HA Guidelines Summary for Shared MDBs in an MSCS Environment

Designing for High Availability (i.e., “failover,” “fault tolerance”) is not only highly desirable for most enterprise software solutions but, in some cases, it is a business requirement. For many of these deployments, cluster technology is the HA tool of choice, however, not all software solutions can be easily deployed in a cluster environment. Further challenges are presented when that deployment involves multiple solutions sharing a common component.

This document outlines best practices for deploying an HA SQL Server based Management Database (MDB) in a Microsoft Cluster Server (MSCS) environment and provides guidelines for situations in which that MDB will be used by multiple products. The specific products and releases include:

- Unicenter Network and Systems Management (NSM) r11.1
- Unicenter Desktop and Server Management (DSM) r11.1, r11.1a
- Unicenter Service Desk (USD) r11.1, r11.2
- Unicenter Asset Portfolio Management (UAPM) r11.1 and 11.2

The r11 versions of each of these products support only an Ingres MDB and are not, therefore, included in this discussion.

Note: HA can be achieved through other methods, such as BrightStor High Availability (BHA) and native database replication utilities, however, these are beyond the scope of this document.

Understanding the Role of HAS

The CA High Availability Service (HAS), which is part of CA Common Services (CCS) automates the process of detecting an active cluster node and enables rapid failover in response to a failed node. HAS is installed automatically whenever a CA solution employing CCS is installed on a clustered computer. The solution’s HA components are then registered with HAS, which monitors those cluster resources and notifies the application whenever a failed or newly active node is detected. In the event that a failure notification is received, that application can then stop the affected component on the failed node and start it up on the newly active (failover) node.

HAS Supports the following two cluster configurations:

- Active/Passive – in which a single instance of a fault tolerant component runs on one of the physical servers in the cluster. The remaining nodes in the cluster are on "standby mode" until a failure on the active node or a manual failover occurs during maintenance.
- Active/Active – in which multiple instances of a fault tolerance component run on both nodes of a two-way cluster. If one of those instances fails, it automatically fails over to the other server.

To be effective, HAS should be active on all server nodes in the cluster.

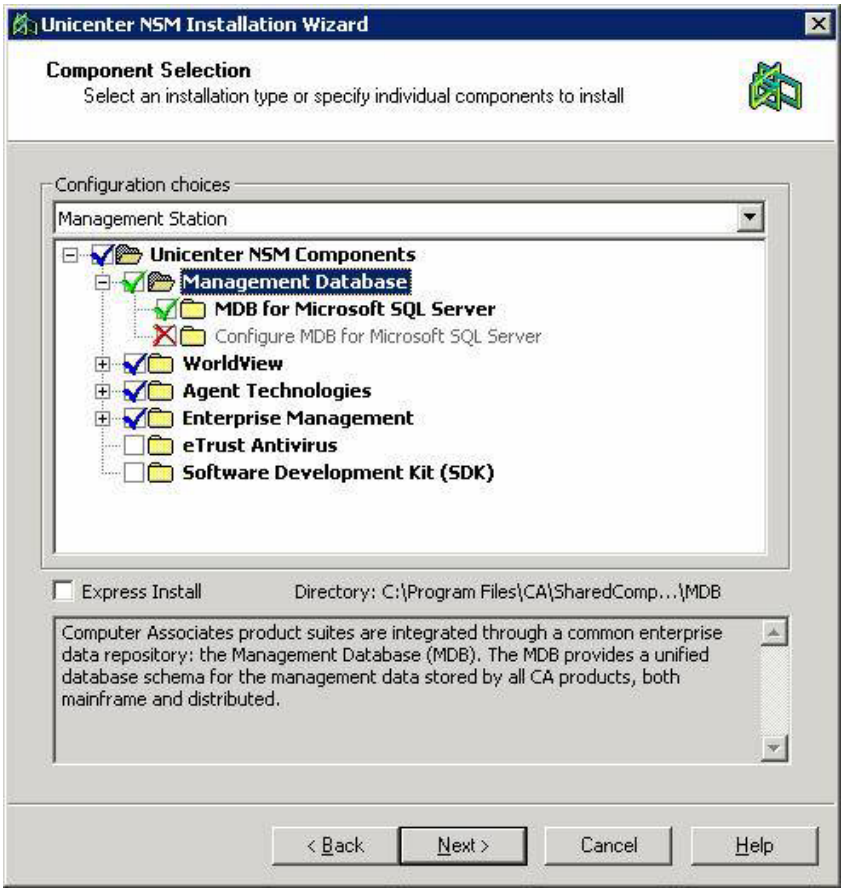
Communication between the cluster software and the deployed solution is managed by the HAS Cluster Service Layer (CSL) – greatly simplifying the HA process.

