Contacting BMC Software

You can access the BMC Software website at http://www.bmc.com. From this website, you can obtain information about the company, its products, corporate offices, special events, and career opportunities.

United States and Canada

Address  
BMC SOFTWARE INC  
2101 CITYWEST BLVD  
HOUSTON TX  
77042-2827  
USA

Telephone  
▪ 713 918 8800  
▪ 800 841 2031

Fax  
713 918 8000

Outside United States and Canada

Telephone  
(01) 713 918 8800

Fax  
(01) 713 918 8000

© Copyright 1999-2015 BMC Software, Inc.

BMC, BMC Software, and the BMC Software logo are the exclusive properties of BMC Software, Inc., are registered with the U.S. Patent and Trademark Office, and may be registered or pending registration in other countries. All other BMC trademarks, service marks, and logos may be registered or pending registration in the U.S. or in other countries. All other trademarks or registered trademarks are the property of their respective owners. IT Infrastructure Library® is a registered trademark of the Office of Government Commerce and is used here by BMC Software, Inc., under license from and with the permission of OGC.

ITIL® is a registered trademark, and a registered community trademark of the Office of Government Commerce, and is registered in the U.S. Patent and Trademark Office, and is used here by BMC Software, Inc., under license from and with the permission of OGC.

IBM® Tivoli® Business Service Manager, IBM Tivoli Workload Scheduler, IBM Cognos, IBM InfoSphere DataStage, IBM iSeries, IBM Websphere, and AIX® are the trademarks or registered trademarks of International Business Machines Corporation in the United States, other countries, or both.

UNIX® is the registered trademark of The Open Group in the US and other countries.

Linux is the registered trademark of Linus Torvalds.

Oracle and Java are registered trademarks of Oracle and/or its affiliates. Other names may be trademarks of their respective owners.

SAP® R/2 and SAP R/3, SAP Business Objects, and SAP NetWeaver are trademarks or registered trademarks of SAP AG in Germany and in several other countries.

BMC Software considers information included in this documentation to be proprietary and confidential. Your use of this information is subject to the terms and conditions of the applicable End User License Agreement for the product and the proprietary and restricted rights notices included in this documentation.

Restricted rights legend
Customer support

You can obtain technical support by using the BMC Software Customer Support website or by contacting Customer Support by telephone or e-mail. To expedite your inquiry, see “Before contacting BMC.”

Support website

You can obtain technical support from BMC 24 hours a day, 7 days a week at http://www.bmc.com/support. From this website, you can:

- Read overviews about support services and programs that BMC offers
- Find the most current information about BMC products
- Search a database for issues similar to yours and possible solutions
- Order or download product documentation
- Download products and maintenance
- Report an issue or ask a question
- Subscribe to receive proactive e-mail alerts when new product notices are released
- Find worldwide BMC support center locations and contact information, including e-mail addresses, fax numbers, and telephone numbers

Support by telephone or e-mail

In the United States and Canada, if you need technical support and do not have access to the web, call 800 537 1813 or send an e-mail message to customer_support@bmc.com (In the subject line, enter SupID:<yourSupportContractID>, such as SupID:12345). Outside the United States and Canada, contact your local support center for assistance.

Before contacting BMC

Have the following information available so that Customer Support can begin working on your issue immediately:

- Product information
  - Product name
  - Product version (release number)
  - License number and password (trial or permanent)
- Operating system and environment information
  - Machine type
  - Operating system type, version, and service pack or other maintenance level such as PUT or PTF
  - System hardware configuration
• Serial numbers
• Related software (database, application, and communication) including type, version, and service pack or maintenance level
  ▪ Sequence of events leading to the issue
  ▪ Commands and options that you used
  ▪ Messages received (and the time and date that you received them)
    • Product error messages
    • Messages from the operating system, such as file system full
    • Messages from related software

License key and password information
If you have questions about your license key or password, contact BMC as follows:
  ▪ (USA or Canada) Contact the Order Services Password Team at 800 841 2031, or send an e-mail message to ContractsPasswordAdministration@bmc.com.
  ▪ (Europe, the Middle East, and Africa) Fax your questions to EMEA Contracts Administration at +31 20 354 8702, or send an e-mail message to password@bmc.com.
  ▪ (Asia-Pacific) Contact your BMC sales representative or your local BMC office.

