CA NetMaster® Network Automation

Best Practices Guide

Release 12.1

This Documentation, which includes embedded help systems and electronically distributed materials, (hereinafter referred to as the “Documentation”) is for your informational purposes only and is subject to change or withdrawal by CA at any time.

This Documentation may not be copied, transferred, reproduced, disclosed, modified or duplicated, in whole or in part, without the prior written consent of CA. This Documentation is confidential and proprietary information of CA and may not be disclosed by you or used for any purpose other than as may be permitted in (i) a separate agreement between you and CA governing your use of the CA software to which the Documentation relates; or (ii) a separate confidentiality agreement between you and CA.

Notwithstanding the foregoing, if you are a licensed user of the software product(s) addressed in the Documentation, you may print or otherwise make available a reasonable number of copies of the Documentation for internal use by you and your employees in connection with that software, provided that all CA copyright notices and legends are affixed to each reproduced copy.

The right to print or otherwise make available copies of the Documentation is limited to the period during which the applicable license for such software remains in full force and effect. Should the license terminate for any reason, it is your responsibility to certify in writing to CA that all copies and partial copies of the Documentation have been returned to CA or destroyed.

TO THE EXTENT PERMITTED BY APPLICABLE LAW, CA PROVIDES THIS DOCUMENTATION “AS IS” WITHOUT WARRANTY OF ANY KIND, INCLUDING WITHOUT LIMITATION, ANY IMPLIED WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, OR NONINFRINGEMENT. IN NO EVENT WILL CA BE LIABLE TO YOU OR ANY THIRD PARTY FOR ANY LOSS OR DAMAGE, DIRECT OR INDIRECT, FROM THE USE OF THIS DOCUMENTATION, INCLUDING WITHOUT LIMITATION, LOST PROFITS, LOST INVESTMENT, BUSINESS INTERRUPTION, GOODWILL, OR LOST DATA, EVEN IF CA IS EXPRESSLY ADVISED IN ADVANCE OF THE POSSIBILITY OF SUCH LOSS OR DAMAGE.

The use of any software product referenced in the Documentation is governed by the applicable license agreement and such license agreement is not modified in any way by the terms of this notice.

The manufacturer of this Documentation is CA.

Provided with “Restricted Rights.” Use, duplication or disclosure by the United States Government is subject to the restrictions set forth in FAR Sections 12.212, 52.227-14, and 52.227-19(c)(1) - (2) and DFARS Section 252.227-7014(b)(3), as applicable, or their successors.

CA Technologies Product References

This document references the following CA Technologies products:

- CA NetMaster® File Transfer Management (CA NetMaster FTM)
- CA NetMaster® Network Automation (CA NetMaster NA)
- CA NetMaster® Network Management for SNA (CA NetMaster NM for SNA)
- CA NetMaster® Network Management for TCP/IP (CA NetMaster NM for TCP/IP)
- CA OPS/MVS® Event Management and Automation (CA OPS/MVS)

Contact CA Technologies

Contact CA Support

For your convenience, CA Technologies provides one site where you can access the information that you need for your Home Office, Small Business, and Enterprise CA Technologies products. At http://ca.com/support, you can access the following resources:

- Online and telephone contact information for technical assistance and customer services
- Information about user communities and forums
- Product and documentation downloads
- CA Support policies and guidelines
- Other helpful resources appropriate for your product

Providing Feedback About Product Documentation

If you have comments or questions about CA Technologies product documentation, you can send a message to techpubs@ca.com.

To provide feedback about CA Technologies product documentation, complete our short customer survey which is available on the CA Support website at http://ca.com/docs.

Best Practices Guide Process

These best practices represent years of product experience, much of which is based on customer experience reported through interviews with development, technical support, and technical services. Therefore, many of these best practices are truly a collaborative effort stemming from customer feedback.

To continue and build on this process, we encourage users to share common themes of product use that might benefit other users. Please consider sharing your best practices with us.

To share your best practices, contact us at techpubs@ca.com and preface your email subject line with "Best Practices for *product name*" so that we can easily identify and categorize them.

Contents

Chapter 1: Introduction

This section contains the following topics:

Purpose of this Guide

The guide provides a brief introduction to the CA Technologies mainframe management strategy and features, and describes the best practices for installing and configuring CA NetMaster NA.