For more information on HAS architecture, including the Cluster Service Layer (CSL), consult the *Unicenter NSM r11.1 Implementation Guide*.

Not all solutions currently deploy CCS and, therefore, not all solutions have direct access to HAS. Those solutions that don't, however, can take advantage of HAS-compliant solutions if they are deployed in the same architecture.

HA Implications for Unicenter NSM

Unicenter NSM does employ CCS\HAS and, as a result, it provides an HA solution out-of-the-box for many of its Windows based components. If cluster software is detected on the target computer, the NSM installation program automatically displays the available HA options.



The list of HA compliant NSM components currently include the following:

- Enterprise Management (Event Management, Job Management Option)
- Advance Event Correlation (AEC)
- Agent Technology
- WorldView

Components which are not HA compliant will not be available for selection. The Alert Management System (AMS), for example, does not support fault tolerance for HAS.

As part of an HA installation you will be prompted to select the **resource group** to which components will be installed. A resource group is the logical entity that combines all of the resources required to make a service or application highly available. Resources can include physical hardware devices (e.g., disk drives and net cards) or logical entities (e.g., logical disk volumes, TCP/IP addresses, entire applications and databases).

- If the MDB is being installed on the **local** machine, the install process will list all eligible SQL resource groups.
- If the MDB is being installed on a separate (i.e., **remote**) machine, the list of eligible resources displayed will depend on whether or not SQL is installed on the *local* computer. If it is, the install process will list all eligible SQL resource groups (non-SQL resource groups will not be listed). If SQL is not installed on the local computer, select any other resource group which has a network name, IP address and physical disk resource types.

If there are multiple **SQL instances**, you will need to first identify the SQL instance where the MDB is to be installed, then select the resource group where the SQL instance is defined.

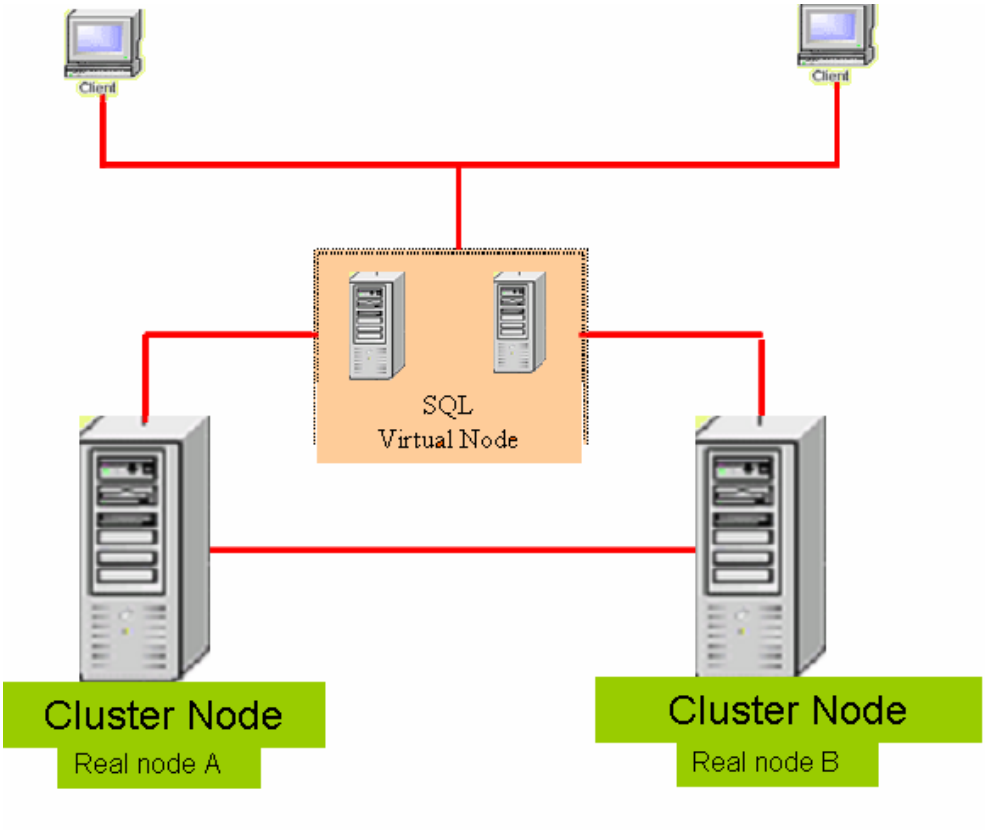
Note: Although NSM supports installation to a non-default SQL instance, not all solutions do and this can become an issue when there are multiple solutions being deployed with a shared MDB. When in doubt, use the default SQL instance.

