FUJITSU

White paper
Integration von PRIMERGY-Servern in HP Systems Insight Manager

Dieses White Paper behandelt die Integration von PRIMERGY-Servern in eine bestehende HP-Serverinfrastruktur mithilfe der Verwaltungstools der PRIMERGY ServerView® Suite.

Content

Einführung

Dieses White Paper behandelt die Integration von PRIMERGY-Servern in eine bestehende HP-Serverinfrastruktur mithilfe der Verwaltungstools der ServerView® Suite (Version 5.00 oder höher). Fujitsu Technology Solutions stellt Tools zur Überwachung von PRIMERGY-Servern in heterogenen Serverfarmen mithilfe von HP Systems Insight Manager zur Verfügung. Systemmeldungen werden mithilfe der Alarm-Management-Funktion von HP SIM weitergeleitet und auf der zentralen Verwaltungskonsole angezeigt. Die Meldungen basieren auf den „Management Information Bases" (MIBs), die in ServerView® enthalten sind. Die ServerView® Suite verwaltet alle PRIMERGY-Server von Fujitsu Technology Solutions.

1 Management Summary

Warum Serververwaltung?

Neue Anwendungen und IT-Konzepte sowie die steigende Komplexität von IT-Strukturen erfordern eine zentrale Serververwaltung. Aufgrund sinkender Budgets sind Verfügbarkeit und Verwaltbarkeit von IT-Systemen wichtiger als je zuvor. Oftmals ist für wichtige Geschäftsanwendungen eine nahezu hundertprozentige Verfügbarkeit erforderlich, wobei Betrieb und Verwaltung von Servern so einfach wie möglich sein sollte.

Erfahrungswerte zeigen, dass rund 80 % der Gesamtbetriebskosten von IT-Systemen nach der Anschaffung anfallen. Dies ist auf die Server- und Netzwerkverwaltung zurückzuführen, die Einhaltung von Sicherheitsstandards und die Ausführung von Wartungsarbeiten. Das PRIMERGY-Verwaltungskonzept für die ServerView® Management Suite unterstützt den reibungslosen Betrieb der IT-Systeme. Die Gesamtbetriebskosten für IT-Infrastrukturen können dank dieser Lösung stark verringert werden.

Obwohl die Verwaltung von PRIMERGY-Servern im Mittelpunkt steht, eignet sich die ServerView® Suite auch für die Integration in fast alle Verwaltungssysteme von Drittanbieter, die auf dem SNMP-Standard basieren.

Warum „Integration"?

Die meisten Verwaltungslösungen von Drittanbietern, die der ServerView® Suite ähneln, bieten zahlreiche Funktionen für die Serververwaltung und die Verwaltung des Server-Lebenszyklus. Zahlreiche Benutzer verwenden diese plattformspezifischen Verwaltungsfunktionen als „ihre" Lösung zur zentralen Serververwaltung.

Sie sind mit den Funktionen der Lösung vertraut, und haben viel Geld in die Schulung ihrer Mitarbeiter investiert, sodass sie nicht bereit sind, groß in zusätzliche Verwaltungstools zu investieren. Daher fordern Benutzer, dass die effiziente Überwachung und Verwaltung von PRIMERGY-Servern mittels der Integration in das bekannte Verwaltungssystem möglich sein sollte, um die Arbeitsbelastung der IT-Mitarbeiter und der plattformspezifische Schulungsbedarf so gering wie möglich zu halten.

Vorteile der ServerView®-Integration

Die Integration von ServerView® in HP SIM bietet folgende Vorteile:

- PRIMERGY-Server werden identifiziert und erkannt.
- Die Verwaltung der PRIMERGY-Server erfolgt über eine zentrale HP SIM-Konsole (ein zentraler Verwaltungspunkt).
- PRIMERGY-Ereignisse werden in der SIM Alarm Console zuverlässig angezeigt, wobei der Schweregrad eines Ereignisses durch verschiedene Farben gekennzeichnet wird.
- Der ServerView® Operations Manager oder der Remote System Monitor bieten detaillierte Analysemöglichkeiten.

Durch die Integration der ServerView® Suite in HP SIM unterstützt Fujitsu Technology Solutions von HP zur Verfügung gestellte Schnittstellen und Richtlinien.

Komponenten der Integration von ServerView®

Die Integration von ServerView® umfasst die folgenden Komponenten, die auf der ServerView® Suite DVD zu finden sind: Software Produkte - ServerView -> Integrationslösungen -> ServerView HP SIM Integration (ServerView® Suite DVD online: http://download.ts.fujitsu.com/prim_supportcd/start.html):

- Dieses White Paper zur Integration von ServerView®
- Fujitsu Technology Solutions MIBs
- Das ServerView® HP Systems Insight Manager Integration Kit (SVToSim.zip):
  - Die MIB-Tools svtosim-loadmibs.cmd, svtosim-domibs.cmd, svtosim-getinfo.vbs, svtosim-unloadmibs.cmd
  - Regeln und Werkzeuge für die Import-Tools von HP Systems Insight Manager (svtosim-single.cmd, svtosim-single-remove.cmd)
  - Skripts zur Aktivierung/Deaktivierung der Integration des Management Controllers von Fujitsu Technology Solutions in HP SIM (iRMC-simintegration-enable.xml, iRMC-simintegration-disable.xml)

2 Lösungen für die Serververwaltung

PRIMERGY ServerView® Suite bietet benutzerfreundliche und umfassende Programme für die Überwachung und Verwaltung von PRIMERGY-Systemen. Die leistungsstarke Alarm-Management-Funktion kann auch über das Internet individuell konfiguriert werden und sorgt für eine rasche und sichere Weiterleitung von Systemmeldungen an Administratoren oder Dienstanbieter. ServerView® verwendet standardisierte Protokolle und Schnittstellen. Administratoren behalten stets den Überblick über den Status des Systems, Verwendungstrends und mögliche Fehlerquellen. Die individuell konfigurierbare Alarm-Management-Funktion stellt sicher, dass Administratoren oder Dienstanbieter rasch reagieren können.

Die ServerView® Suite Verwaltungssoftware besteht aus dem ServerView® Operations Mananger für die Management Station (Manager-/Überwachungsstation) und den ServerView® SNMP Agenten für die zu überwachenden Server.

Der HP Systems Insight Manager umfasst Verwaltungstools für die Überwachung und Verwaltung der HP-Server.

In diesem White Paper wird die Integration von PRIMERGY-Servern in eine HP-Server-Umgebung beschrieben, die vom HP Systems Insight Manager gesteuert wird.

