Problem Overview

================

Product:	IBM Security Guardium
Release:	10.5
Fix ID#:	Guardium v10.5 FAM for NAS
Fix Completion Date:	2018-08-30
Filename:	FAMforNas-V10.6.0.88.zip
MD5Sum:	c39180f260504f3b833c597f9a6ed77c

Finding the Fix/Patch

==============================

This document is intended to provide a reference to the contents of this fix/patch. If applicable, the detailed description of each fix and instructions for applying this fix/patch are contained within the download package. The actual package is available for downloading from the IBM Fix Central web site at https://www.ibm.com/support/fixcentral/

Make the following selections on Fix Central:

Product Group:	IBM Security
Product Selector:	IBM Security Guardium
Installed Version:	10.0
Platform:	Windows
Heading:	Database Agent (S-TAP, GIM, CAS)

Click "Continue", then select "Browse for fixes" and click "Continue" again.

The Guardium File Activity Monitor (FAM) monitors activity across files and directories residing on NAS devices. NAS or network-attached storage is a file-level storage system based on networked appliances containing multiple storage devices.

FAM's ability to monitor these environments enables users to identify threats and streamline operations. For more information, please refer to the attached guide: *File Activity Monitor (FAM) for NAS and SharePoint.*

Note: This version of FAM for NAS is fully supported for use with v10.5 Guardium environment.

2018-August-30

File Activity Monitor (FAM) for NAS and SharePoint

IBM

Contents

File Activity Monitor for NAS and SharePoint

The Guardium File Activity Monitor (FAM) monitors activity across files and directories residing on NAS devices and SharePoint servers in the Windows environment.

NAS or network-attached storage is a file-level storage system based on networked appliances containing multiple storage devices. SharePoint is a web-based collaborating platform and a document management & storage system.

FAM's ability to monitor these environments enables users to identify threats and streamline operations.

Use the following work flow to enable File Activity Monitoring across your NAS devices or SharePoint environment.

Supported Platforms

The Guardium File Activity Monitor (FAM) can be installed on the following Windows platforms, NAS devices and SharePoint versions.

Supported Windows Platforms

FAM can be installed on the following Windows Servers:

- Windows 2016
- Windows 2012 R2
- Windows 2012
- Windows 2008 R2

Supported Network Attached Storage Devices

FAM is compatible with the following Network Attached Storage (NAS) devices:

- Hitachi® 11.2+
- NetApp® Data ONTAP®:
  - Cluster-Mode 8.2+
  - 7-Mode 7.2+
- EMC® VNX®:
  - VNX® 8.1
  - VNX® 7.1
- EMC® Isilon® 7.0+
- EMC® Celera® 6.0+
- EMC® VMAX3™
- EMC® VNXe® 2.0+ (Access Auditing only)
- Dell EMC Unity™

Supported SharePoint Versions

FAM is compatible with the following SharePoint versions:

- SharePoint® 2016
- SharePoint® 2013
- SharePoint® 2010

Monitoring Permissions

Enable these permissions to allow file activity monitoring on your NAS or SharePoint environments.

NAS Permissions

NetApp Data ONTAP Cluster-Mode Permissions

The policy name and credentials are case-sensitive when targeting a NetApp Data ONTAP Cluster-Mode device. The policy name must be `StealthAUDIT` and the engine name must be `StealthAUDITEngine`. A tailored FPolicy is recommended as it decreases the impact on the NetApp device.

The credential that is associated with the FPolicy used to monitor activity must be provisioned with at least the following CLI commands:

CLI command	Access
version	Readonly
volume	Readonly
vserver	Readonly

For more options to enable and configure the FPolicy, use the following CLI commands:

Employing the “Enable and connect FPolicy” Option.

The File Activity Monitor can be configured to ensure that everything is actively monitored with periodic checks on the FPolicy. If the “Enable and connect FPolicy” option is enabled, then the credential requires the following permissions to enable the FPolicy, connect to the FPolicy, and collect events:

CLI Command	Access
version	Readonly
volume	Readonly
vserver	Readonly
vserver fpolicy disable	All
vserver fpolicy enable	All
vserver fpolicy engine-connect	All

Employing the “Configure FPolicy” Option

The File Activity Monitor can automatically configure FPolicy. If the “Configure FPolicy” option is enabled, then the credential requires the following permissions to enable the FPolicy, connect to the FPolicy and collect events:

CLI command	Access
version	Readonly
volume	Readonly
vserver	Readonly
server fpolicy	All
security certificate install (only needed for FPolicy TLS connection)	All

NetApp Data ONTAP 7-Mode Permissions

It is necessary to enable the "file and printer sharing" where FAM is installed.