To ensure that HAS works across the nodes of your cluster you must run HAS under a cluster domain account on Windows.

To install a local HA MDB, you will need to do the following:

1. Install NSM on Node “A” (the active node). In general, you should install all NSM components you intend to use on this node.
2. Offline the NSM resources on Node “A”
3. Move the resource group to Node “B”
4. Install NSM on Node “B” being careful to select the same options as for the Node “A” install. Note that you will not be prompted to select a cluster resource group for this and any subsequent cluster node installs.
5. Customize as needed

The MDB is created during the install on the first cluster node. For subsequent cluster node installs (e.g., Node “B”), the install process merely verifies that the MDB exists and is at the correct MDB level. If this is verified, it will not be upgraded or recreated.



The install process will not permit a mix of non-HA components with HA components if there is any interdependency between them. For example, if the Agent Technology manager was installed as non-HA and, later, you add an EM component, EM will be forced to be non-HA.

Further information on installing Unicenter NSM r11.1 components in a cluster environment can be found in the *Unicenter NSM Implementation Guide* as well as in the following presentations (which are available from the Implementation Best Practices page):

- Unicenter NSM r11.1 and Clusters - Part 1 (overview and MDB considerations)
- Unicenter NSM r11.1 and Clusters - Part 2 (AT, MCC, 2d Map, JMO, Event Mg., and uninstall procedures)
- Unicenter NSM r11.1 and Clusters - Part 3 (installing HA MDB from Unicenter DSM r11.1 media)

HA Implications for Unicenter Desktop and Server Management

Unlike Unicenter NSM, Unicenter DSM does not include CCS and is **not** currently "cluster aware." DSM can, however, use an *existing* HA MDB but the other DSM components (e.g., Domain Manager, Scalability Server, etc) cannot be HA at this stage. These DSM components will have to be installed on a different server which is not HA. Even if DSM is installed on top of an existing HA Unicenter NSM implementation, those DSM components will still not be HA.

If Unicenter NSM is part of the architecture the best practice recommendation is to allow NSM to create the MDB and to have DSM access that MDB remotely. But, if this is not an option, there are two documented alternatives which are summarized below.

The **first option** is to use the DSM media to install the HA MDB to a cluster node and the remaining DSM components on separate nodes outside the cluster. Although the DSM install program supports an MDB only installation option, it restricts that installation to a local MS-SQL server host. Since cluster configurations use virtual node names (which are interpreted as remote location and, therefore, are not accepted by the DSM install dialogs) you will need to temporarily create a SQL alias for the vnode to get around this restriction. Once the installation completes, the alias can be deleted. For details regarding this scenario, consult the "Best Practices for Implementing Unicenter NSM r11.1 in an HA MSCS Environment: Part III" presentation which is available from the Implementation Best Practices page.

A **second option** is to install the DSM to a non-HA environment, then detach the MDB and subsequently reattach it to a SQL instance which **is** HA. To implement this option you will need the following:

- An existing functioning MS-SQL Server instance
- Verification of name resolution and communications between DSM Manager host and SQL Server cluster
- Available host system with local instance of MS-SQL Server which can be used to (temporarily) create the MDB as well as means to transfer the database files created on this host to the SQL cluster (e.g., network connectivity, DVD burner)

The overall process requires the following steps:

1. Install the MDB to the temporary SQL host (but do not install any DSM components at this time).
2. Detach the MDB from the temporary host using standard SQL procedures
3. Copy the MDB database and log files from the temporary host to the designated shared resource drive(s) on the cluster system.
4. Attach the MDB to the MS-SQL Cluster using standard SQL procedures, providing the SQL virtual node name in response to the prompt for the database server name.

