1) copy all apps from shcluster

cp -R SA-* DA-* SplunkEnterpriseSecuritySuite /opt/splunk/etc/apps

[splunk@ost-cla-dep-c01-mgmt apps_20Apr_pre_ES_upgrade]$ du -sh SA-* DA-* SplunkEnterpriseSecuritySuite

284K SA-AccessProtection

500K SA-AuditAndDataProtection

548K SA-EndpointProtection

556K SA-IdentityManagement

3.5M SA-ldapsearch

492K SA-NetworkProtection

44K SA-OST_ES_Notable_Whitelisting

11M SA-ThreatIntelligence

100K SA-UEBA

5.2M SA-Utils

216K DA-ESS-AccessProtection

280K DA-ESS-EndpointProtection

128K DA-ESS-IdentityManagement

716K DA-ESS-NetworkProtection

7.6M DA-ESS-ThreatIntelligence

97M SplunkEnterpriseSecuritySuite

[splunk@ost-cla-dep-c01-mgmt apps_20Apr_pre_ES_upgrade]$ cd -

/opt/splunk/etc/shcluster/apps

[splunk@ost-cla-dep-c01-mgmt apps]$ du -sh SA-* DA-* SplunkEnterpriseSecuritySuite

284K SA-AccessProtection

500K SA-AuditAndDataProtection

548K SA-EndpointProtection

556K SA-IdentityManagement

3.5M SA-ldapsearch

492K SA-NetworkProtection

44K SA-OST_ES_Notable_Whitelisting

11M SA-ThreatIntelligence

100K SA-UEBA

5.2M SA-Utils

216K DA-ESS-AccessProtection

280K DA-ESS-EndpointProtection

128K DA-ESS-IdentityManagement

716K DA-ESS-NetworkProtection

7.6M DA-ESS-ThreatIntelligence

97M SplunkEnterpriseSecuritySuite

[splunk@ost-cla-dep-c01-mgmt apps]$ pwd

/opt/splunk/etc/shcluster/apps

2) ######################## ES upgrade ################

[splunk@ost-cla-dep-c01-mgmt apps]$ /opt/splunk/bin/splunk install app ./splunk-enterprise-security_620.spl -update 1 -auth <admin credentials>

App '/opt/splunk/etc/apps/splunk-enterprise-security_620.spl' installed

[splunk@ost-cla-dep-c01-mgmt apps]$ pwd

/opt/splunk/etc/apps

3) ######################## essinstall output ################

[splunk@ost-cla-dep-c01-mgmt apps]$ /opt/splunk/bin/splunk search '| essinstall --deployment_type shc_deployer' -auth <admin credentials> action=upgrade

INFO: Initialization complete, please restart Splunk

{"stage": "refresh", "description": "Refreshing add-on information", "info": null, "begin": 1650504545.0126493, "completed": 1650504545.4728084}

{"stage": "deprecate_apps", "description": "Deprecating old add-ons", "info": [], "begin": 1650504545.556129, "completed": 1650504545.5571535}

{"stage": "install_apps", "description": "Installing new add-ons", "info": [{"app": "DA-ESS-AccessProtection", "filename": "DA-ESS-AccessProtection-6.2.0-11.spl", "upgrade": true, "status": true, "message": "installed"}, {"app": "DA-ESS-EndpointProtection", "filename": "DA-ESS-

EndpointProtection-6.2.0-11.spl", "upgrade": true, "status": true, "message": "installed"}, {"app": "DA-ESS-IdentityManagement", "filename": "DA-ESS-IdentityManagement-6.2.0-11.spl", "upgrade": true, "status": true, "message": "installed"}, {"app": "DA-ESS-NetworkProtection", "filename": "DA-ESS-NetworkProtection-6.2.0-11.spl", "upgrade": true, "status": true, "message": "installed"}, {"app": "DA-ESS-ThreatIntelligence", "filename": "DA-ESS-ThreatIntelligence-6.2.0-11.spl", "upgrade": true, "status": true, "message": "installed"}, {"app": "SA-AccessProtection", "filename": "SA-AccessProtection-6.2.0-11.spl", "upgrade": true, "status": true, "message": "installed"}, {"app": "SA-AuditAndDataProtection", "filename": "SA-AuditAndDataProtection-6.2.0-11.spl", "upgrade": true, "status": true, "message": "installed"}, {"app": "SA-EndpointProtection", "filename": "SA-EndpointProtection-6.2.0-11.spl", "upgrade": true, "status": true, "message": "installed"}, {"app": "SA-IdentityManagement", "filename": "SA-IdentityManagement-6.2.0-11.spl", "upgrade": true, "status": true, "message": "installed"}, {"app": "SA-NetworkProtection", "filename": "SA-NetworkProtection-6.2.0-11.spl", "upgrade": true, "status": true, "message": "installed"}, {"app": "SA-ThreatIntelligence", "filename": "SA-ThreatIntelligence-6.2.0-11.spl", "upgrade": true, "status": true, "message": "installed"}, {"app": "SA-UEBA", "filename": "SA-UEBA-6.2.0-11.spl", "upgrade": true, "status": true, "message": "installed"}, {"app": "SA-Utils", "filename": "SA-Utils-6.2.0-11.spl", "upgrade": true, "status": true, "message": "installed"}, {"app": "Splunk_ML_Toolkit", "filename": "Splunk_ML_Toolkit-5.1.0-1578006724560.tgz", "upgrade": false, "status": true, "message": "installed"}, {"app": "Splunk_SA_CIM", "filename": "Splunk_SA_CIM-4.16.0-1.tgz", "upgrade": true, "status": true, "message": "installed"}, {"app": "Splunk_SA_Scientific_Python_linux_x86_64", "filename": "Splunk_SA_Scientific_Python_linux_x86_64-2.0.1-0.tgz", "upgrade": false, "status": true, "message": "installed"}, {"app": "Splunk_TA_ueba", "filename": "Splunk_TA_ueba-3.0.0-1747.spl", "upgrade": false, "status": true, "message": "installed"}], "begin": 1650504545.6562624, "completed": 1650504611.4104753}

{"stage": "finalize", "description": "Finalizing installation", "info": null, "begin": 1650504611.4875073, "completed": 1650504673.3577805}

[splunk@ost-cla-dep-c01-mgmt apps]$

4) ########################## Deployer Splunk Restart output ###################

[splunk@ost-cla-dep-c01-mgmt apps]$ /opt/splunk/bin/splunk restart

Stopping splunkd...