Audience

The intended audience of this guide is systems programmers and administrators who install, configure, deploy, and maintain CA NetMaster NA.

Mainframe 2.0 Overview

Mainframe 2.0 is our strategy for providing leadership in the mainframe operating environment. We intend to lead the mainframe marketplace for customer experience, Out-Tasking solutions, and solution innovation. After listening to customer needs and requirements to keep the mainframe operating environment viable and cost-effective, we are providing new tools to simplify usage and to energize this operating environment for years to come.

CA Mainframe Software Manager™ (CA MSM) is an important step in realizing the Mainframe 2.0 strategy. CA MSM simplifies and standardizes the delivery, installation, and maintenance of mainframe products on z/OS systems. CA MSM has a web-based interface with a modern look and feel for managing those solutions. As products adopt Mainframe 2.0 features and CA MSM services, you can acquire, install, and manage your software in a common way.

We follow the IBM z/OS packaging standards using SMP/E, with some additional CA Technologies qualities of service added, to make installation simple and consistent. Additionally, through the synchronization of product releases and the use of common test environments, we will declare a yearly mainframe software stack that includes many new releases with enhanced functionality. This stack is certified for interoperability across the CA Technologies mainframe product portfolio and the base IBM z/OS product stack.

Mainframe 2.0 Features

Mainframe 2.0 has the following main features:

CA Mainframe Software Manager (CA MSM)

Delivers simplified acquisition, installation, and deployment capabilities using a common z/OS-based web application delivered through a browser-based UI. CA MSM includes the following services:

Product Acquisition Service (PAS)

Facilitates the acquisition of our mainframe products and services, including product base installation packages and program temporary fixes (PTFs). This service integrates the inventory of products available on your system with CA Support, providing a seamless environment for managing and downloading software and fixes onto your system.

Software Installation Service (SIS)

Facilitates the installation and maintenance of our mainframe products in the software inventory of the driving system. This service enables you to browse and manage the software inventory using a web interface, and automates tasks for products that use SMP/E to manage installation. You can browse downloaded software packages, and browse and manage one or more consolidated software inventories (CSIs) on the driving system.

Software Deployment Service (SDS)

Facilitates the deployment of CA Technologies mainframe products from the software inventory of the driving system. This service enables you to deploy installed products that are policy-driven with a set of appropriate transport mechanisms across a known topology. The enterprise system topology can include shared DASD environments, networked environments, and z/OS systems. Policies represent a combination of metadata input and user-supplied input. Metadata input identifies the component parts of a product. User-supplied input identifies the deployment criteria, such as where it goes and what it is named.

Software Configuration Service (SCS)

Facilitates the mainframe products configuration from the software inventory of the driving system to the targeted z/OS mainframe operating system. The SCS guides you through the configuration creation process, and through the manual steps to implement the configuration. In addition, the SCS includes an address space communications service running on each targeted z/OS system.

Electronic Software Delivery (ESD)

Enables you to get our products from an FTP server. We have improved this process so that you no longer need to build a tape to install the product.

Best Practices Management

Integrates with IBM Health Checker for z/OS to verify that deployed software follows our best practices. The health checks continually monitor the system and software to provide feedback on whether the software continues to be configured optimally.

Best Practices Guide

Provides best practices for product installation and configuration.

Active and Heartbeat Event Management through CA OPS/MVS EMA

CA Technologies mainframe products can automatically communicate both active status events and heartbeat events to CA OPS/MVS in a consistent manner. The enabling technology for this feature is through a generic event API call that CA OPS/MVS provides to the other products so that they can communicate events to CA OPS/MVS.

Two versions of this API call are provided to support this initiative:

- An active status event API call that allows other products to generate events for the CA OPS/MVS EMA System State Manager (SSM) component when they are starting, up, stopping, or down.
- A heartbeat API call that allows other CA Technologies products to communicate a normal, warning, or problem overall health status and reasoning to CA OPS/MVS EMA on a regular interval.

After a CA Technologies product begins generating heart beat events for CA OPS/MVS, CA OPS/MVS can also react to the lack of a heart beat event from another CA Technologies product address space, treating this as an indication that there is either a potential problem with the CA Technologies product address space, or there is a larger system-level problem.

