IBM Tivoli Risk Manager
버전 4.2 수정팩 1
Readme 파일

주:

이 정보 및 정보가 지원하는 제품을 사용하기 전에 38 페이지의 주의사항에 있는 정보를 읽으십시오.

초판(2004 년 9 월)

이 문서는 새 개정판에서 별도로 명시하지 않는 한, IBM Tivoli Risk Manager 버전 4.2, 수정팩 1 및 모든 후속 릴리스와 수정사항에 적용됩니다.

내용

1 수정팩 정보

이 절에서는 이 수정팩에 대한 일반적인 정보를 제공합니다. 수정팩을 설치하기 전에 이 문서 전체를 읽으십시오.

이 Readme 문서는 Adobe Acrobat 형식으로만 제공됩니다.

이 수정팩에서 제공하는 자국어팩에 대한 정보는 이 Readme 파일의 *자국어팩 정보* 절을 참조하십시오.

1.1 수정팩의 내용

이 수정팩은 다음 내용을 제공합니다.

- readme 파일
- 수정팩의 이미지 보고서
- 수정팩의 CD-ROM 이미지

1.2 이 수정팩이 대체하는 패치

이 수정팩은 다음 패치를 대체합니다.

- 4.2-RMG-0001LA
- 4.2-RMG-0002LA
- 4.2-RMG-0003LA
- 4.2-RMG-0004LA

1.3 지원되는 운영 체제

이 절에서는 이 수정팩이 지원하는 플랫폼과 데이터베이스에 대해 설명합니다.

지원되는 운영 체제 버전 [1]	역할				선택적 구성요소			
	이벤트 서버	분산 연관 서버	게이트웨이	클라이언트	Crystal Reports	네트워크 IDS	웹 IDS	웹 어플리케이션
AIX ® 5L V5.1(32 비트 또는 64 비트)	X	X	X	X		X[3]	X	X
AIX 5.L V5.2(32 비트 또는 64 비트)	X	X	X	X		X[3]	X	X
Solaris® 8(SPARC) [2]	X	X	X	X		X	X	X
Solaris 9(SPARC)	X	X	X	X		X	X	X
HP-UX 11i(32 비트 또는 64 비트)	X	X	X	X			X	X
Windows® 2000 Professional(SP3)	X	X	X	X	X		X	X
Windows 2000 Server(SP3)	X	X	X	X	X		X	X
Windows 2000 Advanced Server(SP3)	X	X	X	X	X		X	X
Windows XP Professional		X	X	X	X		X	X

지원되는 운영 체제 버전 [1]	역할				선택적 구성요소			
	이벤트 서버	분산 연관 서버	게이트웨이	클라이언트	Crystal Reports	네트워크 IDS	웹 IDS	웹 어플리케이션
Windows 2003 Server	X	X	X	X	X		X	X
Red Hat Enterprise Linux AS 2.1(IA32)	X	X	X	X		X	X	X
Red Hat Enterprise Linux AS 3.0(IA32)	X	X	X	X		X		
Red Hat Enterprise Linux ES 3.0(IA32)	X	X	X	X		X		
SUSE LINUX Enterprise Server 8(iA32)	X	X	X	X		X	X	X
SUSE LINUX Enterprise Server 8(pSeries®)				X			X	
SUSE LINUX Enterprise Server 8(zSeries®)	X	X	X	X		X	X	X
SUSE LINUX Enterprise Server 9(iA32)	X	X	X	X		X		X

운영 시스템 참고사항:

1. 이 표의 정보는 이 수정팩이 발표될 당시에 사용 가능한 정보를 기반으로 합니다. 이 표는 운영 체제 공급업체가 표시한 대로, 수정팩 발표 당시에 사용 중인 운영 체제를 반영합니다. 최신 지원 정보는 IBM 의 온라인 지원을 참조하십시오.
2. Solaris 는 Solaris Operating Environment 를 나타내며 이하 Solaris 로 지칭합니다.
3. 네트워크 IDS(Intrusion Detection System)는 64 비트 시스템에서 지원되지 않습니다.

RDBMS 공급업체	버전
IBM DB2®	7.2(FP8), 8.1(FP2)
Oracle	9i, 9i v2
Sybase	12
Microsoft SQL Server	7.0, 2000

1.4 이 수정팩의 새로운 사항

이 절에서는 Tivoli Risk Manager 제품의 변경사항에 대해 설명합니다.

- 큐 관리에 대한 지원이 향상되었습니다. 큐의 크기를 제어하고 큐 상태에 대한 이벤트를 전송할 수 있는 키워드가 이제 제공됩니다. 자세한 정보는 문서 갱신사항 절을 참조하십시오.
- 일반 표현식에 대한 지원이 향상되었습니다. 보다 견고한 최신 버전의 Xerces 일반 표현식 라이브러리가 이제 표준 일반 표현식 구문의 보다 광범위한 지원을 제공합니다. 자세한 정보는 문서 갱신사항 절을 참조하십시오.

- FFDC(First Failure Data Capture)에 대한 지원이 추가되었습니다. 자세한 정보는 문서 갱신사항 절을 참조하십시오.
- RMAgent_Inactive 이벤트에 포함된 msg 속성이 향상되어 더 이상 RMAgent_HeartBeat 이벤트를 전송하지 않는 에이전트의 호스트 이름 및 IP 주소를 포함합니다. 자세한 정보는 문서 갱신사항 절을 참조하십시오.
- Windows 2003 Server 를 지원합니다.

2 설치 및 구성

2.1 사전 설치 소프트웨어

다음 소프트웨어가 Tivoli Risk Manger 수정팩 1 에 필요합니다.

- IBM Tivoli Risk Manager 버전 4.2
- IBM Tivoli Enterprise Console 버전 3.9(FP01 포함)(이벤트 서버 역할 전용)
- Red Hat Enterprise Linux 의 경우, 권장하는 Java 런타임 버전은 IBM JRE 1.3.1-6 이상입니다. 이러한 버전을 사용할 수 없는 경우, IBM 소프트웨어 지원에 문의하십시오.

2.2 설치 참고

이 절에서는 Tivoli Risk Manager 제품 설치 시 필요한 추가 정보에 대해 설명합니다.

- Tivoli Risk Manager 4.2.0-RMG-FP01 수정팩을 설치한 다음 Tivoli Risk Manager 제품의 초기 설치 중에 설치하지 않은 선택적 구성요소(예: Crystal Reports)를 설치하는 경우, 이 프로시저를 수행하는데 필요한 설치 수정팩에 대해 IBM 소프트웨어 지원에 문의하십시오.
- 해당 수정팩은 전체 설치 또는 패치로 설치할 수 있습니다. 설치 방법을 결정하기 위한 자세한 정보는 설치 지시사항 절을 참조하십시오.
- Windows 이벤트 모니터가 레지스트리 키를 작성하여 Windows 이벤트 로그를 읽은 마지막 위치를 표시합니다. 이러한 항목은 이벤트 모니터 또는 Tivoli Risk Manager 에이전트를 다시 시작해야 하는 경우 읽기 시작할 위치를 판별하는데 사용합니다. Tivoli Risk Manager 제품이 설치 제거되는 경우, 설치 제거 프로그램이 레지스트리에서 이러한 레지스트리 키를 제거하지 않습니다. 이벤트 모니터를 다시 설치하는 경우, 이벤트 모니터의 다음 시작 시 이전 레지스트리 키가 사용되며 이벤트 모니터가 이전 이벤트를 읽기 시작합니다.
  Windows 이벤트 모니터가 현재 날짜부터만 읽기 시작하고 이전 이벤트를 읽지 않도록 하려면 처음으로 이벤트 모니터를 시작하기 전에 다음 이벤트 모니터 레지스트리 키를 삭제하십시오.
  HKEY_LOCAL_MACHINE₩SOFTWARE₩Tivoli₩Riskmgr₩Agent₩RMLogfile
- Solaris 시스템에 대한 Tivoli Risk Manager 웹 어플리케이션 구성요소 설치가 매우 느리거나 중지될 수도 있습니다. 열린 파일의 기본 최대수가 WebSphere Application Server 에 너무 낮게 설정되어 Tivoli 웹 어플리케이션 구성요소의 설치를 완료하지 못할 수도 있습니다. 이로써, WebSphere WebSphere Application Server 가 오류 코드를 리턴하지 않고 설치를 계속 재시도합니다.
  다음 명령을 실행하여 파일 디스크립터 한계를 판별할 수 있습니다.

  ulimit -n

  WebSphere Application Server 에 Tivoli Risk Manager 웹 어플리케이션 구성요소의 설치를 완료하려면 다음 절차 중 하나를 사용하여 Tivoli Risk Manager 웹 어플리케이션을 설치하기 전에, (샘플 WebSphere Application Server 어플리케이션이 Tivoli Enterprise Console 웹 어플리케이션과 함께 설치되어 있다는 가정하에) 1024 이상의 최대 파일 디스크립터를 사용하여 설치를 시작해야 합니다. 이를 수행하기 전에 Solaris 문서를 읽어 이러한 변경사항 작성의 주의사항, 실행 및 파생 결과를 먼저 확인하십시오. 정확한 최대 파일 디스크립터의 값은 설치된 WebSphere Application Server 어플리케이션의 수에 따라 변경해야 할 수도 있습니다.

  다음 방법 중 하나를 사용하여 최대 파일 디스크립터를 변경하십시오.

  1. WebSphere Application Server 를 중지하십시오.
  2. 다음 명령을 실행하십시오.
     ulimit -n 1024

3. ulimit 명령이 실행된 세션과 동일한 세션에서 WebSphere Application Server 를 다시 시작하십시오.
4. Tivoli Risk Manager 제품을 설치하십시오.

보다 영구적인 해결책은 /etc/system 파일에서 다음 속성을 설정하여 파일 디스크립터의 시스템 값을 변경하는 것입니다.

rlim_fd_cur
rlim_fd_max

- Sybase 데이터베이스와 함께 Tivoli Risk Manager 제품을 새로 설치하는 경우, Tivoli Risk Manager 테이블은 Tivoli Enterprise Console 제품 데이터베이스의 기본 세그먼트에 설치됩니다. Tivoli Enterprise Console 설치가 정의하는 기본 세그먼트는 매우 작으며 극히 제한된 수의 Tivoli Risk Manager 아카이브 테이블 이벤트만을 보유합니다. Sybase 의 기본 구현과 함께 Tivoli Risk Manager 제품을 사용하도록 기타 디바이스를 추가하여 Tivoli Enterprise Console 데이터베이스의 기본 세그먼트를 늘릴 수 있습니다.

  다음 절차는 TEC_SYSTEM_2 기본 세그먼트에 200MB 디바이스를 작성하여 기본 세그먼트 크기를 늘리는 방법의 예제를 제공합니다.

  주:
  - ALTER DATABASE 문이 새 디바이스를 기본 세그먼트에 자동으로 추가합니다.
  - Sybase 시스템의 사용자 ID 를 사용하여 이 프로시저를 수행할 Sybase 환경을 설정하십시오. 이 사용자 ID 에는 적절한 권한과 Sybase 환경이 있어야 합니다.

  1. 다음과 같이 rm_exp_archive_table.syb.sql 스크립트를 작성하십시오.

```
use master
go
DISK INIT name="TEC_SYSTEM_2",
physname="/data/sybase/data/TEC_SYSTEM_2",
vdevno=14,
size=102400
go
ALTER DATABASE tec
on TEC_SYSTEM_2 = 200
go
```

  2. 다음 매개변수를 평가하고 사용자 설치에 필요한 대로 변경하십시오.
     - DISK INIT name: 설치에 적합한 이름을 선택하십시오.
     - physname: 작성 중인 디바이스의 운영 체제 경로 이름을 지정하십시오.
     - vdevno: 사용하지 않은 번호임을 확인하십시오. 다음 명령을 사용하여 현재 사용 중인 번호를 판별하십시오.

```
select distinct low/16777216 from sysdevices
```

  3. 다음 명령을 실행하여 스크립트를 실행하십시오.

```
isql -Usa -P<pw> -S<system> -i rm_exp_archive_table.syb.sql
```

  <pw> 변수는 SQL 암호이며 *<system>* 변수는 데이터베이스가 설치된 시스템의 이름입니다.