Shutting down. Please wait, as this may take a few minutes.

..... [OK]

Stopping splunk helpers...

[OK]

Done.

Splunk> Map. Reduce. Recycle.

Checking prerequisites...

Checking http port [8000]: open

Checking mgmt port [8089]: open

Checking appserver port [127.0.0.1:8065]: open

Checking kvstore port [8191]: open

Checking configuration... Done.

Checking critical directories... Done

Checking indexes...

Validated: _audit _internal _introspection _metrics _metrics_rollup _telemetry _thefishbucket endpoint_summary history ioc main notable notable_summary risk sequenced_events summary threat_activity whois

Done

Bypassing local license checks since this instance is configured with a remote license master.

Checking filesystem compatibility... Done

Checking conf files for problems...

Invalid key in stanza [nbtstat] in /opt/splunk/etc/apps/SA-ThreatIntelligence/default/alert_actions.conf, line 26: param._cam (value: {

"category": ["Information Gathering"],

"task": ["scan"],

"subject": ["device"],

"technology": [{"vendor": "Operating System", "product": "Utility"}],

"supports_adhoc": true

}).

Invalid key in stanza [notable] in /opt/splunk/etc/apps/SA-ThreatIntelligence/default/alert_actions.conf, line 49: param._cam (value: {

"category": ["Information Conveyance"],

"task": ["create"],

"subject": ["splunk.event"],

"technology": [{"vendor": "Splunk", "product": "Enterprise"}],

"supports_adhoc": true

}).

Invalid key in stanza [nslookup] in /opt/splunk/etc/apps/SA-ThreatIntelligence/default/alert_actions.conf, line 72: param._cam (value: {

"category": ["Information Gathering"],

"task": ["scan"],

"subject": ["device"],

"technology": [{"vendor": "Operating System", "product": "Utility"}],

"supports_adhoc": true

}).

Invalid key in stanza [ping] in /opt/splunk/etc/apps/SA-ThreatIntelligence/default/alert_actions.conf, line 95: param._cam (value: {

"category": ["Information Gathering"],

"task": ["scan"],

"subject": ["device"],

"technology": [{"vendor": "Operating System", "product": "Utility"}],

"supports_adhoc": true

}).

Invalid key in stanza [risk] in /opt/splunk/etc/apps/SA-ThreatIntelligence/default/alert_actions.conf, line 125: param._cam (value: {

"category": ["Information Conveyance"],

"task": ["create"],

"subject": ["splunk.event"],

"technology": [{"vendor": "Splunk", "product": "Enterprise"}],

"supports_adhoc": true

}).

Invalid key in stanza [makestreams] in /opt/splunk/etc/apps/SA-Utils/default/alert_actions.conf, line 44: param._cam (value: {

"category": ["Information Gathering"],

"task": ["create"],

"subject": ["network.capture"],

"technology": [{"vendor": "Splunk", "product": "Splunk App for Stream"}],

"supports_adhoc": true

}).

Invalid key in stanza [dm_accel_settings] in /opt/splunk/etc/apps/SplunkEnterpriseSecuritySuite/default/inputs.conf, line 59: debug (value: false).

Invalid key in stanza [nav_collection:ess_security_intelligence] in /opt/splunk/etc/apps/SplunkEnterpriseSecuritySuite/default/managed_configurations.conf, line 136: nav_collection_status (value: old).

Invalid key in stanza [nav_collection:ess_security_intelligence] in /opt/splunk/etc/apps/SplunkEnterpriseSecuritySuite/default/managed_configurations.conf, line 175: nav_collection_data (value: <collection label="Security Intelligence">

<view name="risk_analysis" />

<divider />

<view name="ess_sequence_list" />

<divider />

<collection label="Protocol Intelligence">

<view name="generic_protocols" />

<view name="traffic_size_analysis" />

<divider />

<view name="dns_activity" />

<view name="dns_search" />

<divider />

<view name="ssl_activity" />

<view name="ssl_search" />

<divider />

<view name="email_activity" />

<view name="email_search" />

<divider />

</collection>

<collection label="Threat Intelligence">

<view name="threat_activity" />

<view name="threat_artifacts" />

</collection>

<collection label="User Intelligence">

<view name="asset_investigator" />

<view name="identity_investigator" />

<divider />

<view name="access_anomalies" />

<view name="uba_anomalies" />

<view name="user_activity" />

</collection>

<collection label="Web Intelligence">

<view name="http_category_analysis" />

<view name="http_user_agent_analysis" />

<view name="new_domain_analysis" />

<view name="url_length_analysis" />

</collection>

</collection>).

Invalid key in stanza [nav_collection:ess_security_domains] in /opt/splunk/etc/apps/SplunkEnterpriseSecuritySuite/default/managed_configurations.conf, line 181: nav_collection_status (value: old).