SSM is a built-in feature of CA OPS/MVS that uses an internal relational data framework to proactively monitor and manage started tasks, online applications, subsystems, JES initiators, and other z/OS resources including your CA Technologies mainframe products. SSM compares the current state of online systems, hardware devices, and the other resources with their desired state, and then automatically makes the necessary corrections when a resource is not in its desired state. This provides proactive and reactive state management of critical resources. As previously noted, SSM is particularly interested in receiving active status events consistently from all CA Technologies products when they are starting, up, stopping, or down. Without this consistent type of events, SSM must maintain separate rules in CA OPS/MVS for each product unique messages that are associated with starting and stopping.

Note: For additional information about the CA Mainframe 2.0 initiative, see http://ca.com//mainframe2.

Chapter 2: Installation and Configuration Best Practices

This section contains the following topics:

Installation

Use CA MSM to acquire, install, and maintain your product.

Business Value:

CA MSM provides a web interface, which works with ESD and standardized installation, to provide a common way to manage CA mainframe products. You can use it to download and install CA NetMaster NA.

CA MSM lets you download product and maintenance releases over the Internet directly to your system from the CA Support website. After you use CA MSM to download your product or maintenance, you use the same interface to install the downloaded software packages using SMP/E.

Additional Considerations:

After you install the product, use the product's Install Utility to set it up. CA MSM can continue to help you maintain your product.

Note: If there is maintenance for VSAM data sets, you must use the Install Utility to update those data sets for each region you have set up.

More Information:

For more information about CA MSM, see the *CA Mainframe Software Manager Product Guide*. For more information about product setup, see the *Installation Guide*.

Address Space Sharing

Always implement CA NetMaster NA with CA NetMaster NM for SNA for performance and usability optimization. If your site also uses CA NetMaster NM for TCP/IP, include CA NetMaster NM for TCP/IP in the same address space. To share the address space, set up a region that includes the products.

CA NetMaster NA can also share address space with the following products:

- CA NetMaster FTM
- CA SOLVE:FTS

Business Value:

Sharing an address space has the following values:

- You require only a single logon to access multiple products from one interface.
- You have better integration between products. You can have a single integrated configured address space instead of having to configure multiple address spaces.
- The multiple products can share resources.

Security Considerations

Implement the NMSAF solution. The NMSAF solution is built around a partial security exit. The solution uses the product's User Access Maintenance Subsystem (UAMS) data set to store information for your product region, and uses your installed security product to perform user validation and password checking (through the IBM-defined system authorization facility (SAF) interfaces).

Business Value:

This setup is ideal for organizations that want the flexibility of allowing the administrator to control specific region authorities, while still ensuring that access to the region is secured by their security product.

More Information:

For more information about the NMSAF solution and UAMS, see the *Security Guide*.

UAMS VSAM Data Set Sharing

Implement record-level sharing (RLS), and include the XOPT=RSLU parameter in the SYSIN member for each product region sharing the UAMS VSAM data set.

Business Value:

Multiple users on multiple systems can update a UAMS VSAM data set at the same time. The standard VSAM share options do not guarantee data set integrity with simultaneous updates from multiple systems. Using RLS, the UAMS VSAM data set can be shared without the possibility of corruption, which reduces the possibility of region outage.

Additional Considerations:

The implementation of RLS requires the proper configuration and availability of SMSVSAM. Some SMS rules for the RLS-managed data sets are also required on the systems using RLS.

More Information:

The *Security Guide* contains more information about the sharing of UAMS data set using RLS. The IBM DFSMS guides describe the implementation of RLS for VSAM data sets. For a comprehensive overview of RLS, see the chapter "VSAM Record Level Sharing" in the IBM Redbooks publication *VSAM Demystified* (SG24-6105).

Background Users

In a multisystem environment, reduce the number of background user IDs you add to security by specifying the same value for NMSUP in all regions.

Business Value:

Particularly in large complexes, this practice assists in simplifying the administration of internal background user IDs and reduces the possibility of outages associated with nonexistent, or incorrectly defined user IDs.

Additional Considerations:

CA NetMaster NA uses background users to perform various tasks. By default, the NMSAF solution checks the background user IDs in advanced program-to-program communications (APPC). You must add them to your installed security product.

