Oracle MiniCluster S7-2 Security Guide

Part No: E69475-13
October 2021

Oracle MiniCluster S7-2 Security Guide

Part No: E69475-13

Copyright © 2018, 2021, Oracle and/or its affiliates. All rights reserved.

This software and related documentation are provided under a license agreement containing restrictions on use and disclosure and are protected by intellectual property laws. Except as expressly permitted in your license agreement or allowed by law, you may not use, copy, reproduce, translate, broadcast, modify, license, transmit, distribute, exhibit, perform, publish, or display any part, in any form, or by any means. Reverse engineering, disassembly, or decompilation of this software, unless required by law for interoperability, is prohibited.

The information contained herein is subject to change without notice and is not warranted to be error-free. If you find any errors, please report them to us in writing.

If this is software or related documentation that is delivered to the U.S. Government or anyone licensing it on behalf of the U.S. Government, then the following notice is applicable:

U.S. GOVERNMENT END USERS: Oracle programs, including any operating system, integrated software, any programs installed on the hardware, and/or documentation, delivered to U.S. Government end users are "commercial computer software" pursuant to the applicable Federal Acquisition Regulation and agency-specific supplemental regulations. As such, use, duplication, disclosure, modification, and adaptation of the programs, including any operating system, integrated software, any programs installed on the hardware, and/or documentation, shall be subject to license terms and license restrictions applicable to the programs. No other rights are granted to the U.S. Government.

This software or hardware is developed for general use in a variety of information management applications. It is not developed or intended for use in any inherently dangerous applications, including applications that may create a risk of personal injury. If you use this software or hardware in dangerous applications, then you shall be responsible to take all appropriate fail-safe, backup, redundancy, and other measures to ensure its safe use. Oracle Corporation and its affiliates disclaim any liability for any damages caused by use of this software or hardware in dangerous applications.

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

Intel and Intel Xeon are trademarks or registered trademarks of Intel Corporation. All SPARC trademarks are used under license and are trademarks or registered trademarks of SPARC International, Inc. AMD, Opteron, the AMD logo, and the AMD Opteron logo are trademarks or registered trademarks of Advanced Micro Devices. UNIX is a registered trademark of The Open Group.

This software or hardware and documentation may provide access to or information about content, products, and services from third parties. Oracle Corporation and its affiliates are not responsible for and expressly disclaim all warranties of any kind with respect to third-party content, products, and services unless otherwise set forth in an applicable agreement between you and Oracle. Oracle Corporation and its affiliates will not be responsible for any loss, costs, or damages incurred due to your access to or use of third-party content, products, or services, except as set forth in an applicable agreement between you and Oracle.

Access to Oracle Support

Oracle customers that have purchased support have access to electronic support through My Oracle Support. For information, visit `http://www.oracle.com/pls/topic/lookup?ctx=acc&id=info` or visit `http://www.oracle.com/pls/topic/lookup?ctx=acc&id=trs` if you are hearing impaired.

Référence: E69475-13

Copyright © 2018, 2021, Oracle et/ou ses affiliés. Tous droits réservés.

Ce logiciel et la documentation qui l'accompagne sont protégés par les lois sur la propriété intellectuelle. Ils sont concédés sous licence et soumis à des restrictions d'utilisation et de divulgation. Sauf stipulation expresse de votre contrat de licence ou de la loi, vous ne pouvez pas copier, reproduire, traduire, diffuser, modifier, accorder de licence, transmettre, distribuer, exposer, exécuter, publier ou afficher le logiciel, même partiellement, sous quelque forme et par quelque procédé que ce soit. Par ailleurs, il est interdit de procéder à toute ingénierie inverse du logiciel, de le désassembler ou de le décompiler, excepté à des fins d'interopérabilité avec des logiciels tiers ou tel que prescrit par la loi.

Les informations fournies dans ce document sont susceptibles de modification sans préavis. Par ailleurs, Oracle Corporation ne garantit pas qu'elles soient exemptes d'erreurs et vous invite, le cas échéant, à lui en faire part par écrit.

Si ce logiciel, ou la documentation qui l'accompagne, est livré sous licence au Gouvernement des Etats-Unis, ou à quiconque qui aurait souscrit la licence de ce logiciel pour le compte du Gouvernement des Etats-Unis, la notice suivante s'applique :

U.S. GOVERNMENT END USERS: Oracle programs, including any operating system, integrated software, any programs installed on the hardware, and/or documentation, delivered to U.S. Government end users are "commercial computer software" pursuant to the applicable Federal Acquisition Regulation and agency-specific supplemental regulations. As such, use, duplication, disclosure, modification, and adaptation of the programs, including any operating system, integrated software, any programs installed on the hardware, and/or documentation, shall be subject to license terms and license restrictions applicable to the programs. No other rights are granted to the U.S. Government.