- 다음 메시지가 설치 중에 표시되어 Java 실행 파일을 찾을 수 없음을 표시합니다.

  "JVM 을 찾을 수 없음"

  해당 원인은 임시 디렉토리가 있는 파일 시스템에 사용 가능한 공간이 충분하지 않기 때문일 수 있습니다. 그런 경우, 다음 중 하나를 수행할 수 있습니다.

  - 해당 파일 시스템에 여유 공간 확보

- 파일 시스템에 추가 공간 할당

필수 공간이 설치된 Java JRE 크기의 최대 세배일 수 있습니다.

- Tivoli Risk Manager 제품을 다시 설치하고 전송 유형을 TME 로 변경한 경우, TMEEndpoint 키워드의 값을 /etc/Tivoli/rma_eif_env.sh 스크립트 파일에서 다음과 같이 true 로 변경하십시오.

  TMEEndpoint=true

2.3 설치 지시사항

이 절에서는 해당 수정팩을 설치하는데 대한 정보를 제공합니다.

Tivoli Risk Manager 4.2.0-RMG-FP01 수정팩은 전체 설치 또는 패치 설치로 설치할 수 있습니다. 전체 설치는 다음 조건 하에서 수행해야 합니다.

- Web 어플리케이션을 DB2 외의 임의의 RDBMS 제품과 사용 중입니다.
- 다음 플랫폼 중 하나에서 해당 수정팩을 설치 중입니다.

  Windows 2003 Server
  Red Hat Enterprise Linux AS 3.0
  Red Hat Enterprise Linux ES 3.0
  SUSE LINUX Enterprise Server 8(iA32)
  SUSE LINUX Enterprise Server 9(iA32)

전체 설치를 위해 사용해야 하는 설치 패키지는 IBM 소프트웨어 지원에 문의하십시오.

2.3.1 패치 설치

다음 명령을 실행하여 패치를 설치하십시오.

rm4201_setup _*<platform>* [-silent | -console]

*<platform>*에 다음 플랫폼 중 하나를 지정하십시오.

aix:	Tivoli Risk Manager 제품이 지원하는 AIX 버전
hpux:	Tivoli Risk Manager 제품이 지원하는 HP-UX 버전
linux:	Tivoli Risk Manager 제품이 지원하는 Linux(IA32) 버전
linuxppc:	Tivoli Risk Manager 제품이 지원하는 Linux(PPC) 버전
solaris:	Tivoli Risk Manager 제품이 지원하는 Solaris(SPARC) 버전
win:	Tivoli Risk Manager 제품이 지원하는 Windows 버전

다음 옵션 중 하나를 지정할 수 있습니다.

-silent	이 옵션은 사용자 입력이 필요하지 않습니다. 영(0)이 아닌 리턴 코드가 있는지 설치 디렉토리의 로그 파일을 점검하여 설치가 완료되었는지 여부를 판별하십시오.
-console	이 옵션은 단말기 설치(텍스트 모드)를 제공합니다. 이 옵션은 Windows 플랫폼에서 사용할 수 없습니다.

옵션을 지정하지 않으면 다음 창이 표시됩니다.

- 언어
- 시작
- 사전 설치

- 사후 설치

이러한 창에는 사용자 입력이 필요하지 않습니다. 각 창이 표시되면 **다음**을 누르십시오.

해당 수정팩을 이벤트 서버에 설치한 경우, 설치를 완료한 후에 다음 절차를 수행하십시오.

1. 사용하려는 룰 베이스가 현재 룰 베이스인지를 확인하십시오.
2. 다음 명령을 실행하십시오.
   rmcorr_cfg -update

   주: 이 명령이 룰 베이스를 갱신합니다. 또한, Tivoli Enterprise Console 이벤트 서버를 중지 및 다시 시작합니다.

2.4 자국어팩 정보

4.2-RMG-FP01 수정팩에 포함된 자국어팩에는 Tivoli Risk Manager 버전 4.2 제품이 지원하는 모든 언어의 갱신된 번역 내용이 들어 있습니다. 이 절에서는 다음과 같은 자국어팩 정보를 제공합니다.

- 자국어팩 참고
- 자국어팩 설치 지시사항

2.4.1 자국어팩 참고

4.2-RMG-FP01 수정팩을 설치하기 전에 이 절의 정보를 검토하십시오.

- 이 수정팩에 포함된 갱신된 자국어 자원이 Tivoli Risk Manager 사용자 인터페이스 및 메시지의 변경사항을 반영합니다.
- 전체 설치와 패치 설치의 차이점은 설치 전에 수행된 사전 필수 점검 및 설치된 파일의 수입니다.
- 패치 설치 중에 표시되는 창은 전체 설치 중에 표시되는 창과 동일합니다.

2.4.2 자국어팩 설치 지시사항

이 절에서는 자국어팩 설치에 대해 설명합니다. Tivoli Risk Manager 버전 4.2 수정팩 01 의 자국어팩은 전체 설치 또는 패치 설치로 설치될 수 있습니다. 기본 제품의 완전 설치를 수행하는 경우 전체 설치를 사용하십시오(자세한 정보는 위의 설치 지시사항 절을 참조하십시오). 기본 제품의 패치 설치 수행 시 패치 설치를 사용하십시오.

2.4.2.1 전체 설치

자국어 자원의 전체 설치를 수행하려면 *IBM Tivoli Risk Manager 설치하기 전에* 버전 4.2 의 자국어 지원 절에 있는 설치 지시사항을 참조하십시오.

2.4.2.2 패치 설치

패치 설치를 수행하려면 다음 명령 중 하나를 실행하십시오.

Windows 플랫폼의 경우는 다음을 수행하십시오.

rmlp4201_setupwin32.exe

UNIX 및 Linux 플랫폼의 경우는 다음을 수행하십시오.

./rmlp4201_setup *<platform>* .bin

*<platform>*의 경우, 다음 플랫폼 중 하나를 지정하십시오.

aix: Tivoli Risk Manager 제품이 지원하는 AIX 버전

hp11x: Tivoli Risk Manager 제품이 지원하는 HP-UX 버전

linux: Tivoli Risk Manager 제품이 지원하는 Linux(IA32) 버전

linuxppc: Tivoli Risk Manager 제품이 지원하는 Linux(PPC) 버전

solaris: Tivoli Risk Manager 제품이 지원하는 Solaris(SPARC) 버전

Linux for zSeries(S/390)의 경우 다음을 수행하십시오.

```
java -Dis.javahome=/opt/IBMJava2-s390-131/jre -cp ./rmlp4201_setup.jar run
```

3 이 수정팩에서 정정된 APAR

이 절에서는 4.2.0-RMG-FP01 수정팩이 제공하는 APAR 수정사항의 해결책과 설명을 제공합니다.

APAR: IY48016

증상: 웹 IDS(Intrusion Detection System)의 여러 인스턴스가 동일한 시스템에서 실행 중인 경우, 모든 인스턴스가 webids.lastread 파일의 동일한 사본을 사용 중이므로 재개 기능이 올바르게 작동하지 않습니다.

해결: 웹 IDS 기능의 각 인스턴스가 이제 webids.lastread 파일의 개별적인 사본을 사용합니다.

APAR: IY50483

증상: Tivoli Risk Manager 또는 Tivoli Enterprise Console 서버에서 tec_rule 프로세스가 확장 CPU 활용화를 표시합니다. 이로써 들어오는 이벤트가 QUEUED 상태로 남게 됩니다.

해결: 인시던트 그룹을 생성하는 Tivoli Risk Manager Tivoli Enterprise Console 룰이 성능을 향상하도록 수정되었습니다. 인시던트 그룹 처리를 위한 추가 구성 옵션이 $RMADHOME/etc/tec/rules 디렉토리의 riskmgr_config.pro 파일에 추가되었습니다. 이러한 옵션의 사용에 대한 자세한 정보는 riskmgr_config.pro 파일의 주석을 참조하십시오.

APAR: IY52322

증상: 부분 이벤트 수신 시 분산 연관 서버가 중지합니다.

해결: 새 Tivoli Enterprise Console API 키워드인 ReadRetryInterval 이 부분 이벤트 수신 시 EIF(Event Integration Facility) API 에 의해 사용되는 시간초과 값을 구성하는데 사용됩니다.

해당 키워드의 기본값은 120 초입니다.

EIF(Event Integration Facility) 송신자가 2KB 를 초과하는 이벤트와 작업하는 경우, 소켓 연결을 사용하여 전달되는 두 패킷으로 이벤트를 나눕니다. 수신자가 해당 이벤트가 부분 이벤트임으로 판별하는 경우, 두 번째 패킷을 검색하여 처리를 완료하기 전에 해당 키워드가 지정한 기간동안 대기합니다. 두 번째 패킷이 이 기간동안 검색되지 않는 경우, 수신된 부분 이벤트를 버리며 메시지가 로그에 작성됩니다.

APAR: IY52323

증상: 시스템이 다시 시작되면 Tivoli Risk Manager 에이전트 간 사용하지 않은 소켓 연결이 닫히지 않습니다.

해결: 에이전트 간 사용하지 않은 소켓 연결이 이제 자동으로 닫힙니다.

APAR IY53525

증상: UNIX 시스템에서, 이벤트 모니터가 로그 파일 회전 시 작성된 새 로그 파일에서 읽지 않습니다.

해결: 이벤트 모니터가 이제 새 로그 파일에서 올바르게 읽습니다.

APAR IY53527

증상: 문서는 이벤트 모니터가 지원하는 일반 표현식 구문에 필수입니다.

해결: 일반 표현식 지원이 향상되었으며 문서가 제공됩니다. 문서 변경사항은 문서 갱신사항 절을 참조하십시오.

APAR: IY53678

증상: 이벤트 모니터가 클래스의 색인 패턴과는 일치하지만 XML 파일의 해당 클래스에 정의된 클래스 패턴과는 일치하지 않는 이벤트 구문 분석 시 Java 널(null) 포인터 예외를 생성합니다.

해결: 이벤트 모니터 처리가 변경되어 이벤트 문자열이 클래스의 색인 패턴과는 일치하지만 클래스 패턴과는 일치하지 않는 경우 해당 문자열을 해당 클래스와의 일치사항으로 간주하지 않으며 다른 일치 클래스의 검색을 계속합니다.

APAR: IY53713

증상: 이벤트 그룹이 데이터베이스에 삽입되고 삽입이 부분적으로만 완료되는 경우 중복 키 예외가 수신됩니다.

해결: 데이터베이스에 이벤트 삽입이 이제 올바르게 완료됩니다. 각 이벤트는 한 번만 삽입됩니다. 중복 키가 감지된 경우, 처리가 향상되어 중복 이벤트를 버립니다.

APAR: IY54408

증상: wrmadmin -i 명령의 반복된 사용으로 인해 시스템의 메모리가 부족하게 되므로 해당 시스템이 중지합니다.

해결: 이제 시스템 메모리 문제를 초래하지 않고 wrmadmin -i 명령을 반복적으로 사용할 수 있습니다.

APAR: IY54568

증상: Windows 이벤트 로그 이벤트 모니터가 이미 처리된 이벤트를 다시 처리합니다.

해결: 이벤트가 반복적으로 다시 처리되지 않습니다.

APAR: IY55241

증상: 네트워크 IDS 파일은 CAN-2002-0562 취약성 특성의 정정사항을 포함하도록 갱신되어야 합니다.

해결: 특성 파일이 올바른 특성을 포함하도록 갱신됩니다.

APAR: IY55319

증상: 다수의 이벤트가 큐되는 경우 wrmqueue 명령이 완료되지 않습니다.

해결: wrmqueue 명령과 연관된 내부 프로세스가 이 문제를 정정하도록 변경됩니다. 이 명령에 대한 자세한 설명은 문서 갱신사항 절을 참조하십시오.

