LOGPOINT

# Use case Catalogue

02/03/23 | 2.0

www.logpoint.com

# Table of Contents



# Version history

| Version | Revision Date | Description | Implemented by |
|---|---|---|---|
| 2.0 | 02-03-2023 | Active Directory Use Cases | Gustav Rødsgaard |



Logpoint A/S | Bryggervangen 55, 4. | 2100 Copenhagen
www.logpoint.com | +45 7060 6100 | info@logpoint.com | CVR: 26301939

# Introduction and Background

The purpose of this document is to describe how you can implement basic monitoring of specific log sources on a Logpoint SIEM platform. We want to help users understand how they can use existing tables, search templates, lists, alerts and dashboards in their own environment to get the best possible results from their log monitoring.

The document is dynamic, we will continue to add new use cases that cover areas of interest to customers and partners and improve existing ones over time.

# Use cases

Use case in this document refers to an area, domain, component of your infrastructure or a regulatory set of rules aligned with a framework or regulations. For each use case, we have selected the alerts, dashboards and search templates that enable basic monitoring of the use case. Alerts and dashboards are a monitoring function that can help verify controls, but they cannot be seen as actual controls in a regulatory framework. A SIEM cannot stand alone against threats and other components should be in place to increase the overall security posture of an organization.

For each use case, we have selected a set of alerts that are relevant for the area as well as dashboards and search templates that provide insights and create value. Be aware that these use cases are generic and are for basic monitoring and might not apply to all types of environments. We will make every attempt to describe where modifications to alerts might be necessary to your environment's alerts/dashboards.

In this document you will find the use cases related to **Active Directory**. If you have requests for other use cases, reach out to your local Customer Success responsible.

# Active Directory (AD) for on Premise

Active Directory is a vital part of most organizations and enterprises today and controls users and entities such as server assets including user and group management. It is important to monitor when changes happen to the Active Directory to determine whether these changes are valid and align with your organization's policies. This could, for instance, be monitoring that domain admin access rights are only granted to a specific set of users. This use case covers on-prem Active Directory. It does not cover Azure Active Directory.

## Prerequisites

The prerequisites for setting up Active Directory Use cases involves configuring and propagating the required Lists & Tables, Enrichment, and Normalizations for the Log sources.

### Lists & Tables

For the AD use cases and for best result with the required **Dashboards** and **Alerts**, configure and populate the following lists:

- **Name**: EXCLUDED_USERS
  - **Description**: Contains names of users in the AD environment that should not trigger Alerts. Proper management of the **EXCLUDED_USERS** list will reduce false positives significantly. This list is prepopulated in Logpoint with value "-" and "*$".



Logpoint A/S | Bryggervangen 55, 4. | 2100 Copenhagen
www.logpoint.com | +45 7060 6100 | info@logpoint.com | CVR: 26301939

- **Name:** DADMINS
  - **Description**: Contains the DOMAIN administrator users for the Domain Admin Alerts. This list is mandatory and the Domain administrators in your environment are added to it so you reduce false positives of the Domain Administrator Alerts using the DADMINS list.

- **Name**: HOMENET
  - **Description:** Contains internal IP Addresses to minimize false positives from Alerts. This list contains the internal IP addresses to exclude from Alerts which are based on network traffic.

- **Name**: LOGPOINT_GROUP
  - **Description**: Monitors users added and/or removed from the Logpoint Group in Active Directory and is used by the Critical Users Dashboard. This list contains the values "Admin" and "Human Resource" by default. You can add any of your AD groups that have access to Logpoint to monitor for Active Directory Changes related to Logpoint access.
- **Name**: DOMAIN
  - **Description**: Contains the DOMAINS in your organization which is used for authentication activities. This List is necessary for Pass the Hash Alerts.

## Enrichment

To help your analysts get the best insights when they look at logs and incidents it's important you apply AD/LDAP enrichment . You can either configure a custom enrichment policy with the fields you want to include from your Active Directory or modify the existing enrichment source UEBA Active Directory to fetch data from your Active Directory. This enrichment source also comes with a preconfigured enrichment policy that can be added to the processing policy of the log sources/devices relevant for the AD use case.