2.1 Integration von ServerView® in HP SIM im Überblick:

- Installieren Sie die ServerView®-SNMP-Agenten auf dem PRIMERGY-Server, sodass sie mit HP SIM kommunizieren können.
- Optional: Installieren Sie zur detaillierten Analyse der PRIMERGY-Server und Generierung von Test-Traps den ServerView® Operations Manager auf einer Management Station Ihrer Wahl.
- Laden Sie die ServerView®-MIBs in HP SIM, sodass das System die von den ServerView®-Agents generierten Ereignisse richtig interpretieren kann.
- Konfigurieren Sie HP SIM entsprechend zur Erkennung der PRIMERGY-Server.
- Testen Sie die Integration.
- Konfigurieren Sie zusätzliche Verwaltungssoftware.

Die Architektur der Integration sieht folgendermaßen aus:

Console	**Management Station**	**PRIMERGY Server**
Web Browser	HP Systems Insight Manager ServerView® Operations Manager (optional)	ServerView Agents

ServerView®-Agents werden auf den zu überwachenden PRIMERGY-Servern installiert. Sie stellen Informationen zur Systemintegrität zur Verfügung und erstellen im Falle von Problemen SNMP-Traps.

Die tatsächliche Überwachungssoftware (HP Systems Insight Manager und der ServerView® Operations Manager) befinden sich auf der Management Station. Es ist jedoch auch möglich, den ServerView® Operations Manager auf einer separaten Management Station zu installieren.

Der Benutzer kann über einen standardmäßigen Internet-Browser auf die Management Station zugreifen.

3 Installation und Konfiguration der ServerView® Suite

3.1 Installation der ServerView® SNMP Agenten

Die ServerView® Agenten können mithilfe des ServerView® Installation Managers gemeinsam mit dem Windows-Betriebssystem oder nach Installation des Betriebssystems mithilfe der ServerView® Suite Software-CD installiert werden.

Die Installation der ServerView® Agenten wird in Kapitel 6 des ServerView®-Installationshandbuchs beschrieben, das sich auf der ServerBooks-CD befindet (im ServerView® Installation Manager Paket enthalten). Eine Online-Version des Installationshandbuchs finden Sie unter: http://manuals.ts.fujitsu.com/serverbooks/

Klicken Sie auf „Industry Standard Servers" - „Software" in der linken Navigationsleiste, dann wählen Sie nacheinander „PRIMERGY ServerView Suite" und „ServerView Suite Installation Manuals" in den beiden Auswahllisten im Hauptfenster.

Nachdem die ServerView®-Agenten auf dem Verwaltungsserver installiert worden sind, müssen Sie den SNMP-Dienst konfigurieren, damit er mit Ihrer HP SIM-Konfiguration übereinstimmt.

1. Konfigurieren Sie die SNMP-Traps, die an die HP SIM Management Station gesendet werden sollen.
2. Konfigurieren Sie den SNMP-Zugriff, sodass HP SIM über SNMP auf den Server zugreifen kann (Leserechte genügen).

Die genaue Vorgehensweise hängt von Ihrem Betriebssystem ab. Einzelheiten finden Sie in der Installationsanleitung für den ServerView® Operations Manager auf der ServerBooks-CD.

Die Konfiguration des SNMP-Zugriffs ist auf Windows-Servern optional, da HP-Sim auch WBEM verwendt um auf die verwalteten Server zuzugreifen. Auf Linux-Servern ist die Konfiguration des SNMPs notwendig.

Die aktuell von HP SIM verwendete SNMP-Community kann folgendermaßen bestimmt werden:

1. Klicken Sie auf „Options -> Protocol Settings -> Global Protocol Settings". „Global Protocol Settings" wird angezeigt.
2. Gehen Sie zum Bereich „Default SNMP settings".
3. Klicken Sie auf „Global Credentials"
4. Klicken Sie auf „OK", um die Einstellungen anzuwenden.

HP SIM kann Bestandsdaten nicht nur aus dem SNMP-basierten Verzeichnis abrufen, sondern auch mithilfe der Web-Based Enterprise Management (WBEM)-Dienste, sofern diese aktiviert und konfiguriert sind. Um die von WMI bereitgestellten Informationen nutzen zu können, müssen Sie folgende Schritte durchführen:

1. Klicken Sie auf „Options -> Protocol Settings -> Global Protocol Settings", setzen Sie ein Häkchen bei ‚Enable WBEM' und klicken Sie auf ‚Global Credentials'. Die Seite „Global Protocol Settings" wird angezeigt.
2. Geben Sie die gewünschte Anzahl an standardmäßigen Benutzernamen und Kennwörtern an. Bei Windows-basierten Systemen muss der Benutzername die Domäne enthalten, beispielsweise Domäne\Benutzername.
3. Um die Suchzeit zu verkürzen, sollten häufig verwendete Root- und Administrator-Kennwörter zuerst aufgelistet werden.
4. Klicken Sie auf „OK", um die Einstellungen anzuwenden.

3.2 Installation des ServerView® Operations Manager

Da der ServerView® Operations Manager Ihnen ausführlichere Informationen über PRIMERGY-Server als HP SIM zur Verfügung stellt, sollte die Lösung auf einer Management Station in Ihrem Netzwerk installiert werden. Es ist ratsam, die Lösung auf demselben System zu installieren, auf dem sich auch HP SIM befindet.

Wenn das Betriebssystem bereits installiert ist, kann der ServerView® Operations Manager mithilfe der Anweisungen auf der ServerView® Suite DVD installiert werden (http://download.ts.fujitsu.com/prim_supportcd/start.html).

Die Installation des ServerView® Operations Manager ist in Kapitel 5 des Installationshandbuchs auf der ServerBooks-CD beschrieben.

Eine Online-Version des Installationshandbuchs finden Sie auch im Internet unter: Eine Online-Version des Installationshandbuchs finden Sie unter: http://manuals.ts.fujitsu.com/serverbooks/

Klicken Sie auf „Industry Standard Servers" - „Software" in der linken Navigationsleiste, dann wählen Sie nacheinander „PRIMERGY ServerView Suite" und „ServerView Suite Installation Manuals" in den beiden Auswahllisten im Hauptfenster.

Hinweis:

Der ServerView® Operations Manager V6.20 sollte nicht für die HP-SIM Integration verwendet werden, da der von HP-SIM generierte SVOM_Aufruf hier zu Probleme führt. Bitte verwenden Sie eine ältere oder eine neuere Version des ServerView® Operations Manager.