Invalid key in stanza [nav_collection:ess_security_domains] in /opt/splunk/etc/apps/SplunkEnterpriseSecuritySuite/default/managed_configurations.conf, line 228: nav_collection_data (value: <collection label="Security Domains">

<collection label="Access">

<view name="access_center" />

<view name="access_tracker" />

<view name="access_search" />

<divider />

<view name="account_management" />

<view name="default_accounts" />

</collection>

<collection label="Endpoint">

<view name="malware_center" />

```
  <view name="malware_search" />
  <view name="malware_operations" />
  <divider />
  <view name="system_center" />
  <view name="time_center" />
  <view name="endpoint_changes" />
  <divider />
  <view name="update_center" />
  <view name="update_search" />
 </collection>
 <collection label="Network">
  <view name="traffic_center" />
  <view name="traffic_search" />
  <divider />
  <view name="ids_center" />
  <view name="ids_search" />
  <divider />
  <view name="vuln_center" />
  <view name="vuln_operations" />
  <view name="vuln_search" />
  <divider />
  <view name="web_center" />
  <view name="web_search" />
  <divider />
  <view name="network_changes" />
  <view name="port_protocol_tracker" />
 </collection>
 <collection label="Identity">
  <view name="asset_center" />
  <divider />
  <view name="identity_center" />
```

<divider />

<view name="session_center" />

</collection>

</collection>).

Invalid key in stanza [nav_collection:ess_audit] in /opt/splunk/etc/apps/SplunkEnterpriseSecuritySuite/default/managed_configurations.conf, line 234: nav_collection_status (value: old).

Invalid key in stanza [nav_collection:ess_audit] in /opt/splunk/etc/apps/SplunkEnterpriseSecuritySuite/default/managed_configurations.conf, line 256: nav_collection_data (value: <collection label="Audit">

<view name="incident_review_audit" />

<view name="ess_investigation_overview" />

<view name="suppression_audit" />

<view name="ess_modular_action_center" />

<divider />

<view name="per_panel_filtering_audit" />

<view name="threat_intelligence_audit" />

<view name="mltk_usage_audit" />

<divider />

<view name="ess_confighealth" />

<view name="datamodel_audit" />

<divider />

<view name="forwarder_auditing" />

<view name="index_auditing" />

<view name="search_auditing" />

<view name="ess_view_auditing" />

<view name="managed_lookups_audit" />

<divider />

<view name="data_protection" />

</collection>).

Invalid key in stanza [nav_collection:ess_search] in /opt/splunk/etc/apps/SplunkEnterpriseSecuritySuite/default/managed_configurations.conf, line 262: nav_collection_status (value: old).

Invalid key in stanza [nav_collection:ess_search] in /opt/splunk/etc/apps/SplunkEnterpriseSecuritySuite/default/managed_configurations.conf, line 269: nav_collection_data (value: <collection label="Search">

<view name="dashboards" />

<view name="reports" />

<view name="data_models" />

<view name="search" />

</collection>).

Invalid key in stanza [nav_collection:ess_configure] in /opt/splunk/etc/apps/SplunkEnterpriseSecuritySuite/default/managed_configurations.conf, line 275: nav_collection_status (value: updated).

Invalid key in stanza [nav_collection:ess_configure] in /opt/splunk/etc/apps/SplunkEnterpriseSecuritySuite/default/managed_configurations.conf, line 309: nav_collection_data (value: <collection label="Configure">

All Configurations

<view name="cim_setup" />

<view name="ta_uba_setup" />

<divider />

<collection label="General">

General Settings

Credential Management

Permissions

Navigation

<divider />

Configuration Checker

</collection>

<collection label="Content">

Content Management

Use Case Library

</collection>

<collection label="Data Enrichment">

Asset and Identity Management

<divider />

Intelligence Downloads

Threat Intelligence Management

Threat Intelligence Uploads

<divider />

Whois Management

</collection>

<collection label="Incident Management">

New Notable Event

Status Configuration

Notable Event Suppressions

Incident Review Settings

</collection>

</collection>).

Invalid key in stanza [nav_collection:ess_user_intelligence] in /opt/splunk/etc/apps/SplunkEnterpriseSecuritySuite/default/managed_configurations.conf, line 316: nav_collection_status (value: old).

Invalid key in stanza [nav_collection:ess_user_intelligence] in /opt/splunk/etc/apps/SplunkEnterpriseSecuritySuite/default/managed_configurations.conf, line 325: nav_collection_data (value: <collection label="User Intelligence">

<view name="asset_investigator" />

<view name="identity_investigator" />

<divider />

<view name="access_anomalies" />

<view name="uba_anomalies" />

<view name="user_activity" />

</collection>).

Invalid key in stanza [nav_collection:ess_general_configuration] in /opt/splunk/etc/apps/SplunkEnterpriseSecuritySuite/default/managed_configurations.conf, line 331: nav_collection_status (value: updated).

Invalid key in stanza [nav_collection:ess_general_configuration] in /opt/splunk/etc/apps/SplunkEnterpriseSecuritySuite/default/managed_configurations.conf, line 340: nav_collection_data (value: <collection label="General">

General Settings

Credential Management

Permissions

Navigation

<divider />

Configuration Checker

</collection>).

Invalid key in stanza [nav_collection:ess_data_enrichment_configuration] in /opt/splunk/etc/apps/SplunkEnterpriseSecuritySuite/default/managed_configurations.conf, line 346: nav_collection_status (value: updated).

Invalid key in stanza [nav_collection:ess_data_enrichment_configuration] in /opt/splunk/etc/apps/SplunkEnterpriseSecuritySuite/default/managed_configurations.conf, line 356: nav_collection_data (value: <collection label="Data Enrichment">

Asset and Identity Management

<divider />

Threat Intelligence Management

Threat Intelligence Downloads

Threat Intelligence Uploads

<divider />

Whois Management

</collection>).

Invalid key in stanza [nav_collection:ess_incident_management_configuration] in /opt/splunk/etc/apps/SplunkEnterpriseSecuritySuite/default/managed_configurations.conf, line 362: nav_collection_status (value: old).

