NetApp® Memory Accelerated Data 1.5

Installation and Setup Guide

October 2019 | 215-14576_A0
doccomments@netapp.com

NetApp®

Contents

Deciding whether to use this guide 5
Understanding the MAX Data components 6
Setup overview 8
Verifying that your MAX Data configuration is supported 9
Setting up the NetApp ONTAP storage system 10
Setting up application servers for MAX Data 11
Preparing for MAX Data installation 11
Setting up a third-party certificate authority 13
Installing the MAX Data software package 16
Setting up MAX Recovery 17
Preparing for MAX Recovery installation 18
Installing the MAX Recovery software package 18
Connecting MAX Data to MAX Recovery 19
Configuring the MAX Data environment 21
Planning backup of MAX Data application server data on ONTAP storage systems 21
Scheduling MAX Data snapshots 21
Running the configuration wizard 21
Recovering MAX Data applications 24
Recovering data from a Snapshot copy 24
Recovering an application to a new server 24
Recovering an application following a disaster 25
Preparing application servers and ONTAP for recovery 26
Creating certificates for exchange with the SVM 26
Creating the MAX Data application configuration file 27
Creating the recovery file 29
Recovering applications from the destination SVM 30
Migrating applications to a new server 30
Archiving an application 31
Managing MAX Data 32
Creating Snapshot copies on demand 32
Deleting Snapshot copies using MAX Data 32
Monitoring applications using MAX Data 33
Managing MAX Data licenses 34
Resizing storage for an application 35
Configuring a spare application server 39
Removing applications from MAX Data 40
Removing a MAX Recovery host from the cluster 40
Uninstalling MAX Data and MAX Recovery 40
Copyright 42
Trademark 43

How to send comments about documentation and receive update notifications 44
Index 45

Deciding whether to use this guide

This guide describes how to install and configure NetApp Memory Accelerated Data (MAX Data). MAX Data software provides ultra-low latency storage with automatic tiering and enterprise-level storage management.

You should use this guide if you want to complete the following tasks:

- Install the MAX Data components on one or more application servers
- Install the MAX Data components on a recovery server
- Cable all components together
- Configure the connection to a NetApp ONTAP storage system
- Verify that the system is set up correctly
- Monitor the system
- Configure backups
- Recover from a storage failure

Related information

NetApp MAX Data Resources
MAX Data 1.5 Quick Start Guide

Understanding the MAX Data components

A MAX Data system includes the application servers with a supported operating system, a supported application, and other hardware components.

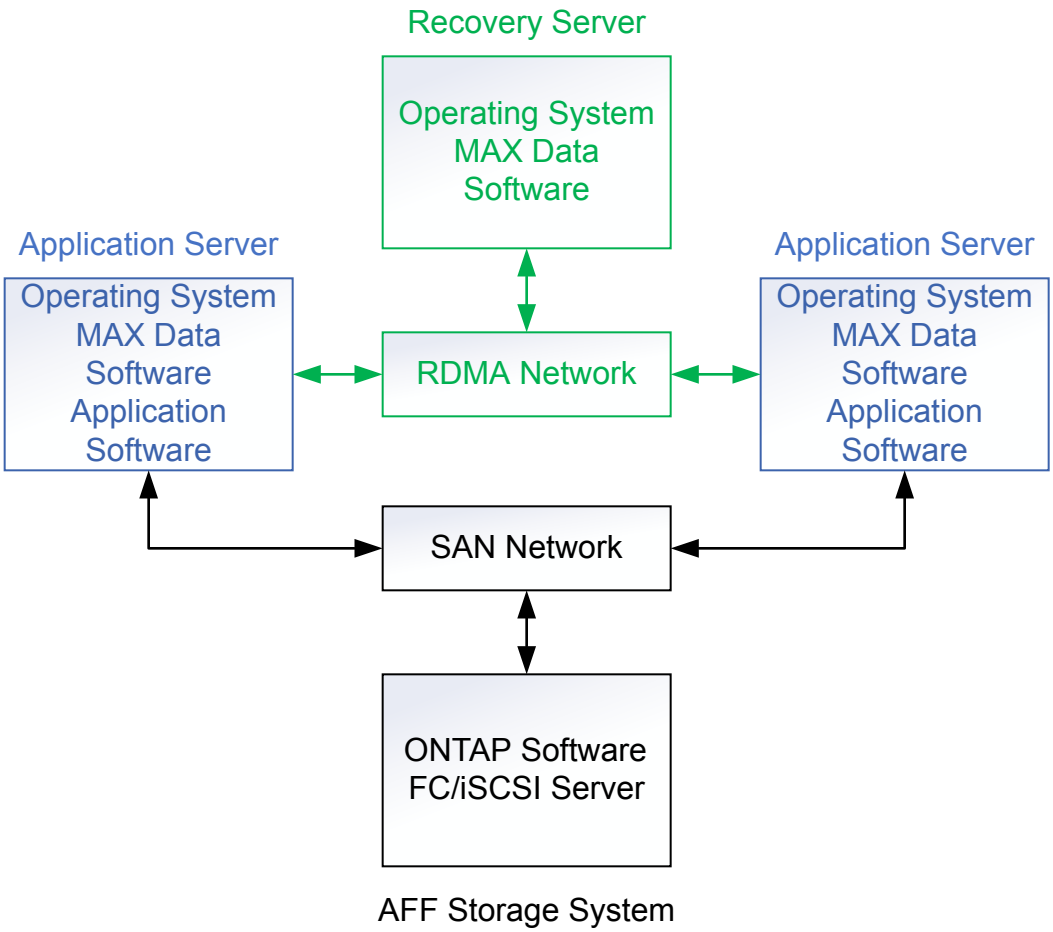
A MAX Data system includes:

- The application servers with a supported operating system and Intel® Optane™ DC Persistent Memory (DCPMM)
- High-speed networks
- An optional NetApp ONTAP storage system (AFF, FAS, or ONTAP Select) with a supported ONTAP software version
- An optional NetApp Memory Accelerated Recovery (MAX Recovery) enabled host server

  Note: The MAX Recovery server is available only in configurations with ONTAP storage systems. It is not available in server-only configurations.

- A supported application

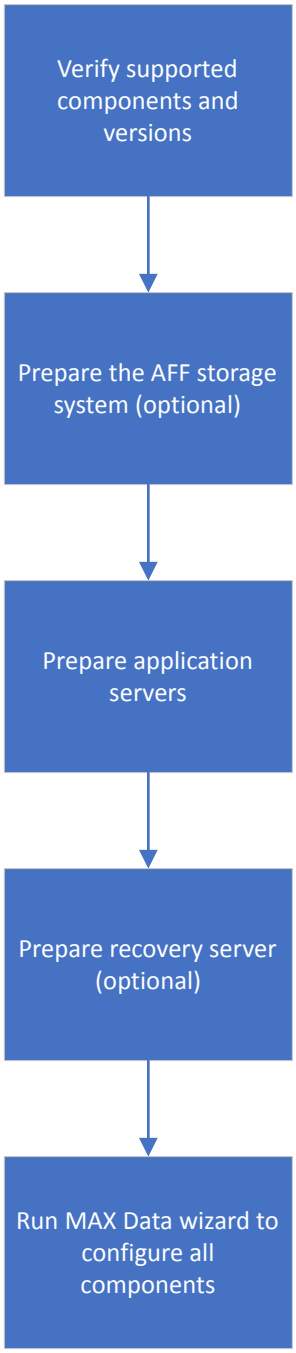
Instead of using Optane DCPMM, you can use DRAM to test MAX Data. You can also use DRAM in a production environment if you also use the optional MAX Recovery enabled host server to mirror your data, or if you are using an application that manages its own high availability and can handle the loss of the in-memory data.


Recovery Server
Operating System
MAX Data
Software
Application Server
Operating System
MAX Data
Software
Application
Software
RDMA Network
Application Server
Operating System
MAX Data
Software
Application
Software
SAN Network
ONTAP Software
FC/iSCSI Server
AFF Storage System

Setup overview

The main steps to setting up the MAX Data environment include verifying and configuring system components and installing MAX Data software.

The following figure shows the setup steps and the order in which you complete them.



Verifying that your MAX Data configuration is supported

You need to verify that your MAX Data configuration uses a supported combination of components.

The Interoperability Matrix Tool (IMT) provides a list of supported components:

NetApp Interoperability Matrix Tool

Note: An ONTAP system is not required in the configuration.

- The server model for MAX Data enabled application server and MAX Recovery enabled host server
- The server operating system version and any required packages and drivers
- The RDMA adapters for connecting MAX Data enabled application server to MAX Recovery enabled host server
- The switch for connecting MAX Data enabled application server to MAX Recovery enabled host server
- The MAX Data software version
- The ONTAP storage system model (optional)
- The ONTAP software version (if ONTAP storage system present)
- For FC connections from the MAX Data enabled application server to the ONTAP storage system, if present:
  - FC initiator cards and firmware
  - FC switch models and firmware
  - Host Utilities
- For iSCSI connections from the MAX Data enabled application server to the AFF system, if present:
  - iSCSI initiator software version or iSCSI hardware initiator card model and firmware
  - Host Utilities

Setting up the NetApp ONTAP storage system

The NetApp ONTAP storage system (AFF, FAS, or ONTAP Select) provides high-speed storage to offload less-used data from the MAX Data enabled application server. If you are using an ONTAP storage system in your configuration, you must connect the systems using FC or iSCSI, and then configure the ONTAP software.

About this task

The data connection from the ONTAP storage cluster to the MAX Data enabled application servers is a standard SAN configuration. The ONTAP SAN documentation describes supported configurations.