Third party Software
For the provisions described in the BMC License Agreement and Order related to third party products or technologies included in the BMC Product, see https://docs.bmc.com/docs/display/workloadautomation/Control-M+Workload+Automation+Documentation and click Third-party software (TPS).
Contents

BMC Control-M – An IT workload automation platform....................................................... 6
Using standard agent-based scheduling............................................................................ 6
Remote Host scheduling ................................................................................................. 7
Remote Host architecture ................................................................................................ 7
Adding a new remote host .............................................................................................. 9
Automatic definition........................................................................................................................ 9
Manual definition (Advanced mode)......................................................................................... 9
Monitoring remote hosts in the BMC Control-M Configuration Manager ......................... 10
Versions, platforms, and configuration – Questions and Answers (Q&A) ......................... 10
Load balancing remote host jobs ................................................................................... 13
SSH ............................................................................................................................................. 13
WMI ............................................................................................................................................ 13
Remote host jobs management in BMC Control-M/Agent ...................................................... 13
Host (Node) group support ........................................................................................................... 14
Handling network disconnections .................................................................................... 14
Management – Questions and Answers (Q&A) ................................................................. 15
Security – Questions and Answers (Q&A) ......................................................................... 16
Command line support.................................................................................................. 18
Agent utilities............................................................................................................... 19
Agent or Remote Host?........................................................................................................ 19
Remote host recent enhancements ................................................................................ 20
BMC Control-M/Agent 8.0.00................................................................................................. 20
Summary..................................................................................................................... 21
BMC Control-M – An IT workload automation platform

Job Scheduling has evolved to a point where it is a critical part of the business process, not just a segment of IT. Process and workload automation are well integrated in most business practices and are essential for the success of every modern organization around the globe. BMC Control-M is a leading workload automation broker and an enterprise scheduling solution, allowing customers to automate and integrate online and batch processes that support the bottom line across multiple platforms and applications.

From a single point of management, BMC Control-M provides workload automation and scheduling control over multiple platforms and applications across the enterprise. This solution maximizes automation by providing cross-application and cross-platform scheduling capabilities, such as job dependencies, workload balancing, management by exception, and status-based job execution.

BMC Control-M prevents scheduling problems from developing into business problems. The solution’s proven success record maximizes data center hardware and software investments over multiple platforms, merging new and traditional technologies to effectively manage heterogeneous environments.

BMC Control-M:

- Automates the details of production management
- Minimizes manual intervention in the production process
- Reduces manual errors and costs, streamlining the production flow
- Simplifies production management through user-friendly capabilities

Using standard agent-based scheduling

Conventional enterprise scheduler architecture is based on centralized servers managing job definitions and executions, with agents installed throughout the enterprise on every host upon which jobs are executed. These agents are responsible for the actual job submission in the target operating system, as well as their tracking and the analysis of each job’s completion results.

Such an architecture allows the reliable running of high-volume workloads. The agent components are run with administrator (root) authorization levels and therefore the overhead of the security management is minimal. On the other hand, such an architecture can increase the enterprise scheduler total cost of ownership, due to the necessity to install the agent components on a high number of hosts, apply ongoing software updates, and administer the software configuration. In addition, having the agent run as administrator on the remote host might be considered a security issue by some sites.
Remote Host scheduling

Remote host solution is a revolutionary technology that can dramatically reduce the total cost of ownership of a workload automation solution by significantly decreasing its footprint throughout the IT landscape. It allows users to manage jobs on remote hosts while maintaining zero footprint on the managed servers. The remote host solution is based on standard and secured communication technologies (SSH and WMI) and is a highly scalable solution.

The remote host solution can be mixed with conventional agents. The question of whether a job submission to a host is performed by using conventional agents or the remote host solution is entirely transparent to the end user.

BMC Control-M remote host technology provides first-day support for new platforms and operating systems releases. It requires no migration or changes to existing job definitions.