Ce logiciel ou matériel a été développé pour un usage général dans le cadre d'applications de gestion des informations. Ce logiciel ou matériel n'est pas conçu ni n'est destiné à être utilisé dans des applications à risque, notamment dans des applications pouvant causer un risque de dommages corporels. Si vous utilisez ce logiciel ou ce matériel dans le cadre d'applications dangereuses, il est de votre responsabilité de prendre toutes les mesures de secours, de sauvegarde, de redondance et autres mesures nécessaires à son utilisation dans des conditions optimales de sécurité. Oracle Corporation et ses affiliés déclinent toute responsabilité quant aux dommages causés par l'utilisation de ce logiciel ou matériel pour des applications dangereuses.

Oracle et Java sont des marques déposées d'Oracle Corporation et/ou de ses affiliés. Tout autre nom mentionné peut correspondre à des marques appartenant à d'autres propriétaires qu'Oracle.

Intel et Intel Xeon sont des marques ou des marques déposées d'Intel Corporation. Toutes les marques SPARC sont utilisées sous licence et sont des marques ou des marques déposées de SPARC International, Inc. AMD, Opteron, le logo AMD et le logo AMD Opteron sont des marques ou des marques déposées d'Advanced Micro Devices. UNIX est une marque déposée de The Open Group.

Ce logiciel ou matériel et la documentation qui l'accompagne peuvent fournir des informations ou des liens donnant accès à des contenus, des produits et des services émanant de tiers. Oracle Corporation et ses affiliés déclinent toute responsabilité ou garantie expresse quant aux contenus, produits ou services émanant de tiers, sauf mention contraire stipulée dans un contrat entre vous et Oracle. En aucun cas, Oracle Corporation et ses affiliés ne sauraient être tenus pour responsables des pertes subies, des coûts occasionnés ou des dommages causés par l'accès à des contenus, produits ou services tiers, ou à leur utilisation, sauf mention contraire stipulée dans un contrat entre vous et Oracle.

Accès aux services de support Oracle

Les clients Oracle qui ont souscrit un contrat de support ont accès au support électronique via My Oracle Support. Pour plus d'informations, visitez le site `http://www.oracle.com/pls/topic/lookup?ctx=acc&id=info` ou le site `http://www.oracle.com/pls/topic/lookup?ctx=acc&id=trs` si vous êtes malentendant.

Contents

Using This Documentation

- **Overview** – Provides information about planning, configuring, and maintaining a secure environment for Oracle MiniCluster S7-2 systems.
- **Audience** – Technicians, system administrators, and authorized service providers.
- **Required knowledge** – Advanced experience with UNIX and database administration.

Product Documentation Library

Documentation and resources for this product and related products are available at https://docs.oracle.com/en/engineered-systems/minicluster-s7-2/

Feedback

Provide feedback about this documentation at http://www.oracle.com/goto/docfeedback.

Understanding Security Principles

This guide provides information about planning, configuring, and maintaining a secure environment for Oracle MiniCluster S7-2 systems.

These topics are covered in this section:

Minimum Required Security Tasks

MiniCluster is configured as a highly secure engineered system from the factory by default, and provides these security features:

- Preconfigured with fully automated security controls for all virtual machines (VMs).
- Encryption is enabled by default, ensuring secure data in rest and in transit.
- Support for smart card authorization.
- VMs are automatically configured with a hardened and minimized OS with host-based firewalls. You can use the BUI to change firewall rules and use the BUI or the CLI to verify the rules.
- Access control requires role based access with least privileges.
- All VMs use encrypted ZFS storage.
- Centralized key management facility, using PKCS#11, and support for FIPS.
- Comprehensive audit policy with centralized audit logs.

- The system and all of the VMs are configured to use PCI-DSS, CIS Equivalent, or DISA-STIG security profile.
- Compliance dashboard that supports easy-to-run compliance benchmarks.

Immediately after the MiniCluster installation, the security administrator should perform these two required tasks:

- Change the Oracle ILOM root password. See "Change the Default Oracle ILOM `root` Passwords" on page 33.
- Review the security information in this guide to understand and verify the MiniCluster security features.