You complete this procedure on the ONTAP storage system, using either ONTAP System Manager or the ONTAP CLI:

Steps

1. Verify that there is an aggregate with adequate space.

   The MAX Data configuration wizard will create one or more LUNs that total 10 times the size of the persistent memory (or DRAM allocated to act in place of persistent memory) for each server. This ratio cannot be changed.

2. Create an SVM:

   a. Record the SVM management IP address, administrator name, and password for use by the MAX Data enabled application server.

   b. Specify the “certificate” authentication method that the SVM user will use for SSL authentication:

      ```
      security login create -user-or-group-name vsadmin -application http -authentication-method cert -vserver vserver_name
      ```

   c. Configure DNS for the SVM.

   d. Verify that you have configured NTP for the ONTAP nodes.

      The time on the ONTAP node must match the time on the MAX Data enabled application servers to within one minute.

   e. Enable the FC or iSCSI protocol on the SVM.

   f. Create at least two data LIFs on each node in the ONTAP cluster for use by the MAX Data enabled application server.

      Note: When using iSCSI, LIFs on the same node must be on the same subnet.

   g. Add any aggregates that the SVM is authorized to use to the aggregate-list of the SVM:

      ```
      vserver modify -vserver vs0 -aggr-list list-of-aggrs
      ```

3. Protect the data stored on the ONTAP nodes by configuring SnapMirror SVM replication (SVM DR) with the identity discard option.

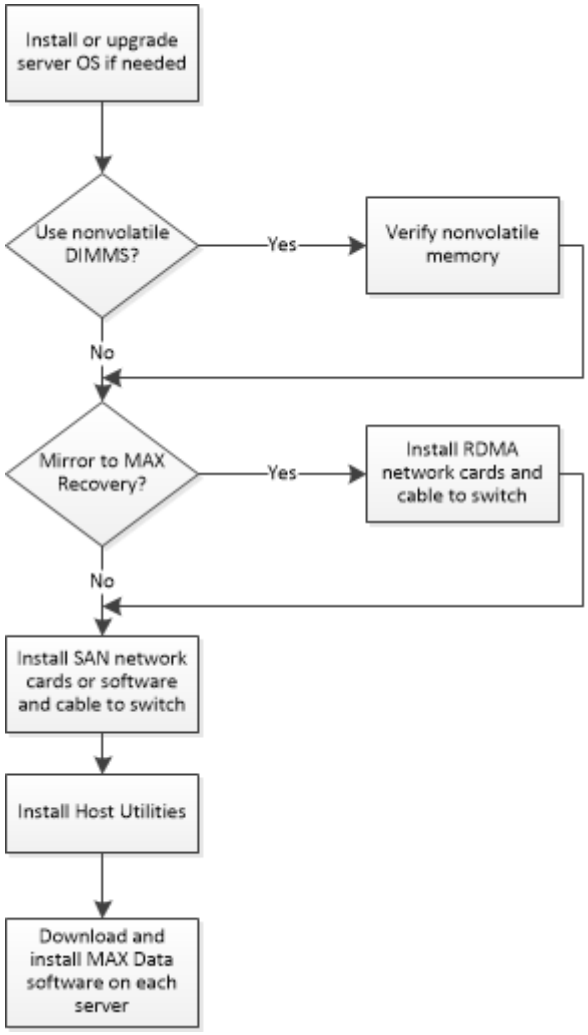
   The ONTAP Documentation Center and the System Manager online help contain detailed steps.

   ONTAP 9 Documentation Center

Setting up application servers for MAX Data

Setting up the application server includes installing the hardware and software components.

The following diagram provides an overview of the setup process:



Preparing for MAX Data installation

Preparing to install MAX Data includes verifying the host server operating system, verifying nonvolatile memory installation, installing the remote direct memory access (RDMA) cards for MAX Recovery mirroring, setting up the SAN network, and installing host utilities.

Install or upgrade the server operating system

If you are not running a supported operating system version, install or upgrade as needed. Only the versions listed in the Interoperability Matrix Tool (IMT) are supported.

Configure DNS on the server.

Configure NTP on the server. The time on the MAX Data enabled application servers must match the time on the AFF nodes (if present) to within one minute.

Verify that the Intel Optane DCPMM is installed

Verify that a supported Intel Optane DCPMM is installed in the server, following the Intel Optane DCPMM standards.

If you are using DRAM instead of NVDIMMs, the MAX Data configuration wizard will partition the memory needed for MAX Data.

Verify that the Intel Optane DCPMM is configured in App Direct mode

The Intel Optane DCPMM must be configured in BIOS in App Direct Mode, with 0% using Memory Mode or in Mixed Mode..

Plan memory requirements

The MAX Data configuration wizard will create four LUNs per mount point that total 10 times the size of the persistent memory (or DRAM allocated to act in place of persistent memory) for each server. This ratio cannot be changed in configurations using an ONTAP storage system.

The goal is to have sufficient nonvolatile memory to hold the working data for the application. At a minimum, you must have enough memory so that the total expected storage for the application does not exceed 10 times the memory.

If you are using DRAM, you must have enough DRAM to partition in place of nonvolatile memory plus the DRAM needed for the operating system and application needs.

Install the RDMA network

Mirroring data from a MAX Data enabled application server to the MAX Recovery enabled host server requires a dedicated physical network for RDMA. Install the supported cards and switch following the instructions provided by the manufacturers, and then cable the components. The *MAX Data Release Notes* specify the number of MAX Data enabled application servers supported by one MAX Recovery enabled host server.

For security, use an isolated network or VLAN to restrict access to only the MAX Data enabled application servers and MAX Recovery enabled host servers.

MAX Data 1.5 Release Notes

Install the SAN network (if using an AFF system)

MAX Data enabled application servers connect to the AFF storage server using either an FC or an iSCSI network. You should use two FC or Ethernet switches for high availability.

The *ONTAP SAN Configuration Guide* contains instructions for setting up and cabling the SAN components.

SAN configuration

Install the Host Utilities (if using an AFF system)

The host utilities include recommended settings and software to assist with configuring the SAN connection to the AFF storage system. Be sure to download the supported version from the NetApp Support Site.

NetApp Support

Follow the installation instructions provided with the package.

The MAX Data configuration wizard sets host OS values. To see the values set by the wizard, use the `multipath -t` command on the host.

Generate certificates for authentication (if using a third-party certificate authority)

MAX Data can either automatically use ONTAP as a certificate authority or, if ONTAP is not present in the configuration, can be configured to use a third-party certificate authority.

For instructions on using third-party certificates, see *Setting up a third-party certificate authority* on page 13.

Setting up a third-party certificate authority

If you choose to use a third-party certificate authority instead of the ONTAP system, or there is no AFF system in the configuration, you can configure the MAX Data servers to use third-party certificates to authenticate each other.

About this task

This task is not required if an AFF system running ONTAP software is in the configuration. In that case, the ONTAP operating system is configured automatically as the certificate authority by the MAX Data configuration wizard.