Invalid key in stanza [nav_collection:ess_incident_management_configuration] in /opt/splunk/etc/apps/SplunkEnterpriseSecuritySuite/default/managed_configurations.conf, line 369: nav_collection_data (value: <collection label="Incident Management">

New Notable Event

Status Configuration

Notable Event Suppressions

Incident Review Settings

</collection>).

Invalid key in stanza [nav_view:ess_investigation_list] in /opt/splunk/etc/apps/SplunkEnterpriseSecuritySuite/default/managed_configurations.conf, line 376: nav_view_status (value: old).

Invalid key in stanza [nav_view:ess_notable_status_list] in /opt/splunk/etc/apps/SplunkEnterpriseSecuritySuite/default/managed_configurations.conf, line 383: nav_view_status (value: old).

Invalid key in stanza [nav_view:ess_content_management] in /opt/splunk/etc/apps/SplunkEnterpriseSecuritySuite/default/managed_configurations.conf, line 390: nav_view_status (value: old).

Invalid key in stanza [nav_view:ess_credential_management_list] in /opt/splunk/etc/apps/SplunkEnterpriseSecuritySuite/default/managed_configurations.conf, line 397: nav_view_status (value: old).

Invalid key in stanza [nav_view:ess_sequence_list] in /opt/splunk/etc/apps/SplunkEnterpriseSecuritySuite/default/managed_configurations.conf, line 404: nav_view_status (value: old).

Invalid key in stanza [nav_view:ess_use_case_library] in /opt/splunk/etc/apps/SplunkEnterpriseSecuritySuite/default/managed_configurations.conf, line 411: nav_view_status (value: old).

Invalid key in stanza [nav_view:ess_investigation_overview] in /opt/splunk/etc/apps/SplunkEnterpriseSecuritySuite/default/managed_configurations.conf, line 418: nav_view_status (value: old).

Invalid key in stanza [transitioner:ess_admin] in /opt/splunk/etc/apps/SplunkEnterpriseSecuritySuite/default/reviewstatuses.conf, line 4: transition_reviewstatus-0_to_1 (value: enabled).

Invalid key in stanza [transitioner:ess_admin] in /opt/splunk/etc/apps/SplunkEnterpriseSecuritySuite/default/reviewstatuses.conf, line 5: transition_reviewstatus-0_to_2 (value: enabled).

Invalid key in stanza [transitioner:ess_admin] in /opt/splunk/etc/apps/SplunkEnterpriseSecuritySuite/default/reviewstatuses.conf, line 6: transition_reviewstatus-0_to_3 (value: enabled).

Invalid key in stanza [transitioner:ess_admin] in /opt/splunk/etc/apps/SplunkEnterpriseSecuritySuite/default/reviewstatuses.conf, line 7: transition_reviewstatus-0_to_4 (value: enabled).

Invalid key in stanza [transitioner:ess_admin] in /opt/splunk/etc/apps/SplunkEnterpriseSecuritySuite/default/reviewstatuses.conf, line 8: transition_reviewstatus-0_to_5 (value: enabled).

Invalid key in stanza [transitioner:ess_admin] in /opt/splunk/etc/apps/SplunkEnterpriseSecuritySuite/default/reviewstatuses.conf, line 9: transition_reviewstatus-1_to_2 (value: enabled).

Invalid key in stanza [transitioner:ess_admin] in /opt/splunk/etc/apps/SplunkEnterpriseSecuritySuite/default/reviewstatuses.conf, line 10: transition_reviewstatus-1_to_3 (value: enabled).

Invalid key in stanza [transitioner:ess_admin] in /opt/splunk/etc/apps/SplunkEnterpriseSecuritySuite/default/reviewstatuses.conf, line 11: transition_reviewstatus-1_to_4 (value: enabled).

Invalid key in stanza [transitioner:ess_admin] in /opt/splunk/etc/apps/SplunkEnterpriseSecuritySuite/default/reviewstatuses.conf, line 12: transition_reviewstatus-1_to_5 (value: enabled).

Invalid key in stanza [transitioner:ess_admin] in /opt/splunk/etc/apps/SplunkEnterpriseSecuritySuite/default/reviewstatuses.conf, line 13: transition_reviewstatus-2_to_1 (value: enabled).

Invalid key in stanza [transitioner:ess_admin] in /opt/splunk/etc/apps/SplunkEnterpriseSecuritySuite/default/reviewstatuses.conf, line 14: transition_reviewstatus-2_to_3 (value: enabled).

Invalid key in stanza [transitioner:ess_admin] in /opt/splunk/etc/apps/SplunkEnterpriseSecuritySuite/default/reviewstatuses.conf, line 15: transition_reviewstatus-2_to_4 (value: enabled).

Invalid key in stanza [transitioner:ess_admin] in /opt/splunk/etc/apps/SplunkEnterpriseSecuritySuite/default/reviewstatuses.conf, line 16: transition_reviewstatus-2_to_5 (value: enabled).

Invalid key in stanza [transitioner:ess_admin] in /opt/splunk/etc/apps/SplunkEnterpriseSecuritySuite/default/reviewstatuses.conf, line 17: transition_reviewstatus-3_to_1 (value: enabled).

Invalid key in stanza [transitioner:ess_admin] in /opt/splunk/etc/apps/SplunkEnterpriseSecuritySuite/default/reviewstatuses.conf, line 18: transition_reviewstatus-3_to_2 (value: enabled).

Invalid key in stanza [transitioner:ess_admin] in /opt/splunk/etc/apps/SplunkEnterpriseSecuritySuite/default/reviewstatuses.conf, line 19: transition_reviewstatus-3_to_4 (value: enabled).

Invalid key in stanza [transitioner:ess_admin] in /opt/splunk/etc/apps/SplunkEnterpriseSecuritySuite/default/reviewstatuses.conf, line 20: transition_reviewstatus-3_to_5 (value: enabled).