APAR IY55895

증상: *IBM Tivoli Risk Manager 어댑터 안내서* 및 여러 어댑터 패키지와 함께 제공되는 기타 PDF 문서가 이벤트 맵핑 테이블을 참조합니다. 해당 테이블은 웹 사이트에 게시되지 않으므로 다운로드 또는 참조가 가능하지 않습니다.

해결: 이벤트 맵핑 테이블 문서(DCF 1171204)가 다음 Risk Manager 지원 사이트에 게시되어 있습니다.

http://www.ibm.com/software/sysmgmt/products/support/IBMTivoliRiskManager.html.

APAR IY55927

증상: DBCS 로케일에서 실행 시, Tivoli Risk Manager 에이전트가 DBCS 문자를 포함하는 이벤트를 버립니다. 다음 메시지가 Tivoli Risk Manager 메시지 로그에 작성되어 있습니다.

HRMAG0135W 이벤트 통합 기능 TECAgent 가 이벤트를 필터했습니다.

해결: Tivoli Risk Manager 에이전트가 이제 DBCS 문자를 포함하는 이벤트를 올바르게 처리합니다.

APAR: IY56431

증상: Tivoli Risk Manager 이벤트 저장소가 대소문자 구분 옵션으로 설치된 경우 Microsoft SQL 을 지원하지 않습니다. 다음 증상이 해당 문제점이 있음을 나타냅니다.

- 이벤트가 Microsoft SQL 이벤트 아카이브에 작성되지 않습니다.
- 다음 오류 메시지가 Tivoli Risk Manager 메시지 로그에 작성됩니다.

  HRMAG0082E SQL 예외:[Microsoft] [SQLServer 2000 Driver for JDBC]

  [SQLServer]올바르지 않은 오브젝트 이름 'RM_T_ARC41'

해결: 다음 명령을 실행하여 이 문제를 정정하는 DDL 파일을 실행하십시오.

```
osql -U tec -P <password> -d tec -S <server> -n -i
%RMADHOME%₩dbschema₩rm_t_arc41_uc.ms.sql
```

4 알려진 제한사항

이 절에서는 각 제한사항과 사용 가능한 문제해결 방법이 있는 경우 해당 방법에 대한 설명을 제공합니다.

4.1 설치

제한사항: 설치 중에 다음과 같은 올바르지 않은 경고 메시지가 표시됩니다.

경고: 로그 출력 /opt/RISKMGR/rminstall_log.txt 를 복사할 수 없습니다.

(해당 파일 또는 디렉토리가 없음)

문제해결 방법: 설치 중에 오류가 발생한 경우 Tivoli Risk Manager 제품을 다시 설치하고 설치 명령에 다음 옵션을 지정하여 /opt/RISKMGR 외의 다른 디렉토리에 로그를 작성하십시오.

-l !*<fully qualified path>*

<fully qualified path> 변수는 rminstall_log.txt 파일의 완전한 경로입니다.

4.2 연관 서버

제한사항: Tivoli Risk Manager 에이전트 이벤트(예: RM_Sensor, RM_Error, RMAgent_Inactive 및 RMAgent_QueueProblem)가 Tivoli Enterprise Console 제품으로 송신되지 않으며 이벤트 콘솔에 표시되지 않습니다. 이 문제는 다음 기준 *모두를* 충족하는 시스템에만 적용됩니다.

- 사용자의 설치가 이벤트 서버이거나 분산 연관 서버 설치입니다.
- 기본 설치를 수행하지 않았습니다. 그 대신, 인시던트 이벤트(RM_Incident)를 Tivoli Enterprise Console 서버에 전송하도록만 선택했습니다. 설치 선택사항에 대한 자세한 정보는 *Tivoli Risk Manager 설치 안내서* 버전 4.2 의 페이지 102 와 114 를 참조하십시오.

문제해결 방법: 이 문제점을 해결하려면 다음 절차를 사용하십시오.

1. 연관 및 이벤트 서버의 $RMADHOME/etc/rmagent.xml 파일을 편집하고 다음 필터 정의를 추가하십시오.

```
<filter name = "nonSensorEvents">
    <OR>
        <isa value = "RM_AgentProblem"/>
        <NOT>
        <isa value = "RM_SensorEvent"/>
        </NOT>
     </OR>
  </filter>
```

2. 다음과 같이 <withfilter name ="incidents"/>문을 수정하여 기존 커넥터 정의가 새 필터 이름 nonSensorEvents 를 지정하도록 변경하십시오.

```
<connector>
    <from name ="correlation"/>
    <to name ="incident_sender"/>
    <withfilter name ="nonSensorEvents"/>
  </connector>
```

3. 변경사항이 적용되도록 에이전트를 다시 시작하십시오.

4.3 Tivoli Enterprise Console 이벤트 서버

제한사항: RMAgent_Inactive 및 RMAgent_QueueProblem 이벤트가 이벤트 콘솔로 전송되면 기타 센서 이벤트와 함께 혼합되어 RM_SensorEvent 그룹 보기에 표시됩니다. Tivoli Event Console 또는 분산 연관 서버의 기본 구성을 배치하는 경우 RM_SensorEvent 그룹 보기가 여러 이벤트를 포함할 수도 있습니다. 이로써, Tivoli Risk Manager 에이전트 및 네트워크의 큐 문제점을 경고하는 Tivoli Risk Manager 에이전트 이벤트를 인식하는데 어렵게 될 수도 있습니다.

문제해결 방법: 에이전트 문제점을 보다 쉽게 모니터하려면 다음 절차를 사용하여 RMAgent_Inactive 및 RMAgent_QueueProblem 이벤트를 포함하도록 이벤트 콘솔의 RM_Error 그룹 보기를 사용자 정의하십시오.

1. 기본 이벤트 콘솔 보기에서 **Windows → 구성**을 누르십시오.
2. 왼쪽 분할창에서 **이벤트 그룹**을 누르십시오.
3. **RM_Error** 를 누르십시오.
4. 창을 마우스 오른쪽 단추로 누르고 **필터 작성**을 누르십시오. 이벤트 그룹 필터 추가 창이 표시됩니다.
5. 이름 필드에 RM_AgentProblem 을 입력하십시오 .
6. 설명 필드에 필터의 설명을 입력하십시오.
7. **제한 조건 추가**를 누르십시오.
8. 속성 목록에서 **클래스**를 선택하십시오.
9. 연산자 목록에서 **유사함**을 선택하십시오.
10. 값에 RMAgent_%를 입력하십시오. (이 값은 대소문자를 구분함).
11. **확인**을 누르십시오.
12. 이벤트 그룹 필터 추가 창에서 **SQL 테스트**를 눌러 필터가 올바른 수의 이벤트를 작성하는지 판별하십시오.
13. **확인**을 눌러 변경사항을 저장하십시오.
14. 이벤트 콘솔을 중지한 후 다시 시작하십시오.
15. **Windows → 요약 도표 보기**를 누르고 RM_Error 콘솔 그룹을 열어 필터가 올바르게 작동하는지 판별하십시오.

4.4 Tivoli Risk Manager 에이전트

- 제한사항: 메모리 제한 조건이 메모리 부족 문제점을 초래할 수 있습니다. 이 문제점은 AIX 시스템에서 가장 두드러집니다. 수신자 또는 송신자의 수가 증가하거나 **instanceCount** 매개변수가 임의의 rmagent.xml 대상 정의에 추가되는 경우 발생할 수 있습니다. 이 문제점은 다수의 송신자 또는 다수의 **instanceCounts** 를 추가하는 경우에도 발생할 수 있습니다. 왜냐하면 두 옵션이 추가 스레드를 작성하여 메모리 사용량을 증가시키기 때문입니다.

  Tivoli Risk Manager 에이전트는 Java 프로세스이며 Java 환경의 메모리 할당으로 제한됩니다. AIX 에서 이 메모리 제한은 /etc/security/limits 파일의 낮은 저장영역 할당 기본값으로 인해 상당히 영향을 받습니다. Tivoli Risk Manager 가 기본 AIX 설치에서 실행 가능하도록 최대 Java 저장영역을 **RmagentMemMax** 매개변수로 의도적으로 제한하며, 이는 RMADHOME/etc/rmad.conf 파일에 정의되어 있습니다. AIX 에서 이 값은 92MB 로 설정되어 있으며, 이 값은 기본 서버 설치에만 충분한 메모리 할당을 제공합니다.

문제해결 방법: RmagentMemMax 매개변수를 임의의 플랫폼에서 사용하여 Tivoli Risk Manager 에 사용 가능한 최대 메모리를 증가할 수 있습니다. 예를 들어, AIX 에서 다음 절차를 수행하십시오.

1. 한계 파일의 스택 값 및 data,rss 의 값을 증가하십시오 (또는 ulimit 명령을 사용).
2. rmad.conf 파일의 RmagentMemMax 값을 늘리십시오.
3. 로그오프한 다음 시스템에 로그온하십시오.
4. wrmadmin -r 명령을 사용하여 Tivoli Risk Manager 에이전트를 다시 시작하십시오.

- 제한사항: 지속성 디렉토리가 있는 디스크가 가득 찬 경우 Tivoli Risk Manager 제품을 다시 시작할 수 없습니다.

  문제해결 방법: Tivoli Risk Manager 제품을 다시 시작하기 전에 충분한 여유 디스크 공간이 있는지 확인하십시오. 다음 공식을 사용하여 필요한 디스크 공간의 양을 판별하십시오.

  (1 + 대상 수) x 20MB

  *대상 수*는 rmagent.xml 파일에 정의된 대상의 수입니다.

- 제한사항: 이벤트 속성의 첫 번째 문자가 작은 따옴표인 경우 작은 따옴표 및 이벤트 속성의 마지막 문자가 제거되므로 이벤트가 손상됩니다. 다음 예제에 msg 이벤트 속성 및 결과의 맨 앞에 나타난 따옴표가 표시됩니다.

  'myHostname' is acting suspiciously

  아카이브 테이블의 대응 MSG 컬럼에는 다음이 포함됩니다.

  myHostname' is acting suspiciousl

  문제해결 방법: 가능하면 이벤트 속성의 맨 앞에 작은 따옴표를 사용하지 마십시오. 그렇지 않은 경우, 사용 가능한 문제해결 방법이 없습니다.

4.5 DNS 분석

제한사항: Solaris 의 경우, wrmdns 명령이 DNS 분석을 시작하지 않습니다.

문제해결 방법: 다음 절차를 수행하여 DNS 분석을 시작하십시오.

1. summary_engine.conf 파일 및 incident_engine.conf 파일을 편집하십시오.
2. 두 파일 모두의 dnsResolver=off 항목을 dnsResolver=on 으로 변경하십시오.
3. 다음 명령을 실행하여 Tivoli Risk Manager 에이전트를 다시 시작하십시오.

   wrmadmin -r

4.6 메시지 및 추적 로깅

- 제한사항: Linux 기본 IP 필터링 및 방화벽 보호가 매우 제한되어 있으므로 일부 Linux 시스템에서 추적 및 로그 레벨 설정을 동적으로 변경하지 못할 수도 있습니다.

  Tivoli Risk Manager 제품에 포함된 JLog 패키지가 Tivoli Risk Manager 에이전트 실행 중 추적 및 로그 설정을 동적으로 변경할 수 있는 기능을 제공합니다. 이 기능에 대한 자세한 정보는 *IBM Tivoli Risk Manager 문제점 판별 안내서*의 명령행 인터페이스 로깅 절을 참조하십시오.

  Tivoli Risk Manager 에이전트 시작 시, 9992 포트에서 인식하는 로그 명령 서버를 작성하는 JLog 로그 매니저를 호출합니다. logcmd 클라이언트 프로그램이 이 포트를 사용하여 로그 명령 서버와 통신합니다. 일부 Linux 시스템에서, Tivoli Risk Manager 에이전트가 실행 중인 경우 9992 포트가 인식되지 않으며 logcmd 명령이 Java ConnectionException 으로 인해 실패합니다. 이는 설치된 방화벽 보호와 IP 필터로 인해 발생합니다. 다음 프로그램 중 하나가 Linux 시스템에 설치되어 있고

Tivoli Risk Manager 에이전트 시작 시 9992 포트가 인식 중인지 알 수 없는 경우 IP 방화벽이 포트가 액세스되지 않도록 예방합니다.