Steps

1. Create a Bash script for your site, using the following example as a template.

Example

```
#!/bin/bash

SSLDIR=/tmp/openssl
LINE="-----------------------------------"
IPADDR=`hostname -I`
LONGNAME=`hostname --fqdn`
SHORTNAME=`hostname -s`

########################################
### Remove old files if they exist
########################################
clear
echo $LINE
if [ -d $SSLDIR ]
then
for i in conf csr out
do
if [ -d "$SSLDIR/$i" ]
then
echo "Removing $SSLDIR/$i and all files"
rm -rf $SSLDIR/$i
fi
done
fi

if [ ! -d $SSLDIR ]
then
mkdir $SSLDIR
fi
mkdir $SSLDIR/out $SSLDIR/conf $SSLDIR/csr

########################################
### Verify these are the right IP And FQDN
########################################
echo $LINE

echo "Are the following correct?"
echo "IP Address: $IPADDR"
echo "FQDN: $LONGNAME"
echo "SHRT: $SHORTNAME"
echo ""
read -p "Are you sure? " -n 1 -r
echo
if [[ ! $REPLY =~ ^[Yy]$ ]]
then
```

```
[[ "$0" = "$BASH_SOURCE" ]] && exit 1 || return 1
fi


#####################################
### Create CA Config File
#####################################
echo $LINE
echo "Create CA Config File"

cat << EOF > $SSLDIR/conf/ca.cnf
[ ca ]
default_ca = CA_default

[ CA_default ]
serial = ca-serial
crl = ca-crl.pem
database = ca-database.txt
name_opt = CA_default
cert_opt = CA_default
default_crl_days = 999
default_md = md5

[ req ]
days = 999
distinguished_name = req_distinguished_name
attributes = req_attributes
prompt = no
output_password = password

[ req_distinguished_name ]
C = US
ST = US
L = RTP
O = netapp.com
OU = IT Department
CN = vsadmin
emailAddress = nobody@netapp.com

[ req_attributes ]
challengePassword = password
EOF

#####################################
### Create the Certificate Sign Request Host Extension File

#####################################
echo $LINE
echo "Create the Certificate Sign Request Host Extension File"

cat <<EOF > $SSLDIR/conf/host.v3.ext
extendedKeyUsage = critical, serverAuth, clientAuth
subjectAltName = @alt_names

[alt_names]
DNS.1 = $LONGNAME
DNS.2 = $SHORTNAME
IP.1 = $IPADDR
EOF


#####################################
### Create Certificate Sign Request Config File
#####################################
echo $LINE
echo "Create Certificate Sign Request Config File"

cat <<EOF > $SSLDIR/conf/host.cnf
[req]
distinguished_name = req_distinguished_name
prompt = no
```

```
[req_distinguished_name]
C = US
ST = North Carolina
L = RTP
O = NetApp.com
OU = IT Department
CN = vsadmin
emailAddress = nobody@netapp.com

EOF

#######################################
### Create new self-signed request

#######################################echo $LINE
echo "Create new self-signed request"
openssl req -new -x509 -days 999 -config ${SSLDIR}/conf/ca.cnf -
keyout ${SSLDIR}/out/ca-key.pem -out ${SSLDIR}/out/ca.pem


#######################################
### Generate private key

#######################################
echo $LINE
echo "Generate private key"
openssl genpkey -out ${SSLDIR}/out/host-key.pem -algorithm RSA -
pkeyopt rsa_keygen_bits:2048

#######################################
### Generate Cert Sign Request with private key and config file
#######################################
echo $LINE
echo "Generate Cert Sign Request with private key and config file"
openssl req -new -config ${SSLDIR}/conf/host.cnf -key ${SSLDIR}/out/
host-key.pem -out ${SSLDIR}/csr/host-csr.pem


#######################################
### Sign the Cert Sign Request with the CA
#######################################
echo $LINE
echo "Sign the Cert Sign Request with the CA"
openssl x509 -req -extfile ${SSLDIR}/conf/host.v3.ext -days 99 -
passin "pass:password" -sha256 -in ${SSLDIR}/csr/host-csr.pem -CA $
{SSLDIR}/out/ca.pem -CAkey ${SSLDIR}/out/ca-key.pem -CAcreateserial -
out ${SSLDIR}/out/host-crt.pem

#######################################
### Combine certificate with private key
#######################################
echo $LINE
echo "Combine certificate with private key"
cat ${SSLDIR}/out/host-crt.pem ${SSLDIR}/out/host-key.pem > $
{SSLDIR}/out/host.cert

#######################################
### Store the signed cert and public certs
#######################################
echo $LINE
echo "Store the signed cert and public certs"
cp -rp ${SSLDIR}/out/{host.cert,ca.pem} /opt/netapp/max/certificates/


#######################################
### Link Certs

#######################################
echo $LINE
echo "Link Certs"
```

```
ln -sf /opt/netapp/max/certificates/host.cert /etc/max/dashboard/
config/signed.pem
ln -sf /opt/netapp/max/certificates/ca.pem /etc/max/dashboard/config/
ca.pem

#####################################
### Check and Restart max-dashboard service
#####################################
echo $LINE
echo "Restarting MAX Dashboard Service"
systemctl restart max-dashboard
echo $LINE
echo "Checking MAX Dashboard Service"
systemctl status max-dashboard
```

2. Run the updated script on the MAX Data server.

Installing the MAX Data software package

The MAX Data software includes an installation script that installs the MAX FS file system and the management UI, installs all required support packages, opens the necessary firewall ports, and configures NetApp AutoSupport reporting.

About this task

You must complete this procedure on the application server.

Steps

1. Obtain the appropriate MAX Data license for the number of servers that you are deploying.

   You add the license during MAX Data configuration.

2. Download the software package from the NetApp Support Site.

   NetApp Support Site

3. Copy the installation package to each server, and then extract the files to a working directory.
4. Log in to the server with root privilege.
5. In the working directory, install the software and open the required firewall ports:

   `./max_install.sh --enable-ports`

   Ports opened by this command are for MAX Data GUI (9444/tcp) and REST server (9443/tcp, 9444/tcp) services.

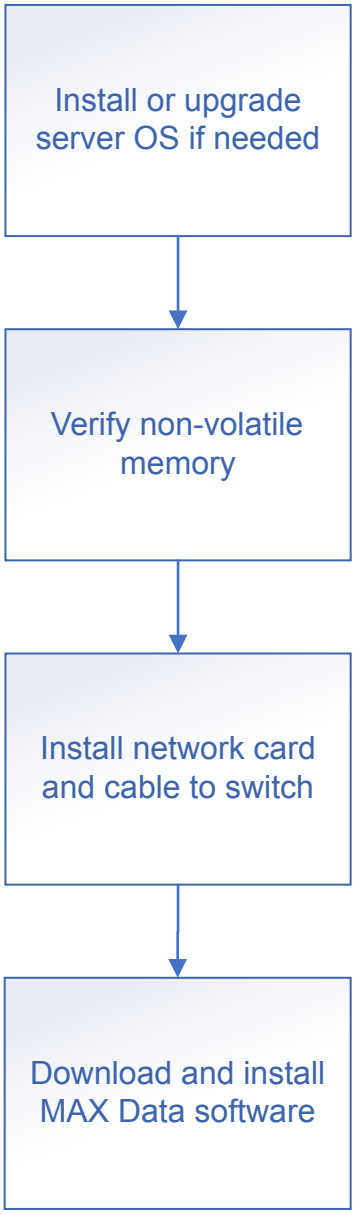
6. Read and accept the end user license agreement.
7. Repeat these steps for each MAX Data enabled application server in your configuration.

Setting up MAX Recovery

The MAX Recovery enabled host server mirrors the data from the MAX Data enabled application servers. If a MAX Data application server ever fails, you can quickly recover the data from the MAX Recovery host server. Setting up the recovery server includes installing the hardware and software components.

The MAX Recovery host server uses the same software installation package as the MAX Data application server.

The following diagram provides an overview of the setup process:



Preparing for MAX Recovery installation

Preparing to install MAX Recovery includes verifying the host operating system, checking for supported NVDIMMs, verifying the memory size, and installing the RDMA network.

Install or upgrade the server operating system

If you are not running a supported operating system version, install or upgrade as needed. Only the versions listed in the Interoperability Matrix Tool (IMT) are supported.

Verify that the Intel Optane DCPMM is installed

Verify that a supported Intel Optane DCPMM is installed in the server, following the Intel Optane DCPMM standards.

Verify that the Intel Optane DCPMM is configured in App Direct mode

The Intel Optane DCPMM must be configured in BIOS in App Direct Mode, with 0% using Memory Mode.

Sizing the MAX Recovery nonvolatile memory

The MAX Recovery enabled host server nonvolatile memory requirement is based on the amount of nonvolatile memory in the servers it is backing up.

1. Calculate the total amount of nonvolatile memory in all of the MAX Recovery enabled host servers that will connect to the recovery server.
2. Verify that the recovery server has at least that much nonvolatile memory installed.

Install the RDMA network

Mirroring data from a MAX Data enabled application server to the MAX Recovery enabled host server requires a dedicated physical network for RDMA. Install the supported cards and switch following the instructions provided by the manufacturers, and then cable the components. The *MAX Data Release Notes* specify the number of MAX Data enabled application servers supported by one MAX Recovery enabled host server.

Verify that jumbo frames are enabled on the network.

For security, use an isolated network or VLAN to restrict access to only the MAX Data enabled application servers and MAX Recovery enabled host servers.

MAX Data 1.5 Release Notes

Installing the MAX Recovery software package

The MAX Recovery enabled host server uses the same software installation package as the MAX Data enabled application server. MAX Recovery requires a separate license from MAX Data.

Before you begin

Obtain the appropriate MAX Recovery license for the number of servers that you are deploying.You will add the license during MAX Recovery configuration.

About this task

The MAX Data software package includes an installation script that installs the MAX FS and the management UI, installs all required support packages, opens the necessary firewall ports, and configures NetApp AutoSupport reporting.

Steps

1. Download the MAX Data software package from the NetApp Support Site.

   NetApp Support Site

2. Copy the installation package to the server, and then extract the files to a working directory.
3. Log in to the server with root privileges.
4. In the working directory, install the software and open firewall ports:

   ```
   ./max_install.sh --enable-ports
   ```

   Ports opened by this command are for the MAX Data GUI (9444/tcp) and REST server (9443/tcp, 9444/tcp) services.

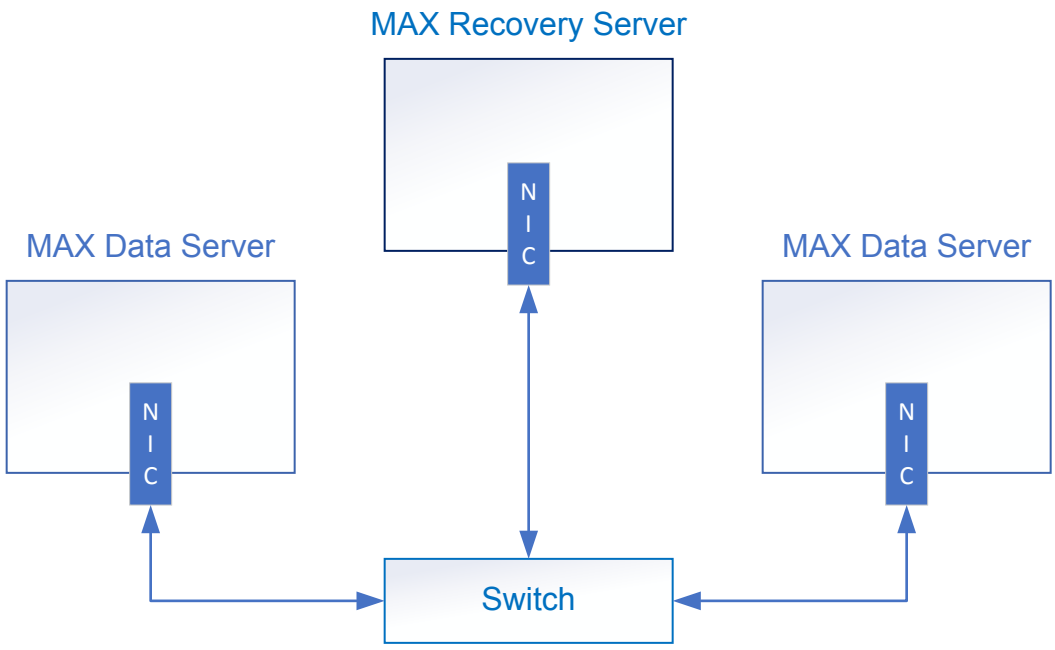
5. Accept the license agreement.