Invalid key in stanza [transitioner:ess_admin] in /opt/splunk/etc/apps/SplunkEnterpriseSecuritySuite/default/reviewstatuses.conf, line 21: transition_reviewstatus-4_to_1 (value: enabled).

Invalid key in stanza [transitioner:ess_admin] in /opt/splunk/etc/apps/SplunkEnterpriseSecuritySuite/default/reviewstatuses.conf, line 22: transition_reviewstatus-4_to_2 (value: enabled).

Invalid key in stanza [transitioner:ess_admin] in /opt/splunk/etc/apps/SplunkEnterpriseSecuritySuite/default/reviewstatuses.conf, line 23: transition_reviewstatus-4_to_3 (value: enabled).

Invalid key in stanza [transitioner:ess_admin] in /opt/splunk/etc/apps/SplunkEnterpriseSecuritySuite/default/reviewstatuses.conf, line 24: transition_reviewstatus-4_to_5 (value: enabled).

Invalid key in stanza [transitioner:ess_admin] in /opt/splunk/etc/apps/SplunkEnterpriseSecuritySuite/default/reviewstatuses.conf, line 25: transition_reviewstatus-5_to_1 (value: enabled).

Invalid key in stanza [transitioner:ess_admin] in /opt/splunk/etc/apps/SplunkEnterpriseSecuritySuite/default/reviewstatuses.conf, line 26: transition_reviewstatus-5_to_2 (value: enabled).

Invalid key in stanza [transitioner:ess_admin] in /opt/splunk/etc/apps/SplunkEnterpriseSecuritySuite/default/reviewstatuses.conf, line 27: transition_reviewstatus-5_to_3 (value: enabled).

Invalid key in stanza [transitioner:ess_admin] in /opt/splunk/etc/apps/SplunkEnterpriseSecuritySuite/default/reviewstatuses.conf, line 28: transition_reviewstatus-5_to_4 (value: enabled).

Invalid key in stanza [transitioner:ess_admin] in /opt/splunk/etc/apps/SplunkEnterpriseSecuritySuite/default/reviewstatuses.conf, line 30: transition_reviewstatus-investigation:0_to_investigation:1 (value: enabled).

Invalid key in stanza [transitioner:ess_admin] in /opt/splunk/etc/apps/SplunkEnterpriseSecuritySuite/default/reviewstatuses.conf, line 31: transition_reviewstatus-investigation:0_to_investigation:2 (value: enabled).

Invalid key in stanza [transitioner:ess_admin] in /opt/splunk/etc/apps/SplunkEnterpriseSecuritySuite/default/reviewstatuses.conf, line 32: transition_reviewstatus-investigation:0_to_investigation:3 (value: enabled).

Invalid key in stanza [transitioner:ess_admin] in /opt/splunk/etc/apps/SplunkEnterpriseSecuritySuite/default/reviewstatuses.conf, line 33: transition_reviewstatus-investigation:0_to_investigation:4 (value: enabled).

Invalid key in stanza [transitioner:ess_admin] in /opt/splunk/etc/apps/SplunkEnterpriseSecuritySuite/default/reviewstatuses.conf, line 34: transition_reviewstatus-investigation:0_to_investigation:5 (value: enabled).

Invalid key in stanza [transitioner:ess_admin] in /opt/splunk/etc/apps/SplunkEnterpriseSecuritySuite/default/reviewstatuses.conf, line 35: transition_reviewstatus-investigation:1_to_investigation:2 (value: enabled).

Invalid key in stanza [transitioner:ess_admin] in /opt/splunk/etc/apps/SplunkEnterpriseSecuritySuite/default/reviewstatuses.conf, line 36: transition_reviewstatus-investigation:1_to_investigation:3 (value: enabled).

Invalid key in stanza [transitioner:ess_admin] in /opt/splunk/etc/apps/SplunkEnterpriseSecuritySuite/default/reviewstatuses.conf, line 37: transition_reviewstatus-investigation:1_to_investigation:4 (value: enabled).

Invalid key in stanza [transitioner:ess_admin] in /opt/splunk/etc/apps/SplunkEnterpriseSecuritySuite/default/reviewstatuses.conf, line 38: transition_reviewstatus-investigation:1_to_investigation:5 (value: enabled).

Invalid key in stanza [transitioner:ess_admin] in /opt/splunk/etc/apps/SplunkEnterpriseSecuritySuite/default/reviewstatuses.conf, line 39: transition_reviewstatus-investigation:2_to_investigation:1 (value: enabled).

Invalid key in stanza [transitioner:ess_admin] in /opt/splunk/etc/apps/SplunkEnterpriseSecuritySuite/default/reviewstatuses.conf, line 40: transition_reviewstatus-investigation:2_to_investigation:3 (value: enabled).

Invalid key in stanza [transitioner:ess_admin] in /opt/splunk/etc/apps/SplunkEnterpriseSecuritySuite/default/reviewstatuses.conf, line 41: transition_reviewstatus-investigation:2_to_investigation:4 (value: enabled).

Invalid key in stanza [transitioner:ess_admin] in /opt/splunk/etc/apps/SplunkEnterpriseSecuritySuite/default/reviewstatuses.conf, line 42: transition_reviewstatus-investigation:2_to_investigation:5 (value: enabled).

Invalid key in stanza [transitioner:ess_admin] in /opt/splunk/etc/apps/SplunkEnterpriseSecuritySuite/default/reviewstatuses.conf, line 43: transition_reviewstatus-investigation:3_to_investigation:1 (value: enabled).

Invalid key in stanza [transitioner:ess_admin] in /opt/splunk/etc/apps/SplunkEnterpriseSecuritySuite/default/reviewstatuses.conf, line 44: transition_reviewstatus-investigation:3_to_investigation:2 (value: enabled).