- lokkit
- ipchains
- iptables
- ipfwadm

문제해결 방법: 9992 포트를 잠금 해제하는 절차는 Linux 시스템 문서를 참조하십시오. 보안상의 이유로 인해 포트를 잠금 상태로 두려는 경우, 추적 설정을 동적으로 변경할 수 없다는 점 이외에는 표준 Tivoli Risk Manager 에이전트 로깅에 문제되는 사항이 없습니다.

- 제한사항: UNIX 시스템에서 로그 파일이 회전 시 압축되어 호스트 IDS 어댑터가 읽기 불가능하게 합니다.

  문제해결 방법: 문제점을 예방하려면 가장 최신에 회전된 로그 파일에 대해 로그 압축 기능을 끄십시오.

- 제한사항: 다음 메시지(HRMAG0147I)가 언제나 반복된 메시지 다음에 바로 오지는 않습니다.

  이전 메시지가 {n}번 반복되었습니다.

  이런 경우, 반복된 메시지를 판별할 방법이 없습니다.

  조치: 사용 가능한 조치가 없습니다.

4.7 네트워크 IDS 구성요소

제한사항: 32 비트 AIX 시스템에서 네트워크 IDS 구성요소 시작 시 구성요소가 시작하지 않을 수도 있습니다. 이는 네트워크 IDS 구성요소가 네트워크를 모니터하기 위해 필요한 /dev/bpf0 디바이스가 정의되지 않았거나 시스템이 마지막으로 다시 부팅된 이후로 올바르게 시작되지 않았기 때문에 발생할 수 있습니다.

문제해결 방법: 다음 절차를 사용하여 /dev/bpf0 디바이스를 재설정하거나 정의하십시오.

1. AIX 단말기 세션에서 tcpdump 명령을 실행하십시오.
2. 이더넷 연결이 시작되었음을 나타내는 다음 메시지가 표시된 후 Ctrl+c 를 눌러 tcpdump 명령을 종결하십시오.

   xxx 에서 인식

   문자 *xxx* 는 이더넷 디바이스 번호를 표시합니다(예제: en0).
3. 다음 명령을 실행하여 네트워크 IDS 프로세스를 중지한 후 다시 시작하십시오.

   stopnids

   startnids

4.8 웹 IDS 구성요소

- 제한사항: webids.cfg 파일에서 fileMatch_value=0 을 코딩하여 웹 IDS 구성요소의 로그 파일 롤오버를 사용 불가능하게 하면 오류 메시지가 표시됩니다.

  문제해결 방법: 이 문제점의 문제해결 방법이 없습니다. 로그 파일 롤오버를 사용 불가능하게 할 수 없습니다.

- 제한사항: 웹 IDS 구성요소가 동일한 시스템의 여러 웹 서버를 모니터하도록 구성되고 서버의 액세스 로그가 모두 동일한 디렉토리에 있는 경우, 해당 구성요소가 루프에 걸립니다.

  문제해결 방법: 웹 서버 액세스 로그를 다른 디렉토리에 저장하십시오.

- 제한사항: **webids -d** 명령이 디버깅 정보를 표준 출력(STDOUT)에 작성하지 않습니다. 자세한 정보는 문서 갱신사항 절을 참조하십시오.

  문제해결 방법: 사용 가능한 문제해결 방법이 없습니다.

4.9 웹 어플리케이션

- 제한사항(APAR IY58098): Java 콘솔을 실행 중인 시스템이 WebSphere Application Server 가 실행 중인 로컬 서브넷에 없는 경우 Tivoli Risk Manager 웹 콘솔에 로그온할 수 없을 수도 있습니다. 이는 rmweb.pl 스크립트가 Tivoli Risk Manager 웹 어플리케이션 설치 시, 웹 어플리케이션 서버를 실행 중인 시스템의 완전한 호스트 이름 대신 단축 호스트 이름으로 갱신되었기 때문입니다.

  문제해결 방법: 다음 절차를 수행하여 웹 어플리케이션 서버의 완전한 호스트 이름을 지정하십시오.

  1. 이벤트 서버의 RMADHOME/cgi-bin 디렉토리에 있는 **rmweb.pl** 스크립트를 편집하십시오.
  2. 다음 행을 찾으십시오(대략 47 번째 라인).

     $output .= "METHOD=POST ACTION=₩"http://server1:9080/rmwebapp42/logon₩">');₩n";
  3. URL 문자열의 짧은 호스트 이름을 완전한 호스트 이름으로 변경하십시오(예제: server1.mycompany.com).

- 제한사항: 이전 버전의 Mozilla 가 설치되어 있는 경우, 웹 어플리케이션을 사용하지 못할 수도 있습니다.

  문제해결 방법: Mozilla 버전 1.7.2 이상을 설치하십시오.

- 제한사항: Tivoli Risk Manager 웹 어플리케이션을 설치 제거한 후에도 Tivoli Risk Manager JDBC 제공자가 여전히 WebSphere Application Server 자원으로 존재합니다.

  문제해결 방법: 다음 절차를 사용하여 Tivoli Risk Manager JDBC 제공자를 제거하십시오.

  1. WebSphere Application Server 관리자 콘솔에 관리자로 로그인하십시오.
  2. **자원**을 누르십시오.
  3. **JDBC 제공자**를 누르십시오.
  4. 범위가 서버 레벨로 설정되어 있는지 확인하십시오.
  5. **리스크 매니저 JDBC 제공자** 선택란을 선택하십시오.
  6. **삭제**를 누르십시오.

- 제한사항: 온라인 도움말에 어댑터 주소에 대한 잘못된 참조가 있습니다. 시스템 주소 창에서 물음표(?)를 누르면, 도움말 패널에 다음 선택사항이 표시되어 시스템 정보를 볼 수 있습니다.

  소스 주소
  대상 주소
  센서 주소
  어댑터 주소
  기타

  문제해결 방법: 문제해결 방법이 없습니다. 어댑터 주소의 정보가 사용 가능하지 않습니다.

5 문서 갱신사항

이 절에서는 Tivoli Risk Manager 버전 4.2 라이브러리의 갱신된 문서에 대해 설명합니다. 다음 절의 정보를 읽어 라이브러리에 적용되어야 하는 수정사항 및 Tivoli Risk Manager 제품의 개선된 기능을 확인하십시오.

- 기타 문서 갱신사항
- 큐 관리 및 조작
- FFDC 및 기타 추적 문서
- 일반 표현식 지원

5.1 기타 문서 정정사항

이 절에서는 Tivoli Risk Manager 라이브러리에 적용되어야 하는 기타 문서 정정사항과 이 수정팩에서 변경된 기능을 설명하는 문서에 대한 정보가 제공됩니다.

5.1.1 IBM Tivoli Risk Manager Administrator's Guide

- 다음 텍스트가 101 페이지의 Customizing Incident-Based Correlation Rules 절에 추가되어야 합니다.

The <threshold> and <aggregate> elements of the rule determine when to generate an incident. The default rules that are provided with the Tivoli Risk Manager product aggregate events by accumulating the rm_Level value of each sensor event until the thresholdCount value is reached, at which point an incident is generated. The rm_Level value represents the relative weight, or severity, of each event. An alternate method is to count the number of events, and generate an incident when the count reaches a particular threshold count. To enable counting events, remove the <aggregate> element from the rule and adjust the thresholdCount parameter to represent the number of events necessary to generate an incident.

The attributeSet parameter in the <cloneable> element of the rule determines which attributes from the event are used to aggregate incoming events as candidates for a possible incident. The three standard correlation attributes that are used in this parameter are any combination of rm_SourceToken, rm_DestinationTokenand rm_CategoryToken attributes. The following is a list of available attributes names that can be specified in the attributeSet parameter. Unless otherwise noted, the attribute name used in the rule is the same as the attribute name from the incoming events.

- rm_SensorToken
- rm_SourceToken
- rm_DestinationToken
- rm_CategoryToken (synonym for rm_ClassCategory)
- rm_CategoryDescription (synonym for rm_ClassCategoryDescription)
- rm_CustomerID
- rm_Signature
- rm_Timestamp32
- rm_Level

- 다음 변경사항은 103 페이지의 Setting an Attribute to a Specific Value 절에 작성되어야 합니다.

  The <parameters> element in the <action> element of a rule can be used to change the value of any RM_Incident event attribute, with the exception of the hostname and msg attributes.

  The second example on page 103 assigns the msg attribute; this example is incorrect and should be deleted.

- 125 페이지에 있는 Resource IDs and Dynamic Data 절의 첫 번째 단락은 다음과 같이 변경해야 합니다.

  Resource IDs and Dynamic Data: The text displayed in these regions is either specified by hard coded text or a resource ID.

  Hard coding the text is an easier way to code the text, because you only have to update one file and you do not have to stop and restart the WebSphere product for the changes to take affect. Note that is you are using the Tivoli Risk Manager product with a localization pack, you should use the resource ID method.

  To use hard coded text, begin and end the text string with &quot.. Use the following procedure to hard code the text.

  1. Edit the AdvisorRules.xml file.
  2. Add the following line to the file:

     title="&quot.View CVE Recommendation &quot."
  3. Save the AdvisorRules.xml file.

  When the Web page is displayed, *View CVE Recommendations* is displayed in the title area.

  You can also use dynamic data within hard coded text by coding a variable in the string that specifies an event or incident attribute. For example, to display the rm_Category attribute value within hard coded text, the text in step 2 would be coded as follows:

  title="&quot.View Recommendations for &rm_Category Event &quot."

  125 페이지에 있는 Resource IDs and Dynamic Data 절의 나머지는 변경하지 않습니다. 이 정보를 검토하여 동적 데이터 및 자원 ID 사용에 대해 보다 자세히 학습하십시오.

- 47 페이지의 Filtering Attributes 절은 다음과 같이 변경해야 합니다.

  ### Filtering Attributes

  You can filter your attributes so they are not sent to the Tivoli Enterprise Console server.

  You can add a configuration option to the eif_sender.conf file at your agent and distributed correlation server to not send some extended slots to the Tivoli Enterprise Console server.

  For example, add the following line to eif_sender.conf:

  filterAttributes=/opt/RISKMGR/etc/templates/sensorevent_attributeFilter.xml

  For an example of this filtering, see the RMADHOME /etc/templates/sensorevent_attributeFilter.xml file.

- 다음 키워드가 Appendix A, Event Integration Facility Sender and Receiver Keywords 에 문서화되어야 합니다.

  filterAttributes=pathname ...

  Specifies the full path name of one or more XML files that contain attribute filtering specifications. The specifications can be used to filter out extended attributes from

the event before it is transmitted. Attribute filtering is useful for an Event Integration Facility sender subcomponent that is sending events to a Tivoli Event Console server, to eliminate unnecessary network traffic and improve performance.

For a sample attribute filtering specification file, see the following file:

RMADHOME /etc/templates/sensorevent_attributeFilter.xml

ReadRetryInterval=seconds

Specifies the number of seconds the Event Integration Facility receiver waits when a partial event is received. If the receiver determines that the event is a partial event, it waits for the period of time that is specified by this keyword before it retrieves the second packet and completes the process. If the second packet is not received during this period of time, the partial event that was received is discarded and a message is written to the log. The default value is 120 seconds.

- 192 페이지의 Manually Configuring the Event Monitor 절에서 3 단계에 있는 예제가 올바르지 않습니다. 다음과 같이 <source name="monitor_receiver_webids"가 있는 라인을 <source name="monitor_receiver_nids"로 변경해야 합니다.

```
<!-- Event Monitor for NIDS -->
<source name="monitor_receiver_nids"
class="com.tivoli.RiskManager.Agent.Transports.Receivers.rmaMonitorReceiver">
<set key="RMA_conf" value="/opt/RISKMGR/etc/monitor_receiver_nids.conf"/>
</source>
```

- 87 페이지의 Heartbeat Monitoring 절을 다음과 같이 변경해야 합니다.

