Learn Discover Product documentation Development languages Topics Sign in

Filter by title

… / Audit Other Logon/Logoff Events /

4649(S): A replay attack was detected.

Article • 09/07/2021 • 1 contributor

This event generates on domain controllers when **KRB_AP_ERR_REPEAT** Kerberos response was sent to the client.

Domain controllers cache information from recently received tickets. If the server name, client name, time, and microsecond fields from the Authenticator match recently seen entries in the cache, it will return KRB_AP_ERR_REPEAT. You can read more about this in RFC-1510. One potential cause for this is a misconfigured network device between the client and server that could send the same packet(s) repeatedly.

There is no example of this event in this document.

Subcategory: Audit Other Logon/Logoff Events

Event Schema:

A replay attack was detected.

Subject:

> *Security ID:%1*
>
> *Account Name:%2*
>
> *Account Domain:%3*
>
> *Logon ID:%4*

Credentials Which Were Replayed:

> *Account Name:%5*
>
> *Account Domain:%6*

Process Information:

> *Process ID:%12*

- Audit MPSSVC Rule-Level Policy Change
- Audit Other Policy Change Events
- Audit Sensitive Privilege Use

> *Process Name:%13*

Network Information:

> *Workstation Name:%10*

Detailed Authentication Information:

> *Request Type:%7*
>
> *Logon Process:%8*
>
> *Authentication Package:%9*
>
> *Transited Services:%11*

This event indicates that a Kerberos replay attack was detected- a request was received twice with identical information. This condition could be caused by network misconfiguration."

Required Server Roles: Active Directory domain controller.

Minimum OS Version: Windows Server 2008.

Event Versions: 0.

Security Monitoring Recommendations

For 4649(S): A replay attack was detected.

- This event can be a sign of Kerberos replay attack or, among other things, network device configuration or routing problems. In both cases, we recommend triggering an alert and investigating the reason the event was generated.