**Enrichment Source à Enrichment Policy à Processing Policy à Apply to device**

## Log Sources

For the Active Directory use case some of the most common windows event logs are required for the alerts and dashboards to function properly. The following logs are required:

- **Log type**: Windows Event Log
- **Categories**: System, Application, Security, Directory Service
- **Log Levels**: Critical, Warning, Error, Information

The most common way to ingest the logs to Logpoint are with the Logpoint Agent, NXlog agent or via Windows Event forwarding. This document does not describe how to configure log sources. If you have issues configuring log sources, contact Logpoint support or your local Customer Success responsible.

## Normalization

It's important to know what kind of Normalizers you will need to normalize Active Directory data. The configurations required for your normalizations policy are:

| Normalization Policy | |
|---|---|
| **Compiled Normalizer:** | • WindowsSysmonCompiledNormalizer<br>• LPA_Windows |
| **Normalizations Packages:** | • LP_Integrity Scanner<br>• LP_File Integrity Monitor Nxlog JSON |



Logpoint A/S | Bryggervangen 55, 4. | 2100 Copenhagen
www.logpoint.com | +45 7060 6100 | info@logpoint.com | CVR: 26301939

# Alerts

Incidents don't always happen while you are looking at your data, it is a good idea to include some alerts in your Logpoint solution to get notified when something suspicious happens.
The following alerts are those we consider the most vital to basic Active Directory monitoring.

When the Vendor Alert question is set to Yes this means that the Alert Rule out of the box in Logpoint and can be found under Vendor Alerts on the Alert Rules box in the Logpoint GUI.

When the Vendor Alert question is no this means that you must add your own Alert with the specifications mentioned in the box and also its dependencies such as any Lists used in the Alert.

### Active Directory login / log out

| Default Brute Force Attack Successful | |
|---|---|
| **Technical description:** | Is triggered when there are 5 failed user login attempts followed by a successful login from the same user within 5 minutes. |
| **Search query:** | [label=User label=Login label=Fail -target_user=*$<br>\| rename target_user as user<br>\| chart count() as cnt by user<br>\| search cnt > 5 ] as s1 followed by<br>[label=User label=Login label=Successful<br>\| rename target_user as user] as s2 on s1.user = s2.user<br>\| rename s2.user as User |
| **Considerations:** | This Alert's search uses a large amount of system resources and could affect Logpoint performance |
| **Vendor Alert?** | Yes |

| LP_Default Brute Force Attack Attempt - Multiple Unique Users | |
|---|---|
| **Technical description:** | Is triggered whenever unique multiple user authentications fail from the same source within 10 minutes. The default value for unique multiple users is 5. |
| **Search query:** | label=User label=Login label=Fail source_address=* -target_user=*$<br>\| rename target_user as user<br>\| chart distinct_count(user) as DC by source_address<br>\| search DC>5 |
| **Considerations:** | This Alert usually can have a high rate of false positives. To reduce the rate, increase the unique user value to a number higher than 5. |
| **Vendor Alert?** | Yes |



Logpoint A/S | Bryggervangen 55, 4. | 2100 Copenhagen
www.logpoint.com | +45 7060 6100 | info@logpoint.com | CVR: 26301939

| Admin User Remote Logon Detected | |
|---|---|
| **Technical description:** | Searches for successful logins with the logontype 10 which indicates that the logon was remote. It also looks for specific admin users with “Admin” in their username. |
| **Search query:** | norm_id=WinServer event_id=4624 logon_type="10" (authentication_package="Negotiate" OR package="Negotiate") user="Admin-*" -user IN EXCLUDED_USERS<br>\| rename package as authentication_package |
| **Considerations:** | If you have Admin users that don’t use “Admin” in their usernames, make a list of admin usernames that should also be monitored for remote logons. |
| **Vendor Alert?** | Yes |

