Splunk® Enterprise Security
Administer Splunk Enterprise Security 7.0.1

Enable entity zones for assets and identities in Splunk Enterprise Security

Generated: 5/12/2022 5:59 am

Enable entity zones for assets and identities in Splunk Enterprise Security

Entity zones are disabled for assets and identities by default. You can enable entity zones in situations when you have mergers or acquisitions with other companies, for example, and you have similar IP address spaces that you need to keep separate.

Prerequisites

Perform the following prerequisite tasks before starting on these settings:

1. Collect and extract asset and identity data in Splunk Enterprise Security.
2. Format the asset or identity list as a lookup in Splunk Enterprise Security.
3. Configure a new asset or identity list in Splunk Enterprise Security.

Enable entity zones

Enable entity zones in the global settings as follows:

1. From the Splunk Enterprise Security menu bar, select **Configure > Data Enrichment > Asset and Identity Management**.
2. Click the **Global Settings** tab.
3. Scroll to the **Enable Zones for Assets or Identities** panel.
4. Use the toggle to enable for **Assets** or **Identities**.
5. Type a lowercase word to use as a default zone name. This word auto-populates in the `cim_entity_zone` fields if you do not specify your own values when formatting an asset or identity list as a lookup.
6. (Optional) Click **Configure Zones** to build a clause and specify a condition.
    1. In the **Condition** field, type a conditional statement that will evaluate to either true or false.

        The condition has to match against a raw event field and value, such as: dest = "192.0.2.1", src = "host1", location = "San Jose", and so on.

        1. If the condition is not matched, the default zone name auto-populates in the `cim_entity_zone`.
        2. If the condition is matched, such as `city = "San Jose"`, the zone that you configure in the next step will auto-populate in the `cim_entity_zone` field with the value for this zone.
    2. In the **Zone** field, type the name of a zone to assign when the match is made.
7. Click **+Add Clause** to add additional clauses.
8. Click **x** to delete clauses.
9. Click **Confirm** to save the clauses.
10. Click **Save**.

As mentioned, the field and value that you specify in the conditional statement have to match raw event data. You can't write a conditional statement to match on a field and value from an automatic lookup. The conditional statement has to match a raw event because the entity zone field evaluation happens before the lookup enrichment happens. So the `cim_entity_zone` field in the raw event is populated in one the following ways:

- Populated with the **Zone** name from the conditional statement when evaluating against raw events.
- Populated with the **Default** zone name when evaluating against raw events.

The `cim_entity_zone` in the raw event is only populated in the previously mentioned ways. ES attempts to match the raw event using a "lookup field" and the `cim_entity_zone` field. If the lookup and the raw event have matching values, then the event is enriched.

For more information about how correlation enriches notable events with asset and identity data at search time, see Manage assets and identities to enrich notables in Splunk Enterprise Security.

Any events that do not have `cim_entity_zone` specified in a lookup, or do not match any conditional statements, are assigned the default zone.

In situations where you have a `cim_entity_zone` value specified in your lookup for your known entities, the default `cim_entity_zone` value is not assigned if a similar event occurs from an unknown entity.

Disable entity zones for Assets and Identities

Disable entity zones in the global settings as follows:

1. From the Splunk Enterprise Security menu bar, select **Configure > Data Enrichment > Asset and Identity Management**.
2. Click the **Global Settings** tab.
3. Scroll to the **Enable Zones for Assets or Identities** panel.
4. Use the toggle to disable for **Assets** or **Identities**. Any previously existing default zone is disabled, not deleted.
5. Click **Save**.

See Format an asset or identity list as a lookup in Splunk Enterprise Security.

Example

Using assets as an example, consider a default zone name of **my_zone** and a source file with the same `ip` of 10.0.2.109, `nt_host` of host1 and host2 in different zones, a `cim_entity_zone` defined as an asset lookup header, and one empty `cim_entity_zone` value such as the following:

```
ip,mac,nt_host,dns,owner,priority,lat,long,city,country,bunit,category,pci_domain,is_expected,should
_timesync,should_update,requires_av,cim_entity _zone
192.0.2.94,,host1,,,,,,,,,,,,,,
192.0.2.155,,host1,,,,,,,,,,,,,,zone2
192.0.2.90,,host2,,, ,,,,,,,,,,,zone1
192.0.2.39,,host2,,,,,,,,,,,,,,zone1
10.0.2.109,,host2,,,,,,,,,,,,,,zone1
10.0 .2.109,,host3,,,,,,,,,,,,,,zone3
10.0.2.109,,host4,,,,,,,,,,,,,,zone3
```

If you enable entity zones, the behavior is to use the default zone name for the empty `cim_entity_zone` value and not to merge key fields such as `ip` and `nt_host` that are in different zones.

cim_entity_zone	asset	ip	nt_host	pci_domain
my_zone	192.0.2.94 host1	192.0.2.94	host1	untrust
zone2	192.0.2.155 host1	192.0.2.155	host1	untrust
zone1	192.0.2.90 192.0.2.39 10.0.2.109 host2	192.0.2.90 192.0.2.39 10.0.2.109	host2	untrust
zone3		10.0.2.109		untrust

cim_entity_zone	asset	ip	nt_host	pci_domain
	10.0.2.109 host3 host4		host3 host4	

If you disable entity zones, the behavior is to merge key fields such as `ip` and `nt_host` as usual.

asset	ip	nt_host	pci_domain
192.0.2.94 192.0.2.155 host1	192.0.2.94 192.0.2.155	host1	untrust
192.0.2.90 192.0.2.39 10.0.2.109 host2 host3 host4	192.0.2.90 192.0.2.39 10.0.2.109	host2 host3 host4	untrust