Note: The following NMSAF SXCTL parameters set the user ID checking: APPCCHECK and SYSCHECK.

The following list identifies the background user IDs:

- *xxxx*AOMP
- *xxxx*BLOG
- *xxxx*BMON
- *xxxx*BSVR
- *xxxx*BSYS
- *xxxx*LOGP
- *xxxx*PPOP

xxxx

Is the prefix specified by the NMSUP region job control language (JCL) parameter.

By specifying the same value for NMSUP in all regions, you only have to add one background user to security. For example, if you set NMSUP to MFNM in all regions, then the user ID for the *xxxx*BSYS background users in those regions is MFNMBSYS.

To use NMSUP, add the following statement to the TESTEXEC(RUNSYSIN) members for the regions, using the same *xxxx* value:

```
PPREF='NMSUP=xxxx'
```

More Information:

For information about SXCTL, see the *Security Guide*.

Configuration for Optimal Performance

As a performance pattern develops for your product, tune the relevant controls. You probably never have to tune many of the controls.

Business Value:

Reviewing the configuration and tuning parameters helps ensure that you are not performing unnecessary processing, such as collecting and logging data that your organization does not require, thus saving CPU cycles. As you become more familiar with the capabilities of the product, you can make informed decisions on what functions are desirable and therefore only incur overhead where there are obvious benefits.

Additional Considerations:

A product with the breadth and capability of CA NetMaster NA supports many external tuning controls. Configuring every last aspect of its operation can seem like a large task. However, you can set up an effective environment by simply using the default settings.

If you have a newly implemented region, a basic configuration is created with some essential parameters updated during setup. Further customization can be performed progressively.

More Information:

For more information about product setup and initial startup, see the *Installation Guide*.

zIIPs

If IBM System z Integrated Information Processors (zIIPs) are available, elect to use zIIPs when you set up your regions.

Business Value:

Using zIIPs provides the following benefits:

- Reducing the execution time on the normal central processing unit (CPU), providing savings in billable CPU time
- Freeing up processing cycles from the CPU to other work
- Exploiting the processing power of zIIPs

More Information:

The following JCL parameters control the usage of zIIPs: PAEXMODE for the SOLVE Subsystem Interface and XM for the region. For information about the parameters, see the *SOLVE Subsystem Interface Guide* and *the Reference Guide*.

Network Discovery

Review and customize the AUTOSNACNTL parameter group to discover only those resources that are relevant to your automation requirements. For example, we do not recommend that you discover all logical units (LUs). If you must monitor some LUs, then customize your filter to identify this subset specifically.

Business Value:

Monitoring everything wastes system resources and is very distracting—you can be distracted by inconsequential alerts while missing the important ones. Removing unnecessary monitoring also reduces the processing the region has to do.

Additional Considerations:

CA NetMaster NA performs a network discovery based on a customizable discovery filter. In a large SNA network, based on the scope of the discovery, you can discover tens of thousands of resources. While CA NetMaster NA scales to monitor large networks, it is prudent to discover only relevant resources.

More Information:

For more information about how to customize SNA resource discovery, see the *Administration Guide*.

Standardized Object Naming

Name resources in a standard way.

Business Value:

Presentation, management, and control of CA NetMaster NA objects (resources, rule sets, and rules) is better when objects are organized and named in a structured and standard way. A naming standard makes the product easier to use (less training with less user error). Additionally, generic automation is easier when dealing with objects that conform to a standard, reducing the effort and maintenance required for building automation.

Example: SNA Group Resource Names

An SNA group lets you monitor the status of a set of SNA resources that support a business function. The following naming example organizes the SNA groups in a structured way. The example uses the first part of the name to identify the location of a resource and the second part of the name to identify the function supported by that resource. For example, the LOC001ATM SNA group supports the automatic teller machine (ATM) at the location, LOC001.

```
LOC001ATM
LOC002ATM
LOC003ATM
```

Transient Logs

Tune your transient logs to reduce storage. Disable all logging initially, and then implement logging for business critical resources (applications).

Business Value:

Mainframe storage costs money and should be used only if there is a business requirement. Tuning the size of transient logs enables you to set storage at a level appropriate to your business requirements.