Remote Host architecture

To the person defining the scheduling definition or monitoring the scheduling production activity, it is entirely transparent if there is a BMC Control-M/Agent installed or if the jobs are submitted using remote host scheduling. This configuration is controlled by the Control-M administrator, using the Control-M Configuration Manager.

When installing BMC Control-M/Server, a BMC Control-M/Agent is automatically installed as well. This agent is referred to as <local> and can be used to submit jobs to remote hosts.

BMC Control-M remote host scheduling is scalable and designed for high-availability configurations. Multiple BMC Control-M/Agents can be used to submit and manage jobs on remote hosts. This ability allows users to balance the workload of the remote host jobs’ management between multiple hosts running BMC Control-M/Agents, while avoiding a single point of failure. The remote host technology is based on market standard technologies, providing secure and reliable communication.
Control-M Best Practices - Remote Host

SSH (Secure Shell) is a package available out of the box with all tier-1 UNIX® platforms (HP, AIX®, Solaris™, Linux®) and additional platforms, such as iSeries and OpenVMS. It is also available for Microsoft Windows and most tier-2 platforms as complementary packages (OpenServer, UnixWare, IRIX, NCR). When using SSH, you can use either a user/password authentication or SSH private/public keys.

WMI (Windows Management Instrumentation) is a Microsoft Windows-based API available out of the box on all Microsoft Windows platforms. When using BMC Control-M remote host technology, the BMC Control-M/Agent that submits and manages the job connects to the remote host that runs the job using the credentials of the job owner, which is a user defined on the remote host operating system.

The job owner’s credentials (either user/passwords or SSH keys) are stored encrypted in the BMC Control-M/Server database. These credentials can be managed by using the BMC Control-M Configuration Manager graphical interface or a command line utility.
Adding a new remote host

Automatic definition

When submitting a job to a new remote host, BMC Control-M/Server first checks if there is a BMC Control-M/Agent running on this host. If not, it tries to connect to the remote host using the default remote settings. These settings define the communication protocol to be used (SSH or WMI), communication port, and the BMC Control-M/Agents that will be used for submitting and managing the jobs on this remote host.

Manual definition (Advanced mode)

New remote hosts can also be added manually to the BMC Control-M topology, without first running jobs on them. This can be done interactively using the new remote host wizard in the BMC Control-M Configuration Manager or using a command line utility in batch mode.

Using the same interfaces, existing BMC Control-M/Agents can also be converted to remote hosts.
Monitoring remote hosts in the BMC Control-M Configuration Manager

Remote host components are displayed in BMC Control-M Configuration Manager at the same hierarchy level as BMC Control-M/Agent.

The availability status of each remote host is displayed, along with the operating system details and the list of BMC Control-M/Agents that can manage jobs on it.

Versions, platforms, and configuration – Questions and Answers (Q&A)

Question
Which BMC Control-M/Agents can communicate with remote hosts? For example, can I use BMC Control-M/Agent for iSeries or Tandem?

Answer
- The BMC Control-M/Agents that can be used to manage jobs on remote hosts are BMC Control-M/Agent for UNIX, Linux, and Microsoft Windows
- When using WMI, the BMC Control-M/Agent that is used to connect to the remote host must be installed on a Microsoft Windows platform

Question
Will the use of remote host scheduling affect my BMC Control-M license?

Answer
No. The remote host scheduling is licensed in exactly the same way as traditional agent-based scheduling: per tasks or per managed servers

Question
On what platforms can I run jobs in the remote host mode?

Answer
- When using SSH, jobs can run in the remote host mode on:
  - All UNIX flavors
  - All Microsoft Windows platforms
Control-M Best Practices - Remote Host

- Linux
- z/OS USS (Agent 6.4 or higher)
- OpenVMS (Agent 6.4 FP1 or higher)
- When using WMI, jobs can run in the remote host mode on all Microsoft Windows platforms supported by Control-M.

**Question**
What versions of SSH communication protocol are supported and how can I verify that the version that is used by my SSH server is supported?

**Answer**
SSH communication protocol 2 is supported.

- Run `ctmping -nodeid <remote host name>`.
- If your SSH server does not support protocol version2, you will find a descriptive message in BMC Control-M/Agent log.