### Domain Admin Alerts

| Windows User Removed from Domain Enterprise Admin | |
|---|---|
| **Technical description:** | Is triggered whenever a user is removed from the "Domain Admins" or the "Enterprise Admins" user group. |
| **Search query:** | norm_id=WinServer* action="removed" (group_name="Enterprise Admins" OR group_name="Domain Admins" OR group="Enterprise Admins" OR group="Domain Admins")<br>(member=* OR target_user=*)<br>-user IN EXCLUDED_USERS<br>\| rename group_name as group, target_user as member |
| **Considerations:** | You can add additional groups to the Alert’s search.<br>Remember to fill out the excluded users list to avoid getting Alert’s for those users. |
| **Vendor Alert?** | Yes |

| Windows User Added to Domain Enterprise Admin | |
|---|---|
| **Technical description:** | Is triggered when any user is added to either “Domain Admins” or “Enterprise Admins” user group. |
| **Search query:** | norm_id=WinServer* action="added" (group_name="Enterprise Admins" OR group_name="Domain Admins" OR group="Enterprise Admins" OR group="Domain Admins")<br>member=* -user IN EXCLUDED_USERS<br>\| rename target_user as member, group_name as group |
| **Considerations:** | You can add additional groups to the Alert’s search.<br>Remember to fill out the excluded users list to avoid getting Alert’s for those users. |
| **Vendor Alert?** | Yes |



Logpoint A/S | Bryggervangen 55, 4. | 2100 Copenhagen
www.logpoint.com | +45 7060 6100 | info@logpoint.com | CVR: 26301939

| Password Never Expires on Domain Admin Account | |
|---|---|
| **Technical description:** | Lists all domain Admin accounts from the DADMINS list that changed their setting to “Never expire”. |
| **Search query:** | norm_id=WinServer label=Change label=Management label=Account label=User<br>(user_account_control=*2089* OR "'Don't Expire Password' - Enabled" OR "'Don't Expire Password' - Disabled") user="DADMIN*" -user=*$ -target_user=*$ user=*<br>\| chart count() by user, domain, log_ts, action, target_user, user_account_control |
| **Considerations:** | Your organization may have security policies in place that makes it impossible for Domain Accounts to set their password to never expire. |
| **Vendor Alert?** | No |

| Failed Login Attempts from Domain Admin | |
|---|---|
| **Technical description:** | Searches for all failed login attempts from Domain Accounts in the DADMINS list. |
| **Search query:** | event_id=4625 (target_user="DADMIN*" OR user="DADMIN*")<br>\| chart count() by user, target_user, displayName, logon_type, reason, host, workstation, log_ts |
| **Considerations:** | To get logins from outside Domain Controller servers, you will need the logs from regular windows servers too. |
| **Vendor Alert?** | No |

| Domain Admin Login from External IP address | |
|---|---|
| **Technical description:** | Lists all the successful logins from Domain Accounts in the DADMIN list with the remote logontype 10. |
| **Search query:** | logon_type=10 event_id=4624 label=Login (user="DADMIN*" OR target_user="DADMIN*") -source_address IN HOMENET<br>\| rename target_user as user<br>\| process eval("user_upper=upper(user)")<br>\| chart count() by user_upper , source_address, logon_type |
| **Considerations:** | This might be okay in the case of a hybrid workplace but should still be monitored. |
| **Vendor Alert?** | No |



Logpoint A/S | Bryggervangen 55, 4. | 2100 Copenhagen
www.logpoint.com | +45 7060 6100 | info@logpoint.com | CVR: 26301939

| User Changes for Domain Admin Account | |
|---|---|
| **Technical description:** | Lists all the user changes made to Domain Accounts from the DADMINS list. |
| **Search query:** | norm_id=WinServer label=User label=Account label=Management -user="ANONYMOUS LOGON" target_user="DADMIN*" -domain="NT AUTHORITY" action=*<br>\| chart count() by user, target_user, action, message, log_ts |
| **Considerations:** | For this Alert to work you must create and insert usernames of Domain Accounts to monitor in the DADMINS list. |
| **Vendor Alert?** | No |