Full details are provided in the "Implementing Unicenter Desktop and Server Management (DSM) with Microsoft SQL Servers" document which is also available from the Implementation Best Practices page.

Regardless of which scenario you implement, CAF will need to be manually restarted in the event the MDB fails over. These restrictions should be resolved in the future release of DSM.

HA Implications for USD

Help desk is often viewed as mission critical. Therefore, Fault Tolerance\HA is considered high on the list of requirements for USD.

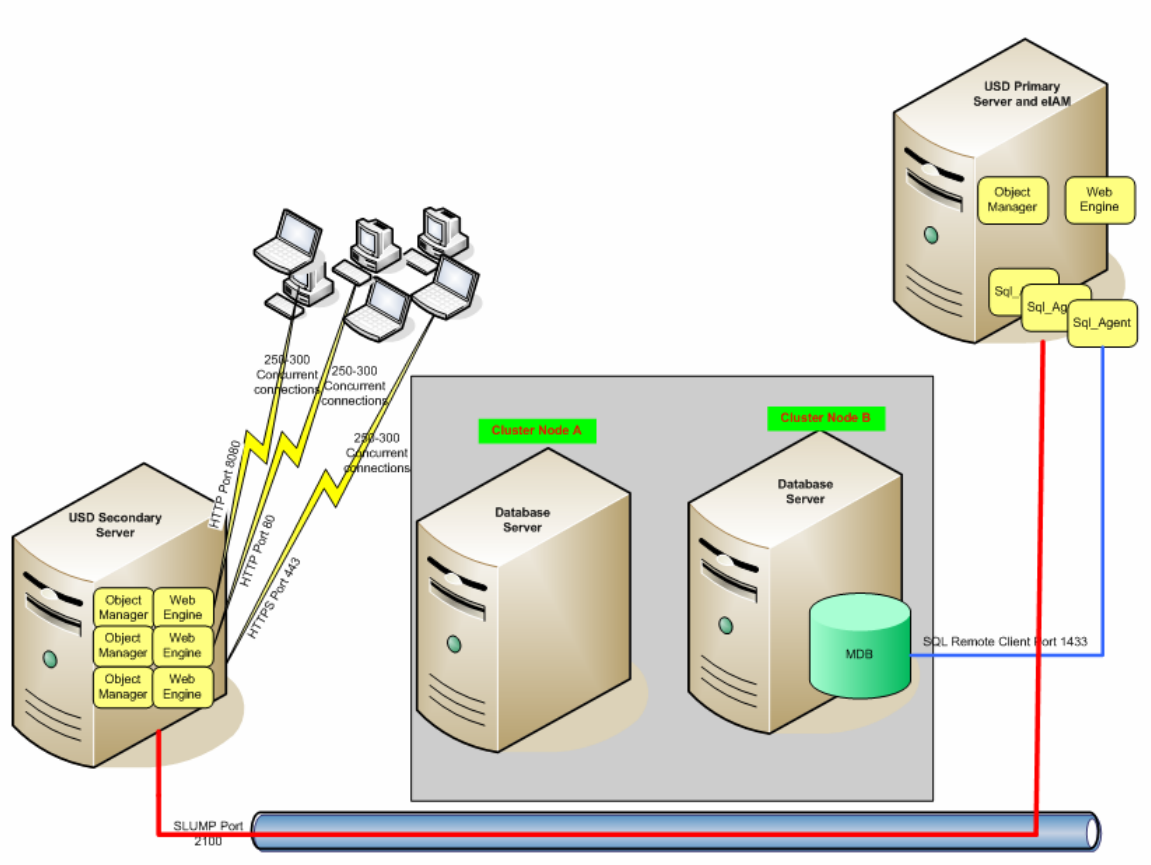
As with DSM, USD is **not** itself cluster aware, but USD r11.1 can *share* an HA MDB that has been installed in an MSCS cluster by Unicenter NSM. This is considered the best practice approach for establishing an HA MDB.