**Question**
How can I convert conventional BMC Control-M/Agent definitions to remote hosts?

**Answer**
Shut down the BMC Control-M/Agent(s).

- If only a few BMC Control-M/Agents are being converted, use the BMC Control-M Configuration Manager. Right click on each BMC Control-M/Agent entry and select the “Convert to Remote Host” option.
- If a large number of BMC Control-M/Agents need to be converted, use `ctmhostmap`. Before the conversion, define all jobs owners using the BMC Control-M Configuration Manager (interactive) or using the `ctmsetown` utility (batch).

**Question**
Where should I install the BMC Control-M/Agent that will be used to access remote hosts?

**Answer**
During the installation of BMC Control-M/Server, BMC Control-M/Agent is installed on the same host and identified as `<local>` in various dialogs and is used by default. Additional BMC Control-M/Agents can be installed on other machines to balance the workload or as desired.

**Question**
I would like to run jobs in remote host mode on UNIX and Windows clusters. Are there any considerations for using “virtual” names for remote hosts.

**Answer**

- The use of virtual hostnames for communicating with remote hosts is supported both with SSH and WMI remote hosts.
- When the virtual hostname represent more than a single physical server (for example, when communicating with a cluster), use the “Authorize SSH Known Hosts…” option in BMC Control-M configuration manager to add SSH signatures for each of the physical hosts.
- No configuration changes are required when using WMI.
Control-M Best Practices - Remote Host

Question
Can I install BMC Control Modules on remote hosts?

Answer
Control Modules are installed on conventional BMC Control-M/Agents. Note however, that the number of instances required for most Control Modules is very small. For example, a single installation of the Control Module for SAP can schedule and manage all SAP jobs on multiple SAP instances within an organization.
Load balancing remote host jobs

The amount of concurrent remote host jobs that can be managed on a remote host is dependent upon the resources available from the operating system, such as number of concurrent processes and threads, file descriptors, available memory, and disk space.

SSH

- SSH servers allow unlimited number of concurrent sessions. By default, some SSH servers are configured to limit the amount of concurrent logins, but this limitation can be configured. Note that this limitation does not refer to the amount of concurrent sessions, but rather to the login procedure and the credentials authentication process.
- Control-M/Agent initiates two network sessions (SSH & SFTP) for each job submitted to a remote host.
  - On UNIX and Linux operating systems, the SSH session is terminated shortly after the job is submitted and the SFTP session is kept for monitoring the submitted job.
  - On Windows, both sessions are kept open during the entire job execution.
- Each network session can generate one or more system processes. This differs from one operating system flavor to another.
- Starting from Control-M Agent 8.0.00 there is SSH connection pool that Jobs can share if they run on the same remote host with the same owner.
- In some operating systems, the maximum number of processes that can be initiated by the same user should be adjusted to the amount of current remote host jobs running by the same job owner.

WMI

WMI allows the running of around 100 concurrent jobs in the remote host mode. This volume depends purely on the operating system and hardware capacity. Each job submitted to a remote host using the WMI interface is represented by a single process on the remote host. This limitation only applies to concurrent runs – there is no technical limitation on the overall number of jobs.

Remote host jobs management in BMC Control-M/Agent

Each BMC Control-M/Agent can submit and manage several thousands of concurrent jobs on a single or multiple remote hosts. There is no “daily” limitation beyond the capacity of the operating system and hardware. Calculating the number of jobs that a single BMC Control-M/Agent can manage on remote hosts can be done by estimating the amount of conventional “local” jobs that the agent machine can run. Each “local” job is represented by a single process or thread on the BMC Control-M/Agent machine. Each job submitted to a remote host is also represented by a single process or thread on the BMC Control-M/Agent machine.

Therefore, if a certain machine can manage 2,000 concurrent “local” jobs, it can also submit and manage 2,000 remote host jobs to remote hosts or 1,000 “local” jobs and 1,000 remote host jobs.
Host (Node) group support

Host (Node) Groups include definitions of logical node names, which represent either BMC Control-M/Autodiscovery or remote hosts connected using the remote host technology. When submitting jobs to a node group, the jobs are balanced between all the nodes in the group, regardless of whether these are conventional agents or remote hosts.