4 Laden von ServerView®-MIBs in HP SIM

In den ServerView®-MIB-Dateien werden Ereignisse beschrieben, die von den PRIMERGY-Servern generiert werden. Diese Dateien sind unter „Software CD" im Verzeichnis: Software\ServerView\MIBs zu finden. Die MIBs werden folgendermaßen in HP SIM integriert:

1. Entpacken Sie das ServerView® Integration Toolkit in ein von Ihnen gewähltes Verzeichnis.
2. Entpacken Sie die Datei „SNMPMIBs.zip" in einen Unterordner SNMPMIBs in diesem Verzeichnis.
3. Öffnen Sie ein Befehlsfenster (cmd.exe).
4. Ändern Sie das Arbeitsverzeichnis mithilfe des cd-Befehls in das ServerView® Integration Toolkit Verzeichnis.
5. Geben Sie den Befehl svtosim-loadmibs" ein. Die ServerView®-MIBs werden nun in das MIBs Verzeichnis von HP SIM kopiert, dort kompiliert und in HP SIM integriert. Dieser Vorgang nimmt einige Zeit in Anspruch.

HP SIM kann nun SNMP-Traps interpretieren, die von ServerView® erstellt wurden.

Hinweis:

Wenn das Nutzerkonto, mit dem dieser Vorgang ausgeführt wird, keine Administrator-Rechte unter HP-SIM hat, wird die Kompilation und Integration der MIBs fehlschlagen. Fügen Sie in diesem Fall dem Aufruf einen entsprechendes Nutzerkonto und Passwort hinzu. Z.B.:

```
svtosim-loadmibs.cmd –user "Domain\User" –pwd "Password"
```

5 Konfiguration von HP SIM zur Erkennung von PRIMERGY-Servern

5.1 Erkennung

Wenn ein neues System mittels Ping Sweep oder durch Erhalt eines neuen SNMP-Trap erkannt wird, wird es zur HP SIM-Datenbank hinzugefügt. Der System Type Manager stellt mehrere Anfragen an das neue Gerät, um seine Identität zu bestimmen. Mithilfe der nachfolgenden Schritte können Sie HP SIM so konfigurieren, dass in den ServerView®-MIBs nach Informationen gesucht wird, um dem System Type Manager mitzuteilen, dass es sich bei dem erkannten Gerät um einen PRIMERGY-Server handelt.

Die ServerView® Integration bietet die Möglichkeit, den Device Type Manager über ein Batch-Skript (svtosim-single.cmd) so zu konfigurieren, dass PRIMERGY Server erkannt werden. Zudem konfiguriert es die Custom Management Page in HP-SIM für PRIMERGY Server so, dass entweder der Single System View des ServerView® Operations Managers aufgerufen wird oder der Remote System Monitor der ServerView® Agenten.

Hinweise:

- Die Verwendung des Remote System Monitor erfordert V7.01 oder später der ServerView® Agenten auf dem überwachten Server.
- Die Custom Management Page wird für alle PRIMERGY Server gesetzt. Für Server, auf denen ServerView® Agenten kleiner V7.01 installiert sind, ist dann keine Custom Management Page verfügbar.
- Die Erkennung von PRIMERGY Servern setzt den WMIMapper von HP voraus. Es sollte die aktuellste Version zusammen mit HP-Sim installiert sein.

Führen Sie folgende Schritte aus:

1. Wenn Sie das ServerView® HP-SIM Integration Kit bereits integriert haben, deinstallieren Sie diese Integration, wie in Abschnitt 9 beschrieben.
2. Gehen Sie zum Verzeichnis „\Software\Integration_Solutions\HP_SIM" auf der ServerView® Software-CD.
3. Entpacken Sie SVtoSIM.zip in ein Verzeichnis Ihrer Wahl.
4. Standardmäßig ist verwendet die Integration über das Skipt „svtosim-single.cmd" den ServerView® Operations Manager Single System View als Custom Management Page. Das Skript geht davon aus, dass das ServerView®-Front-End und HP SIM auf der Management Station installiert sind, auf der der Internet-Browser des Benutzers gestartet wird und dass die SNMP Community ‚public' lautet.
   Um eine Integration mit der tatsächlichen Konfiguration zu ermöglichen, können die folgenden Argumente (Groß-/Kleinschreibung wird unterschieden) verwendet werden.
   a. Mit `–mon svom` oder `–mon sysmon` kann festgelegt werden, ob der ServerView® Operations Manager Single System View oder der Remote System Monitor der ServerView® Agenten als Custom Management Page verwendet wird.
   b. Wenn der ServerView® Operations Manager für die Custom Management Page verwendet werden soll, kann mit der Option `–svomserver SERVER` die Zieladresse für den ServerView® Operations Manager geändert werden.

c. Wenn der ServerView® Operations Manager für die Custom Management Page verwendet werden soll, kann mit der Option `–svomcom COMMUNITY` der Name der SNMP Community geändert werden.

5. Öffnen Sie ein Befehlsfenster (cmd.exe).
6. Wechseln Sie in das ServerView® Integration Toolkit Verzeichnis, in dem sich „svtosim-single.cmd" befindet.
7. Rufen Sie „svtosim-single.cmd" mit den zu Ihrer Umgebung passenden Kommandozeilenoptionen auf.

Hinweis:

Folgende Ports werden vom ServerView® Operations Manager benutzt:

Port Number	Usage
3170	Sicherer HTTPS Zugang für SV Operations Manager
3172	Sicherer HTTPS Zugang für System Monitor.

Nachdem nun die neuen PRIMERGY-Server der HP SIM-Datenbank hinzugefügt worden sind (zwei Einträge pro PRIMERGY-Server, einer für ein auf Windows-basierendes System und einer für ein auf Linux basierendes System), ist HP SIM in der Lage, PRIMERGY-Server ordnungsgemäß zu erkennen.

Hinweise:

Wenn das Nutzerkonto, mit dem dieser Vorgang ausgeführt wird, keine Administrator-Rechte unter HP-SIM hat, wird die Integration der Regeln fehlschlagen. Fügen Sie in diesem Fall dem Aufruf einen entsprechendes Nutzerkonto und Passwort hinzu. Z.B.:

```
svtosim-single.cmd –user "Domain\User" –pwd "Password"
```

Wenn der WBEM Service mit W2K8 oder später zur Erkennung verwendet wird, können sehr vereinfachte Regeln für PRIMERGY Server verwendet werden. Diese Version des HP Integration Toolkits unterstützt nur noch PRIMERGY Server mit W2K8 und später oder Linux.