Additional Considerations:

Transient logs provide a snapshot history of activities at the resource level. From a resource monitor, you can use the SETTLOG command to disable logging or reset the log size for one or more monitored resources.

Online Help

Use online help to find out more about the interface in context.

Business Value:

CA NetMaster NA has many features and can be overwhelming to new users. However, you have access to substantial online help at the 3270 interface, usually by pressing F1. You are encouraged to request online help, to promote product understanding, save time on issue resolution, and potentially save money on basic product training.

Interfaces and Integration Points

Integrate with other CA products to help you manage your business.

Business Value:

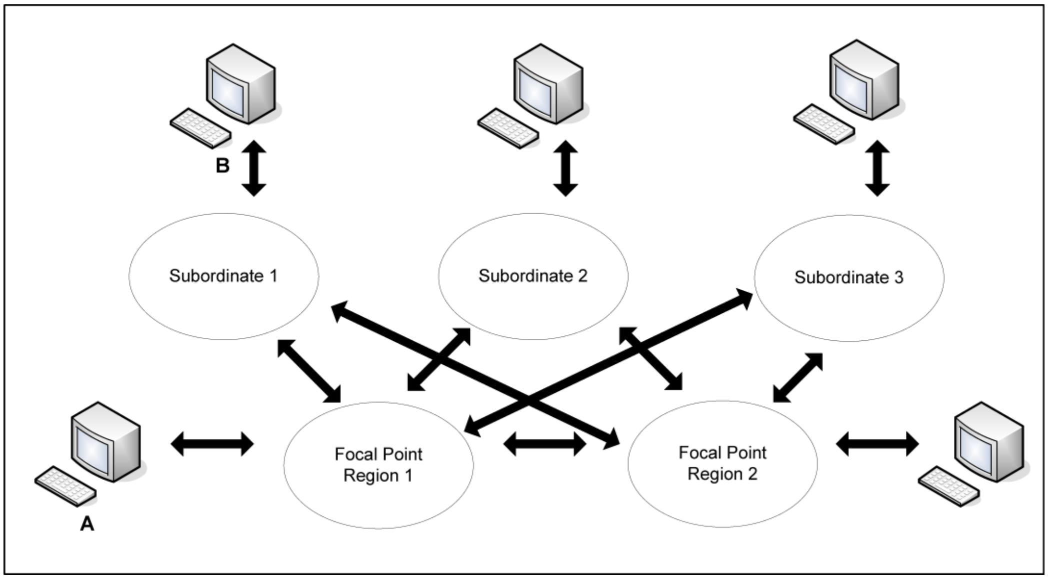
CA NetMaster NA integrates with the following CA products:

- **Other CA NetMaster products**—All CA NetMaster products can share the same address space. They can also communicate with each other using their multisystem capabilities. The use of common monitors, such as the alert monitor and the status monitor, supports the combined monitoring and control of network events and resources irrespective of whether they are IP, SNA, or file transfer related.
- **CA Service Desk**—CA NetMaster NA supports the automatic creation of trouble tickets in CA Service Desk, facilitating problem notification and resolution.
- **CA OPS/MVS**—CA OPS/MVS can forward system events programmatically to CA NetMaster NA for display on the alert monitor. It is an ideal consolidation point for all mainframe network and system events. The integration facilitates the flow of information between CA management products and users.

Multisystem Deployment

If you have multiple systems, deploy CA NetMaster NA in a multisystem environment to provide a consolidated view of your enterprise.

The following diagram shows an example of a multisystem environment. Logging on to Console A allows visibility to all resources. Logging on to Console B allows visibility to the subordinate system image only.



Business Value:

Particularly in large multisystem environments, deployment can be both arduous and time consuming. Following an effective and proven process has the following values:

- Reduce the time taken to migrate to new releases, and therefore enable access to new functions more readily.
- Free key resources to perform other tasks, such as the exploitation of product functions.
- Reduce the likelihood of errors and subsequent outages associated with poor deployment processes.

Additional Considerations:

You should always deploy CA NetMaster NA with CA NetMaster NM for SNA.

More Information:

For information about the deployment of these products, see the *CA NetMaster Network Management for SNA Best Practices Guide*.

Index