NIST SP 800-53 access control

You need to monitor account administration and login attempts and failures in order to ensure compliance with NIST SP 800-53 rev5.

Required data

- Data normalized to the following Common Information Models:
  - Authentication
  - Change
  - Network Traffic

To optimize the searches shown below, you should specify an index and a time range.

► Account management

These searches help you monitor the use of system accounts.

Anomalous change detection

To get a count of events calculated to have a high probability of being anomalies, run the following search.

```
| tstats count(All_Changes.action) AS count FROM datamodel=Change where All_Changes.action=* BY All_Changes.result, All_Changes.user, All_Changes.dest
| stats sum(count) AS total BY All_Changes.result, All_Changes.user, All_Changes.dest
| anomalydetection "All_Changes.result" "All_Changes.user" "All_Changes.dest" "total"
| stats count AS outlierCount
```

Account activity overview

To see statistics related to account changes users are making on your hosts, run the following search.

```
tstats count FROM datamodel=Change WHERE nodename=All_Changes.Account_Management BY All_Changes.result, All_Changes.dest, All_Changes.user
| rename All_Changes.user AS user, All_Changes.result AS subject, All_Changes.dest AS host
| eventstats sum(count) AS percent
| eval percent=round(count*100/percent,2)
| stats sum(count) AS count BY subject, host, user, percent
| table subject, host, user, count, percent
| sort 20 -count
| rename subject AS Subject, host AS Host, user AS User, count AS Count, percent AS Percent
```

Remove the - from `sort 20 -count` to see the least common account management events first.

The information provided in Splunk Lantern is intended for informational and educational purposes only. All information is provided in good faith, however, Splunk disclaims any and all representations and warranties, express and implied, regarding the information provided, including without limitation any warranties and representations regarding the completeness, adequacy or accuracy of the information. You agree to take full responsibility for the results arising from the use of the information provided.
**Account creation activity by host**

To see data regarding newly created accounts, run the following search.

```
| tstats count FROM datamodel=Change WHERE All_Changes.action=created All_Changes.Account_Management.src_user=* BY All_Changes.user, All_Changes.Account_Management.src_user, All_Changes.action, All_Changes.dest
| rename All_Changes.Account_Management.src_user AS src_user, All_Changes.user AS user, All_Changes.action AS action, All_Changes.dest AS host
| table host action, user, src_user
| rename host AS Host, action AS Action user AS User, src_user AS "Performing User"
```

In the first line of the search, change `All_changes.action=created` to `All_changes.action=deleted` to see deleted accounts instead of created ones.

---

**Access enforcement**

These searches help you enforce approved authorizations for logical access to information and system resources in accordance with applicable access control policies.

Update the subnets in the `cidrmatch functions` as needed.

**Successful remote logins**

To get a count of successful logins to your systems, run the following search.

```
| tstats count FROM datamodel=Authentication WHERE nodename=Authentication.Successful_Authentication BY Authentication.src, Authentication.user, Authentication.action
| rename Authentication.src AS src, Authentication.user AS user, Authentication.action AS action
| where (NOT cidrmatch("10.0.0.0/8",src)) AND (NOT cidrmatch("172.16.0.0/12",src)) AND (NOT cidrmatch("192.168.0.0/16",src)) AND (NOT cidrmatch("127.0.0.0/8", src))
| stats sum(count)
```

In the first line of the search, change `nodename=Authentication.Successful_Authentication` to `nodename=Authentication.Failed_Authentication` to see failed logins instead of successful ones.

**Successful remote logins by location**

To see where your users are logging in from, run the following search. You can change the `nodename` to `Authentication.Failed_Authentication` if needed. You can also change the `globallimit` value to show more results.

```
| tstats count FROM datamodel=Authentication WHERE nodename=Authentication.Successful_Authentication BY Authentication.src, Authentication.user, Authentication.action
| rename Authentication.src AS src, Authentication.user AS user, Authentication.action AS action
| where (NOT cidrmatch("10.0.0.0/8",src)) AND (NOT cidrmatch("172.16.0.0/12",src)) AND (NOT cidrmatch("192.168.0.0/16",src)) AND (NOT cidrmatch("127.0.0.0/8", src))
| stats sum(count) AS total BY src
| iplocation src
```