Although USD installation media can also be used to install a remote HA MDB, the same SQL alias workaround is required. By default, the USD Remote Components (i.e., the MDB) installation process will not recognize the SQL Virtual Cluster Node, which it considers to be a remote node. It will, therefore, prevent the MDB from being installed on that node. Temporarily defining a SQL alias to represent the Vnode allows you to bypass this restriction.

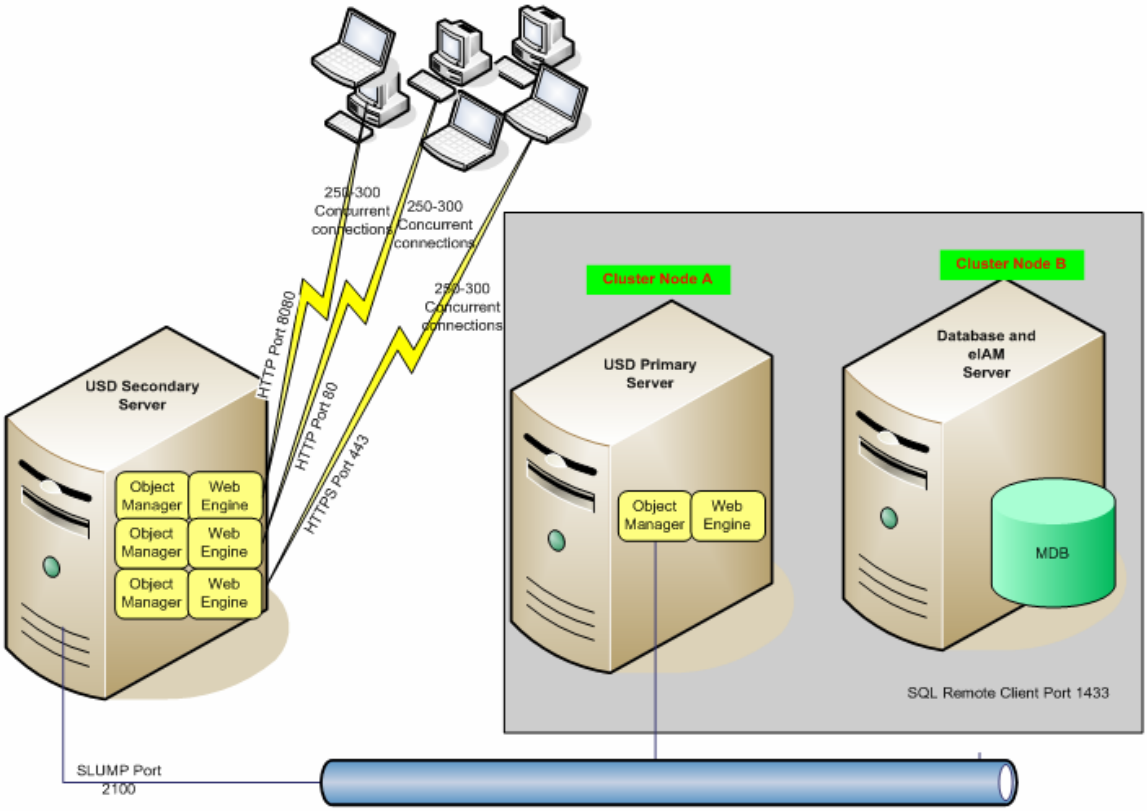
Note: The SQL alias is only required for the duration of the install and can be discarded once that completes.

There are three documented scenarios for deploying an HA MDB for USD (in the absence of a shared HA NSM created MDB). Each utilizes a different placement for the MDB, the Primary Server and eTrust Identity and Access Management (eIAM). They are:

- **Scenario 1**: In the first scenario, the USD Remote Components (which include the MDB) are installed on a cluster node to create an HA SQL MDB. The Primary Server and eIAM are then installed on a separate, non-HA server.