An FPolicy must be configured on the target device for file activity monitoring. A tailored FPolicy is recommended as it decreases the impact on the NetApp device. The credential associated with the FPolicy used to monitor activity must be provisioned with access to the following API calls:

- login-http-admin api-system-api-list
- api-system-get-version
- api-cifs-share-list-iter-* api-volume-list-info-iter-*

If the File Activity Monitor will be automatically configuring the FPolicy, then the following command is also needed:

- api-fpolicy*

If the File Activity Monitor will be configured to use the “Enable and connect to the FPolicy” option, then the following command is also needed:

- cli-fpolicy*

The credential must also have the following permissions on the target device:

- Group membership in both of the following groups:
- ONTAP Power Users
- ONTAP backup Operators

EMC Celeriac or Unity device

The EMC Common Event Enabler (CEE) should be installed on the Windows proxy server where FAM agent is deployed.

EMC Isilon device

The EMC Common Event Enabler (CEE) should be installed on the Windows proxy server where the File Activity Monitor agent is deployed.

Hitachi

A Hitachi device can host multiple Enterprise Virtual Servers (EVS). Each EVS has multiple file systems. Auditing is enabled and configured per file system. HNAS generates the audit log files in EVT format (a standard event log format in Windows XP/2003 and earlier). Hitachi stores the generated audit logs in a user specified location on the file system. FAM accesses this location to collect the log files as they are generated. The credential used to monitor activity must be provisioned with:

- Capability of enabling a File System Audit Policy on the Hitachi device
- Audit rights to the Hitachi log directory

Firewall rules - Windows Proxy Server

NetApp Data ONTAP Cluster-Mode Firewall Rules

The following firewall settings are required for communication between FAM and the NetApp Data ONTAP Cluster-Mode device:

Communication Direction	Protocol	Ports	Description
FAM to NetApp	HTTP (Optional)	80	ONTAPI
FAM to NetApp	HTTPS (Optional)	443	ONTAPI
NetApp to FAM	TCP	9999	FPolicy events

NetApp Data ONTAP 7-Mode Firewall Rule

The following firewall settings are required for communication between FAM and the NetApp Data ONTAP 7-Mode device:

Communication Direction	Protocol	Ports	Description
FAM to NetApp*	HTTP (optional)	80	ONTAPI
FAM to NetApp*	HTTP (optional)	443	ONTAPI
FAM to NetApp	TCP	135, 139 Dynamic Range (49152-65535)	RPC
FAM to NetApp	TCP	445	SMB
FAM to NetApp	UDP	137, 138	RPC
NetApp to FAM	TCP	135, 139 Dynamic Range (49152-65535)	RPC
NetApp to FAM	TCP	445	SMB
NetApp to FAM	UDP	137, 138	RPC

*Only required if using the FPolicy Configuration and FPolicy Enable and Connect options within the File Activity Monitor.

EMC Firewall Rules

The following firewall settings are required for communication between FAM and the EMC Celerra, Dell EMC Unity, or EMC Isilon device:

Communication Direction	Protocol	Ports	Description
EMC Isilon Device to CEE Server	TCP	TCP 12228	CEE Communication
EMC Device (other than Isilon) to CEE Server	TCP	RPC Dynamic Range	CEE Communication

Hitachi Firewall Rules

The following firewall settings are required for communication between FAM and the Hitachi device:

Communication Direction	Protocol	Ports	Description
Unidirectional	TCP	445	SMB

SharePoint Permissions

- The provided domain user must be a local admin on the SharePoint application server.
- Auditing settings must be enabled on SharePoint.

Installation

Use these instructions to install the File Activity Monitor (FAM) on your NAS or SharePoint environment.

Before you begin

- Please review the permissions before proceeding: "Monitoring Permissions" on page 2.
- For detailed platform prerequisites and support, see "Supported Platforms" on page 1.
- Third-party prerequisite: To monitor an EMC device, the EMC Common Event Enabler (CEE) must be installed on the Windows proxy server where FAM is installed.