Invalid key in stanza [transitioner:ess_admin] in /opt/splunk/etc/apps/SplunkEnterpriseSecuritySuite/default/reviewstatuses.conf, line 45: transition_reviewstatus-investigation:3_to_investigation:4 (value: enabled).

Invalid key in stanza [transitioner:ess_admin] in /opt/splunk/etc/apps/SplunkEnterpriseSecuritySuite/default/reviewstatuses.conf, line 46: transition_reviewstatus-investigation:3_to_investigation:5 (value: enabled).

Invalid key in stanza [transitioner:ess_admin] in /opt/splunk/etc/apps/SplunkEnterpriseSecuritySuite/default/reviewstatuses.conf, line 47: transition_reviewstatus-investigation:4_to_investigation:1 (value: enabled).

Invalid key in stanza [transitioner:ess_admin] in /opt/splunk/etc/apps/SplunkEnterpriseSecuritySuite/default/reviewstatuses.conf, line 48: transition_reviewstatus-investigation:4_to_investigation:2 (value: enabled).

Invalid key in stanza [transitioner:ess_admin] in /opt/splunk/etc/apps/SplunkEnterpriseSecuritySuite/default/reviewstatuses.conf, line 49: transition_reviewstatus-investigation:4_to_investigation:3 (value: enabled).

Invalid key in stanza [transitioner:ess_admin] in /opt/splunk/etc/apps/SplunkEnterpriseSecuritySuite/default/reviewstatuses.conf, line 50: transition_reviewstatus-investigation:4_to_investigation:5 (value: enabled).

Invalid key in stanza [transitioner:ess_admin] in /opt/splunk/etc/apps/SplunkEnterpriseSecuritySuite/default/reviewstatuses.conf, line 51: transition_reviewstatus-investigation:5_to_investigation:1 (value: enabled).

Invalid key in stanza [transitioner:ess_admin] in /opt/splunk/etc/apps/SplunkEnterpriseSecuritySuite/default/reviewstatuses.conf, line 52: transition_reviewstatus-investigation:5_to_investigation:2 (value: enabled).

Invalid key in stanza [transitioner:ess_admin] in /opt/splunk/etc/apps/SplunkEnterpriseSecuritySuite/default/reviewstatuses.conf, line 53: transition_reviewstatus-investigation:5_to_investigation:3 (value: enabled).

Invalid key in stanza [transitioner:ess_admin] in /opt/splunk/etc/apps/SplunkEnterpriseSecuritySuite/default/reviewstatuses.conf, line 54: transition_reviewstatus-investigation:5_to_investigation:4 (value: enabled).

Invalid key in stanza [transitioner:ess_analyst] in /opt/splunk/etc/apps/SplunkEnterpriseSecuritySuite/default/reviewstatuses.conf, line 59: transition_reviewstatus-0_to_1 (value: enabled).

Invalid key in stanza [transitioner:ess_analyst] in /opt/splunk/etc/apps/SplunkEnterpriseSecuritySuite/default/reviewstatuses.conf, line 60: transition_reviewstatus-0_to_2 (value: enabled).

Invalid key in stanza [transitioner:ess_analyst] in /opt/splunk/etc/apps/SplunkEnterpriseSecuritySuite/default/reviewstatuses.conf, line 61: transition_reviewstatus-0_to_3 (value: enabled).

Invalid key in stanza [transitioner:ess_analyst] in /opt/splunk/etc/apps/SplunkEnterpriseSecuritySuite/default/reviewstatuses.conf, line 62: transition_reviewstatus-0_to_4 (value: enabled).

Invalid key in stanza [transitioner:ess_analyst] in /opt/splunk/etc/apps/SplunkEnterpriseSecuritySuite/default/reviewstatuses.conf, line 63: transition_reviewstatus-0_to_5 (value: enabled).

Invalid key in stanza [transitioner:ess_analyst] in /opt/splunk/etc/apps/SplunkEnterpriseSecuritySuite/default/reviewstatuses.conf, line 64: transition_reviewstatus-1_to_2 (value: enabled).

Invalid key in stanza [transitioner:ess_analyst] in /opt/splunk/etc/apps/SplunkEnterpriseSecuritySuite/default/reviewstatuses.conf, line 65: transition_reviewstatus-1_to_3 (value: enabled).

Invalid key in stanza [transitioner:ess_analyst] in /opt/splunk/etc/apps/SplunkEnterpriseSecuritySuite/default/reviewstatuses.conf, line 66: transition_reviewstatus-1_to_4 (value: enabled).

Invalid key in stanza [transitioner:ess_analyst] in /opt/splunk/etc/apps/SplunkEnterpriseSecuritySuite/default/reviewstatuses.conf, line 67: transition_reviewstatus-1_to_5 (value: enabled).

Invalid key in stanza [transitioner:ess_analyst] in /opt/splunk/etc/apps/SplunkEnterpriseSecuritySuite/default/reviewstatuses.conf, line 68: transition_reviewstatus-2_to_1 (value: enabled).

Invalid key in stanza [transitioner:ess_analyst] in /opt/splunk/etc/apps/SplunkEnterpriseSecuritySuite/default/reviewstatuses.conf, line 69: transition_reviewstatus-2_to_3 (value: enabled).

Invalid key in stanza [transitioner:ess_analyst] in /opt/splunk/etc/apps/SplunkEnterpriseSecuritySuite/default/reviewstatuses.conf, line 70: transition_reviewstatus-2_to_4 (value: enabled).

Invalid key in stanza [transitioner:ess_analyst] in /opt/splunk/etc/apps/SplunkEnterpriseSecuritySuite/default/reviewstatuses.conf, line 71: transition_reviewstatus-2_to_5 (value: enabled).

Invalid key in stanza [transitioner:ess_analyst] in /opt/splunk/etc/apps/SplunkEnterpriseSecuritySuite/default/reviewstatuses.conf, line 72: transition_reviewstatus-3_to_1 (value: enabled).