5.2 Ein PRIMERGY System mit W2K3 oder ohne WBEM-Zugriff hinzufügen

Erzeugen Sie mit svtosim-single.cmd als Leitfaden eine Batch-Datei, in der die Regeln sowohl für Windows als auch für Linux enthalten sind. Fügen Sie ein HP SIM Administratorkonto hinzu, wenn nötig:

```
mxstm [--user "<user>" --pass="<password>"] -a -n "<newPrimergyModel>" -p snmp -x type=Server -x priority=1 -x
osname="Microsoft Windows" -x sysoid=1.3.6.1.4.1.311.1.1.3.1.2 -x sysoidrule=3 -x
oid=1.3.6.1.4.1.231.2.10.2.2.5.10.3.1.4 -x oidval="<newPrimergyValue>" -x oidrule=1 -x
url=127.0.0.1:3169/ServerView/ServerView.html?IPAddress=$IPADDRESS&Community=<community>
mxstm [--user "<user>" --pass="<password>"] -a -n "<newPrimergyModel>" -p snmp -x type=Server -x priority=1 -x
osname="Linux"  -x sysoid=1.3.6.1.4.1.8072.3.2.10 -x sysoidrule=3 -x oid=1.3.6.1.4.1.231.2.10.2.2.5.10.3.1.4 -x
oidval="<newPrimergyValue>" -x oidrule=1 -x
url=127.0.0.1:3169/ServerView/ServerView.html?IPAddress=$IPADDRESS&Community=<community>
```

Dabei ist

- <newPrimergyModel> der Name des PRIMERGY Systems das in der ‚All server' Liste angezeigt wird und die entsprechende Regel unter ‚Manage System Types beschreibt
- <newPrimergyValue> der Name des PRIMERGY Systems in exakt der Schreibweise, wie er von SNMP für die OID .1.3.6.1.4.1.231.2.10.2.2.5.10.3.1.4 geliefert wird.
- <community> der Name einer SNMP Community mit Leserecht
- Wenn der SystemMonitor verwendet werden soll, ändern Sie den `url` Parameter zu `https://$IPADDRESS:3172/ssm/desktop/`

Hinweis:

Bei der ServerView® Operations Manager URL wird Groß- und Kleinschreibung beachtet, bei der SystemMonitor URL nicht.

Informationen zum mxstm Kommando finden sich im HP-SIM CLI Guide. Der PRIMERGY Name lässt sich beispielsweise über snmputil ermitteln:

```
snmputil getnext <host> <community> .1.3.6.1.4.1.231.2.10.2.2.5.10.3.1.4
```

Hier ist <host> die IP-Adresse oder der Hostname des neuen PRIMERGY Systems und <community> der Name einer SNMP Community mit Leserecht.

Regeln zur Identifikation eines neuen PRIMERGY Systems können auch direkt in HP-SIM über die Menu-Option ‚Optionen' – ‚Manage System Types' erstellt werden. Nachdem die Liste der bereits existierenden Regeln angezeigt wurde, klicken sie auf ‚Neu' und folgen Sie diesen Schritten:

1. Kopieren Sie die OID 1.3.6.1.4.1.231.2.10.2.2.5.10.3.1.4 in das Feld 'MIB variable object identifier' klicken Sie 'Retrieve from system'. Die OID erscheint im Feld unter 'Retrieve from System'. Geben sie die Community ein und die IP-Adresse oder den Namen des PRIMERGY systems und klicken Sie auf 'Get Response'.
   Der Wert der OID wird unterhalb neben dem Feld 'Response Value' angezeigt. Kopieren Sie den Namen und fügen Sie ihn im Feld 'Object Value' ein.
2. Füllen Sie das Feld 'System Object Identifier' mit der OID 1.3.6.1.4.1.311.1.1.3.1.2 für Windows oder mit der OID 1.3.6.1.4.1.8072.3.2.10 für Linux.
3. Wählen Sie 'Server' in der Combobox 'System Type'
4. Füllen Sie das Feld 'Product Model mit einem Namen zur Identifikation der Regel (dieser Name wird wird in der 'All Servers' Liste angezeigt).
5. Füllen Sie das Feld 'Custom Management Page' mit
   `'https://<SvomServer>:3170/ServerView/serverview.html?IPAddress=$ipaddress&Community=<community>'`
   wobei <SvomServer> der Server ist, auf dem SVOM installiert ist und <community> der Name einer SNMP Community mit Leserecht ist.
   Oder, wenn der SystemMonitor verwendet werden soll, füllen Sie das Feld 'Custom Management Page' mit
   `'https://$IPADDRESS:3172/ssm/desktop/'`

5.3 Erkennung eines PRIMERGY Management Controllers

Management Controller von PRIMERGY-Servern (iRMC S2, iRMC S3, iRMC S4) sind standardmäßig so konfiguriert, dass sie sich auf Anfrage von HP SIM als Management Controller zu erkennen geben. Nachdem ein PRIMERGY-Server und sein Management Controller in HP SIM integriert worden sind, wird der Management Controller automatisch dem Server zugeordnet.

Hinweis:

Der Management Controller iRMC S4 kann nur von neueren Versionen von HP-SIM erkannt werden. Verwenden Sie mindestens V7.4.

Sobald der Management Controller erkannt und zugeordnet worden ist, wird er sowohl über die Serverliste als auch über die Systemseite mit dem Server verbunden. Beachten Sie, dass iRMC stets als „Lights-Out 100" erkannt wird.

Serverliste:

HS Summary: 0 Critical 0 Major 0 Minor 4 Normal 0 Disabled 0 Unknown Total: 4

HS	MP	SW	ES	System Name	System Type	System Address	Product Name	OS Name
				172.17.51.102 in Server rx300s5-pst	Management Processor	172.17.51.102	Lights-Out 100 Remote ...	Embedded
				hpsim-pst Hosted by tx300s4-pst	Server	172.17.55.249		Microsoft Windows Serv...
				rx300s5-pst	Server	172.17.51.2	PRIMERGY RX300 S5	Microsoft(R) Windows(R...
				tx300s4-pst	Server	172.17.50.22	PRIMERGY TX300 S4	Microsoft Windows Serv...