---

The information provided in Splunk Lantern is intended for informational and educational purposes only. All information is provided in good faith, however, Splunk disclaims any and all representations and warranties, express and implied, regarding the information provided, including without limitation any warranties and representations regarding the completeness, adequacy or accuracy of the information. You agree to take full responsibility for the results arising from the use of the information provided.
Successful privileged account logins

To see which of your privileged users are logging in, run the following search.

```splunk
| tstats count FROM datamodel=Authentication WHERE nodename=Authentication.Privileged_Authentication.Successful_Privileged_Authentication BY Authentication.src, Authentication.user
| rename Authentication.src AS src, Authentication.user AS user
| where (cidrmatch("10.0.0.0/8", src)) OR (cidrmatch("172.16.0.0/12", src)) OR (cidrmatch("192.168.0.0/16", src)) OR (cidrmatch("127.0.0.0/8", src))
| stats sum(count)
```

Privileged account authentications over time

To see privileged users logging into your systems over time, run the following search.

```splunk
| tstats count FROM datamodel=Authentication WHERE nodename=Authentication.Privileged_Authentication.Successful_Privileged_Authentication BY Authentication.src, Authentication.user, _time
| rename Authentication.src AS src, Authentication.user AS user
| where (cidrmatch("10.0.0.0/8", src)) OR (cidrmatch("172.16.0.0/12", src)) OR (cidrmatch("192.168.0.0/16", src)) OR (cidrmatch("127.0.0.0/8", src))
| timechart sum(count) AS auths BY user
```

Unsuccessful logon attempts

Use these searches to enforce a limit of consecutive invalid logon attempts by a user during a defined time-period.

Update the subnets in the `cidrmatch functions` as needed.

Authentication outliers

To view local users who are logging in more frequently than others, run the following search. There are a number of parameters in this search you might want to change to fit your organizational needs:

- the `span` in the `timechart command`
- the `window` in the `streamstats command`
- the `lowerBound` and `upperBound` in the `eval command` to define what an outlier is

You can also add NOT to each cidrmatch function to run this search on remote users instead of local users.

```splunk
| tstats count FROM datamodel=Authentication BY _time, Authentication.src span=1ms
| rename Authentication.src AS src
| where (cidrmatch("10.0.0.0/8", src)) OR (cidrmatch("172.16.0.0/12", src)) OR (cidrmatch("192.168.0.0/16", src)) OR (cidrmatch("127.0.0.0/8", src))
| timechart span=1hr count AS auths
```
| streamstats window=60 current=true avg("auths") AS avg stdev("auths") AS stdev | fillnull value=0 | eval lowerBound=if((avg-stdev*exact(2))>0,(avg-stdev*exact(2)),0) | eval upperBound=(avg+stdev*exact(2)) | eval isOutlier=if('auths' < lowerBound OR 'auths' > upperBound, 1, 0) | fields _time, "auths", lowerBound, upperBound, isOutlier, *

Location of failed remote login attempts

To see global locations where failed attempts to log in to your systems are coming from, run the following search.

| tstats count FROM datamodel=Authentication WHERE nodename=Authentication.Failed_Authentication BY Authentication.src | rename Authentication.src AS src | where (NOT cidrmatch ("10.0.0.0/8",src)) AND (NOT cidrmatch ("172.16.0.0/12",src)) AND (NOT cidrmatch ("192.168.0.0/16",src)) AND (NOT cidrmatch ("127.0.0.0/8",src)) | stats sum(count) AS total BY src | iplocation src | geostats sum(total) BY Country globallimit=200

Failed local login attempts

To see local failed attempts to log in to your systems, run the following search.

| tstats count FROM datamodel=Authentication WHERE nodename=Authentication.Failed_Authentication BY Authentication.src _time span=1h | rename Authentication.src AS src | where (cidrmatch ("10.0.0.0/8",src)) OR (cidrmatch ("172.16.0.0/12",src)) OR (cidrmatch ("192.168.0.0/16",src)) OR (cidrmatch ("127.0.0.0/8",src)) | stats sum(count) BY _time

Failed remote login attempts sorted by time

For a chronological view of failed remote login attempts, run the following search.

| tstats count FROM datamodel=Authentication WHERE nodename=Authentication.Failed_Authentication BY Authentication.src _time span=1h | rename Authentication.src AS src | where (NOT cidrmatch ("10.0.0.0/8",src)) AND (NOT cidrmatch ("172.16.0.0/12",src)) AND (NOT cidrmatch ("192.168.0.0/16",src)) AND (NOT cidrmatch ("127.0.0.0/8",src)) | stats sum(count) BY _time