Invalid key in stanza [transitioner:ess_analyst] in /opt/splunk/etc/apps/SplunkEnterpriseSecuritySuite/default/reviewstatuses.conf, line 73: transition_reviewstatus-3_to_2 (value: enabled).

Invalid key in stanza [transitioner:ess_analyst] in /opt/splunk/etc/apps/SplunkEnterpriseSecuritySuite/default/reviewstatuses.conf, line 74: transition_reviewstatus-3_to_4 (value: enabled).

Invalid key in stanza [transitioner:ess_analyst] in /opt/splunk/etc/apps/SplunkEnterpriseSecuritySuite/default/reviewstatuses.conf, line 75: transition_reviewstatus-3_to_5 (value: enabled).

Invalid key in stanza [transitioner:ess_analyst] in /opt/splunk/etc/apps/SplunkEnterpriseSecuritySuite/default/reviewstatuses.conf, line 76: transition_reviewstatus-4_to_1 (value: enabled).

Invalid key in stanza [transitioner:ess_analyst] in /opt/splunk/etc/apps/SplunkEnterpriseSecuritySuite/default/reviewstatuses.conf, line 77: transition_reviewstatus-4_to_2 (value: enabled).

Invalid key in stanza [transitioner:ess_analyst] in /opt/splunk/etc/apps/SplunkEnterpriseSecuritySuite/default/reviewstatuses.conf, line 78: transition_reviewstatus-4_to_3 (value: enabled).

Invalid key in stanza [transitioner:ess_analyst] in /opt/splunk/etc/apps/SplunkEnterpriseSecuritySuite/default/reviewstatuses.conf, line 79: transition_reviewstatus-4_to_5 (value: enabled).

Invalid key in stanza [transitioner:ess_analyst] in /opt/splunk/etc/apps/SplunkEnterpriseSecuritySuite/default/reviewstatuses.conf, line 80: transition_reviewstatus-5_to_1 (value: enabled).

Invalid key in stanza [transitioner:ess_analyst] in /opt/splunk/etc/apps/SplunkEnterpriseSecuritySuite/default/reviewstatuses.conf, line 81: transition_reviewstatus-5_to_2 (value: enabled).

Invalid key in stanza [transitioner:ess_analyst] in /opt/splunk/etc/apps/SplunkEnterpriseSecuritySuite/default/reviewstatuses.conf, line 82: transition_reviewstatus-5_to_3 (value: enabled).

Invalid key in stanza [transitioner:ess_analyst] in /opt/splunk/etc/apps/SplunkEnterpriseSecuritySuite/default/reviewstatuses.conf, line 83: transition_reviewstatus-5_to_4 (value: enabled).

Invalid key in stanza [transitioner:ess_analyst] in /opt/splunk/etc/apps/SplunkEnterpriseSecuritySuite/default/reviewstatuses.conf, line 85: transition_reviewstatus-investigation:0_to_investigation:1 (value: enabled).

Invalid key in stanza [transitioner:ess_analyst] in /opt/splunk/etc/apps/SplunkEnterpriseSecuritySuite/default/reviewstatuses.conf, line 86: transition_reviewstatus-investigation:0_to_investigation:2 (value: enabled).

Invalid key in stanza [transitioner:ess_analyst] in /opt/splunk/etc/apps/SplunkEnterpriseSecuritySuite/default/reviewstatuses.conf, line 87: transition_reviewstatus-investigation:0_to_investigation:3 (value: enabled).

Invalid key in stanza [transitioner:ess_analyst] in /opt/splunk/etc/apps/SplunkEnterpriseSecuritySuite/default/reviewstatuses.conf, line 88: transition_reviewstatus-investigation:0_to_investigation:4 (value: enabled).

Invalid key in stanza [transitioner:ess_analyst] in /opt/splunk/etc/apps/SplunkEnterpriseSecuritySuite/default/reviewstatuses.conf, line 89: transition_reviewstatus-investigation:0_to_investigation:5 (value: enabled).

Invalid key in stanza [transitioner:ess_analyst] in /opt/splunk/etc/apps/SplunkEnterpriseSecuritySuite/default/reviewstatuses.conf, line 90: transition_reviewstatus-investigation:1_to_investigation:2 (value: enabled).

Invalid key in stanza [transitioner:ess_analyst] in /opt/splunk/etc/apps/SplunkEnterpriseSecuritySuite/default/reviewstatuses.conf, line 91: transition_reviewstatus-investigation:1_to_investigation:3 (value: enabled).

Invalid key in stanza [transitioner:ess_analyst] in /opt/splunk/etc/apps/SplunkEnterpriseSecuritySuite/default/reviewstatuses.conf, line 92: transition_reviewstatus-investigation:1_to_investigation:4 (value: enabled).

Invalid key in stanza [transitioner:ess_analyst] in /opt/splunk/etc/apps/SplunkEnterpriseSecuritySuite/default/reviewstatuses.conf, line 93: transition_reviewstatus-investigation:1_to_investigation:5 (value: enabled).

Invalid key in stanza [transitioner:ess_analyst] in /opt/splunk/etc/apps/SplunkEnterpriseSecuritySuite/default/reviewstatuses.conf, line 94: transition_reviewstatus-investigation:2_to_investigation:1 (value: enabled).

Invalid key in stanza [transitioner:ess_analyst] in /opt/splunk/etc/apps/SplunkEnterpriseSecuritySuite/default/reviewstatuses.conf, line 95: transition_reviewstatus-investigation:2_to_investigation:3 (value: enabled).

Invalid key in stanza [transitioner:ess_analyst] in /opt/splunk/etc/apps/SplunkEnterpriseSecuritySuite/default/reviewstatuses.conf, line 96: transition_reviewstatus-investigation:2_to_investigation:4 (value: enabled).