Tivoli Risk Manager self-monitors the agents deployed in your network and warns you when an agent becomes inactive. The warning is an RMAgent_Inactive event generated at one of your correlation servers. RMAgent_Inactive events are included in the Tivoli Enterprise Console database and viewed on the console. The following warning message is displayed:

Missing heartbeat for agent: *<hostname>/<ip address>*

The *<hostname>* and *<ip address>* are the host name and IP address values for the agent which is no longer sending RMAgent_HeartBeat events.

By default, each agent is configured to generate RMAgent_HeartBeat events. Each correlation server is configured to monitor the RMAgent_HeartBeat events and generate RMAgent_Inactive events when an agent stops sending regular RMAgent_HeartBeat events. By default, there will be an RM_Sensor event created to represent each agent that generates RMAgent_HeartBeat events. The RMAgent_HeartBeat events are not typically forwarded to your Tivoli Enterprise Console server or database.

5.1.2 IBM Tivoli Risk Manager Command Reference

webids -d 명령을 사용하여 디버깅 정보를 표준 출력(STDOUT)에 작성한 다음 다른 파일로 경로 재지정할 수 있다고 25 페이지에 잘못 설명되어 있습니다. 이 옵션은 올바르게 작동하지 않으므로 사용하지 마십시오.

5.1.3 IBM Tivoli Risk Manager 설치 안내서

부록 E, 구성요소 제거에 다음 정보를 포함시켜야 합니다.

Tivoli Risk Manager 구성요소를 설치 제거하기 전에 다음 태스크를 수행하십시오.

1. 모든 Tivoli Risk Manager 어댑터를 종료하십시오.
2. wrmadmin -k 명령을 실행하여 Tivoli Risk Manager 제품을 종료하십시오.
3. 이벤트 서버를 제거 중인 경우, 다음 태스크를 수행하십시오.
   a. 다음 명령 중 하나를 실행하십시오.
      UNIX 의 경우: rmcorr_cfg -delete

      Windows 의 경우: bash rmcorr_cfg -delete

      주: 이 명령이 다음을 수행합니다.

      - 이 명령이 기본 룰 베이스를 로드합니다. 사용자 정의된 룰 베이스를 사용하려면 GUI 또는 wrb 명령을 사용하여 수동으로 로드하십시오.
      - Tivoli Enterprise Console 이벤트 서버를 중지한 후 다시 시작하십시오.

   b. wrmadmin -k 명령을 실행하십시오.
4. 구성요소를 설치 제거하십시오. 제거할 구성요소를 위해 사용해야 하는 명령에 대한 정보는 177 페이지의 표 11 을 참조하십시오.

주:

1. 변경된 Tivoli Risk Manager 파일 또는 추가된 어댑터 파일이 Tivoli Risk Manager 디렉토리에서 제거되지 않았습니다.
2. 이벤트 서버에서 Tivoli Risk Manager 아카이브 테이블, 데이터베이스 보기 및 이벤트 콘솔 이벤트 그룹이 설치 제거 중에 제거되지 않습니다. 이러한 구성요소를 제거하려면 수동으로 제거해야 합니다.

5.1.4 IBM Tivoli Risk Manager 문제점 판별 안내서

다음 정보가 23 페이지의 TME(Tivoli Management Environment) 전송 연결 유형 절에 추가되어야 합니다.

Tivoli Risk Manager 제품의 재설치 시 전송 유형이 TME 로 변경된 경우, TMEEndpoint 키워드의 값을 다음과 같이 /etc/Tivoli/rma_eif_env.sh script 파일에서 true 로 변경해야 합니다.

```
TMEEndpoint=true
```

5.2 큐 관리 및 조작

이 절에서는 APAR IY55319 큐 조작 및 관리의 향상된 내용에 대해 설명합니다. 지속적 큐가 사용하는 디스크 공간을 효과적으로 관리하도록 개선되었습니다. 이 변경에 앞서 이벤트가 확장된 기간 동안 처리된 것보다 빨리 큐에 놓인 경우 Tivoli Risk Manager 제품이 실패하며 관리자에게 원인이 전달되지 않습니다. 이 문제점을 해결하기 위해 큐를 관리하고 관리자에게 큐의 상태를 알려주는 구성 매개변수가 추가되었습니다. 이러한 변경사항에 대한 자세한 정보는 IBM Tivoli Risk Manager Administrator's Guide 의 Queues and Event Persistence 절에 대한 다음 변경사항을 검토하십시오.

큐 및 이벤트 지속성

rmagent.xml 파일에서 커넥터의 설정을 참조하는 에이전트의 각 하위 구성요소에 해당 처리와 연관된 큐가 있습니다. 하위 구성요소가 처리해야 하는 이벤트는 커넥터의 송신자 설정에서 지정된 하위 구성요소가 연관 큐에 놓습니다. 실행 중인 하위 구성요소가 이벤트를 처리할 준비가 되면 큐에서 이벤트를 제거합니다.

지속성 이해

지속성은 rmagent.xml 파일의 persist 매개변수가 제어합니다. 기본적으로, 이벤트가 큐에 놓일 때 디스크에 지속적이게 됩니다. 처리 하위 구성요소가 태스크 완료 시, 이벤트가 디스크에서 제거됩니다. 엔

진과 대상 구성요소 큐 모두를 이벤트가 디스크에 지속적이지 않게 구성할 수 있습니다. 이벤트를 지속하려는지 여부를 판별하기 전에 다음 정보를 주의깊게 검토하십시오.

다음 표는 이벤트 지속성에 관한 정보를 제공합니다.

설명	지속성	비지속성
AI 이벤트가 디스크에 작성됨	예	아니오
실패한 이벤트가 디스크에 작성됨	예	예
큐된 이벤트가 에이전트 중지 시 디스크에(실패한 재시도 이벤트로서) 작성됨	아니오	예
에이전트 시작 시 실패한(재시도) 이벤트가 처리됨	예	예
실패한(영구적) 이벤트가 디스크에 작성됨	예	예

지속성을 해제하려는 이유

디스크에 이벤트 데이터 쓰기 및 나중에 제거하기를 생략하므로 처리가 빨라질 수 있습니다.

지속성을 해제하지 않는 이유

시스템에 에이전트에 사용 가능한 무제한 메모리가 없습니다. 이벤트가 디스크에 지속적이지 않는 경우, 메모리에서 유지보수되어야 합니다. 예기치 않은 오류 조건으로 에이전트가 종결되는 경우 이벤트를 잃지 않고 싶습니다. 지속성을 해제하면 이벤트 데이터를 잃을 수도 있습니다.

지속성을 해제해야 합니까?

지속성 해제 옵션이 더 이상 사용되지 않습니다. 지속성을 사용하도록 강력하게 권장됩니다.

지속성을 해제하려면 rmagent.xml 파일을 편집하고 하위 구성요소 정의에 persist="no"를 추가하십시오. 예를 들면 다음과 같습니다.

```
<destination name="eif_sender"
        class="com.tivoli.RiskManager.Agent.Transports.Senders.rmaEifSender"
        persist="no" >
</destination>
```

큐 관리 및 제어 매개변수

다음 선택적 매개변수는 rmagent.xml 구성 파일에서 <destination> 매개변수와 함께 사용되어 큐의 조작 및 관리를 제어합니다.

- persist
- queueMaxSize
- queueThresholdSize
- queueMessageInterval
- errorRoute

이벤트가 큐될 때 큐의 크기 및 여유 디스크 공간의 양이 평가됩니다. 큐의 크기가 queueMaxSize 및 queueThresholdSize 매개변수가 지정한 크기에 도달하면 RMAgent_QueueProblem 이벤트는 errorRoute 매개변수가 지정한 이벤트 콘솔로 전송됩니다. queueMessageInterval 매개변수가 큐 경고 이벤트가 전송되는 빈도를 제어합니다. 큐될 이벤트가 없거나 큐가 이미 대기 상태 중 하나에 있는 경우, 큐 크기 및 디스크 공간이 평가되지 않으며 큐 경고 이벤트가 생성되지 않습니다.

다음 정보가 각 매개변수의 설명을 제공합니다.

queueThresholdSize

- 이 매개변수가 큐 경고 이벤트가 이벤트 콘솔에 전송되기 전에 도달해야 하는 큐의 크기를 지정합니다. 이 값이 처음으로 도달되면 첫 번째 이벤트가 전송되며 queueMessageInterval 매개변수가 지정한 시간 간격으로 errorRoute 매개변수가 지정한 이벤트 콘솔에 다시 전송됩니다.
- 큐가 이 매개변수가 지정한 크기에 도달하면 해당 구성요소의 처리 이벤트를 중지하지 않습니다.
- 이 매개변수의 값은 0 - 2147483647 의 정수입니다. 기본값 0 은 크기 제한이 없음을 표시합니다.
- 큐가 이 상태에 있으면 해당 상태는 wrmqueue -l 명령이 표시하는 대로 실행 중(THRESHOLD)입니다.

queueMaxSize

- 이 매개변수는 큐가 포함할 수 있는 최대 이벤트 수를 지정합니다. 큐의 이벤트 수가 값에 접근하면 큐에 이벤트를 전송하는 구성요소가 처리를 중지하고 큐 경고 이벤트가 이벤트 콘솔에 전송됩니다. 이 값이 처음으로 도달되면 첫 번째 이벤트가 전송되며 queueMessageInterval 매개변수가 지정한 시간 간격으로 errorRoute 매개변수가 지정한 이벤트 콘솔에 다시 전송됩니다. 기본 간격은 15 분입니다.
- 이 매개변수의 값은 0 - 2147483647 의 정수입니다. 기본값 0 은 크기 제한이 없음을 표시합니다. 이 매개변수의 값은 queueThresholdsize 매개변수 값보다 커야 합니다.
- 큐가 최대 크기에 도달하면 해당 상태는 wrmqueue -l 명령이 표시하는 대로 대기(MAX)가 됩니다.

queueMessageInterval

- 이 매개변수가 다음 RMAgent_QueueProblem 큐 경고 이벤트가 전송되기 전에 시간을 지정합니다(밀리초 단위). 이 매개변수를 사용하여 큐가 queueMaxSize 또는 queueThresholdSize 매개변수로 지정한 크기를 초과하는 경우 전송되는 큐 경고 이벤트의 수를 제한하십시오.
- 기본값은 900000(15 분)입니다.

errorRoute

- 이 매개변수는 queueMaxSize 또는 queueThresholdSize 매개변수 값이 초과되는 경우 큐 경고 이벤트가 전송되는 구성요소(일반적으로 이벤트 콘솔)를 지정합니다.
- 큐 경고 이벤트가 이 라우트의 모든 기타 이벤트와 함께 큐됩니다. 오류 라우트에 별도의 대상 주소를 정의하여 큐 경고 이벤트 전송을 신속히 처리하는데 이 매개변수를 사용하십시오. 이로써, 큐 경고 이벤트가 제때에 확실히 전달됩니다.
- 여러 오류 라우트를 정의할 수 있습니다. RMAgent_QueueProblem 큐 경고 이벤트가 모든 정의된 오류 라우트에 전송됩니다.
- 기본 오류 라우트가 없습니다. 이 매개변수가 지정되지 않은 경우, RMAgent_QueueProblem 큐 경고 이벤트가 전송됩니다.

큐 관리 및 제어 매개변수를 사용하는 예제

이 절에서는 다음 시나리오를 기반으로 큐관리 및 제어 매개변수를 사용하는 예제를 제공합니다.