### General Active Directory Alerts

| Eventlog Cleared Detected | |
|---|---|
| **Technical description:** | Is triggered whenever one of the Windows Eventlogs has been cleared. |
| **Search query:** | norm_id=WinServer event_id=104 event_source="Microsoft-Windows-Eventlog" -user IN EXCLUDED_USERS |
| **Considerations:** | This Alert should never be triggered because there is no reason to ever delete the Windows Event log manually. If it is triggered, an investigation into the incident is a good idea. You might want to consider replacing “EXCLUDED_USERS” with another list to monitor for the alert. |
| **Vendor Alert?** | Yes |

| Windows Password Never Expires | |
|---|---|
| **Technical description:** | Is triggered whenever a user has been granted the “Password Never Expires” Right (event id 4738). |
| **Search query:** | norm_id=WinServer* label=Change label=Management label=Account label=User user_account_control="*Don't Expire Password - Enabled"<br>-target_user=*$ -user IN EXCLUDED_USERS<br>\| rename caller_user as user, caller_domain as domain |
| **Considerations:** | Activating this Alert does not mean it will trigger for users who already have their password set to never expire. |
| **Vendor Alert?** | Yes |



Logpoint A/S | Bryggervangen 55, 4. | 2100 Copenhagen
www.logpoint.com | +45 7060 6100 | info@logpoint.com | CVR: 26301939

| LP_Windows Login Attempt on Disabled Account | |
|---|---|
| **Technical description:** | This Alert searches for Failed Logins with the disabled account status code 0xC0000072 |
| **Search query:** | norm_id=WinServer* label=User label=Login label=Fail sub_status_code="0xC0000072" -target_user=*$ -user=*$ -user IN EXCLUDED_USERS \| rename user as target_user, domain as target_domain, reason as failure_reason |
| **Considerations:** | This alert will alert on all failed logins with the disabled account status code. You can create a list of disabled accounts if you only want to monitor a specific set of disabled accounts, such as former Domain administrator accounts. |
| **Vendor Alert?** | Yes |

| Windows Login failure on Expired Account | |
|---|---|
| **Technical description:** | This Alert searches for Failed Logins with the disabled account status code 0xC0000193 |
| **Search query:** | norm_id=WinServer* label=User label=Login label=Fail sub_status_code="0xC0000193" -target_user=*$ -user=*$ -user IN EXCLUDED_USERS \| rename user as target_user, domain as target_domain, reason as failure_reason |
| **Considerations:** | • This Alert will be alert on all failed logins on Expired Accounts in your system. You could use a list to only monitor a certain set of accounts to minimize false positives.<br>• This is not a vendor Alert. The Vendor Alert for Expired account is using the status code 0xC0000071 which is for failed logins on expired passwords. |
| **Vendor Alert?** | No |

| LP_Suspicious Kerberos RC4 Ticket Encryption | |
|---|---|
| **Technical description:** | This Alert looks for suspicious Kerberos RC4 Ticket encryption to detect possible kerberoasting attack. |
| **Search query:** | norm_id=WinServer event_id=4769 ticket_option="0x40810000" Encryption_type="0x17" -service="$*" -user IN EXCLUDED_USERS |
| **Considerations:** | • To further minimize kerberoasting happening in your environment we recommend to have long passwords on the service accounts and changed often.<br>• False positives are inevitable from doing kerberoasting detection in logs, so you need to have a clear understanding of the trends of your environment. |
| **Vendor Alert?** | Yes |