Handling network disconnections

The ability to handle network disconnections between BMC Control-M/Agent and a remote host includes several configuration parameters controlling the number of connection retries and timeouts. These parameters can be configured via the BMC Control-M Configuration Manager.
Management – Questions and Answers (Q&A)

**Question**
How can I find out which remote hosts can be accessed by each BMC Control-M/Agent and which BMC Control-M/Agent can access which remote hosts?

**Answer**
In BMC Control-M Configuration Manager, use the “Show Remote Hosts” option from the BMC Control-M/Agent context menu and “Show Agents” in the remote host context menu.

**Question**
Some of the servers where I need to schedule jobs are located in areas with unstable networks. Can BMC Control-M handle network disconnections for the remote host jobs?

**Answer**
- Network disconnections can be recovered, regardless of whether they occur between BMC Control-M/Server and BMC Control-M/Agent (any version) or between BMC Control-M/Agent and a remote host, and regardless of whether the jobs are still running or if they have ended.
- Recovery from network disconnections is supported when you use remote hosts on UNIX, Linux, and OpenVMS (by using SSH) and when you use remote hosts on Windows (by using WMI).

**Question**
How can I check the connection status of a remote host?

**Answer**
The status of all remote hosts (along with all other BMC Control-M components) is displayed in the BMC Control-M Configuration Manager. The status is periodically updated. To initiate a manual update, right click on a remote host entry and select Ping.

**Question**
Can remote host jobs include shout post-processing actions?

**Answer**
Yes. Shouts to MAIL are performed by the BMC Control-M/Agent that is used to manage the jobs on the remote host. Other types of shouts are performed by BMC Control-M/Server (as with jobs running on conventional BMC Control-M/Agents).

**Question**
Can I submit jobs from different BMC Control-M/Servers to the same remote host?

**Answer**
Yes. Each BMC Control-M/Server connects to the remote host individually using a unique connection. You can use the same job owner for multiple jobs running simultaneously, managed by different BMC Control-M/Servers.

**Question**
Can jobs running on remote hosts access network resources from the node they run on?
Answer

- When the remote host is configured for SSH communication mode, jobs can access any network resource.
  For example, when running a script located on central repository server, having a batch program accessing a shared folder or printing the job’s output to a network printer.

- When the remote host is configured for WMI communication mode, such network resources can be accessed when the job owner is a domain user and the DELEGATE impersonation level is granted to the user and to any computer included in the chain of calls.
  This authorization is granted on the domain controller server using the “Active directory Users and Computers” interface.

Question

Where are Output (Sysout) handling post processing actions, such as copy or move Output, performed?

Answer

By default, Output handling post processing actions are performed on the BMC Control-M/Agent that submit and track the jobs.

- You can set the RJX_COPY_OUTPUT_REMOTE parameter value to Y in BMC Control-M/Agent OS.dat file to enable the Output handling on the remote host instead.

- This ability requires BMC Control-M/Agent 6.4.01.100 (fix-pack 1)

Question

The jobs I run on a certain remote host generate a very large Output. Can I disable the Output copy from the remote host to BMC Control-M/Agent?

Answer

You can configure BMC Control-M/Agent not to copy Output files from remote hosts to the agent computer when those jobs complete by setting the “Download Output from Remote Host when job ends” parameter value to N in the BMC Control-M Configuration Manager.

- When this mode is configured, the view Output action is not available for the remote host jobs managed by this BMC Control-M/Agent and ON statement defined in the jobs are ignored.

Security – Questions and Answers (Q&A)

Question

I am planning to run jobs on a Windows-based server in the remote host mode using WMI interface. What are the security-related aspects I should be aware of?

Answer

The BMC Control-M job owner must be a member in the Windows “Administrators” authorization group. In addition, in order to perform post-processing actions (analyze the job’s Output), and view/edit the jobs script, you must have the Outputs folder shared and available for BMC Control-M/Agent user.
Control-M Best Practices - Remote Host

**Question**
The servers that I plan to run jobs on are located behind a firewall. Can I schedule the jobs using the remote host technology?