Connecting MAX Data to MAX Recovery

The network that connects the data servers to the recovery server must be a dedicated, high-speed network with RDMA capability.

About this task

The following diagram shows how the components are connected:



Steps

1. Install a supported NIC in each data server.
2. Install a supported NIC in the recovery server.

3. Install a supported switch.
4. Cable each NIC to the switch, as shown in the diagram.
5. Log in to the switch, and then verify that the supported firmware version is installed.

   The NIC and switch documentation contain instructions for updating the firmware, if needed.
6. Verify that RDMA networking is correctly installed and is using jumbo frames.
   a. For Mellanox RNICs, use the `ibv_devinfo` command to check the MTU setting.
   b. Use the `ibv_rc_pingpong` command to verify end-to-end support.

      Example

      The following example uses Mellanox ConnectX4 RNICs:

      MAX Data enabled server:

      ```
      ibv_rc_pingpong -g 0 -d NIC_id -m 4096 -i 1 IP_address
      ```

      MAX Recovery enabled server:

      ```
      ibv_rc_pingpong -d NIC_id -g 0 -i 1 -m 4096
      ```

Configuring the MAX Data environment

You use the MAX Data cluster configuration wizard to configure the entire MAX Data environment, including application servers running MAX Data software, the optional ONTAP storage system, and optional recovery servers running MAX Data software.

Planning backup of MAX Data application server data on ONTAP storage systems

If your configuration includes an ONTAP storage system, the best practice for backing up a MAX Data enabled application server is to mirror the MAX Data file system to a MAX Recovery enabled host server and store snapshots of the MAX Data file system on the ONTAP storage system.

Restoring from the MAX Recovery enabled host server helps achieve no data loss (recovery point objective zero). Snapshot copies enable you to restore previous versions of the file system data.

Scheduling MAX Data snapshots

You should schedule snapshots of the application files when you provision storage in the MAX Data configuration wizard.

You can schedule snapshots in the MAX Data configuration wizard when you enter the application data.

The MAX Data software coordinates the snapshots between the MAX Data file system and ONTAP. First a local copy is made, and then the local snapshot is transferred to the ONTAP storage system as an ONTAP Snapshot copy. You can choose the copy frequency, and you can make local copies more frequently than the remote copies.

The snapshots can be used for backup recovery only if they were created by the MAX Data host.

Running the configuration wizard

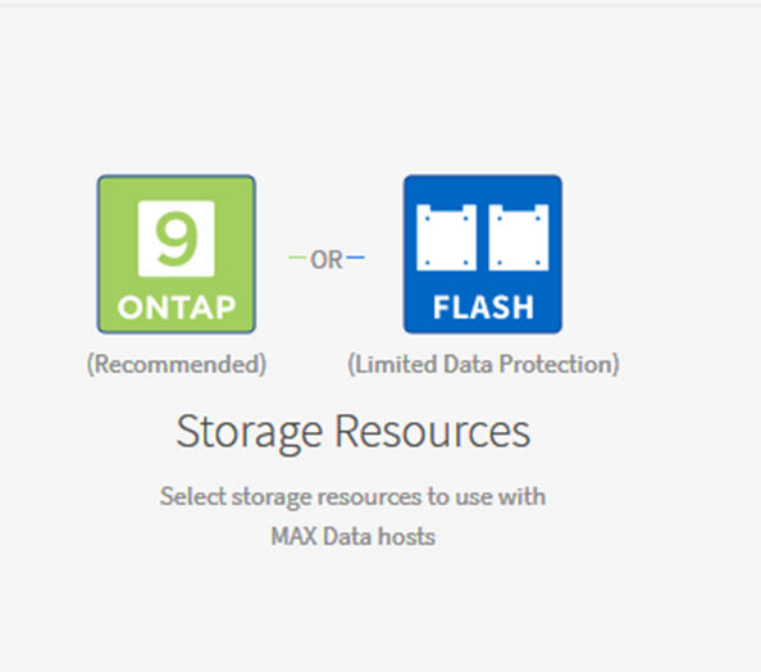
If you have more than one application server running the MAX Data software and using the same SVM credentials, you can run the configuration wizard from any of those servers.

About this task

Note: When DRAM is used in place of nonvolatile memory DIMMs, the configuration wizard reboots the operating system during the configuration. Be sure that rebooting will not disrupt any other workloads on the servers. You need to reconnect to the server after the reboot is complete.

Steps

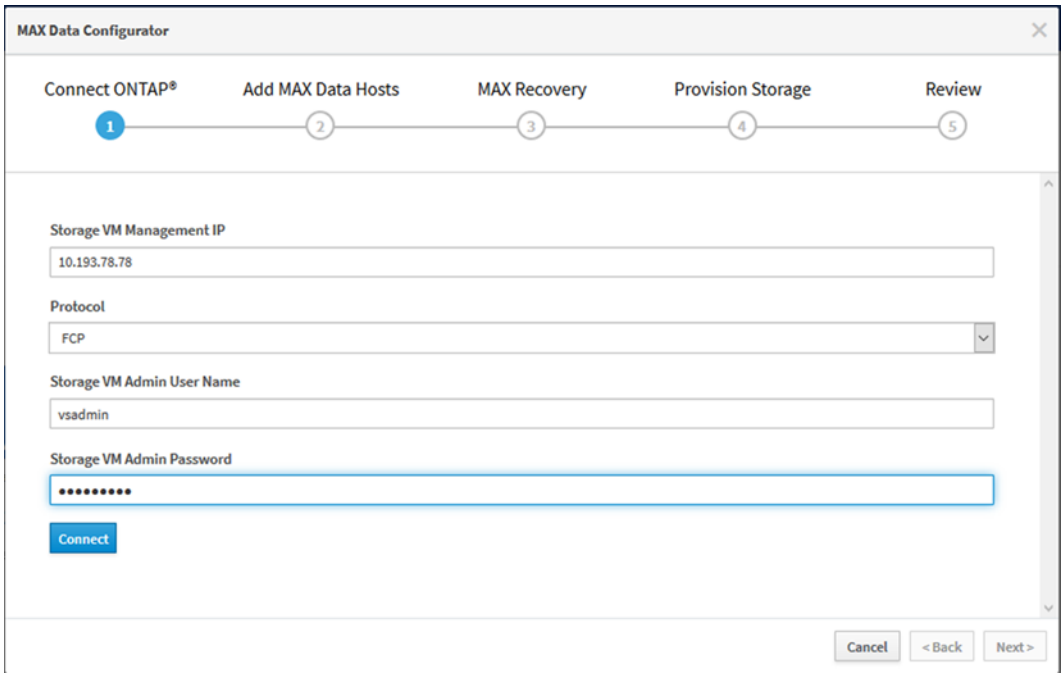
1. Open a web browser on a server where you installed MAX Data, and point it at `https://` *`hostname`*`|`*`IP_address`*`:9444`
2. Log in with root privileges.
3. Depending on whether your configuration will include an ONTAP system, select the appropriate storage resource icon.



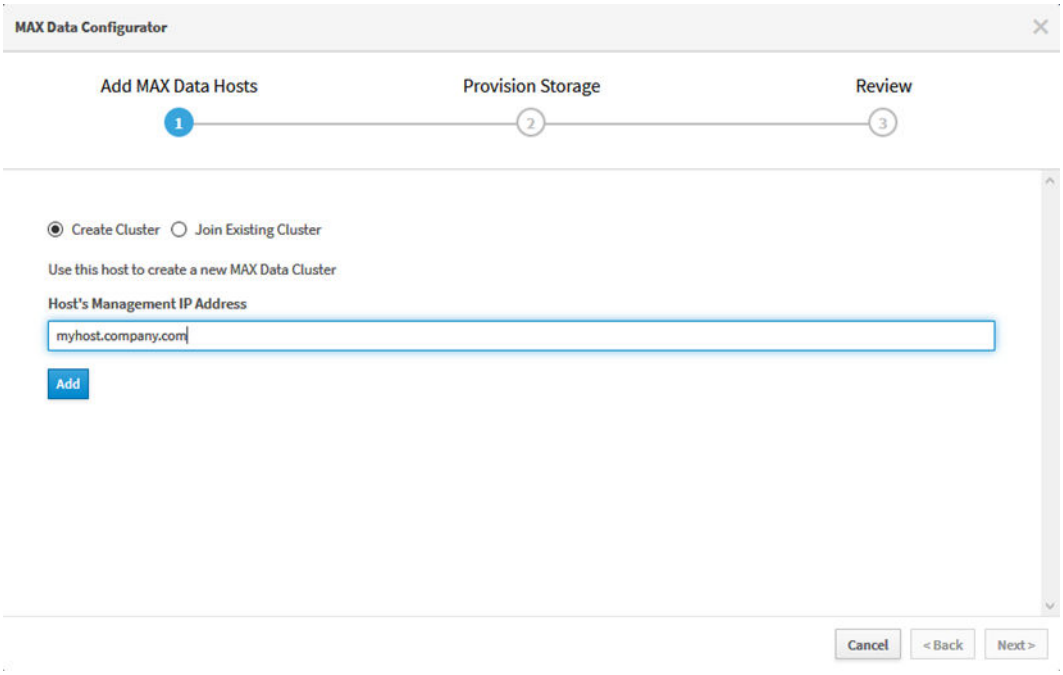
- Select ONTAP if your configuration will include an ONTAP storage system.
- Select FLASH if your configuration will use flash storage in a server-only configuration.