Procedure

1. Determine what environment to use, NAS or SharePoint. If a user wants to monitor a NAS device, install FAM on a Windows server that can access the NAS device through the network. But if a user wants to monitor SharePoint, install FAM directly on the SharePoint server or SharePoint server farm.

   Note: There should be no other Guardium products on this server.
2. Download the FAM for NAS or FAM for SharePoint package from Fix Central to the server and unzip this file.
3. Navigate to the FAM package installer directory and run the executable file `setup.exe` in the installer directory.
4. Follow the prompts in the wizard to complete the installation.

   Note:

   For NAS, the default installation directory is `C:\Program Files\IBM\FAMforNAS`

   For SharePoint, the default installation directory is `C:\Program Files\IBM\FAMforSP`

Configuration

After installing, configure the File Activity Monitor (FAM) to begin monitoring your NAS or SharePoint environment.

Configuring a NAS Device

On the Guardium File Activity Monitor, use these options on the **Monitored Hosts** tab to configure a NAS device:

Add:
From the list, select the NAS device to be monitored

Edit:
Click the **Edit** button in the menu and use the following tabs to configure the NAS device.

(a) Selected NAS Device
On the selected NAS device tab, use the text field to provide the name of the NAS server.

(b) Operations
Select the activity events to monitor. These operations can relate to file or directory activity.

(c) Path Filtering
This tab, on a host's properties window, allows users to add collection scope filters for file paths. Specified paths can be included in or excluded from being monitored.

(d) Account Exclusions
The accounts added here will be excluded from being monitored for file system activity.

(e) Unix IDs

This tab provides configuration options to translate Unix IDs (UID) to Windows SIDs. This applies only to NetApp devices and EMC devices, When there is an activity on a NAS device, UIDs are returned for that activity event. Depending on the operating system, the UID can be mapped to Active Directory accounts using the uidNumber attribute in Active Directory. The activity agent resolves the Active Directory SID based on the UID from the activity event.

Configuring SharePoint

On the Guardium File Activity Monitor, use these options on the **Monitored Hosts** tab to configure a SharePoint device:

Add:

Add the SharePoint server or server farm to be monitored.

Edit:

Click the **Edit** button in the menu and use the following tabs to configure SharePoint.

(a) SharePoint

Provide credentials that have administrative privileges on both the local system as well as SharePoint. Then click on **Connect**.

(b) Operations

Select the SharePoint operations and Permission operations to monitor.

(c) Account Exclusions

The accounts added here will be excluded from being monitored for SharePoint activity.

Viewing Results

To view file activity reports on your NAS devices or SharePoint, create a custom query.

Click here for instructions on creating a custom query.

The query should have the following attributes added as **fields**:

Sequence	Entity	Attribute
1	Session	Timestamp
2	Client/Server	OS User
3	Object	Object name
4	Command	SQL Verb
5	Client/Server	Server Host name
6	Client/Server	Client Host name

Sequence	Entity	Attribute
1	Session	Timestamp
2	Client/Server	OS User
3	Object	Object name
4	Command	SQL Verb
5	Client/Server	Server Host name
6	Client/Server	Server IP

For attribute descriptions, refer to the table below:

Attribute	Description
Timestamp	Session start time
Object name	Name of the object such as libraries, files, site or directories
OS User	User that operated on the file
SQL Verb	The type of operation done on the file
Server Host Name	Target host name (NAS), Local host name (SharePoint)
Client Host Name (NAS), Server IP (SharePoint)	Host name of the client (NAS), Local IP (SharePoint)

To filter data for either NAS or SharePoint, add the attribute `Service Name` from the Client/Server entity as a condition and set the operator to “=”. For NAS filtering, specify `NASFAM` as the value. For SharePoint, specify `SPFAM` as the value.

After the query is saved, it can be viewed as a report on the dashboard. Click here for more information on creating dashboards.

Click here to learn more about creating reports and customizing columns using the report builder.

Note: In order to view results, create and install a custom policy. The default installed policy is "Ignore Data Activity for Unknown Connections [template]", which ignores all traffic. For more information on how to create a policy, see Creating policies