목표	사용된 매개변수	예제
큐된 이벤트의 수가 100 000 을 초과하지 않도록 확인하십시오.	queueMaxSize	queueMaxSize = "100000"
큐된 이벤트의 수가 10 000 에 도달하면 큐 경고 이벤트를 전송하도록 합니다.	queueThresholdSize	queueThresholdSize="10000"
큐 경고 이벤트가 전송되도록 합니다.	errorRoute	예제는 아래를 참조하십시오.
매분마다 한 번씩 큐 경고 이벤트가 전송되도록 합니다.	queueMessageInterval	queueMessageInterval="60000"

다음 예제가 위에 나열된 목표에 지정된 모든 큐 매개변수를 표시합니다.

```
<destination name = "incident_sender_slow" class =
"com.tivoli.RiskManager.Agent.Transports.Senders.rmaEIFSender" queueMaxSize =
"100000" queueThresholdSize="10000" queueMessageInterval="60000">
 </destination>

<destination name = "error_route" class =
"com.tivoli.RiskManager.Agent.Transports.Senders.rmaEIFSender"
errorRoute="yes">
    <set key="RMA_conf" value="c:₩IBM₩RISKMGR₩etc₩error_route.conf"/>
</destination>
```

큐 관리 이벤트의 예제

이 절에서는 큐 관리 이벤트의 예제를 제공합니다. 부분 이벤트만이 표시됨을 참고하십시오.

- 다음 이벤트는 큐된 이벤트의 수가 **queueThresholdSize** 매개변수로 지정한 큐 임계값 크기에 도달했거나 초과했음을 알려줍니다.

  ```
  RMAgent_QueueProblem
  msg='QueueProblem:Component=db_sender:Reason=The queue threshold size has
  been exceeded.:currentSize=1001:thresholdSize=1000:maxSize=10000"
  severity=WARNING
  ```

- 다음 이벤트는 큐된 이벤트의 수가 **queueMaxSize** 매개변수로 지정한 큐 최대 크기에 가깝거나 초과했음을 알려줍니다.

  ```
  RMAgent_QueueProblem
  msg='QueueProblem:Component=db_sender:Reason=The queue maximum size has
  been exceeded.:currentSize=9992:thresholdSize=1000:maxSize=10000"
  severity=CRITICAL
  ```

- 다음 이벤트는 지속적 큐가 사용 중인 하드 드라이브에 더 이상 사용 가능한 공간이 없음을 알려줍니다.

  RMAgent_QueueProblem
  msg='QueueProblem:Component=db_sender:Reason=The disk the queue is using has no more space available.:currentSize=999:thresholdSize=1000:maxSize=10000" severity=CRITICAL

- 다음 이벤트는 큐가 실패했으며 수동 개입이 필요함을 알려줍니다.

  RMAgent_QueueProblem
  msg='QueueProblem Component=db_sender:Reason=The queue failed for an unknown reason.:currentSize=4567:thresholdSize=1000:maxSize=10000" severity=FATAL

wrmqueue -l command description

wrmqueue 명령의 **-l** 옵션은 다음과 같이 *IBM Tivoli Risk Manager Command Reference* 에서 변경되어야 합니다.

l 또는 -list

이 옵션이 큐에 대한 정보를 나열합니다. 출력이 세 절에 표시되며 다음 정보를 나열된 순서로 제공합니다.

1. 큐 이름, 상태 및 정의
2. 큐의 이벤트 수
3. 실패한 이벤트 수

다음 출력은 **wrmqueue -l** 출력의 예제입니다.

큐 이름	상태	유형	지속
요약	실행 중	엔진	예
eif_sender1	대기(MAX)	송신자	예
eif_sender2	실행 중(THRESHOLD)	송신자	아니오
eif_sender3	대기(DISKFULL)	송신자	예
eif_sender4	실패	송신자	아니오

큐 이름	큐된 수	처리된 수	초당 수
요약	xxxxxxxxxx	xxxxxxxxxx	xxxxx.xx
eif_sender1	xxxxxxxxxx	xxxxxxxxxx	xxxxx.xx
eif_sender2	xxxxxxxxxx	xxxxxxxxxx	xxxxx.xx
eif_sender3	xxxxxxxxxx	xxxxxxxxxx	xxxxx.xx
eif_sender4	xxxxxxxxxx	xxxxxxxxxx	xxxxx.xx

큐 이름	실패 수
요약	ttttttttt(rrrrrrrrr)
eif_sender1	ttttttttt(rrrrrrrrr)
eif_sender2	ttttttttt(rrrrrrrrr)
eif_sender3	ttttttttt(rrrrrrrrr)
eif_sender4	ttttttttt(rrrrrrrrr)

다음 정보가 **wrmqueue** 명령의 **-l** 옵션이 제공하는 출력을 표시합니다.

컬럼 제목	정보 설명
큐 이름	큐 이름.
상태	큐 상태(구성요소가 아님). 상태는 다음 값 중 하나로 표시합니다. 실행 중 — 큐가 문제없이 작동 중입니다. 대기(MAX) — 구성된 최대 큐 크기가 도달했으며 이 큐에 이벤트를 전송 중인 모든 구성요소가 대기 상태에 놓입니다. 실행 중(THRESHOLD) — 구성된 임계값 큐 크기가 초과되었습니다. 대기(DISKFULL) — Tivoli Risk Manager 지속적 파일이 저장된 디스크가 가득 차 에이전트가 공간이 사용 가능할 때까지 대기합니다. 실패 — 큐가 실패했습니다. 이 문제점을 해결하는데 대한 정보는 *Tivoli Risk Manager 문제점 판별 안내서*를 참조하십시오.
유형	이 큐에서 이벤트를 읽는 구성요소 유형은 다음과 같습니다. • 엔진 • 송신자
지속	이벤트가 메모리에 저장되었는지 하드 디스크에 저장되었는지 여부를 표시합니다.
큐에 넣어진 수	구성요소가 처리하는데 사용 가능한 이벤트 수.
처리된 수	에이전트가 마지막으로 시작된 이후 처리가 완료된 이벤트의 수.
초당 수	마지막 **wrmqueue -l** 명령이 실행된 이래 또는 **wrmqueue -l** 명령이 처음으로 실행되는 경우 에이전트가 다시 시작한 이후 초당 처리된 이벤트의 수.
실패한 수	*ttttttttt* 는 에이전트가 마지막으로 시작된 이래 구성요소가 처리할 수 없었던 이벤트의 전체 수입니다. *rrrrrrrrr* 은 에이전트가 다시 시작되면 재시도될 실패한 큐 시도의 수입니다.

5.3 메시지 및 추적 로깅

이 절에서는 새 FFDC(First Failure Data Capture) 기능과 *IBM Tivoli Risk Manager 문제점 판별 안내서*, 2 장의 메시지 및 추적 로깅 및 기타 진단 도구에 대한 기타 변경사항에 대한 정보를 제공합니다.

추적 로깅

Tivoli Risk Manager 제품이 레벨 3 의 추적 세부사항을 제공합니다. 세부사항의 가장 낮은 레벨 DEBUG_MIN 이 기본 레벨입니다. 이 레벨에서는 오류 조건만이 추적됩니다. 다음 두 레벨은 DEBUG_MID 및 DEBUG_MAX 로서 보다 자세한 정보를 제공합니다. 로깅 구성 파일의 매개변수를 변경하거나 로깅 명령행 인터페이스를 호출하여 레벨을 수정할 수 있습니다. 추적 로그 데이터는 현재 영어로만 사용 가능합니다.

모든 추적 정보를 저장하도록 메모리 버퍼가 기본으로 사용됩니다. 이로써 시스템 성능의 추적 영향이 최소화됩니다. 예외 발생 시에만 버퍼가 디스크로 플러시합니다. 디스크에 직접 쓰도록 추적 로깅을 구성하여 예외가 발생하지 않는 경우 추적 데이터를 저장할 수도 있습니다. 추적 로깅을 구성하는 방법에 대한 예제는 "Tivoli Risk Manager 에이전트 및 이벤트 모니터 추적 사용자 정의" 절을 참조하십시오.

추적 로그는 다음 파일 및 디렉토리에 있습니다.

- Linux 및 UNIX 시스템의 Tivoli Risk Manager C 프로그램 추적 로그는 /usr/ibm/tivoli/common/HRM/logs/*<application>*.error.log 에 있습니다. *<application>* 변수가 어플리케이션의 이름을 지정합니다.
- Windows 시스템의 Tivoli Risk Manager C 프로그램 추적 로그는 C:₩Program Files₩ibm₩tivoli₩common₩HRM₩logs₩*<application>*.error.log 에 있습니다. *<application>* 변수가 어플리케이션의 이름을 지정합니다.
- Linux 및 UNIX 시스템의 Tivoli Risk Manager 에이전트 구성요소 추적 로그는 /usr/ibm/tivoli/common/HRM/logs/traceHRM*n*.log 에 있습니다.
- Windows 시스템의 Tivoli Risk Manager 에이전트 구성요소 추적 로그는 C:₩Program Files₩ibm₩tivoli₩common₩HRM₩logs₩traceHRM*n*.log 에 있습니다.
- Tivoli Risk Manager 데이터베이스 유틸리티, wrmdbclose and wrmdbclear 이 추적 레코드를 각각 별도의 파일 traceHRM_DBClose.log 및 traceHRM_DBClear.log 에 작성합니다.

Tivoli Risk Manager 에이전트 및 이벤트 모니터 추적 레코드가 traceHRM*n*.log 라는 순차적으로 번호 지정된 파일에 작성됩니다. 여기서, *n* 은 번호입니다. 추적 로그 프로그램이 최대 5 개의 파일에 각각 1MB 크기로 작성합니다. 5MB 에 적합 가능한 양보다 더 많은 추적 레코드가 작성된 경우, 추적 파일이 랩됩니다. 이러한 추적 파일 제한은 로그 프로그램 구성 파일을 사용하여 모두 사용자 정의 가능합니다. 추적 파일의 수를 변경하려면 file.trace.maxFiles 매개변수를 사용하십시오. 각 추적 파일의 최대 크기를 변경하려면 file.trace.maxFileSize 매개변수를 사용하십시오.

대부분의 로그 메시지는 메시지 로그 및 추적 로그 모두에 작성됩니다. 모든 메시지가 추적 로그에 작성되었는지 확인하려면 추적 파일을 다음과 같이 메시지 로그 프로그램의 listenerNames 에 추가하십시오.

```
rmLogger.msg.listenerNames=file.message file.trace
```

First Failure Data Capture

FFDC(First Failure Data Capture)는 오류 조건 시 추적 정보의 스냅샷입니다. 추적 로깅 구성을 사용자 정의함으로써, 추적 스냅샷이 모든 오류 또는 선택한 오류를 캡처하도록 할 수 있습니다. 각 스냅샷은 후속 추적 스냅샷이 겹쳐쓰지 않는 고유한 추적 파일을 작성합니다. 기본적으로, FFDC 는 Tivoli Risk Manager 제품에서 활성이지 않습니다. 추적 로깅 구성을 변경하여 활성화될 수 있습니다. 구성 변경에 대한 정보는 "Tivoli Risk Manager 에이전트 및 이벤트 모니터 추적 사용자 정의" 절을 참조하십시오. FFDC 스냅샷은 Tivoli Risk Manager 에이전트 및 이벤트 모니터에만 사용 가능합니다.

FFDC 로그는 다음 파일 및 디렉토리에 있습니다.

UNIX 시스템: /usr/ibm/tivoli/common/HRM/FFDC/*YYYY.MM.DD*/traceHRM*n*.log

Windows 시스템: C:₩Program Files₩ibm₩tivoli₩common₩HRM₩FFDC₩*YYYY.MM.DD*₩traceHRM*n*.log

변수 *YYYY.MM.DD* 는 스냅샷이 발생한 날짜이며 *n* 은 주어진 날짜의 스냅샷 순서를 나타내는 숫자입니다.

XML 로깅

다음 메시지 및 추적 로그 레코드 컬럼은 Tivoli Risk Manager 제품이 사용합니다.