- **Scenario 2**: In the second scenario, an HA SQL MDB is installed (also without eIAM) on an active cluster node only. Installing remote components to other cluster nodes is **not** required in this scenario. The Primary Server is then installed on the same cluster – but to a different cluster group while eIAM is installed on a third, *non*-HA server. During normal operations, the Primary Server and MDB will be active on different cluster nodes. In the event the second cluster node is lost, the Primary Server and MDB may be active on the same cluster node (depending on how many nodes are in the cluster). They can also be active on different cluster nodes in the event the active nodes have been swapped around.
- **Scenario 3**: In the third scenario, an HA MDB and HA Primary Server are also installed in the same cluster but in different cluster groups. The key difference between this and the previous scenario, however, is that eIAM is installed in the same cluster as well.



Regardless of which scenario is implemented, the failover is not entirely automatic. If the MDB fails over to another cluster node, active clients will need to relogin to USD.

Details on implementing these scenarios can be found in the "Best Practices for Implementing Unicenter Service Desk r11.1 in an HA MSCS Environment" presentation series available on the Implementation Best Practices site.

- Part 1 of the series outlines installation of remote components without eIAM
- Part 2 outlines installation of the non-HA Primary Server with eIAM.
- Part 3 outlines how to install the HA Primary Server
- Part 4 details how to install the HA MDB with eIAM and an HA Primary Server (i.e., Scenario 3)

The usdCluster.zip and usdPSCluster.zip resource kits are available from the same location. These kits include customizable files which can be used to simplify resource definition for the USD Service.

HA Implications for UAPM

UAPM does not support HA out of the box but, by following best practices recommendations, it can be implemented as cluster-aware.

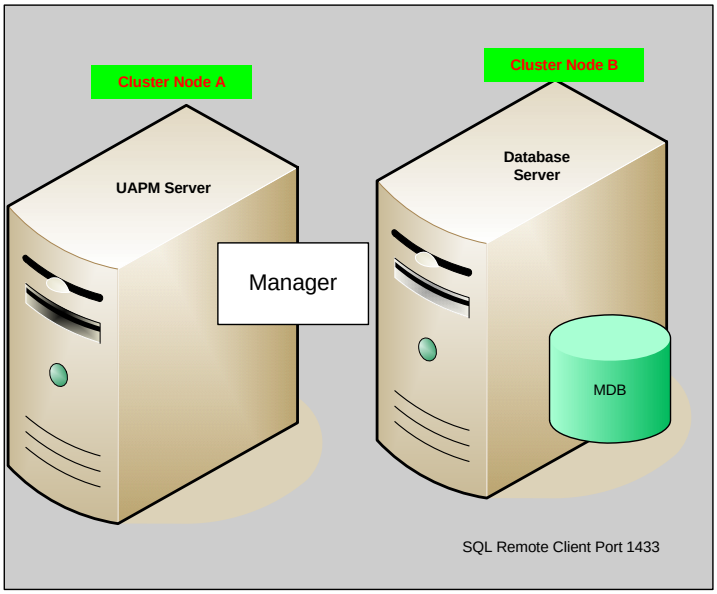
The cluster group to which UAPM will be installed should be different from the SQL client group in order to allow UAPM and the MDB to be active on different cluster nodes. If required, however, they can both share the same SQL cluster group.

TO install an HA MDB for UAPM you will need to do the following:

1. Install optional components (i.e., the MDB) on **all** nodes in the cluster. Unless an existing MDB will be used, the UAPM MDB will be created on the first cluster node. For subsequent nodes the install process will simply create the required registry entries.
    a. First, install optional components on Node “A”
    b. Move SQL group
    c. Install optional components on Node “B”– using same options, including same sql user id and password
2. Install UAPM managers to same cluster but different cluster group node.
    a. First, install UAPM managers on Node “A”
    b. Use uapmcluster resource kit to define cluster resources for UAPM
    c. Online cluster resources
    d. Use UAPM configurator to customize UAPM
    e. Offline cluster resources
    f. Move group to Node “B”
    g. Repeat install on Node “B” – selecting same options. No need to run the database utility.

The cluster group on which the UAPM Manager cluster resources will be defined can be same group as Microsoft SQL Group or a different cluster group.

To understand how the MDB and UAPM Managers components can be installed on the same Microsoft Cluster but in different cluster groups, consider the following graphic:



In this configuration, when a failover occurs the MDB and manager's components can end up being active on the same node or the MDB may end up being active on NodeA while the manager components are active on NodeB.