Logpoint A/S | Bryggervangen 55, 4. | 2100 Copenhagen
www.logpoint.com | +45 7060 6100 | info@logpoint.com | CVR: 26301939

| LP_Password Spraying Attack Detected | |
|---|---|
| **Technical description:** | This alert will trigger when the same source address fails login on more than 5 different users |
| **Search query:** | norm_id=WinServer event_id=4625 -user IN EXCLUDED_USERS -user IN EXCLUDED_USERS \| chart distinct_count(user) as UserCount, distinct_list(user) as Users by source_address \| search UserCount > 5 |
| **Considerations:** | You can increase the amount of users from 5 in the search query to fit your organizations needs. |
| **Vendor Alert?** | Yes |

| LP_Windows Possible Failed Lateral Movement using Pass the Hash | |
|---|---|
| **Technical description:** | This alert is triggered whenever there is logon attempt to move laterally using Pass the Hash. DOMAIN is the list of valid Domains with expected authentication activities. |
| **Search query:** | norm_id=WinServer* label=User label=Login label=Fail logon_type=9 -caller_domain IN DOMAIN -target_user="ANONYMOUS LOGON" -user="ANONYMOUS LOGON" -user IN EXCLUDED_USERS \| rename target_user as user, target_domain as domain |
| **Considerations:** | Alerting on possible failed lateral movements by using the technique Pass the Hash can give an indication of how much your organization is being targeted. |
| **Vendor Alert?** | Yes |

| LP_Windows Possible Successful Lateral Movement using Pass the Hash | |
|---|---|
| **Technical description:** | This alert is triggered whenever there is logon attempt to move laterally using Pass the Hash. DOMAIN is the list of valid Domains with expected authentication activities. |
| **Search query:** | norm_id=WinServer* label=User label=Login label=Successful logon_type=3 -caller_domain IN DOMAIN -user="ANONYMOUS LOGON" -user=*$ caller_user=* caller_domain=* user=* domain=* source_address=* -user IN EXCLUDED_USERS |
| **Considerations:** | This Alert is indictive of a possible successful Lateral movement by using the technique Pass the Hash. If this alert triggers action is needed from your organization since this might be an indicator that an adversary is inside your network. |
| **Vendor Alert?** | Yes |



Logpoint A/S | Bryggervangen 55, 4. | 2100 Copenhagen
www.logpoint.com | +45 7060 6100 | info@logpoint.com | CVR: 26301939

| LP_Windows Domain Policy Change | |
|---|---|
| **Technical description:** | This Alert looks for changes made in the Domain Policy (Event id. 4739). |
| **Search query:** | norm_id=WinServer* label=Domain label=Policy label=Change user=*$ -user IN EXCLUDED_USERS\| rename target_domain as domain |
| **Considerations:** | Unless planned already. Any changes made to the Domain Policy should be investigated. |
| **Vendor Alert?** | Yes |

| Kerberos Policy Change | |
|---|---|
| **Technical description:** | This Alert looks for the Kerberos Policy change event (Event id 4713). |
| **Search query:** | norm_id = winserver* label = Kerberos label = Policy label = Change \| chart count() by log_ts, target_user, user, message, policy |
| **Considerations:** | Unless planned already. Any changes made to the Kerberos Policy should be investigated. |
| **Vendor Alert?** | No |



Logpoint A/S | Bryggervangen 55, 4. | 2100 Copenhagen
www.logpoint.com | +45 7060 6100 | info@logpoint.com | CVR: 26301939

# Dashboards

Dashboards are a great addition to alerts in a SIEM platform. Dashboards show trends and give an indication of how healthy your environment is. As dashboards are resource intensive, we recommend to only create and use those dashboards that you will use for daily monitoring to limit wasting system resources.

The following tables describe the dashboards relevant for the Active Directory use case:

| **User Management Dashboard** | |
|---|---|
| **Dashboard name:** | LP_AD: USER ACCOUNT MANAGEMENT |
| **Technical description:** | This Dashboard has Widgets to inform the user of User Account management activities in their Active Directory environment. |
| **Widgets** | 1. Activities in User Account Management<br>2. Top 10 Actions in User Account Management<br>3. Activities in User Account Management<br>4. Top 10 Users in Account Creation<br>5. User Accounts Created<br>6. Top 10 Users in Account Deletion<br>7. User Accounts Deleted<br>8. Created Accounts<br>9. Deleted Accounts<br>10. Top 10 Users in Accounts Changed<br>11. Top 10 Accounts Changed<br>12. Changed Accounts<br>13. Top 10 User Accounts Locked<br>14. User Accounts Unlocked<br>15. Success vs Failure Password Change Attempts<br>16. Password Set or Reset Attempts |
| **Considerations** | Some widgets display top 10 data, this gives you an idea of what's going on however important information may be missed. This can be adjusted to fit the needs of your organization. However, increasing the data being presented in a dashboard may also lower performance. |