Time	Millis	Server
ServerFormat	ProductID	Component
LogText	SourceFile	SourceMethod
Thread	Exception	MessageId
TraceLevel	Severity	

예제

다음 쿼리가 메시지 로그 파일의 내용을 ASCII 로 표시합니다.

```
viewer.sh -sascii /usr/ibm/tivoli/common/HRM/logs/msgHRM.log
```

다음 쿼리가 추적 로그 파일의 내용을 HTML 로 외부 파일에 작성합니다.

```
viewer.sh  /usr/ibm/tivoli/common/HRM/logs/traceHRM*.log > trace_logs.html
```

다음 쿼리가 추적 로그 파일의 선택한 컬럼을 HTML 형식으로 외부 파일에 작성합니다.

```
viewer.sh -q "select
Time,Component,Thread,SourceFile,SourceMethod,LogText,EXCEPTION where true
/usr/ibm/tivoli/common/HRM/logs/traceHRM*.log > trace_logs.html
```

다음 쿼리가 메시지 로그 파일의 선택한 오류 메시지 컬럼을 HTML 형식으로 외부 파일에 작성합니다.

```
viewer.sh -q "select
Time,MessageId,LogText,Component,Thread,SourceFile,SourceMethod where
Severity = 'ERROR'" /usr/ibm/tivoli/common/HRM/logs/msgHRM.log >
error_log.html
```

Tivoli Risk Manager 에이전트 및 이벤트 모니터 추적 사용자 정의

Tivoli Risk Manager 에이전트 추적 로깅은 $RMADHOME/etc/RMLogger.properties 추적 로깅 구성 파일의 매개변수가 제어합니다. 예를 들어, rmLogger.trc.level 매개변수는 에이전트가 실행되는 동안 수집된 추적 정보의 양을 제어합니다. rmLogger.trc.listenerNames 매개변수는 추적 정보가 메모리에 작성되어야 하는지 또는 디스크의 파일에 작성되어야 하는지 제어합니다. 에이전트가 수행하는 추적 로깅의 양을 늘리려면 보다 많은 정보가 캡처되고 해당 정보가 작성되는 대로 디스크에 쓰도록 일반적으로 이러한 매개변수 모두가 변경되어야 합니다.

추적 구성을 변경하는 두 가지 방법이 있습니다.

- RMLogger.properties 파일에 매개변수 값을 변경한 다음 에이전트를 다시 시작하여 영구적으로 변경.

  예를 들어, 다음 절차를 사용하여 에이전트 추적 로깅을 영구적으로 늘리십시오.

  1. $RMADHOME/etc/RMLogger.properties 파일을 편집하여 다음 매개변수를 변경하십시오.
     ```
     rmLogger.trc.level=DEBUG_MAX
     rmLogger.trc.listenerNames=file.trace
     ```
  2. 에이전트를 다시 시작하십시오.

- 명령행 인터페이스 로깅을 사용하여 임시로 매개변수 값을 변경합니다(명령행 인터페이스 로깅 절 참조). 이 방법으로 변경된 사항은 에이전트가 실행 중임을 필수로 하며 에이전트가 실행 중인 동안에만 적용됩니다.

  예를 들어, 다음 절차를 사용하여 에이전트가 실행 중인 동안 에이전트 추적 로깅을 임시로 증가시키십시오.

  1. $RMADHOME/logviewer 디렉토리로 변경하십시오.
  2. 이 디렉토리에서 다음 명령을 입력하십시오.
     logcmd set rmLogger.trc level=DEBUG_MAX
     logcmd set rmLogger.trc listenerNames=file.trace

정보가 많이 로깅될수록 추적 로그가 더욱 커집니다. 추적 파일의 최대 수에 도달하면 이전 추적 데이터가 새 데이터에 의해 겹쳐쓰여집니다. 기본 추적 구성은 각각 1MB 씩 5 개의 추적 파일입니다. 추적 파일 용량을 각각 2MB 씩 10 개의 파일로 늘리려면 다음 명령을 실행하십시오.

```
logcmd set file.trace maxFiles=10
logcmd set file.trace maxFileSize=2048
```

이러한 설정값은 에이전트가 실행 중인 동안에만 적용됩니다. 에이전트를 중지하고 다시 시작하면 이러한 설정값이 기본 설정값으로 되돌아가게 됩니다. 에이전트 실행 중에 에이전트 추적 로깅을 줄이려면 다음 명령을 실행하십시오.

```
logcmd set rmLogger.trc level=DEBUG_MIN
logcmd set rmLogger.trc listenerNames=memory
```

FFDC(First Failure Data Capture) 스냅샷을 사용하려면 다음과 같이 추적 구성을 사용자 정의하십시오.

```
rmLogger.trc.listenerNames=snap.memory
rmLogger.msg.listenerNames=file.message ffdc.snap
```

이러한 모든 구성 변경사항은 이벤트 모니터를 포함하여 모든 Tivoli Risk Manager 에이전트 구성요소에 적용됩니다. 이벤트 모니터를 나머지 다른 에이전트와 달리 구성하려는 경우, 구성 파일 또는 명령행 인터페이스에서 rmLogger.trc 대신에 rmLogger.trc.monitor 를 사용하십시오. 예를 들어, 이벤트 모니터 추적 로깅을 중간 레벨로 설정하고 해당 소유 파일에 작성하려면 다음 매개변수를 설정하십시오.

```
rmLogger.trc.monitor.level=DEBUG_MID
rmLogger.trc.monitor.listenerNames=file.trace.monitor
file.trace.monitor.fileName=trace_monitor.log
```

다음 명령을 실행하여 구성에 정의된 모든 추적 로그 프로그램을 나열하십시오.

```
logcmd list rmLogger.trc
```

다음 명령을 실행하여 추적 로그 프로그램의 현재 설정값을 나열하십시오.

```
logcmd config rmLogger.trc
```

다음 명령을 사용하여 이벤트 모니터 추적 로그 프로그램의 현재 설정값을 나열하십시오.

```
logcmd config rmLogger.trc.monitor
```

5.4 일반 표현식 지원

이 절에서는 APAR IY53527 의 일반 표현식 지원의 향상된 내용에 대해 설명합니다. 일반 표현식 사용에 대한 다음 정보는 *IBM Tivoli Risk Manager Administrator's Guide 에 추가되어야 합니다.*

일반 표현식 지원

IBM Tivoli Risk Manager 버전 4.2 에서 다음 기능이 Tivoli Risk Manager 제품에 대한 일반 표현식 지원의 소개에 있는 이벤트 모니터에 추가되었습니다.

- 사전 필터
- 색인
- 이벤트 패턴을 지정하는 향상된 기능

이 새 기능이 전체 성능을 향상시키고 형식 파일의 작성을 간단하게 합니다. 이제 형식 파일에서 이벤트 패턴을 이전 릴리스에서 제공된 단순한 와일드카드 토큰과 더불어 일반 표현식으로 표현할 수 있습니다.

이러한 새 기능을 구현하도록 Xerces 의 일반 표현식 라이브러리를 사용합니다. Xerces 일반 표현식 일치 엔진은 전통적인 (비 POSIX) NFA(Non-deterministic Finite Automaton) 일반 표현식 엔진의 구현입니다. 라이브러리가 다음과 같이 대부분의 지원되는 일반 표현식 구조를 지원합니다.

구조	기호	설명	예제	결과
단순 문자 클래스	[ ]	문자 클래스(또는 문자 세트)의 기본 양식. 이 구조를 사용하여 여러 문자 중 한 문자와만 일치시키십시오.	gr[ae]y	gray 또는 grey 와 일치합니다.
부정 문자 클래스	[^]	나열된 문자 외에 모든 문자와 일치시킵니다. 대괄호를 연 후에 탈자 기호(^)를 입력하여 문자 클래스를 부정합니다.	gr[^ae]y	gray 및 grey 모두와 일치하지 않습니다.
반복 문자	? * +	이전 토큰과 0 번 또는 한 번 일치 이전 토큰과 0 번 이상 일치 이전 토큰과 1 번 이상 일치		
속기 문자	₩d ₩D ₩s ₩S ₩w ₩W	모든 숫자와 일치 모든 비숫자와 일치 모든 공백 스페이스 문자와 일치 모든 비공백 스페이스 문자와 일치 모든 단어 문자와 일치 모든 비단어 문자와 일치		
점	[.]	거의 모든 문자와 일치합니다. 이 구조 사용 시 주의를 사용하십시오. 점(또는 마침표)은 가장 일반적으로 사용하는 메타문자 중 하나이며 가장 일반적으로 잘못 사용되는 메타문자이기도 합니다.		
Anchors	 ^ $	문자와 일치가 아니라 위치를 표시하는데 사용합니다. 문자 전, 후 또는 사이의 위치에 일치시키며 특정 위치의 regex 일치를 고정하는데 사용합니다. 라인의 시작을 표시합니다. 라인의 끝을 표시합니다.		

단어 경계	₩b ₩B ₩w ₩W	단어 경계를 표시합니다. 전체 단어를 일치시키는데 사용합니다. ₩ b 의 부정 버전 비단어 문자와 일치시키는데 사용합니다. ₩w'의 부정 버전.	₩b(is|art)₩ b	단어 is 또는 단어 art 와 일치시킵니다.
범위	[-]	값의 범위를 지정하는데 사용합니다. 문자 클래스 안에 여러 범위를 지정하거나 범위 및 단어 문자를 결합함을 참고하십시오.	[0-9] [0-9a-fxA-FX]	0-9 의 단일 숫자와 일치시킵니다. 16 진수 또는 문자 X 와 일치시킵니다.
한정기호	{}	한정기호를 사용하여 수량 표현을 확장하십시오. ?, * 및 + 또한 한정기호입니다.	{n} {n,} {n,m}	정확히 *n* 번 일치시킵니다. 최소 *n* 번 일치시킵니다. 최소 *n* 번 일치시키지만 *m* 번 이상은 일치시키지 않습니다.
Lookahead	(?=) (?!)	다음 문자와 일치	q(?=u) q(?!u)	a u 가 다음에 오는 a q 를 일치시킵니다. a u 가 다음에 오지 않는 a q 를 일치시킵니다.
Lookbehind	(?<=)	이전 문자와 일치	(?<=a)b (?<!a)b	문자 a 가 앞에 오는 문자 b 를 일치시킵니다. 문자 a 가 앞에 오지 않은 문자 b 를 일치시킵니다.
그룹 대체	(a|e) gr[ae]y	단일 일반 표현식을 주어진 여러 가능한 표현식에 일치시킵니다. 표현식의 맨 처음 또는 마지막에 '('및')'가 지정되어 있으면 일치가 올바르게 구현되지 않습니다. 이는 Xerces 라이브러리의 문제점으로 인한 것입니다.	gr(a|e)y gr[ae]y (gray|grey)	gray 또는 grey 와 일치시킵니다.

다음 표는 지원하지 않는 구조 및 사용 가능한 대체 구조를 표시합니다.

구조	설명	대체 구조
Unions	두 개 이상의 별도 문자 클래스로 구성된 단일 문자 클래스를 지정합니다. Union 의 예는 [0-4[6-8]]일 수 있으며, 이는 5 를 제외한 0-8 의 모든 수와 일치해야 합니다.	중첩 대괄호를 피하고 동일한 결과를 달성하는 [0-46-8]을 지정하십시오.
교차	공통인 모든 사항과 일치하는 단일 문자 클래스를 지정합니다. 교차의 예제는 [0-4&&[4678]]이며 숫자 4 에 일치합니다. 교차는 Unions 와 유사하면 비슷한 상황에서 사용합니다.	Unions 에 지정된 동일한 대체 구조를 사용하십시오.
빼기	공통 사항을 제외한 모두와 일치하는 단일 문자 클래스를 지정합니다. 빼기는 본질적으로 부정 교차입니다. 빼기의 예제는 [0-9&&[^345]]이며 3, 4 및 5 를 제외하고 0-9 의 모든 숫자와 일치합니다.	분명한 양식으로 표현식을 지정하십시오. 예를 들어, [0-26-9]입니다.

6 추가 또는 대체된 파일

이 절에서는 이 수정팩의 새 파일 및 변경된 파일을 나열합니다. RMADHOME 는 RMADHOME 환경 변수가 참조하는 Tivoli Risk Manager 설치 디렉토리를 나타냅니다.