Abbildung 1: Serverliste mit zugeordneten Management Controllern

Systemseite:

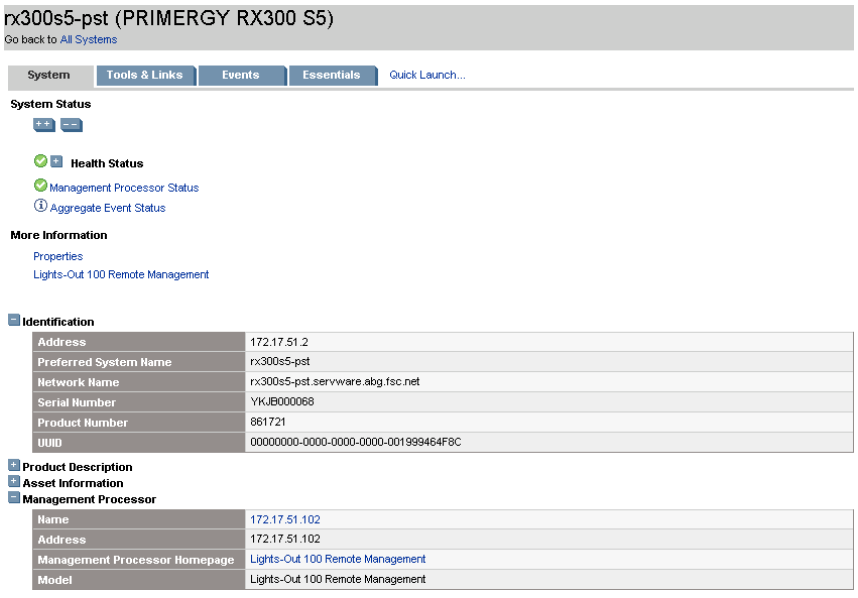


Abbildung 2: Systemseite mit zugeordneten Management Controllern

Wenn Sie die automatische Erkennung und Zuordnung der PRIMERGY-Management Controller nicht wünschen, können Sie diese Funktion über die iRMC-Webschnittstelle deaktivieren. Melden Sie sich bei iRMC an, wählen Sie links in der Navigationsleiste „Server Management", und deaktivieren Sie im Bereich „HP System Insight Manager (HP SIM) Integration Options" das Kontrollkästchen „HP SIM Integration Disabled".

Um die Funktion erneut nutzen zu können, aktivieren Sie das Kontrollkästchen.

Die Funktion zur Integration des Management Controllers in HP SIM kann auch automatisch deaktiviert werden, wenn es sich beim Serverbetriebssystem um ein Windows-Betriebssystem handelt. Kopieren Sie „iRMC-simintegration-disable.xml" in den Ordner %ProgramFiles%\Fujitsu\ServerView Suite\Agents\Server Control\Incoming. Dadurch wird die Datei automatisch bearbeitet. Nach Bearbeitung wird der Name in „iRMC-simintegration-disable.out" geändert. Mithilfe von „iRMC-simintegration-enable.xml" können Sie die Funktion zur Integration des Management Controllers in HP SIM erneut aktivieren.

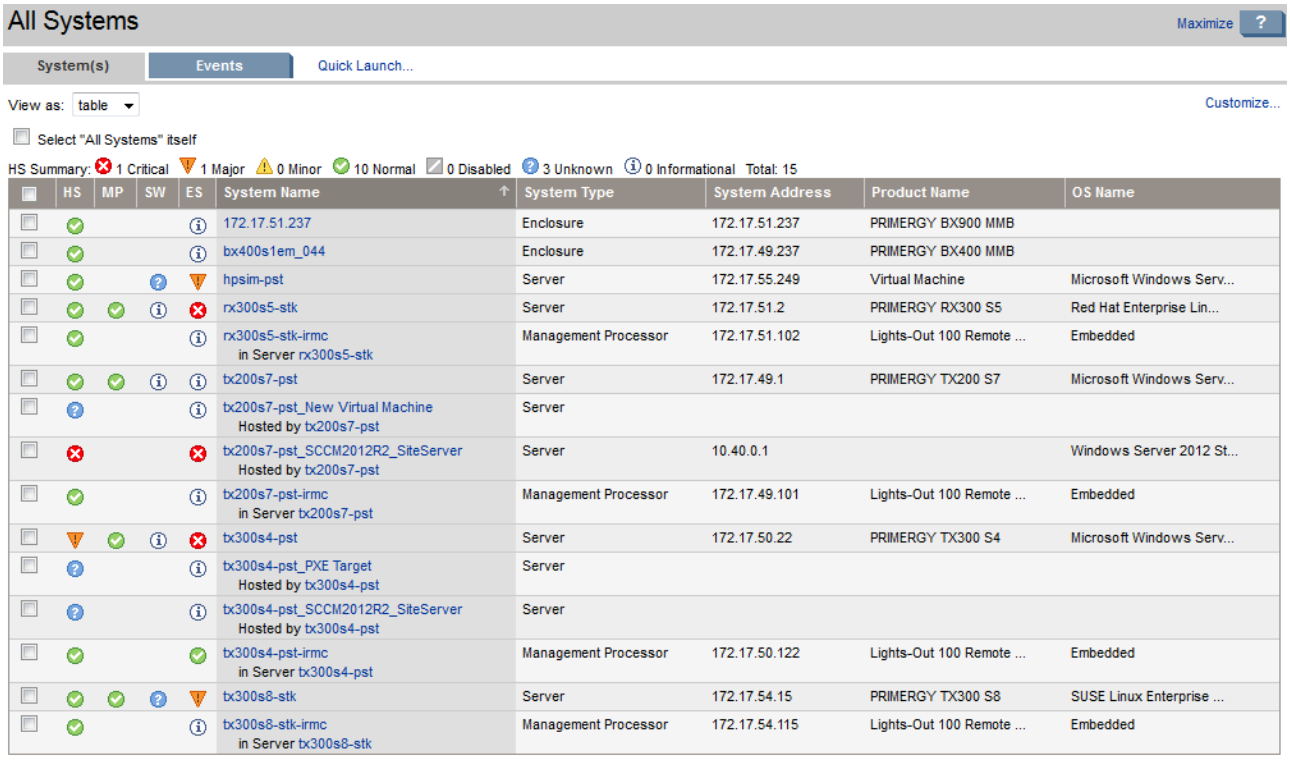
Bei Linux kann die Funktion über die Befehlszeile aktiviert/deaktiviert werden. Geben Sie `„eecdcp -c oc=E002 oe=1968 oi=0 cab=0 0x'01'"` ein, um die Funktion zu deaktivieren, und `„eecdcp -c oc=E002 oe=1968 oi=0 cab=0 0x'00'"`, um sie zu aktivieren.

6 Testen der Integration

6.1 Erkennung von PRIMERGY-Systemen

Nachdem die oben beschriebenen Einstellungen des Device Type Managers durchgeführt wurden, wird jedes PRIMERGY System, das dem HP System Insight Manager nun bekannt ist, automatisch bei den üblichen System-Suchläufen erkannt werden.