4. Follow configuration wizard prompts, entering the requested information including ONTAP credentials (if necessary), network addresses, desired memory configuration, licenses, and details about your application.

   The following image shows the initial configuration wizard screen when the configuration includes an ONTAP AFF system.



The following image shows the initial configuration wizard screen for a server-only configuration.



5. If desired, and the configuration includes an AFF system running ONTAP software, specify the MAX Recovery enabled host server to configure.

Recovering MAX Data applications

When configured with an AFF system, MAX Data provides a variety of options for protecting and recovering application data, including recovery using Snapshot copies and MAX Recovery hosts, data migration to an alternate host, application archiving, and SnapMirror SVM replication (SVMDR).

Recovering data from a Snapshot copy

If the application server running MAX Data is still functional, you can recover lost files from a Snapshot copy.

About this task

You can recover files using either the MAX Data GUI or command line interface.

Step

1. Recover the lost files:
   - If you want to use the MAX Data GUI:
     a. Open a web browser on a server where you installed MAX Data, and then point it to `https://hostname|IP_address:9444`
     b. Click the **Snapshots** tab.
     c. Select the desired copy, and then click the **Action** button on the far right.
     d. Click **Restore**.
        The file system is restored to the state at the time the selected Snapshot copy was made.
   - If you want to use the MAX Data CLI:
     a. Log in to the server with root privileges.
     b. Recover the files:

        `max_configurator snapshot restore --app app_name --app_component app_component_name --snap_name snapshot_name`

        Example

        `max_configurator snapshot restore --app madmax02 --app_component datafiles --snap_name newsnapshot`

        The file system is restored to the state at the time the selected Snapshot copy was made.

Recovering an application to a new server

If the application server running MAX Data is no longer functional, you can recover the application to a different MAX Data enabled application server. If you are using the optional MAX Recovery

enabled host server to mirror your MAX Data application logs, you can quickly recover data with a recovery point objective (RPO) of zero data loss.

Before you begin

A replacement application server with MAX Data software installed must already be provisioned. The replacement server must have the same specifications as the server it replaces.

Setting up application servers for MAX Data on page 11

About this task

You can recover applications through the MAX Data GUI of any surviving application server by adding a new server to the cluster. If there is no application server available, you can open the MAX Data GUI from the new server or, if available, through the MAX Recovery server.

Steps

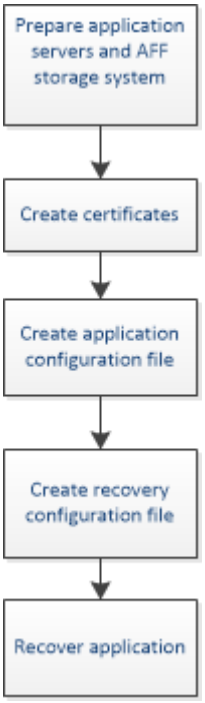
1. Open a web browser on a server where you installed MAX Data, and then point it to `https://hostname|IP_address:9444`
2. Log in with root credentials.
3. On the **Cluster** tab, click **Configure**.
4. Click **Add MAX Data hosts**.
5. Enter the IP address and credentials for the replacement application server.
6. On the **Provision Storage** page, select the **Recover Application** button, and then specify the recovery parameters:
   a. Select **Recover Application**.
   b. For **datafiles**, select **Snapshot copy**, and then select the latest Snapshot copy from which to recover.
   c. For **logs**, select **Recover from high availability MAX Recovery server**.

      Optionally, if you want to recover from a specific Snapshot copy instead of the MAX Recovery enabled host server, select an entry from the list of Snapshot copies.
   d. Scroll to the bottom of the page, and then click **Recover** to start the recovery.

Recovering an application following a disaster

If a disaster occurs, you can recover an application from the destination SVM. The destination SVM protects MAX Data by mirroring Snapshot copies according to the Remote Snapshot Copies schedule set up during MAX Data configuration.

The following is a summary of the disaster recovery process:



Preparing application servers and ONTAP for recovery

Recovering MAX Data requires provisioning replacement application servers and setting up the SVM on the ONTAP storage system.

Provisioning replacement application servers

For each application in the SVM, a replacement application server with MAX Data software installed must already be provisioned.

Setting up application servers for MAX Data on page 11

Preparing the ONTAP storage system

ONTAP storage systems used for SnapMirror SVM replication (SVMDR) are read-only systems. You must set up ONTAP to serve as the SVM for MAX Data, which includes making the system writable and configuring LIFs on each node of the ONTAP cluster.

Setting up the NetApp AFF storage system contains instructions for preparing the system for use with MAX Data.

Setting up the NetApp ONTAP storage system on page 10

Creating certificates for exchange with the SVM

The MAX Data enabled application server and AFF system (SVM) use certificates to authenticate each other. Under normal operating conditions, MAX Data automatically generates these certificates. For disaster recovery, you must manually create the certificates.

Steps

1. Log in to the server with root privileges.
2. In the working directory where you copied the software package, generate the certificate:

   ```
   ./max_configurator certificate create
   ```

3. Follow the command prompts, entering the requested information including the destination SVM management IP address, SVM admin name, MAX Data IP address or host FQDN, and SVM password.

After you are done, a message appears indicating that the system successfully created the certificate.

Creating the MAX Data application configuration file

The disaster recovery procedure requires that you create a configuration file that has been updated with the destination SVM and replacement MAX Data enabled application server information.

About this task

You need to create the configuration file for each application server.

Steps

1. Edit a copy of an existing configuration file, or create a new file from the sample configuration.

   The format must be JSON. The following table describes the values associated with each key:

Key entry		**Key value**
`version`		MAX Data version installed on application server.
`ontap`	`svm_management_ip`	Destination SVM management IP address.
	`svm_admin_name`	Administrator name.
	`svm_name`	Name assigned to the destination SVM.
	`data_protocol`	SAN protocol: “fcp” or “iscsi”, depending on the network.

Key entry			Key value
`application`	`name`		Name assigned to the MAX Data server.
	`type`		Application type can be “mongodb”, “oracle”, or “san”.
	`m1fs`	`name`	MAX Data filesystem (MAX FS). Depending on the application, requires configuration values for data and log files. The example uses entries named “datafiles” and “logs”.
		`role`	Recovery server configuration. Use “single-node” only.
		`flavor`	Memory configuration. Use “pm” for nonvolatile memory (NVDIMM-N). Use “mimic_pm” for DRAM used to mimic persistent memory.
		`pmem_capacity_gb`	Persistent memory size. Set this value to match the amount of memory allocated to MAX Data.
		`remote_syncsnap_freq_minutes`	Policy for mirroring Snapshot copies to a destination SVM. Valid values are 15 (minutes), 60 (1 hour), and 360 (6 hours).
		`local_syncsnap_freq_minutes`	Policy for Snapshot copies. Valid values are 15 (minutes), 60 (1 hour), and 360 (6 hours).

Example

```
{
    "version": "1.0",
    "ontap": {
        "svm_management_ip": "10.234.84.161",
        "svm_admin_name": "vsadmin",
        "svm_name": "vs3",
        "data_protocol": "iscsi"
    },
    "application": [
        {
            "name": "scspr0537330014_new",
            "type": "oracle",
            "m1fs": [
                {
                    "name": "datafiles",
                    "role": "single_node",
                    "flavor": "mimic_pm",
                    "pmem_capacity_gb": 1,
                    "remote_syncsnap_freq_minutes": 60,
                    "local_syncsnap_freq_minutes": 15
                },
                {
                    "name": "logs",
```

```
                    "role": "single_node",
                    "flavor": "mimic_pm",
                    "pmem_capacity_gb": 1,
                    "remote_syncsnap_freq_minutes": 60,
                    "local_syncsnap_freq_minutes": 15
                }
            ]
        }
    ]
}
```

2. Save the file with a `.json` extension.

Creating the recovery file

The disaster recovery procedure requires a recovery file that specifies the component Snapshot copies to use for recovery.

About this task

You need to create a recovery file for each application server.

Steps

1. Create a recovery file from the sample configuration.

   The format must be JSON. The following table describes the values associated with each key.

Key entry			Key value
`application`	`name`		Name assigned to MAX Data server.
	`mlfs`	`name`	MAX Data filesystem (MAX FS). Depending on the application, requires configuration values for data and log files. The example uses entries named “datafiles” and “logs”.
		`scenario`	Use “snapshot” only.
		`snapshot_name`	Snapshot copy from which to recover MAX Data. You can get the Snapshot copy name from the destination SVM.

Example

```
{
    "application" : [
    {
        "name" : "scspr0537330014_new",
        "m1fs" : [
            {
            "name" : "datafiles",
            "scenario" : "snapshot",
            "snapshot_name": "scspr0537330014_data002"
            },
            {
            "name" : "logs",
            "scenario" : "snapshot",
            "snapshot_name": "scspr0537330014_logs002"
            }
        ]
    }
    ]
}
```

2. Save the file with a `.json` extension.

Recovering applications from the destination SVM

If a disaster occurs, you can recover applications from the destination SVM.

