Install_Directory>/3rdparty/activemq`	It binds to local ports to accept TCP connections in order to perform its duties as a communication server. It reads local configuration files and uses the java executable.
		java (das_core)	ActiveMQ also has an SSL proxy that acts as an SSL bridge between the message bus and a client connecting through SSL.	Network access (binds to ports greater than 1024) File read access to: ◆ `<Install_Directory>/config` ◆ `<Install_Directory>/lib` ◆ `<Install_Directory>/jre` File write access to: ◆ `<Install_Directory>/3rdparty/activemq` ◆ `<Install_Directory>/data` ◆ `<Install_Directory>/log` ◆ `<Install_Directory>/config`	It binds to local ports to accept SSL connections in order to perform its duties as a communication server. It reads local configuration files and uses the java executable. It writes log files, caches data, and writes to ActiveMQ's internal database on the local file system. It also will write certificates to config directory when required.

B.6 Sentinel Service

Table B-6 *Sentinel Service*

Sentinel Component	**Sentinel Service**	**Sentinel Process**	**Function summary**	**Permission's required**	**Permission Explanation**
Sentinel Service	Sentinel	wrapper	Registers as a service with the operating system and, when executed, launches the java Sentinel Service.	Network access File read access to: ◆ `<Install_Directory>/config` ◆ `<Install_Directory>/lib` ◆ `<Install_Directory>/jre` File write access to: ◆ `<Install_Directory>/log`	It communicates over the network with ActiveMQ for configuration and status reporting. It reads local configuration files and uses the java executable. It writes log files to the local file system.
		java (sentinel)	The java Sentinel Service process that is responsible for launching, restarting, and reporting status on the other Sentinel Server processes.		

B.7 Reporting Engine

Table B-7 *Reporting Engine*

Sentinel Component	Sentinel Application	Sentinel Service	Sentinel Process	Function summary	Permission's required
Reporting Engine	Web Interface	-	-	Jasper Report engine is the reporting tool with Sentinel 6.1 Rapid Deployment. The Jasper Reporting Service executes within the das_core container. It handles all reporting requests and serves as the interface to the JasperReportEngine library methods. The Jasper Reporting Service uses the JasperReportEngine library methods to execute reports and format the report output and place the results in the report result plugins that are displayed as a results on the Reporting Page of the Web UI.	Admin rights The Jasper Reporting Service needs permissions to: ◆ Read jar files from the `<Install_Directory>/lib` directory (to dynamically load `jasperreport.jar` and `jfreecharts.jar` files) ◆ Read configuration files from the `<Install_Directory>/config` directory. ◆ Read/write plugins to the `<Install_Directory>/data/` pluginrepository (done via the plugin managerof Sentinel) ◆ Read/write temp files.

Sentinel 6.1 Rapid Deployment Log Locations

C

The purpose of this document is to provide information of the log file locations for the following components of Sentinel™.

The naming convention for the log files is that they include with the name of the process, the instance number (almost always 0 unless there are multiple instances of das_binary installed), and the log number in the log rotation sequence. For examples, see below.

C.1 Sentinel Data Manager

Logs activities executed using Sentinel Data Manager for the specific client running on that machine.

```
<Install_Directory>/log/db.*.log
```

C.2 iTRAC

Logs activities related to iTRAC.

```
<Install_Directory>/log/itrac_engine.log
```

C.3 Advisor

Logs activities related to Advisor data download and process.

```
<Install_Directory>/log/advisor_script.log
<Install_Directory>/log/advisor0.*.log
```

C.4 DAS Server

Logs activities related to DAS server process.

```
<Install_Directory>/log/das_core0.*.log
```

C.5 Event Insertion

Logs activities related to event insertion into the database.

```
<Install_Directory>/log/das_binary0.*.log
```

C.6 Messaging

Logs activities related to Messaging.

```
<Install_Directory>/log/activemq.*.log
```

C.7 Collector Manager

Logs activities related to Collector Manager.

For Windows:

```
<Install_Directory>\log\collector_mgr0.*.log
```

For UNIX:

```
<Install_Directory>/log/collector_mgr0.*.log
```

C.8 Correlation Engine

Logs activities related to Correlation Engine.

```
<Install_Directory>/log/correlation_engine0.*.log
```

C.9 Sentinel Control Center

Logs activities related to the Sentinel Control Center.

```
<Install_Directory>/log/control_center0.*.log
```

C.10 Solution Designer

Logs activities related to Solution Designer.

```
<Install_Directory>/log/solution_designer0.*.log
```

C.11 Multiple Instances

In some environments, there can be multiple instances of a process running, for example, the Sentinel Control Center or Sentinel Collector Manager. In this case, the first instance's log files are named as, for example, `collector_mgr0.0.log`. The second instance substitutes a `1` for the first `0` in the log file name, for example, `collector_mgr1.0.log`.

If other processes have log files for more than one instance running, that could indicate a system problem.