



We use optional cookies to improve your experience on our websites, such as through social media connections, and to display personalized advertising based on your online activity. If you reject optional cookies, only cookies necessary to provide you the services will be used. You may change your selection by clicking “Manage Cookies” at the bottom of the page. [Privacy Statement](#) [Third-Party Cookies](#)

Accept

Reject

Manage cookies

Microsoft Ignite

Nov 19–22, 2024

Register now >



Learn

Discover >

Product documentation >

Development languages >

Topics >



Sign in

ⓘ We're no longer updating this content regularly. Check the [Microsoft Product Lifecycle](#) for information about how this product, service, technology, or API is supported.

[Return to main site](#)



Filter by title

> Audit Security Group Management

>

>

>

>

>

>

>

>

>

>

>

>

>

>

>

>

>

>

>

>

>

>

>

>

>

>

... / [Audit Computer Account Management](#) /



4743(S): A computer account was deleted.

Article • 09/07/2021 • [1 contributor](#)

Event Properties - Event 4743, Microsoft Windows security auditing.

GeneralDetails

A computer account was deleted.

Subject:

Security ID:CONTOSO\dadmin

Account Name:dadmin

Account Domain:CONTOSO

Logon ID:0x3007B

Target Computer:

Security ID:S-1-5-21-3457937927-2839227994-823803824-6118

Account Name:COMPUTERACCOUNT\$

Account Domain:CONTOSO

Additional Information:

Privileges:-

Log Name:Security

Source:Microsoft Windows security auditing

Event ID:4743

Level:Information

User:N/A

OpCode:Info

More Information:[Event Log Online](#)

Logged:8/14/2015 8:57:08 AM

Task Category:Computer Account Management

Keywords:Audit Success

Computer:DC01.contoso.local

Copy

Close

Subcategory: [Audit Computer Account Management](#)

Event Description:

This event generates every time a computer object is deleted.

This event generates only on domain controllers.

Note For

recommendations, see [Security Monitoring Recommendations](#) for this event.

Event XML:



Copy

```
- <Event xmlns="http://schemas.microsoft.com/win/2004/08/events/event">
- <System>
  <Provider Name="Microsoft-Windows-Security-Auditing" Guid="{54849625-5478-4994-B4D1-486984D401D2}" />
  <EventID>4743</EventID>
  <Version>0</Version>
  <Level>0</Level>
  <Task>13825</Task>
  <Opcode>0</Opcode>
  <Keywords>0x8020000000000000</Keywords>
  <TimeCreated SystemTime="2015-08-14T15:57:08.104214100Z" />
  <EventRecordID>172103</EventRecordID>
```

Event Viewer - Security - Windows Event Viewer

- > Audit Registry
 - Audit Removable Storage
- > Audit SAM

```
<Correlation />
<Execution ProcessID="520" ThreadID="1108" />
<Channel>Security</Channel>
<Computer>DC01.contoso.local</Computer>
<Security />
</System>
- <EventData>
  <Data Name="TargetUserName">COMPUTERACCOUNT$</Data>
  <Data Name="TargetDomainName">CONTOSO</Data>
  <Data Name="TargetSid">S-1-5-21-3457937927-2839227994-823803824-6118</Data>
  <Data Name="SubjectUserSid">S-1-5-21-3457937927-2839227994-823803824-1104</Data>
  <Data Name="SubjectUserName">dadmin</Data>
  <Data Name="SubjectDomainName">CONTOSO</Data>
  <Data Name="SubjectLogonId">0x3007b</Data>
  <Data Name="PrivilegeList">-</Data>
</EventData>
</Event>
```

Required Server Roles: Active Directory domain controller.

Minimum OS Version: Windows Server 2008.

Event Versions: 0.

Field Descriptions:

Subject:

- **Security ID** [Type = SID]: SID of account that requested the “delete Computer object” operation. Event Viewer automatically tries to resolve SIDs and show the account name. If the SID cannot be resolved, you will see the source data in the event.

Note A **security identifier (SID)** is a unique value of variable length used to identify a trustee (security principal). Each account has a unique SID that is issued by an authority, such as an Active Directory domain controller, and stored in a security database. Each time a user logs on, the system retrieves the SID for that user from the database and places it in the access token for that user. The system uses the SID in the access token to identify the user in all subsequent interactions with Windows security. When a SID has been used as the unique identifier for a user or group, it cannot ever be used again to identify another user or group. For more information about SIDs, see [Security identifiers](#).

- **Account Name** [Type = UnicodeString]: the name of the account that requested the “delete Computer object” operation.
- **Account Domain** [Type = UnicodeString]: subject’s domain name. Formats vary, and include the following:
 - Domain NETBIOS name example: CONTOSO
 - Lowercase full domain name: contoso.local
 - Uppercase full domain name: CONTOSO.LOCAL
 - For some [well-known security principals](#), such as LOCAL SERVICE or ANONYMOUS LOGON, the value of this field is “NT AUTHORITY”.
- **Logon ID** [Type = HexInt64]: hexadecimal value that can help you correlate this event with recent events that might contain the same Logon ID, for example, “[4624](#): An account was successfully logged on.”

Target Computer:

- **Security ID** [Type = SID]: SID of deleted computer account. Event Viewer automatically tries to resolve SIDs and show the account name. If the SID cannot be resolved, you will see the source data in the event.

- **Account Name** [Type = UnicodeString]: the name of the computer account that was deleted. For example: WIN81\$
- **Account Domain** [Type = UnicodeString]: domain name of deleted computer account. Formats vary, and include the following:
 - Domain NETBIOS name example: CONTOSO
 - Lowercase full domain name: contoso.local
 - Uppercase full domain name: CONTOSO.LOCAL

Additional Information:

- **Privileges** [Type = UnicodeString]: the list of user privileges which were used during the operation, for example, SeBackupPrivilege. This parameter might not be captured in the event, and in that case appears as "-". See full list of user privileges in "Table 8. User Privileges."

Security Monitoring Recommendations

For 4743(S): A computer account was deleted.

Important For this event, also see [Appendix A: Security monitoring recommendations for many audit events](#).

- If you have critical domain computer accounts (database servers, domain controllers, administration workstations, and so on) for which you need to monitor each action (especially deletion), monitor this event with the "**Target Computer\Security ID**" or "**Target Computer\Account Name**" that corresponds to the high-value account or accounts.