These procedures can also be adapted to install HA optional components and HA UAMP managers in 2 different clusters or to intermix an HA and non-HA setup.

Note: If UAPM is installed with other products, such as Unicenter Service Desk (USD), then you should select the same group in which USD is installed.

If the MSCS cluster includes multiple named SQL instances, it is important to correctly identify the SQL Cluster Group on which the MDB will be created. Installing multiple MDBs on one server is **not recommended** and some products may fail to work if multiple MDBs are created on the same Microsoft Cluster.

Note: The eIAM option provides the ability to use a directory service, such as Novell, Active Directory, or eTrust, as the authentication method for managing access to the UAPM Web GU. The UAPM install process, however, only requires eIAM to be installed with an Ingres MDB. Since this document is only applicable to MS-SQL MDBs, it does not include considerations for selecting eIAM.

Now put them all together...

In general, if you need to deploy an HA MDB in an MSCS environment, and **if Unicenter NSM is to be included**, the best practice recommendation is to **use NSM to create the MDB**. NSM will automatically detect the MSCS cluster and configure the MDB accordingly.

If, however, **Unicenter NSM is not one of the solutions** being implemented, the standard DSM, USD and UAPM installation procedures can be modified to enable those products to install the MDB to an MSCS cluster node, thereby enabling the MDB to be HA. The USD Primary Server and eIAM component as well as the UAPM managers can also be installed to a cluster node, however, the remaining DSM application components cannot and will, therefore, require alternative failover considerations. Other caveats include:

- If UAPM is installed with other products, such as Unicenter Service Desk (USD), then you should select the same resource group for UAPM.
- Since DSM is not HA, it should not be installed with an HA UAPM.
- Neither USD nor DSM has complete, automatic failover for the application itself. If the MDB does failover to a new node in the cluster, CAF will need to be manually restarted (for DSM) and users will need to relogin (for USD).

Additional Notes Regarding Shared and Multiple MDBs

Installing multiple MDBs on one server is not recommended and some products may fail to work if multiple MDBs are created on the same Microsoft Cluster. You should also be aware that not all products support named SQL instances (for example, at the time this document was written DSM did not support non-default SQL instances). If the MDB will be shared by multiple products and you are not sure if all of those products support installation to named SQL instances, you are encouraged to use the default SQL instance for the MDB install.

Installation order is also not important in SQL – though it is for Ingres - provided you install the MDB for **each** product. This step is required to create the necessary database users for each product. Further, NSM requires the MDB to be locked down. This means that, if the MDB is installed by a non-NSM component, then it must be subsequently configured by the NSM install – otherwise, NSM cannot use it.

Note: If the products have different release levels, install the earliest release first to ensure that the latest MDB patches are applied last.

Common services are created and installed automatically when you install the MDB from the NSM install media. When installing a NSM MDB, you will also need to install the WorldView Manager and WorldView Provider on the same server – otherwise you will not be able to view that MDB from the MCC.

Recommended Resources

This document summarizes procedures which are discussed in more detail in the following links. All of these links can be found in the Fault Tolerance section of the Implementation Best Practices page. The Implementation Best Practices page is accessible from SupportConnect through the following URL:

http://supportconnectw.ca.com/premium/impcd/r11/StartHere.htm

Click the Fault Tolerance link on the left hand side of the home page or click the following link to go directly to the Fault Tolerance section:

http://supportconnectw.ca.com/premium/impcd/r11/FaultTolerance/FaultTolerance_Frame.htm

Note: You will be prompted to login to SupportConnect before viewing the Implementation Best Practices page and its contents.