**Answer**
- When using SSH, you should open the SSH server port (default is 22) in the firewall. SFTP port is the same.
- When using WMI, open the WMI RPC port (default is 135) and the Microsoft Directory Services port (default is 445) for the Outputs shared folder.
- Alternatively, you can install BMC Control-M/Agent behind the firewall to be used as the remote host interface and use persistent connection mode for the communication between BMC Control-M/Server and BMC Control-M/Agent.

**Question**
My organization uses Active Directory and NIS to maintain identical credentials for each user on all servers. Do I still need to create separate settings for each user/host in Owners Authentication Settings?

**Answer**
No. Use the <All> selection for the hostname field in the “Owners Authentication settings” dialog.

**Question**
Assuming I need to change the job’s owner’s passwords every ‘x’ days, how can I automate this procedure?

**Answer**
- All remote host authentication management can be done via BMC Control-M Configuration Manager interactive interface or the BMC Control-M/Server command line interfaces: ‘ctmsetown’ & ‘ctmkeygen’.
- The ‘ctmsetown’ utility is available both at the BMC Control-M/Server and the BMC Control-M/Agents accounts. When running the ‘ctmsetown’ utility via BMC Control-M/Agent, only the password update action is available.

**Question**
I am planning to upgrade remote host hardware in the near future. Will it have any effect on BMC Control-M?

**Answer**
- If WMI is used, there is no effect and no configuration changes are required.
- When using SSH communication protocol, run the “Authorize SSH Known Hosts...” option in BMC Control-M Configuration Manager for the remote host server.
  - This action is available with BMC Control-M/EM 6.4.01.200 (fix-pack 2) or higher and BMC Control-M/Agent 6.4.01.100 (fix-pack 1) or higher.
  - When running previous versions of those BMC Control-M components, the host entry in the ‘known_hosts’ file in each relevant BMC Control-M/Agent should be manually deleted.
Question
What types of SSH keys are supported?
Answer
OpenSSH and SSH2

Question
How are SSH keys created and managed?
Answer
- Remote host SSH keys can be created and managed using the “Manage Agentless SSH Keys” in BMC Control-M Configuration Manager, available with BMC Control-M/EM 6.4.01.200 (fix-pack 2) or higher and BMC Control-M/Server 6.4.01.200 (fix-pack 2) or higher.
- Then the key can be selected for the relevant owner and hosts in the Owner’s Authentication Settings dialog.
- The private keys are saved in the BMC Control-M/Server database (encrypted) and the public keys are stored in files that should be deployed on the remote hosts SSH servers.
- When using previous versions of those product components, use the ‘ctmkeygen’ utility in BMC Control-M/Server.

Question
How many SSH keys do I need?
Answer
You can use the same SSH key for several job’s owners or use a dedicated SSH key for each owner. This decision should be taken according to your site security policy.

Question
Which users can update job owner’s credentials?
Answer
- When updating the credentials using the BMC Control-M Configuration Manager, the ability to manage credentials is set in the BMC Control-M/EM Authorization settings.
- When updating the credentials in batch, you can run the ‘ctmsetown’ utility from the BMC Control-M/Server account or from BMC Control-M/Agent (for passwords changes).

Command line support
Most remote host configuration tasks can be performed either via the BMC Control-M Configuration Manager graphical interface or using command line utilities. These utilities allow mass changes of configuration settings and the ability to change the configuration settings in batch. Common utilities available for remote host scheduling:
- “ctmhostmap” – allows the management of remote hosts connection settings
- “ctmsetown” – allows the management of an owner’s authentication settings
- “ctmkeygen” – allows the management of SSH authentication keys
Agent utilities

Starting from BMC Control-M Agent V8 Agent utilities activation (such as create jobs via ctmcreate, manipulate conditions via ctmcontb) on Remote Host is supported. In order to utilize this functionality you should configure UPLOAD_REMOTE_UTILS Control-M Agent system parameter to “Y”.

Agent or Remote Host?