Bitte beachten Sie, dass für eine erfolgreiche Integration alle PRIMERGY-Server erneut identifiziert werden müssen. Dazu können Sie sie beispielsweise von der Systemliste entfernen und dann neu identifizieren.



HS	MP	SW	ES	System Name	System Type	System Address	Product Name	OS Name
				172.17.51.237	Enclosure	172.17.51.237	PRIMERGY BX900 MMB	
				bx400s1em_044	Enclosure	172.17.49.237	PRIMERGY BX400 MMB	
				hpsim-pst	Server	172.17.55.249	Virtual Machine	Microsoft Windows Serv...
				rx300s5-stk	Server	172.17.51.2	PRIMERGY RX300 S5	Red Hat Enterprise Lin...
				rx300s5-stk-irmc in Server rx300s5-stk	Management Processor	172.17.51.102	Lights-Out 100 Remote ...	Embedded
				tx200s7-pst	Server	172.17.49.1	PRIMERGY TX200 S7	Microsoft Windows Serv...
				tx200s7-pst_New Virtual Machine Hosted by tx200s7-pst	Server			
				tx200s7-pst_SCCM2012R2_SiteServer Hosted by tx200s7-pst	Server	10.40.0.1		Windows Server 2012 St...
				tx200s7-pst-irmc in Server tx200s7-pst	Management Processor	172.17.49.101	Lights-Out 100 Remote ...	Embedded
				tx300s4-pst	Server	172.17.50.22	PRIMERGY TX300 S4	Microsoft Windows Serv...
				tx300s4-pst_PXE Target Hosted by tx300s4-pst	Server			
				tx300s4-pst_SCCM2012R2_SiteServer Hosted by tx300s4-pst	Server			
				tx300s4-pst-irmc in Server tx300s4-pst	Management Processor	172.17.50.122	Lights-Out 100 Remote ...	Embedded
				tx300s8-stk	Server	172.17.54.15	PRIMERGY TX300 S8	SUSE Linux Enterprise ...
				tx300s8-stk-irmc in Server tx300s8-stk	Management Processor	172.17.54.115	Lights-Out 100 Remote ...	Embedded

Abbildung 3: PRIMERGY-Server in der HP SIM-Serverliste

6.3 Aufruf von ServerView® über HP SIM

Um ausführlichere Informationen zu Ihrem PRIMERGY-Server zu erhalten, können Sie den ServerView® Operations Manager oder den SystemMonitor von der HP SIM-Konsole aus für einzelne Server starten. Dazu sind folgende Schritte erforderlich:

1. Klicken Sie auf der Seite „All Systems" auf den Namen oder die IP-Adresse des Servers, den Sie überprüfen möchten. Die Systemseite wird geöffnet.
2. Klicken Sie auf die Registerkarte „Tools & Links" (siehe Abbildung 5)
3. Wählen Sie den Link „Custom Management Page" aus. In einem ServerView® Operations Manager oder einem Remote System Monitor Fenster werden Details zum ausgewählten PRIMERGY-Server angezeigt (siehe Abbildungen 6 und 7).