Invalid key in stanza [transitioner:ess_analyst] in /opt/splunk/etc/apps/SplunkEnterpriseSecuritySuite/default/reviewstatuses.conf, line 97: transition_reviewstatus-investigation:2_to_investigation:5 (value: enabled).

Invalid key in stanza [transitioner:ess_analyst] in /opt/splunk/etc/apps/SplunkEnterpriseSecuritySuite/default/reviewstatuses.conf, line 98: transition_reviewstatus-investigation:3_to_investigation:1 (value: enabled).

Invalid key in stanza [transitioner:ess_analyst] in /opt/splunk/etc/apps/SplunkEnterpriseSecuritySuite/default/reviewstatuses.conf, line 99: transition_reviewstatus-investigation:3_to_investigation:2 (value: enabled).

Invalid key in stanza [transitioner:ess_analyst] in /opt/splunk/etc/apps/SplunkEnterpriseSecuritySuite/default/reviewstatuses.conf, line 100: transition_reviewstatus-investigation:3_to_investigation:4 (value: enabled).

Invalid key in stanza [transitioner:ess_analyst] in /opt/splunk/etc/apps/SplunkEnterpriseSecuritySuite/default/reviewstatuses.conf, line 101: transition_reviewstatus-investigation:3_to_investigation:5 (value: enabled).

Invalid key in stanza [transitioner:ess_analyst] in /opt/splunk/etc/apps/SplunkEnterpriseSecuritySuite/default/reviewstatuses.conf, line 102: transition_reviewstatus-investigation:4_to_investigation:1 (value: enabled).

Invalid key in stanza [transitioner:ess_analyst] in /opt/splunk/etc/apps/SplunkEnterpriseSecuritySuite/default/reviewstatuses.conf, line 103: transition_reviewstatus-investigation:4_to_investigation:2 (value: enabled).

Invalid key in stanza [transitioner:ess_analyst] in /opt/splunk/etc/apps/SplunkEnterpriseSecuritySuite/default/reviewstatuses.conf, line 104: transition_reviewstatus-investigation:4_to_investigation:3 (value: enabled).

Invalid key in stanza [transitioner:ess_analyst] in /opt/splunk/etc/apps/SplunkEnterpriseSecuritySuite/default/reviewstatuses.conf, line 105: transition_reviewstatus-investigation:4_to_investigation:5 (value: enabled).

Invalid key in stanza [transitioner:ess_analyst] in /opt/splunk/etc/apps/SplunkEnterpriseSecuritySuite/default/reviewstatuses.conf, line 106: transition_reviewstatus-investigation:5_to_investigation:1 (value: enabled).

Invalid key in stanza [transitioner:ess_analyst] in /opt/splunk/etc/apps/SplunkEnterpriseSecuritySuite/default/reviewstatuses.conf, line 107: transition_reviewstatus-investigation:5_to_investigation:2 (value: enabled).

Invalid key in stanza [transitioner:ess_analyst] in /opt/splunk/etc/apps/SplunkEnterpriseSecuritySuite/default/reviewstatuses.conf, line 108: transition_reviewstatus-investigation:5_to_investigation:3 (value: enabled).

Invalid key in stanza [transitioner:ess_analyst] in /opt/splunk/etc/apps/SplunkEnterpriseSecuritySuite/default/reviewstatuses.conf, line 109: transition_reviewstatus-investigation:5_to_investigation:4 (value: enabled).

Your indexes and inputs configurations are not internally consistent. For more information, run 'splunk btool check --debug'

Done

Checking default conf files for edits...

Validating installed files against hashes from '/opt/splunk/splunk-8.1.3-63079c59e632-linux-2.6-x86_64-manifest'

All installed files intact.

Done

All preliminary checks passed.

Starting splunk server daemon (splunkd)...

Done

[OK]

Waiting for web server at https://127.0.0.1:8000 to be available..... Done

If you get stuck, we're here to help.

Look for answers here: http://docs.splunk.com

The Splunk web interface is at https://ost-cla-dep-c01-mgmt.linux.ostravam.corp.telstra.com:8000

[splunk@ost-cla-dep-c01-mgmt apps]$

########################## POST Upgrade ######################

[splunk@ost-cla-dep-c01-mgmt apps]$ du -sh SA-* DA-* SplunkEnterpriseSecuritySuite

284K SA-AccessProtection

500K SA-AuditAndDataProtection

548K SA-EndpointProtection

556K SA-IdentityManagement

3.5M SA-ldapsearch

500K SA-NetworkProtection

44K SA-OST_ES_Notable_Whitelisting

11M SA-ThreatIntelligence

100K SA-UEBA

5.4M SA-Utils

216K DA-ESS-AccessProtection

280K DA-ESS-EndpointProtection

128K DA-ESS-IdentityManagement

716K DA-ESS-NetworkProtection

7.6M DA-ESS-ThreatIntelligence

829M SplunkEnterpriseSecuritySuite

[splunk@ost-cla-dep-c01-mgmt apps]$ cd -

/opt/splunk/etc/shcluster/apps

[splunk@ost-cla-dep-c01-mgmt apps]$ du -sh SA-* DA-* SplunkEnterpriseSecuritySuite

304K SA-AccessProtection

976K SA-AuditAndDataProtection

596K SA-EndpointProtection

4.6M SA-IdentityManagement

3.5M SA-ldapsearch

680K SA-NetworkProtection

44K SA-OST_ES_Notable_Whitelisting

15M SA-ThreatIntelligence

212K SA-UEBA

5.3M SA-Utils

572K DA-ESS-AccessProtection

900K DA-ESS-EndpointProtection

2.0M DA-ESS-IdentityManagement

7.2M DA-ESS-NetworkProtection

5.2M DA-ESS-ThreatIntelligence

827M SplunkEnterpriseSecuritySuite