Core Security Principles

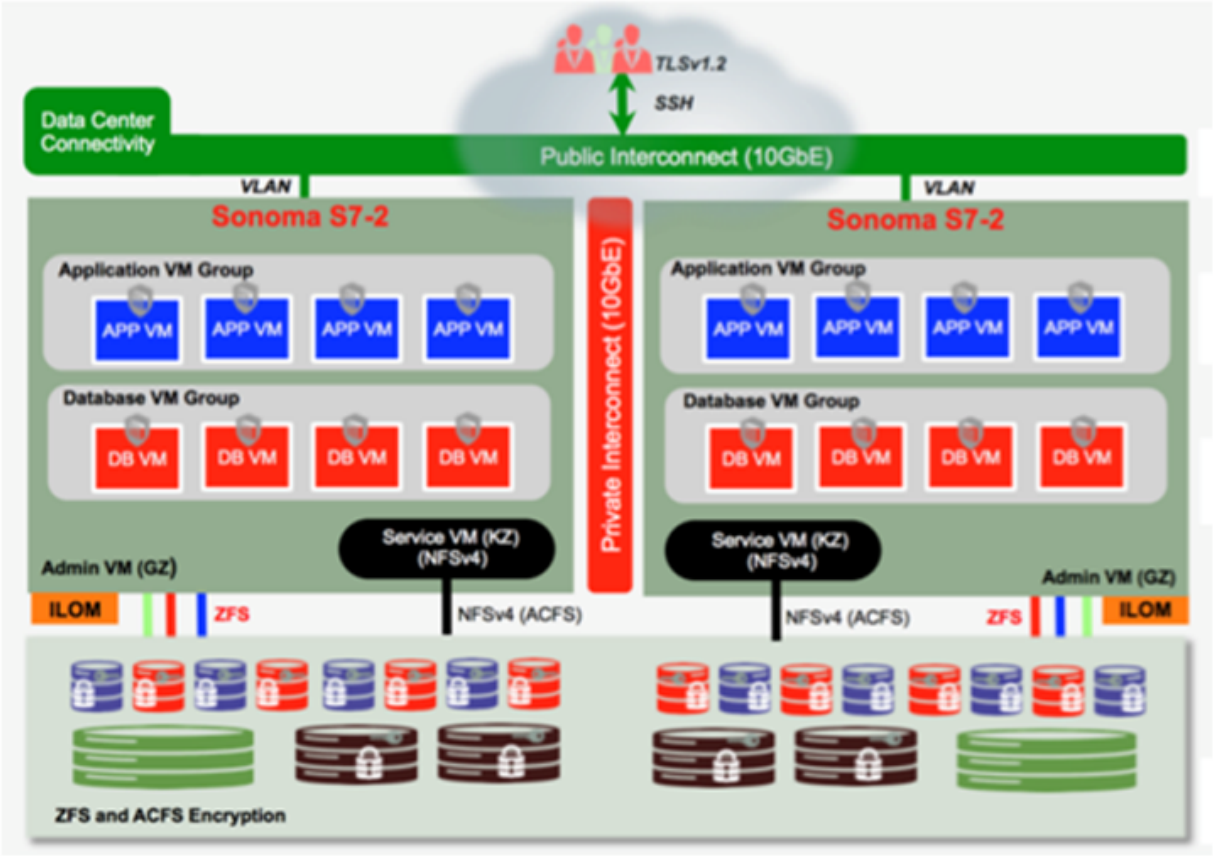
MiniCluster is a secure cloud infrastructure platform for application and database consolidation that delivers dedicated compute infrastructure as a service (IaaS) based cloud services. Built as a multi-purpose engineered system, MiniCluster combines the computing power of Oracle's SPARC S7 processor, the efficient virtualization capabilities of SPARC Solaris, and the optimized database performance of Oracle database integrated with dedicated storage. In addition, a 10 GbE network allows clients to access services running on MiniCluster. A second 10 GbE network provides the conduit through which communication occurs between the VM environment on the SPARC S7 servers and hosted applications.

The SPARC S7 processor features always-on hardware-assisted cryptographic functionality. This functionality helps MiniCluster–hosted entities protect information with high-performance data protection at rest, in use, and in transit. The processor also features the Silicon Secured Memory capability, which detects and prevents attacks related to memory data corruption and memory scraping, thereby ensuring the integrity of application data.

MiniCluster is preconfigured with over 250 out-of-the-box security controls that reduce the attack surface of the system by performing these actions:

- Disabling services, ports, and protocols that are not absolutely necessary.
- Configuring the exposed services to accept only trusted connections.

The system supports a variety of configuration and deployment options. This figure illustrates a typical deployment that consolidates Oracle Database and applications workloads.



Secure Virtual Machines

Security within a MiniCluster compute node is provided on multiple levels. It starts with secure verified boot of the compute nodes, a hardened and minimized OS that runs as isolated VMs to prevent workloads and data from being accessed by unauthorized users and systems.