Before you begin

- Replacement MAX Data enabled application servers must be available, and the SVM must be set up on the ONTAP system.
- Certificates must have been created on each application server.
- Configuration and recovery files must have been created on each application.

About this task

You must complete the procedure for each application server running MAX Data.

Steps

1. Log in to the server with root privileges.
2. Start the recovery process:

   ```
   max_configurator config --conf_file appconfig.json --recover_file
   recoverappconfig.json
   ```

   The system runs a series of checks and configuration steps, prompting you to reboot the system when complete.
3. Press **Enter** to reboot the server.
4. Following reboot, open a browser and then point it to the server running MAX Data: `https://hostname|IP address:9444`.
5. Click **File System Monitoring** to check the MAX Data mount points and verify recovery.

Migrating applications to a new server

You can migrate applications from a server running MAX Data to a different MAX Data enabled application server to increase system capacity or performance, manage systems, or perform maintenance on the existing system.

Before you begin

A replacement application server with MAX Data software installed must already be provisioned. The replacement server must have the same or greater specifications than the server it replaces.

Setting up application servers for MAX Data on page 11

Steps

1. Point a web browser to a MAX Data application server: `https://hostname|IP_address:9444`
2. Log in with root credentials.
3. On the **Cluster** tab, click **Configure**.
4. Click **Add MAX Data hosts**.

5. Enter the IP address and credentials for the replacement server.
6. Click **Next**.
7. On the **Provision Storage** page, select the **Recover Appplication** radio button, sand then specify the recovery parameters:
   a. Select **Recovery Flow**, and then choose **Migration** from the pull-down menu.
   b. Select **Original Host**, and then use pull-down menu to specify the host from which you want to migrate the application.
   c. Click **Recover** to start the recovery and deploy the configuration.

      The server will reboot. At the end of the process, all data will be available in the replacement application server. The original server will be marked “Archived” in the MAX Data GUI.

Archiving an application

You can archive the MAX Data application for extended storage.

About this task

During the archiving process, MAX Data moves all data from non-volatile memory to the AFF storage as part of the unmounting process for the application. This can take several minutes.

Steps

1. Point a web browser to an application server using MAX Data: `https://hostname|IP_address:9444`
2. Log in with root credentials.
3. Click the **Cluster** tab.

   The MAX Data Cluster page appears. This page provides information about each MAX Data application server and MAX Recovery host configured in the cluster.
4. Identify the entry that will be the archive target.
5. From the menu icon at the right of the screen, select **Archive Applications**.

   At the end of the process, all data will be available in ONTAP, and the application server will be marked “Archived” in MAX Data.

After you finish

When you are ready to recover the archived data, follow the procedure “Migrating applications to a new server” to move the data to a new application server.

Migrating applications to a new server on page 30

Managing MAX Data

Procedures for managing MAX Data and MAX Recovery operations include creating or deleting Snapshot copies, monitoring applications, managing MAX Data licenses, adding spare servers, and removing applications.

Creating Snapshot copies on demand

You can generate a Snapshot copy of an application on demand using either the MAX Data GUI or MAX Data command line interface (CLI).

Step

1. You can create Snapshot copies using either the MAX Data GUI or command-line interface (CLI).

   - If you want to use the MAX Data GUI:

     a. Open a web browser on a server where you installed MAX Data, and then point it to `https://hostname|IP_address:9444`

     b. Select the **Hosts** tab.

     c. Click the **Snapshots** tab.

     d. Select a mount from the **MAX FS Mount** pull-down menu.

     e. Click the camera icon (), and then enter a name for the Snapshot copy.
     MAX Data displays a message indicating that the operation was successful for the specified file.

   - If you want to use the MAX Data CLI:

     a. Log in to the server with root privileges.

     b. Create the files:

     `max_configurator snapshot create --app app_name --app_component app_component_name --snap_name snapshot_name`

     Example

     `max_configurator snapshot create --app madmaxd02 --app_component datafiles --snap_name newsnapshot`

     MAX Data displays a message indicating that the operation was successful for the specified file.

Deleting Snapshot copies using MAX Data

For MAX Data enabled application servers, you can manually delete both data and logs component Snapshot copies.

About this task

You can delete Snapshot copies using either the MAX Data GUI or command-line interface (CLI).

Step

1. Delete the Snapshot copies:
   - If you want to use the MAX Data GUI:
     a. Open a web browser on a server where you installed MAX Data, and then point it to `https://hostname|IP_address:9444`
     b. Select the **Hosts** tab.
     c. Click the **Snapshots** tab.
     d. Select a mount from the **MAX FS Mount** pull-down menu.
     e. Select the desired Snapshot copy to delete.
     f. Click the **menu** icon on the far right, and then select **Delete**.
     MAX Data displays a message indicating that the operation was successful for the specified file.
   - If you want to use the MAX Data CLI:
     a. Log in to the server with root privileges.
     b. Delete the files:
     `max_configurator snapshot delete --app app_name --app_component app_component_name --snap_name snapshot_name`
     Examples
     `max_configurator snapshot delete --app madmaxd19 --app_component datafiles --snap_name snapshot123`
     `max_configurator snapshot delete --app madmaxd19 --app_component logs --snap_name snapshotabc`
     MAX Data displays a message indicating that the operation was successful for the specified file.

Monitoring applications using MAX Data

You can use MAX Data to monitor capacity and performance metrics for the application server. You can also view logs.

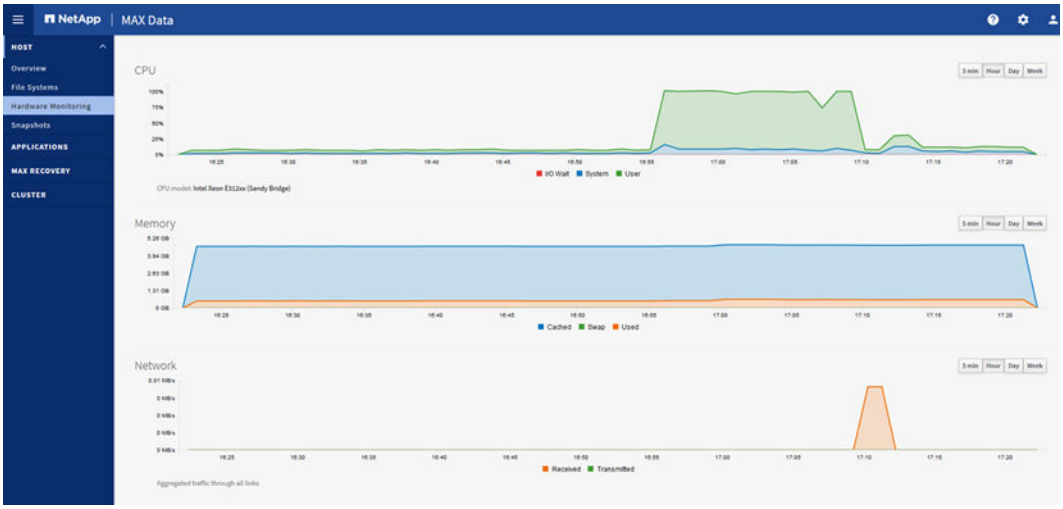
Steps

1. Open a web browser on a server where you installed MAX Data, and then point it to `https://hostname|IP_address:9444`
2. Log in with root credentials.
3. Click the **Host** tab on the top left, and then click one of the monitoring tabs.

Monitoring tab	Description
File systems	Describes the application mount points, capacity trends, usage breakdown, and data locality trends. Click links to see additional details.
Hardware Monitoring	Illustrates the hardware resource activity for the system, including CPU, memory, and network utilization.

Monitoring tab	Description
MAX Recovery	Displays MAX Recovery host server information, including the connected hosts and storage utilization.
Snapshots	List of Snapshot copies for an application. Use the pull-down menus to change application and backup views.

The following is an example of the **Hardware Monitoring** tab. Your system might look slightly different.



Managing MAX Data licenses

You can manage MAX Data and MAX Recovery licenses in the MAX Data **Licenses** tab.

About this task

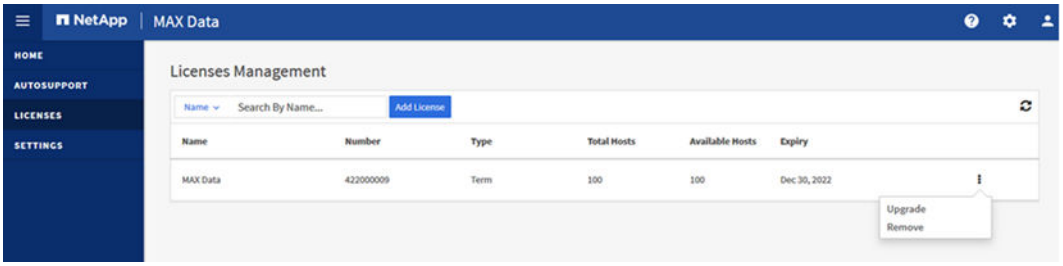
Typically, licenses are added to a specific MAX Data application server or MAX Recovery host at configuration time. Using the GUI, you can monitor, add, upgrade, and delete licenses.

Steps

1. Open a web browser on a server where you installed MAX Data, and then point it to `https://hostname|IP_address:9444`
2. Log in with root credentials.
3. If the **HOME** tab is not displayed, click the settings icon:

4. Click the MAX Data **LICENSES** tab.

   The Licenses Management page appears. This page displays the number of hosts supported by each license, the number of hosts using the license, and the license expiration date.



5. Click a specific license to review which hosts are using the license.
6. Add, upgrade, or remove a license in the MAX Data cluster:
   - If you want to add a new license:
     a. Click **Add License**.
     b. Upload the license file.