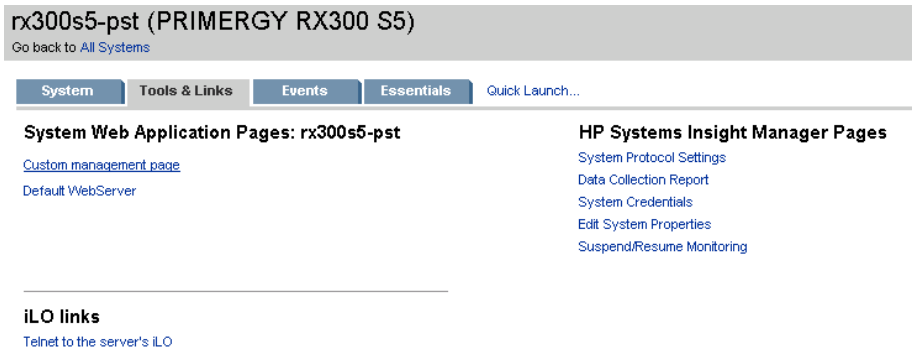


Abbildung 5: Systems Page

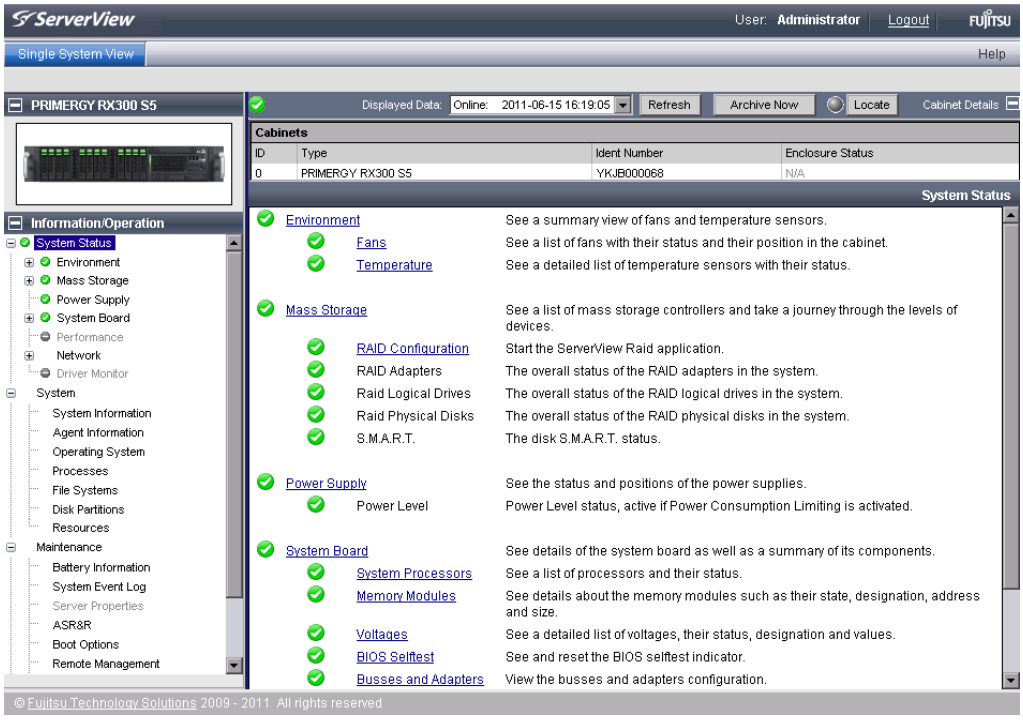


Abbildung 6: ServerView® Operations Manager Einzelserver-Ansicht

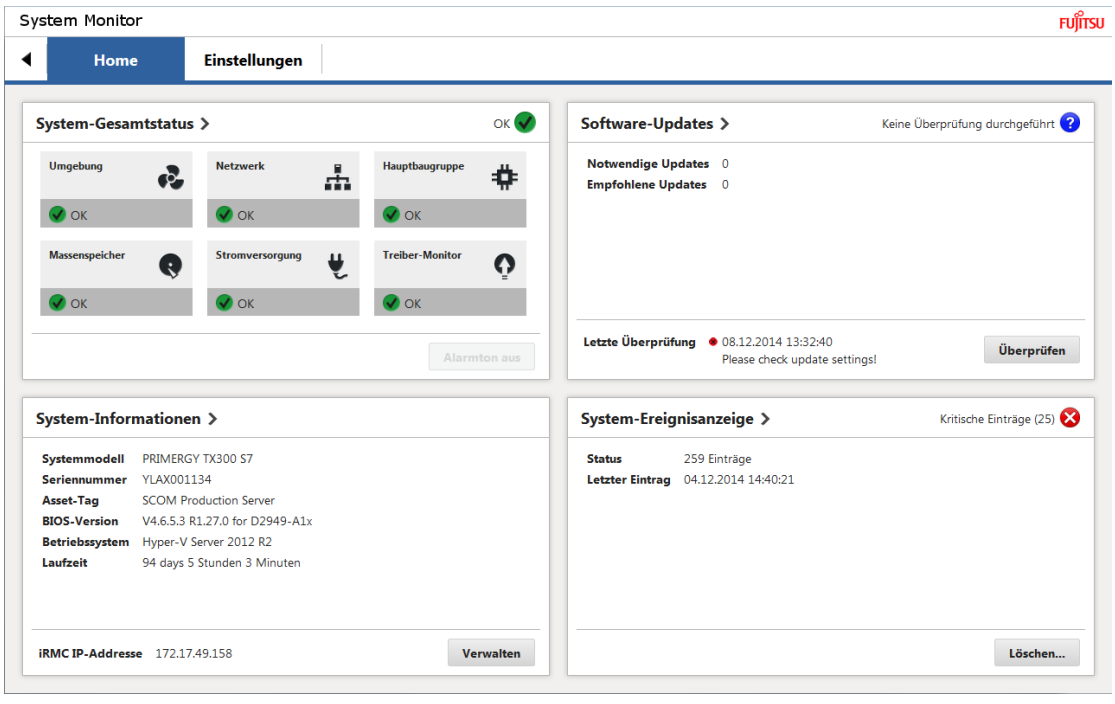


Abbildung 7: Remote System Monitor

6.4 Generierung von Test-Traps

Für Administratoren sind bei den zahlreichen Informationen, die in den MIB-Dateien enthalten sind, insbesondere die Traps und Fehleranzeigen der ServerView®-Agents von Interesse. Wie auf Ereignisse reagiert wird, hängt von ihrem Schweregrad ab. Informations-Traps („informational") dienen Administratoren nur zur Information, während kritische Ereignisse („critical") beispielsweise ein sofortiges Handeln erfordern können.

Um zu testen, ob die Ereignisse vom verwalteten Server korrekt an HP SIM weitergegeben werden, können Test-Traps folgendermaßen erstellt werden:

1. Starten Sie das ServerView®-Front-End. Nach dem Startbildschirm wird die Serverliste angezeigt (siehe Abbildung 7).
2. Klicken Sie mit der rechten Maustaste auf den zu testenden Server, und wählen Sie „Test connectivity" aus.
3. Wählen Sie bei HP SIM im linken Bildschirmbereich „All Events" aus, und prüfen Sie die Ereignisse, die generiert worden sind.

7 Konfiguration zusätzlicher Verwaltungssoftware

Zusätzlich zu den oben beschriebenen Integrationsmethoden gibt es einige HP SIM-Softwarekomponenten, die auch für PRIMERGY-Server geeignet sind. Dazu gehören:

- Vulnerability und Patch Management (VPM)
- Virtual Machine Manager (VMM)
- Remote Ausführung von Aufgaben über SSH

Die Vorgehensweise wird in den folgenden Abschnitten beschrieben.

7.1 Vulnerability und Patch Management (VPM)

Mithilfe der Integration von VPM können Sicherheitsschwachstellen erkannt und beseitigt werden. Um VPM für PRIMERGY-Server zu installieren und zu konfigurieren, sind die folgenden Schritte erforderlich:

1. Installieren Sie VPM auf demselben Server wie HP SIM.
2. Wählen Sie den verwalteten Knoten aus.
3. Setzen Sie den VPM-Agent ein, indem Sie „Deploy -> Vulnerability and Patch Management -> VPM Patch Agent" auswählen.
4. Wenden Sie den Lizenzschlüssel für VPM an, indem Sie „Deploy -> License Manager -> Deploy Keys" auswählen.
5. Identifizieren Sie das verwaltete System erneut. Dadurch erscheint ein Symbol in der Spalte „VPM".
6. Wählen Sie „Tools -> System Information -> System Page" und dann „Vulnerability Status".
1. Sie können alternativ auch das Symbol in der Spalte „VPM" auswählen.
7. Wählen Sie „Scan for Vulnerability", und stellen Sie den Assistenten fertig.

7.2 Virtual Machine Manager (VMM)

Das Virtual Machine Management-Paket umfasst Funktionen zur zentralen Verwaltung und Steuerung von virtuellen VMWare- und Microsoft-Rechnern und stellt einen physischen Host für die Zuordnung virtueller Rechner zur Verfügung.

Sie können VMM in HP SIM folgendermaßen einrichten:

1. Wählen Sie den verwalteten Knoten aus.
2. Stellen Sie den VMM-Agent bereit, indem Sie „Deploy -> Deploy Drivers, Firmware and Agent -> Install VMM Agent -> Windows" auswählen.
3. Prüfen Sie, ob HP SIM die Seriennummer des Systems erkannt hat. Sollte dies nicht der Fall sein, geben Sie die Seriennummer manuell ein (über „Edit System properties"), da die Lizenz ansonsten nicht aktiviert wird.
4. Wenden Sie den Lizenzschlüssel für VMM an, indem Sie die VMM-Serverschlüssel auswählen. Wählen Sie „Deploy -> License Manager -> Deploy Keys" aus.
5. Identifizieren Sie das verwaltete System erneut. Ein grünes Häkchen wird angezeigt.
6. Wählen Sie „Tools -> System Information -> System Page" und dann „Virtual Machines" aus.
   Sie können alternativ auch auf das Symbol in der Spalte „VMM" klicken.