/etc/init.d/rc.rmagent (Solaris 및 Linux)
/etc/rc.rmagent (AIX)
/etc/Tivoli/rma_eif_env.sh(SUSE Linux 버전 8 이상에서 LD_ASSUME_KERNEL 제거)
RMADHOME /bin/rma_webids-init(UNIX 또는 Linux 전용)
RMADHOME/bin/RMCAH040201.sys(HPUX 전용)
RMADHOME/bin/RMCAL040201.sys(Linux 전용)
RMADHOME/bin/RMCAS040201.sys(Solaris 전용)
RMADHOME/bin/RMCAW040201.sys(Windows 전용)
RMADHOME/bin/RMCAX040201.sys(AIX 전용)
RMADHOME/bin/rmEventLog.dll(Windows 전용)
RMADHOME/bin/webids[.bat]
RMADHOME/bin/wrmadmin[.exe]
RMADHOME/bin/wrmdns(Windows & Solaris 를 제외한 모두)
RMADHOME/bin/wrmqueue(Windows & Solaris 를 제외한 모두)
RMADHOME/dbschema/rm_t_arc41_uc.ms.sql
RMADHOME/etc/incident_engine.conf
RMADHOME/etc/rmagent.dtd
RMADHOME/etc/rmclasspath.conf
RMADHOME/etc/RMLogger.properties
RMADHOME/etc/summary_engine.conf
RMADHOME/etc/tec/rules/riskmanager.wic
RMADHOME/etc/templates/baroc/rmagent.baroc
RMADHOME/etc/templates/incident_engine.conf
RMADHOME/etc/templates/rmagent.dtd
RMADHOME/etc/templates/rmclasspath.conf
RMADHOME/etc/templates/RMLogger.properties
RMADHOME/etc/templates/summary_engine.conf
RMADHOME/etc/templates/tec/rules/riskmgr_config.pro
RMADHOME/etc/templates/tec/rules/riskmanager.wic
RMADHOME/etc/templates/tec/rules/riskmgr_config.pro
RMADHOME/etc/tec/rules/riskmanager.wic
RMADHOME/lib/eif.jar
RMADHOME/lib/evd.jar
RMADHOME/lib/jffdc.jar
RMADHOME/lib/jlog.jar
RMADHOME/lib/rm_dbaccess.jar
RMADHOME/lib/rm_dbutil.jar
RMADHOME/lib/rm_util.jar
RMADHOME/lib/rmagent_msg.properties
RMADHOME/lib/rmagent.jar
RMADHOME/lib/rmeventmonitor.jar
RMADHOME/lib/rmsvrcfg.jar
RMADHOME/logviewer/logcmd.sh(UNIX 또는 Linux 전용)
RMADHOME/logviewer/logcmd.bat(Windows 전용)
RMADHOME/msg_cat/C/rmeif.cat
RMADHOME/nids/templates/rules/www.rules
RMADHOME/reports/rm_ra_03.rpt(Windows 전용)
₩Program Files/ibm/tivoli/common/HRM/scripts/getpd.bat(Windows 전용)
₩Program Files/ibm/tivoli/common/HRM/scripts/getpdinfo.bat(Windows 전용)

/sbin/init.d/rc.rmagent(HP)
/usr/ibm/tivoli/common/HRM/scripts/getpdinfo(UNIX 또는 Linux 전용)

7 소프트웨어 지원 문의

Tivoli 제품에 문제가 있는 경우, 다음 IBM 소프트웨어 지원 웹 사이트를 참조하십시오.
http://www.ibm.com/software/sysmgmt/products/support/

소프트웨어 지원을 문의하려면 다음 웹 사이트에서 IBM Software Support Guide 를 참조하십시오.

http://techsupport.services.ibm.com/guides/handbook.html

이 서적은 문제의 심각도에 따라 IBM 소프트웨어 지원에 문의하는 방법 및 다음 정보를 제공합니다.

- 등록 및 적합성
- 사용자가 속한 국가의 전화 번호 및 전자 우편 주소
- 지원을 요청하기 전에 알아야 할 정보

8 주의사항

이 정보는 미국에서 제공되는 제품 및 서비스용으로 작성된 것입니다.

IBM 은 다른 국가에서는 이 자료에 기술된 제품, 서비스 또는 기능을 제공하지 않을 수도 있습니다. 현재 사용할 수 있는 제품 및 서비스에 대한 정보는 한국 IBM 담당자에게 문의하십시오. 이 책에서 IBM 제품, 프로그램 또는 서비스를 언급하는 것이 IBM 제품, 프로그램 또는 서비스만을 사용할 수 있다는 것을 의미하지는 않습니다. IBM 의 지적 재산권을 침해하지 않는 한, 기능상으로 동등한 제품, 프로그램 또는 서비스를 대신 사용할 수 있습니다. 그러나 비 IBM 제품, 프로그램 또는 서비스의 운영에 대한 평가 및 검증은 사용자의 책임입니다.

IBM 은 이 책에서 다루고 있는 특정 내용에 대해 특허를 보유하고 있거나 현재 특허 출원 중일 수 있습니다. 이 책을 제공한다고 해서 특허에 대한 라이센스까지 부여하는 것은 아닙니다. 라이센스에 대한 의문사항은 다음으로 문의하십시오.

135-270
서울특별시 강남구 도곡동 467-12, 군인공제회관빌딩
한국 아이.비.엠 주식회사
고객만족센터
전화번호: 080-023-8080

2 바이트(DBCS) 정보에 관한 라이센스 문의는 한국 IBM 고객만족센터에 문의하거나 다음 주소로 서면 문의하시기 바랍니다.

IBM World Trade Asia Corporation
Licensing
2-31 Roppongi 3-chome, Minato-ku
Tokyo 106, Japan

다음 단락은 현지법과 상충하는 영국이나 기타 국가에서는 적용되지 않습니다.

IBM 은 타인의 권리 비침해, 상품성 및 특정 목적에의 적합성에 대한 묵시적 보증을 포함하여(단, 이에 한하지 않음) 묵시적이든 명시적이든 어떠한 종류의 보증없이 이 책을 현상태대로 제공합니다.

일부 국가에서는 특정 거래에서 명시적 또는 묵시적 보증의 면책사항을 허용하지 않으므로, 이 사항이 적용되지 않을 수도 있습니다.

이 정보에는 기술적으로 부정확한 내용이나 인쇄상의 오류가 있을 수 있습니다. 이 정보는 주기적으로 변경되며, 변경된 사항은 최신판에 통합됩니다. IBM 은 이 책에 설명한 제품 및(또는) 프로그램을 사전 통고없이 언제든지 개선 및(또는) 변경할 수 있습니다.

이 정보에서 언급되는 비 IBM 의 웹 사이트는 단지 편의상 제공된 것으로, 어떤 방식으로든 이들 웹 사이트를 옹호하고자 하는 것은 아닙니다. 해당 웹 사이트의 자료는 본 IBM 제품 자료의 일부가 아니므로 해당 웹 사이트 사용으로 인한 위험은 사용자 본인이 감수해야 합니다.

IBM 은 귀하의 권리를 침해하지 않는 범위 내에서 적절하다고 생각하는 방식으로 귀하가 제공한 정보를 사용하거나 배포할 수 있습니다.

(1) 독립적으로 작성된 프로그램과 기타 프로그램(본 프로그램 포함) 간의 정보 교환 및 (2) 교환된 정보의 상호 이용을 목적으로 정보를 원하는 프로그램 라이센스 사용자는 다음 주소로 문의하십시오.

135-270
서울특별시 강남구 도곡동 467-12, 군인공제회관빌딩
한국 아이.비.엠 주식회사
고객만족센터

이러한 정보는 해당 조건(예를 들어, 사용료 지불 등)에 따라 사용할 수 있습니다.

이 정보에 기술된 라이센스가 부여된 프로그램 및 이 프로그램에 대해 사용 가능한 모든 라이센스가 부여된 자료는 IBM 이 IBM 기본 계약, IBM 프로그램 라이센스 계약(IPLA) 또는 이와 동등한 계약에 따라 제공한 것입니다.

본 문서에 포함된 모든 성능 데이터는 제한된 환경에서 산출된 것입니다. 따라서 다른 운영 환경에서 얻어진 결과는 상당히 다를 수 있습니다. 일부 성능은 개발 레벨 상태의 시스템에서 측정되었을 수 있으므로 이러한 측정치가 일반적으로 사용되고 있는 시스템에서도 동일하게 나타날 것이라고는 보증할 수 없습니다. 또한, 일부 성능은 추정을 통해 추측되었을 수도 있으므로 실제 결과는 다를 수 있습니다. 이 책의 사용자는 본인의 특정 환경에 대해 해당 데이터를 검증해야 합니다.

비 IBM 제품에 관한 정보는 해당 제품의 공급업체, 공개 자료 또는 기타 범용 소스로부터 얻은 것입니다. IBM 에서는 이러한 비 IBM 제품을 테스트하지 않았으므로, 이들 제품과 관련된 성능의 정확성, 호환성 또는 기타 주장에 대해서는 확신할 수 없습니다. 비 IBM 제품의 성능에 대한 의문사항은 해당 제품의 공급업체에 문의하십시오.

IBM 이 제시하는 방향 또는 의도에 관한 모든 언급은 특별한 통지없이 변경될 수 있습니다.

이 정보에는 일상의 비즈니스 운영에서 사용되는 자료 및 보고서에 대한 예제가 들어 있습니다. 이 예제에는 가능한 완벽하게 개념을 설명하기 위하여 개인, 회사, 상표 및 제품의 이름이 포함될 수 있습니다. 이들 이름은 모두 가공의 것이며 실제 기업의 이름 및 주소와 유사하더라도 이는 전적으로 우연입니다.

라이센스:

이 정보에는 여러 가지 운영 플랫폼에서의 프로그래밍 기법을 보여주는 원시 언어로 된 샘플 응용프로그램이 들어 있습니다. 귀하는 샘플 프로그램의 작성 기준이 된 운영 플랫폼의 응용프로그램 프로그래밍 인터페이스에 부합하는 응용프로그램을 개발, 사용, 마케팅 및 배포하기 위한 목적으로 이러한 샘플 프로그램을 추가 비용없이 어떤 형태로든 복사, 수정 및 배포할 수 있습니다. 이러한 샘플 프로그램은 모든 조건하에서 철처히 테스트된 것은 아닙니다. 따라서 IBM 은 이러한 샘플 프로그램의 신뢰성, 서비스 가능성 또는 기능을 보증하거나 암시하지 않습니다. 귀하는 IBM 의 응용프로그램 프로그래밍 인터페이스(API)에 부합하는 응용프로그램을 개발, 사용, 판매 또는 배포할 목적으로 추가 비용없이 이러한 샘플 응용프로그램을 어떠한 형태로든 복사, 수정 및 배포할 수 있습니다.

이 정보를 소프트카피로 보는 경우에는 사진과 컬러 삽화가 표시되지 않을 수도 있습니다.

상표

다음 용어는 미국 또는 기타 국가에서 사용되는 IBM Corporation 의 상표입니다.

IBM, IBM 로고, Tivoli, Tivoli 로고, AIX, DB2, Tivoli Enterprise Console, TME, pSeries 및 zSeries 는 미국 또는 기타 국가에서 사용되는 IBM Corporation 또는 Tivoli Systems Inc.의 상표 또는 등록상표입니다.

Linux 는 미국 또는 기타 국가에서 사용되는 Linus Torvalds 의 상표입니다.

Microsoft 및 Windows 는 미국 또는 기타 국가에서 Microsoft Corporation 의 등록상표입니다.

UNIX 는 미국 또는 기타 국가에서 사용되는 Open Group 의 등록상표입니다.

Java 및 모든 Java 기반 상표는 미국 또는 기타 국가에서 사용되는 Sun Microsystems, Inc.의 상표입니다.

기타 회사, 제품 및 서비스 이름은 타사의 상표 또는 서비스표입니다.

IBM