     The new license appears in the list.
   - If you want to upgrade a license:
     a. Identify the MAX Data or MAX Recovery license that you want to upgrade.
     b. From the menu icon at the right of the screen, select **Upgrade**.
     c. Upload the new license file.
     d. Log in to the server with root privileges.
     e. Restart the dashboard:
        ```
        systemctl restart max-dashboard
        ```

     The upgraded license appears in the list.
   - If you want to remove a license:
     a. Identify the MAX Data or MAX Recovery license that you want to remove.

        Note: Click a specific license to review which hosts are using the license.

     b. From the menu icon at the right of the screen, select **Remove**.

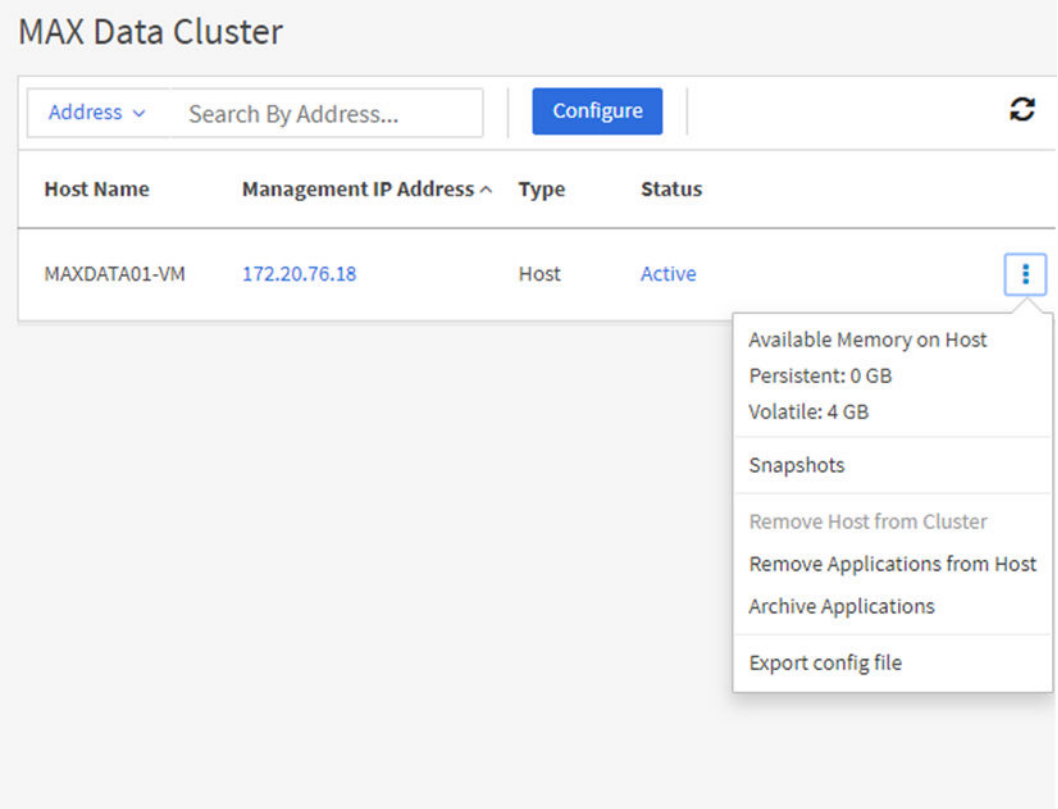
     The license is removed from the list.

Resizing storage for an application

To resize the amount of storage configured for an application on a host, you must archive the application and then redeploy the host with the new memory configuration.

Steps

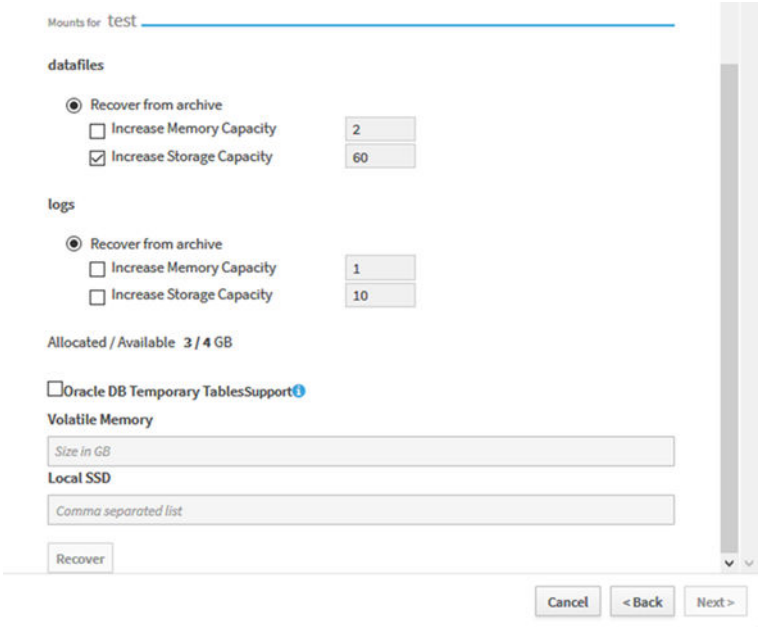
1. Navigate to the host in the MAX Data Cluster tab and select **Archive Applications** on the pop-up menu.



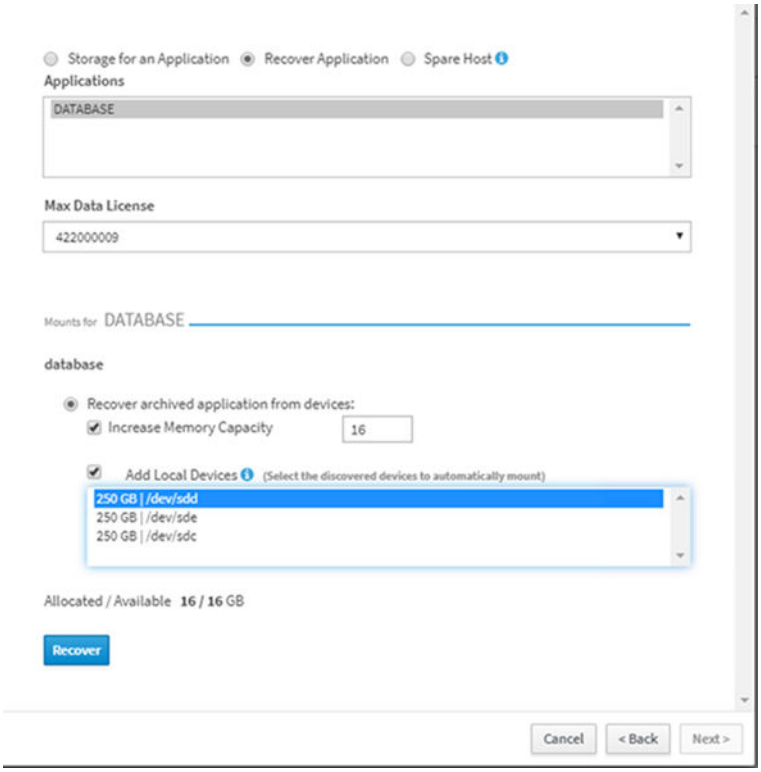
2. Confirm the archive operation when prompted.
3. After the archiving operation is complete, on the MAX Data Cluster tab, select the host and click Configure to launch the MAX Data Configurator.
4. In the MAX Data Configurator, click **Next** or **Skip** to advance through the tabs to display the Provision Storage tab.
5. On Provision Storage tab, select the Recover Application and select the option to Increase Memory Capacity.

   If your configuration includes an ONTAP storage system, you can increase either the allocated local memory capacity or the ONTAP LUN capacity:

   - Use the Increase Memory Capacity field to increase the local memory.
   - Use the Increase Storage Capacity field to increase the memory on the storage system.

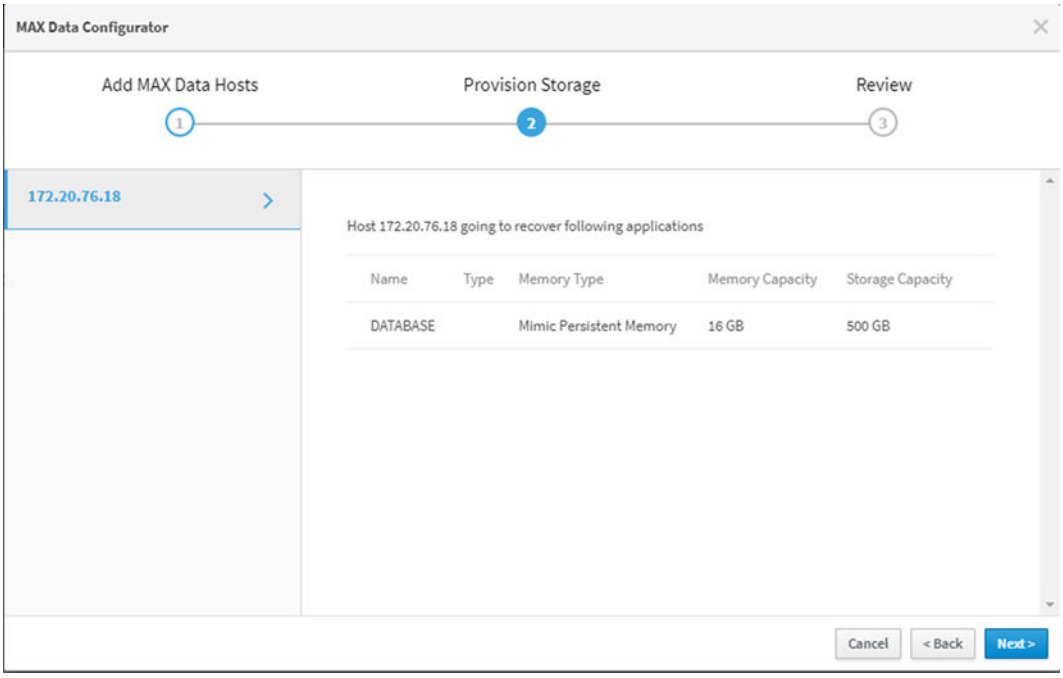


If you have a server-only configuration, you can increase the local memory capacity and add local devices as desired.