7.3 Remote Ausführung von Aufgaben über SSH

Durch Installation und Konfiguration von SSH können Aufgaben und zeitlich festgelegte Jobs von HP SIM auf PRIMERGY-Servern ausgeführt werden. Geeignet ist beispielsweise OpenSSH.

Nach Installation von OpenSSH kopieren Sie eine Kopie des von SSH generierten öffentlichen Schlüssels von HP SIM auf den verwalteten Server. Wenn Sie den Kopiervorgang über die GUI ausführen möchten, sind folgende Schritte erforderlich:

1. Wählen Sie den verwalteten Knoten aus.
2. Wählen Sie „Configure -> Configure and Repair Agents" aus.
3. Geben Sie die Zugangsdaten eines Administrators des verwalteten Systems ein.
4. Deaktivieren Sie die Funktion „Configure SNMP", da sie nur für HP-Server geeignet ist.
5. Deaktivieren Sie die Optionen „Trust relationship", „Set administrator password for Insight Management Agents version 7.1 or earlier" und „Create subscriptions for WBEM events".
6. Wählen Sie „Configure secure shell (SSH) access" aus und dann „Host based authentication".
7. Klicken Sie auf „Run Now".

8 Einschränkungen und Hinweise

Bei iRMC Controllern mit älteren Firmware Versionen ist die automatische Erkennung und Zuordnung des Management Controllers mit dem Server nicht möglich. Die erforderlichen Minimalversionen der Firmware sind:

- iRMC S1: keine Erkennung möglich.
- iRMC S2: 5.59A
- iRMC S3: 6.27A
- iRMC S4: Jede. HP-SIM Version wenigstens V7.4.

Da es keine HP-Agenten zur Versionskontrolle für PRIMERGY-Server gibt, ist der Status „Management Processor" und „Software" immer unbekannt oder leer.

HP SIM ist nicht in der Lage, für PRIMERGY-Server ein Bild für Blade-Gehäuse anzuzeigen oder den Servern Informationen bezüglich Racks oder Gehäusen zuzuordnen.

Manchmal werden PRIMERGY-Server als „Unknown device" integriert. Dies ist häufig auf fehlgeschlagene SNMP/WMI-Anfragen zurückzuführen. Stellen Sie sicher, dass für SNMP- und WMI-Anfragen die korrekte Authentifizierung verwendet wird. Wenn die globalen SNMP- und WMI-Zugangsdaten für bestimmte Server nicht verwendet werden können, können Sie in den Systemprotokolleinstellungen auf der Seite „Tools & Links" von HP SIM serverspezifische Zugangsdaten einrichten.

Einige PRIMERGY-Server werden nicht als Server erkannt. Dies ist auf HP SIM zurückzuführen, da Server hier mitunter nicht ordnungsgemäß erkannt werden. Der Systemtyp eines Servers kann manuell über die Serverseite „Tools & Links" von HP SIM berichtigt werden, indem Sie „Edit System Properties" auswählen.

Wenn der WBEM Service mit W2K8 oder später zur Erkennung verwendet wird, können sehr vereinfachte Regeln für PRIMERGY Server verwendet werden. Diese Version des HP Integration Toolkits unterstützt nur noch PRIMERGY Server mit W2K8 und später oder Linux.

Der ServerView® Operations Manager V6.20 sollte nicht für die HP-SIM Integration verwendet werden, da der von HP-SIM generierte SVOM_Aufruf hier zu Probleme führt. Bitte verwenden Sie eine ältere oder eine neuere Version des ServerView® Operations Manager.

Der Remote System Monitor kann nur verwendet werden, wenn ServerView® Agents V7.01 oder neuer auf den überwachten Servern installiert ist. Wenn dies nicht der Fall ist, verwenden Sie den ServerView® Operations Manager.

9 Deinstallation der ServerView®-Integration

Die ServerView® Integration wird über ein Batch-Skript (svtosim-single-remove.cmd), das mit dem Kit geliefert wird, de-installiert.

Die ServerView®-Integration lässt sich folgendermaßen deinstallieren:

1. Öffnen Sie ein Befehlsfenster (cmd.exe).
2. Wechseln sie mittels des cd Kommandos in das Verzeichnis, in dem sich die Integration befindet.
3. Rufen Sie „svtosim-single-remove.cmd" auf.
4. Um die MIB –Integration zu entfernen, rufen Sie „svtosim-unloadmibs.cmd" auf.

Hinweis:

Wenn das Nutzerkonto, mit dem dieser Vorgang ausgeführt wird, keine Administrator-Rechte unter HP-SIM hat, wird die Deinstallation der ServerView®-Integration fehlschlagen. Fügen Sie in diesem Fall dem Aufruf einen entsprechendes Nutzerkonto und Passwort hinzu. Z.B.:

```
svtosim-single-remove.cmd –user "Server\Administrator" –pwd "Password"
svtosim-unloadmibs.cmd –user "Server\Administrator" –pwd "Password"
```

Anhang A: ServerView®-MIBs

Gehäuseverwaltung

MIB-Datei	Anmerkung
S31.MIB	Informationen zum Gehäuse des PRIMERGY-Bladeservers zur Verfügung
SC.mib SC2.mib	Stellen detaillierte Informationen zur Integrität eines PRIMERGY-Servers zur Verfügung
Status.mib	Stellt Statusinformationen für verschiedene Subsysteme zur Verfügung
Threshold.mib	Stellt Informationenfür das Leistungsmanagement von ServerView® zur Verfügung
egeneraV1.mib	Stellt Informationen zu PRIMERGY BladeFrame-Systemen zur Verfügung
domagt.mib	Stellt Informationen zu von PrimePower ServerView® verwalteten Domänen zur Verfügung

RAID- und Festplattenverwaltung

MIB-Datei	Anmerkung
RAID.mib	Stellt Informationen zu generischen RAID-Subsystemen zur Verfügung

Contact
FUJITSU Technology Solutions GmbH
Website: ts.fujitsu.com

© Copyright 2016 FUJITSU Technology Solutions GmbH
All rights reserved, including intellectual property rights. Technical data subject to modifications and delivery subject to availability. Any liability that the data and illustrations are complete, actual or correct is excluded. Designations may be trademarks availability. Any liability that the data and illustrations are complete, actual or correct is excluded. Designations may be trademarks availability. Any liability that the data and illustrations are complete, actual or correct is excluded. Designations may be trademarks and/or copyrights of the respective manufacturer, the use of which by third parties for their own purposes may infringe the rights of such owner. For further information see ts.fujitsu.com/terms of use.html