Alerts Specification

NetWrix SCOM Management Pack for Active Directory Change Reporter Technical Article

Table of Contents

Contacting NetWrix Support

If you have any questions please feel free to contact the NetWrix support team.

NetWrix provides unlimited phone and email support for customers who purchase the commercial version (including evaluation). In addition, on the NetWrix Support Forum, a limited support is provided for customers who use the freeware version.

Disclaimer

The information in this publication is furnished for information use only, does not constitute a commitment from NetWrix Corporation of any features or functions discussed and is subject to change without notice. NetWrix Corporation assumes no responsibility or liability for any errors or inaccuracies that may appear in this publication.

1. Applies To

NetWrix SCOM Management Pack for Active Directory Change Reporter.

2. Summary

NetWrix Active Directory Change Reporter records change events to the NetWrix Change Reporter event log if integration with Microsoft System Center Operations Manager (also known as *SCOM*) is enabled. NetWrix SCOM Management Pack for Active Directory Change Reporter is a solution that uses this event log to capture all changes made to Active Directory and feeds the audit data to SCOM, which generates appropriate reports and alerts.

This article describes alerts triggered by SCOM alerting rules. For each alert, the following information is available:

- Alert severity level
- Trigger events
- Name and brief description of the alerting rule that triggered the alert.

3. Alerts

This section describes SCOM alerts. The alerts fall into two categories: *Audit alerts* and *Data Collection alerts*.

3.1 Audit Alerts

This section describes alerts triggered by changes made to Active Directory objects. The alerts help you detect unauthorized changes and violations of your security policy.

3.1.1 Administration Groups Changed

Severity Level	Warning
Trigger Events	Removing or adding members to the administration groups. The administration groups list includes: *Enterprise Admins, Domain Admins, Schema Admins, Account Operators, Administrators, Incoming Forest Trust Builders, Server Operators,* and *Backup Operators* groups.
Rule Name	Administrative Group Membership Changed.
Rule Description	Tracks changes to the administration groups membership.

3.1.2 Administrative Password Reset

Severity Level	Information
Trigger Events	A user password has been reset.
Rule Name	Administrative Password Reset.
Rule Description	Tracks changes to user password.

3.1.3 Changes to Domain Trust Relationships

Severity Level	Information.
Trigger Events	Any changes to domain trusts (e.g. some trusts have been added or removed).
Rule Name	Changes to Domain Trust Relationships
Rule Description	Tracks changes to domain trusts.

3.1.4 Domain Controller Modifications

Severity Level	Information
Trigger Events	Any changes to properties of DC computer objects.
Rule Name	Domain Controller Modifications
Rule Description	Tracks changes to Domain Controller computers.

3.1.5 Domain Controller Demoted

Severity Level	Information
Trigger Events	A domain controller has been demoted.
Rule Name	Domain Controller Demoted.
Rule Description	Tracks changes to servers role.

3.1.6 Domain Controller Promoted

Severity Level	Information
Trigger Events	A member server or a standalone computer has been promoted to domain controller.
Rule Name	Domain Controller Promoted.
Rule Description	Tracks changes to servers role.

3.1.7 Security Group Membership Changes

Severity Level	Information
Trigger Events	Removing or adding members to security groups (including local, global, and universal groups).
Rule Name	Security Group Membership Changes.
Rule Description	Detects membership changes in all security groups.

3.1.8 Security Group Removed

Severity Level	Information
Trigger Events	Deletion of security groups (including local, global, and universal groups).
Rule Name	Security Group Removed.
Rule Description	Monitors deletions of security groups.

3.1.9 User Account Lockout

Severity Level	Warning
Trigger Events	User account was locked.
Rule Name	User Account Lockout.
Rule Description	Detects user account lockouts.

3.1.10 User Account Enabled

Severity Level	Information
Trigger Events	A disabled user account was enabled.
Rule Name	User Account Enabled.
Rule Description	Monitors enabling of user account.

3.1.11 User Account Disabled

Severity Level	Information
Trigger Events	User account was disabled.
Rule Name	User Account Disabled.
Rule Description	Monitors disabling of users accounts.

3.2 Data Collection Alerts

This section describes alerts triggered by errors and warnings encountered when NetWrix Active Directory Change Reporter gathers the audit data.

3.2.1 Data Collection Warning

Alert Severity Level	Warning
Trigger Events	Active Directory Change Reporter encountered warnings while data gathering.
Alert Name	Data Collection Warning.
Description	Monitors status of Active Directory Change Reporter data collection tasks.

3.2.2 Data Collection Error

Alert Severity Level	Critical
Trigger Events	Active Directory Change Reporter encountered errors while data gathering.
Alert Name	Data Collection Error.
Description	Monitors status of Active Directory Change Reporter data collection tasks.

4. Additional Information

Last updated: June 28, 2011

For more information, refer to
http://www.netwrix.com/scom_active_directory_management_pack.html