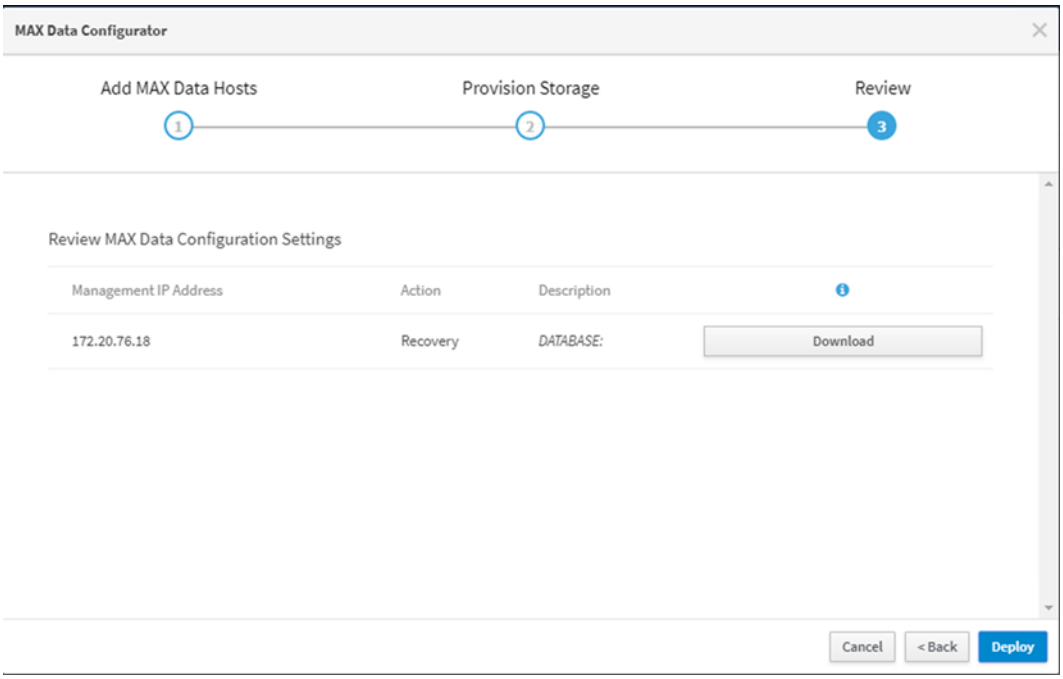


6. After making the desired changes, click **Recover**.

   The changes are reflected in the application information.



7. Click **Next**.
8. Confirm the information on the Review tab.



9. Click **Deploy**.

Configuring a spare application server

You can configure an application server to use as a spare for future MAX Data operations, including recovery or migration.

Before you begin

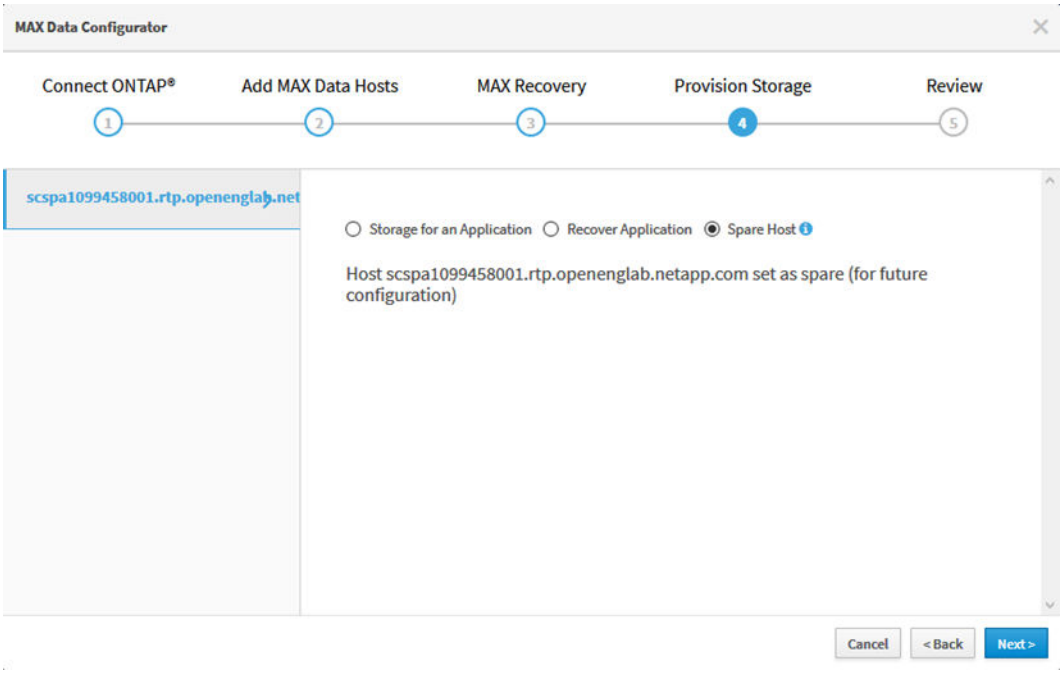
A replacement application server with MAX Data software installed must already be provisioned.

Setting up application servers for MAX Data on page 11

Steps

1. Point a web browser to a MAX Data server: `https://hostname|IP_address:9444`
2. Log in with root credentials.
3. On the **Cluster** tab, click **Configure**.
4. Click **Add MAX Data hosts**.
5. Enter the IP address and credentials for the spare application server.
6. On the **MAX Recovery** page, click the **Skip** button.
7. On the **Provision Storage** page, select the **Spare Host** radio button.

   A message appears indicating that the host has been set as a spare server.



8. Scroll to the bottom of the page, and then click **Review** to continue to the **Review** page.
9. Verify the information on the page, and then click **Deploy**.

Removing applications from MAX Data

You can remove applications from MAX Data enabled servers to unconfigure the settings on the application server and the ONTAP ONTAP storage cluster while keeping MAX Data installed.

Steps

1. Stop the application to end I/O on MAX FS mounts.
2. Open a web browser on a server where you installed MAX Data, and then point it to `https://hostname|IP_address:9444`
3. Log in with root credentials.
4. Click the **Cluster** tab.
5. For each server listed, click the **menu** icon at the end of the row, and then select **Remove Applications from Host**.

   This step unmounts all MAX Data file systems, frees all volatile memory (DRAM allocated to act in place of persistent memory) for the server if it is used, and deletes all partitions from the persistent memory resource. Additionally, all MAX Data storage and metadata is deleted from the ONTAP cluster. Finally, the MAX Data enabled application server will reboot.

Removing a MAX Recovery host from the cluster

You can remove a MAX Recovery enabled host server from the cluster using the MAX Data GUI.

Steps

1. Open a web browser on a server where you installed MAX Data, and then point it to `https://hostname|IP_address:9444`
2. Log in with root credentials.
3. Click the **MAX Recovery Servers** tab.
4. Click the **menu** icon at the end of the data row, and then select **Clean Mirrored Data**.

   Mirrored data must be removed from the MAX Recovery host server prior to removing that host from the MAX Data cluster.
5. Click the **menu** icon at the end of the data row, and then select **Remove Host from Cluster**.

Uninstalling MAX Data and MAX Recovery

You can remove MAX Data and MAX Recovery software from the host where you installed it.

Before you begin

MAX Data and MAX Recovery enabled servers must already be removed from the MAX Data cluster.

Removing applications from MAX Data on page 40

Removing a MAX Recovery host from the cluster on page 40

Steps

1. Log in to the server with root credentials.
2. In the working directory where you copied the software package, uninstall the software:

   ```
   ./max_uninstall.sh
   ```
3. Repeat these steps for each MAX Data enabled application server and MAX Recovery enabled host server in your configuration.

Copyright

Trademark

How to send comments about documentation and receive update notifications

You can help us to improve the quality of our documentation by sending us your feedback. You can receive automatic notification when production-level (GA/FCS) documentation is initially released or important changes are made to existing production-level documents.

If you have suggestions for improving this document, send us your comments by email.

doccomments@netapp.com

To help us direct your comments to the correct division, include in the subject line the product name, version, and operating system.

If you want to be notified automatically when production-level documentation is released or important changes are made to existing production-level documents, follow Twitter account @NetAppDoc.

You can also contact us in the following ways:

- NetApp, Inc., 1395 Crossman Ave., Sunnyvale, CA 94089 U.S.
- Telephone: +1 (408) 822-6000
- Fax: +1 (408) 822-4501
- Support telephone: +1 (888) 463-8277

Index

C

comments
how to send feedback about documentation *44*

D

documentation
how to receive automatic notification of changes to *44*
how to send feedback about *44*

F

feedback
how to send comments about documentation *44*

I

information
how to send feedback about improving documentation *44*

S

suggestions
how to send feedback about documentation *44*

T

Twitter
how to receive automatic notification of documentation changes *44*