The "Unicenter Highly Available Overview" presentation provides, as its name suggests, an overview of the Highly Available Unicenter and BSO solutions. It can be accessed from the following direct link:

http://supportconnectw.ca.com/premium/impcd/r11/FaultTolerance/doc/Unicenter%20Highly%20Available%20Overview.ppt

The following presentations detail Best Practice Recommendations for deploying in a Microsoft Cluster Server (MSCS) environment:

For **Unicenter NSM r11.0 (Ingres)** consult the following links:

- Unicenter NSM r11 and Clusters – Part 1 (http://supportconnectw.ca.com/premium/impcd/r11/FaultTolerance/doc/r110HA_MSCS_PartI.ppt)
- Unicenter NSM r11 and Clusters – Part 2 (http://supportconnectw.ca.com/premium/impcd/r11/FaultTolerance/doc/r110HA_MSCS_PartII.ppt)

For **Unicenter NSM r11.1 (MS-SQL)** consult the following links:

- Unicenter NSM mr11.1 and Clusters – Part 1 (http://supportconnectw.ca.com/premium/impcd/r11/FaultTolerance/doc/r111HA_MSCS_PartI.ppt)
- Unicenter NSM r11.1 and Clusters – Part 2 (http://supportconnectw.ca.com/premium/impcd/r11/FaultTolerance/doc/r111HA_MSCS_PartII.ppt)
- Unicenter NSM r11.1 and Clusters – Part 3, installing HA MDB from Unicenter DSM r11.1 media (http://supportconnectw.ca.com/premium/impcd/r11/FaultTolerance/doc/r111HA_MSCS_PartIII.ppt)

For **Unicenter Desktop and Server Management r11.1,** information on implementing the MDB in a clustered MSCS SQL server can be found in the "Unicenter DSM with SQL Cluster" PDF available at the following link:

http://supportconnectw.ca.com/premium/impcd/r11/FaultTolerance/doc/Unicenter%20DSM%20with%20SQL%20Cluster.pdf

For **Unicenter Service Desk r11.1** (MS-SQL) consult the following links:

- Best Practices for Implementing USD r11.1 in an HA MSCS Environment - Part 1 (http://supportconnectw.ca.com/premium/impcd/r11/FaultTolerance/doc/r111HA_USDMSCS_PartI.ppt)
- Best Practices for Implementing USD r11.1 in an HA MSCS Environment - Part 2 (http://supportconnectw.ca.com/premium/impcd/r11/FaultTolerance/doc/r111HA_USDMSCS_PartII.ppt)
- Best Practices for Implementing USD r11.1 in an HA MSCS Environment - Part 3 (http://supportconnectw.ca.com/premium/impcd/r11/FaultTolerance/doc/r111HA_USDMSCS_PartIII.ppt)
- Best Practices for Implementing USD r11.1 in an HA MSCS Environment - Part 4 (http://supportconnectw.ca.com/premium/impcd/r11/FaultTolerance/doc/r111HA_USDMSCS_PartIV.ppt)
- Implementing USD r11.1 in an MSCS Environment (PDF format) (http://supportconnectw.ca.com/premium/impcd/r11/FaultTolerance/doc/usd_mscs_mdb.pdf)

In addition, the usdCluster.zip and usdPSCluster.zip resource kits, which can be used to simplify cluster resource definition, are available from the following links:

http://supportconnectw.ca.com/premium/impcd/r11/FaultTolerance/doc/usdCluster.zip

http://supportconnectw.ca.com/premium/impcd/r11/FaultTolerance/doc/usdPSCluster.zip

For **Unicenter Asset Portfolio Management (UAPM) r11.2**:

- Best Practices for Implementing UAPM r11.2 in an HA MSCS Environment - Part 1, Optional Components (http://supportconnectw.ca.com/premium/impcd/r11/FaultTolerance/doc/r111HA_UAPMMSCS_OptionalComponents.ppt)

- Best Practices for Implementing UAPM r11.2 in an HA MSCS Environment - Part 2 – UAPM Managers install (http://supportconnectw.ca.com/premium/impcd/r11/FaultTolerance/doc/r112HA_UAPMMSCS_Manager.ppt)

The second UAPM presentation references the uAPMCluster Resource Kit which assists in definition of UAPM cluster resources. This kit can be downloaded from the following link:

http://supportconnectw.ca.com/premium/impcd/r11/FaultTolerance/downloads/uAPMCluster.zip

Doc versions of these presentations are available in PDF format by clicking the following links:

http://supportconnectw.ca.com/premium/impcd/r11/FaultTolerance/doc/UAPMMSCS_OptionalComponents.pdf

http://supportconnectw.ca.com/premium/impcd/r11/FaultTolerance/doc/UAPMMSCS_ManagerComponents.pdf