BMC Control-M architecture enables the use of remote host technology side-by-side with conventional agents. The decision on when to use conventional agents and when to use remote host technology should be taken based on the following factors:

- **Target host platform**: In order to utilize the remote host capabilities, the target host must support the remote host technology infrastructure.

- **Operating system**: The operating system running on the remote host must be supported by the remote host technology. If your operating system is UNIX, Linux, Windows, OpenVMS, z/OS USS or OS/400 (PASE), than the remote host technology can be used. If the target host is running the Tandem Guardian or Unisys 2200 operating systems for example, use a conventional agent instead.

- **Communication standards**: The communication standards used by the remote host technology must be available on the target host. When using the SSH standard, for example, an SSH server version 2 compliant server (such as SSH Tectia, OpenSSH, WinSSHD or F-Secure) must be available on the remote host. When using WMI, the WMI Windows service must be running on the target host.

- **Job’s Output**: When a job completes its execution on a remote host in remote host mode, the job’s output (Sysout) is moved by default to the host of the BMC Control-M/Agent that has submitted the job. Alternatively, you can disable the Output transfer from the remote host to BMC Control-M/Agent in case Output analysis is not required. If the job’s Output is very large, and Output analysis is required, consider using a conventional agent instead to avoid overloading the network traffic. The decision on whether to use the remote host technology or conventional agent should be taken in this case based on the network bandwidth capacity and load.

- **BMC Control-M/Agent functionality**: BMC Control-M File Watching functionality requires a BMC Control-M/Agent component running on the target host:
  
  - When using a conventional agent the CTMFW utility can be used to monitor a file’s availability on the target host. This utility is not available when using remote host technology. Alternatively, you can use the BMC Control-M/CM for Advanced File Transfer to monitor files availability on remote hosts. This can be done using the same SSH server utilized by the remote host technology or by using native FTP server on Windows platforms (when remote host is configured for WMI)

- **Control Modules**: BMC Control-M Control Modules can only be installed on conventional agents. Note however, that the number of instances required for most Control Modules is very small. For example, a single installation of the Control Module (CM) for SAP can schedule and manage all SAP
Control-M Best Practices - Remote Host

jobs on multiple SAP instances within an organization. A single installation of the Control Module (CM) for AFT can manage file transfers throughout the entire enterprise. In fact, the Control Modules can be considered as “remote host” since they do not have to be installed on the same host as the application servers. For that matter, the BMC Control-M/Agent can be considered as the infrastructure behind the Control Modules and the new remote host technology can be considered as the last piece in the puzzle, acting as a “CM” for operating systems jobs.

- **Number and frequency of jobs**: The number and frequency of jobs running on the target host should be taken into account when considering remote host vs. conventional agents. A certain overhead is added when initiating connections to remote hosts, which can delay or limit the volume of job submissions. Where high performance, high volume, and fast throughput are essential, dedicated agents provide better support. When a simple and fast deployment of workloads on a high number of servers is required, remote host scheduling offers tremendous benefits.

- **Owner’s credentials**: Conventional agent’s components can run with administrator (root) authorization levels, and therefore, the overhead of the security management is minimal. On the other hand, having the agent run as administrator on the remote host might be considered as a security issue by some sites. When BMC Control-M connects to remote hosts, the connection is performed by the job’s owner credentials (either user and password, or an SSH key). It requires the management of each owner’s credentials in BMC Control-M (even though a single credentials entry can refer to <All> hosts rather than to each and every specific host) but on the other hand, does not require the use of administrator authorizations.

**Remote host recent enhancements**

**BMC Control-M/Agent 8.0.00**

- Ability to execute command line utilities, such as ctmcreate, ctcontb, etc. from the Remote Host.
- Ability to reuse SSH connections among Jobs running with the same owner by configuring Remote Host connection pool
Summary

The BMC Control-M remote host solution significantly reduces BMC Control-M costs by reducing the amount of BMC Control-M/Agents. It simplifies the product implementation by bundling BMC Control-M/Server and BMC Control-M/Agent installations.

Remote host technology can increase the span of control by extending the benefits of enterprise scheduling to the entire IT landscape. The remote host solution reduces the time it takes to submit the first job on a new server, allowing automatic definitions using default communication settings and first day support for new platforms.