Source and destination for all failed logins

To see to source and destination for all failed login attempts to your systems, run the following search.

| tstats count FROM datamodel=Authentication WHERE nodename=Authentication.Failed_Authentication BY _time, Authentication.src, Authentication.dest, Authentication.user span=10m

The information provided in Splunk Lantern is intended for informational and educational purposes only. All information is provided in good faith, however, Splunk disclaims any and all representations and warranties, express and implied, regarding the information provided, including without limitation any warranties and representations regarding the completeness, adequacy or accuracy of the information. You agree to take full responsibility for the results arising from the use of the information provided.
Remote access

Use these searches to authorize remote access to the system prior to allowing such connections.

Remote access attempts from sources on an allow list

If you have a lookup file of allowed remote hosts, you can get a count of the remote access attempts from allowed hosts.

```
| tstats count FROM datamodel=Authentication BY Authentication.src
| rename Authentication.src AS src
| where (NOT cidrmatch("10.0.0.0/8",src)) AND (NOT cidrmatch("172.16.0.0/12",src)) AND (NOT cidrmatch("192.168.0.0/16",src)) AND (NOT cidrmatch("127.0.0.0/8", src))
| lookup whitelist_remote remote_host AS src
| eval approval_status = if(is_approved ==1, "Whitelisted","Not_Whitelisted")
| search approval_status = "Whitelisted"
| stats sum(count) AS count
```

In the search command, change the approval_status to Not_Whitelisted to see hosts that are not on your allow list.

Remote access attempts from approved and unapproved systems

If you have a lookup file of approved systems, you can get a count of approved and unapproved systems that attempt remote access.

```
tstats count FROM datamodel=Authentication BY Authentication.src
| rename Authentication.src AS src
| where (NOT cidrmatch("10.0.0.0/8",src)) AND (NOT cidrmatch("172.16.0.0/12",src)) AND (NOT cidrmatch("192.168.0.0/16",src)) AND (NOT cidrmatch("127.0.0.0/8", src))
| lookup whitelist_remote remote_host AS src
| eval approval_status = if(is_approved ==1, "Approved","Unapproved")
| chart sum(count) AS count BY approval_status
```

Wireless access

Use these searches to authorize wireless access to the system prior to allowing such connections.

Wireless access control count

To see all authentications to your wireless network over time, run the following search.

```
| tstats count FROM datamodel=Network_Traffic BY All_Traffic.wifi All_Traffic.action All_Traffic.user All_...
```

The information provided in Splunk Lantern is intended for informational and educational purposes only. All information is provided in good faith, however, Splunk disclaims any and all representations and warranties, express and implied, regarding the information provided, including without limitation any warranties and representations regarding the completeness, adequacy or accuracy of the information. You agree to take full responsibility for the results arising from the use of the information provided.
Count of wireless authentications

To see how many times each user authenticated to your wireless network, run the following search.

```
| tstats count FROM datamodel=Network_Traffic BY All_Traffic.wifi All_Traffic.action All_Traffic.user All_Traffic.session_id AS session_id 
| rename All_Traffic.wifi AS wifi All_Traffic.action AS action All_Traffic.user AS user All_Traffic.session_id AS session_id 
| search (user="*") action=success 
| chart count BY user useother=0 usenull=0
```

In the `search` command, change `action=success` to `action=failure` to see failed authentications instead of successful ones.

Wireless authentication data

To see a table of user authentications to your wireless network, run the following search.

```
| tstats count FROM datamodel=Network_Traffic BY All_Traffic.wifi All_Traffic.action All_Traffic.user All_Traffic.session_id AS session_id 
| rename All_Traffic.wifi AS wifi All_Traffic.action AS action All_Traffic.user AS user All_Traffic.session_id AS session_id 
| search (user="*") action=success 
| stats count BY action, user 
| fields user, action, count 
| sort -count
```

In the `search` command, change `action=success` to `action=failure` to see failed authentications instead of successful ones.

Next steps

After running these access controls and taking appropriate action, you may want to look into other NIST SP 800-53 rev5 controls:

- Audit and accountability
- Configuration management
- Identification and authentication
- Incident response
- Risk assessment
- System and information integrity