Logpoint A/S | Bryggervangen 55, 4. | 2100 Copenhagen
www.logpoint.com | +45 7060 6100 | info@logpoint.com | CVR: 26301939

| Critical User Activity Dashboard | |
|---|---|
| **Dashboard name:** | LP_AD: CRITICAL USER ACTIVITIES |
| **Technical description:** | This Dashboard informs the user of Critical user Activities in the Active Directory environment. |
| **Widgets** | 1. Users Added to Administrator Group<br>2. Users Removed from Administrator Group<br>3. Users Disabled<br>4. Users Enabled<br>5. Password Never Expires<br>6. Users Created with a $<br>7. Users Changed to End with $<br>8. User Added to a LogPoint Group in Active Directory<br>9. User Removed from a LogPoint Group in Active Directory |
| **Considerations** | • For the Logpoint Group Widgets to work, you must configure Logpoint Group in your AD environment of users who have access to Logpoint and update the list LOGPOINT_GROUPS.<br>• The settings for the Widget “Users Added / Removed from Administrator Group” uses “Admins” or “Administrators” in their names. If you use a different name for these groups, you can change the widget’s settings. |



Logpoint A/S | Bryggervangen 55, 4. | 2100 Copenhagen
www.logpoint.com | +45 7060 6100 | info@logpoint.com | CVR: 26301939

## Search Template

To ease the investigation of incidents we have included a search template that can be used to search for Windows event logs. Search templates are used on an ad-hoc basis when you need to investigate a specific incident or for threat hunting in your environment. We recommend you add more widgets to the search templates when you create and use specific queries to perform root cause analysis.

| Windows Investigation Search Template | |
|---|---|
| **Dashboard name:** | Windows and AD |
| **Technical description:** | Looks at failed logins, Kerberos success', Kerberos ticket requests, activities in User Account management and users with special privileges. |
| **Widgets** | 1. Failed logins by user, device_name, logon_process<br>2. Failed Kerberos excluding service accounts<br>3. Kerberos success excluding service accounts<br>4. Kerberos ticket requests excluding service accounts<br>5. Activities in User Account Management by action, user, target_user label=User label=Account label=Management<br>6. Special privileges excluding service accounts<br>7. Security-enabled global group |
| **Dashboard name:** | ENDPOINT ACTIVITIES |
| **Technical description:** | Below are the names of the Widgets regarding Endpoint Activities. These widgets are based on potentially malicious processes |
| **Widgets** | 1. Process Execution from Suspicious Paths,<br>2. Malicious Office Executions<br>3. Run Keys Addition<br>4. PsExec Trace<br>5. Suspicious Scheduled Tasks<br>6. Process Masquerade<br>7. Suspicious RunDLL32 Proxy Execution |
| **Dashboard name:** | CLI ACTIVITIES |
| **Technical description:** | The Widgets in CLI Activities are based off the Event ID 4688: A new process has been created. In general, the 3 Widgets list a time representation of Powershell and CMD commands, Child Processes spawned from Powershell or cmd and command prompt or Powershell commands having more than 150 characters. You can change the character value to fit your organizations´ needs. |
| **Widgets** | 1. CLI Activity<br>2. CLI Child Processes<br>3. Long Command Lines |
| **Considerations** | This Search Template is built using widgets from the Vendor Template Ransomware Hunt with additions of widgets regarding generic Active Directory and Windows information.<br>When using the Search template as the user you can filter out the searches from the widgets by adding specific values to the following fields: User, Host, Source IP, Destination IP, Port and File. By default, these values include anything. |



Logpoint A/S | Bryggervangen 55, 4. | 2100 Copenhagen
www.logpoint.com | +45 7060 6100 | info@logpoint.com | CVR: 26301939