Oracle Solaris Zones technology is used on VMs in MiniCluster to host isolated compute environments and segregate different applications running on the same OS. This isolation protects the applications from unintentional or malicious activities happening in other VMs. Despite running on the same kernel, each Solaris zone has its own isolated identity, resources, namespace, and processes. Essentially, Solaris zones provide built-in virtualization with strong isolation and flexible resource controls at a smaller CPU and memory footprint than traditional

VMs running on Type 1 hypervisors. Each VM is configured with a security profile that defines a comprehensive set of security controls and policies that are automatically applied during the installation process. ZFS pools and data sets allow further division and isolation of storage into more granular units for VMs and can have their own security policies.

Access Control

To protect application data, workloads, and the underlying infrastructure where it runs, MiniCluster offers comprehensive yet flexible access control capabilities for both users and administrators. MiniCluster leverages Oracle Solaris for a variety of access control methods for users and applications accessing system services. While traditional user name and password pairs are still widely used, you can integrate stronger methods of authentication using the Oracle Solaris pluggable authentication modules (PAM) architecture, allowing the use of LDAP, Kerberos, and public key authentication. The MiniCluster compute environment builds on a comprehensive role-based access control (RBAC) facility that allows organizations the flexibility to delegate user and administrative access as needed.

By eliminating the notion of a super-user, the RBAC capability in Oracle Solaris enables separation of duty and supports the notion of administrative roles, authorizations, fine-grained privileges, and rights profiles that collectively are used to assign rights to users and administrators. RBAC is integrated with other core Oracle Solaris services, including the Oracle Solaris Service Management Facility (SMF) and the VMs, to provide a consistent architecture to support all OS–level access control needs. MiniCluster leverages the RBAC capability of Oracle Solaris as a foundation for their access control architecture, allowing organizations to manage, control, and audit OS and virtualization management access from a centralized authority. All critical operations are carried out using a separation-of-duties principle supported by a multi-person authorization workflow. The system requires that two or more people approve every security sensitive operation. Collectively, these capabilities can be used to provide a high degree of assurance for the identity of users and the way critical business operations are handled.

All of the devices in MiniCluster system include the ability to limit network access to services either using architectural methods (for example, network isolation), or by using packet filtering or access control lists to limit communication to, from, and between physical and virtual devices as well as to the services exposed by the system. MiniCluster deploys a secure-by-default posture whereby no network services except Secure Shell (SSH) are enabled to accept inbound network traffic. Other enabled network services listen internally for requests within the Oracle Solaris OS (VM or zone). This ensures that all network services are disabled by default or are set to listen for local system communications only. You can customize this configuration based upon your requirements. MiniCluster is pre-configured with a network and transport layer (stateful) packet filtering using the Oracle Solaris packet filtering feature.

Smart Card Authentication

Oracle MiniCluster supports smart cards that are based on Public Key Infrastructure (PKI) credentials for authentication to Application and Database VMs. Two-factor authentication using US.. DoD Common Access Card (CAC) and U.S. Government-issued Personal Identity Verification (PIV) cards are supported for SSH clients who use a smart card and smart card reader. Smart card authentication does not support `mcinstall` and `oracle` users.

Note - The subject UID on the PKI credential must be the same as the user name in the MiniCluster environment. This assures user authentication and nonrepudiation for SSH-based access over the network to Application and Database VMs.

Smart cards use a PIN, rather than a password. The smart card is protected from misuse by the PIN, which is known only to the smart card's owner. To use the smart card, insert the card in a smart card reader that is attached to a computer and type the PIN when prompted. The smart card can be used only by someone who possesses the smart card and knows the PIN. For SSH use, a CAC, PIV, or X.509 certificate-based smart card should remain in the reader for the duration of the session. When the smart card is removed from the reader, the credentials are unavailable in the existing SSH session and to any applications.

You should use OpenSSH libraries for SSH clients. When OpenSSH is enabled, you must also enable OpenSSL in FIPS-140 mode, because OpenSSH relies on them in the Oracle MiniCluster STIG environment. Type the following to enable OpenSSL in FIPS-140 mode:

```
# pkg set-mediator -I fips-140 openssl
```

To learn how to access the Oracle Solaris environment in MiniCluster Application and Database VMs with a smart card and log in to the Solaris environment, refer to Chapter 7, “Using Smart Cards for Multifactor Authentication in Oracle Solaris” in *Managing Kerberos and Other Authentication Services in Oracle Solaris 11.3*.

Data Protection

The SPARC S7 processor in MiniCluster facilitates hardware-assisted, high-performance encryption for the data protection needs of security-sensitive IT environments. The SPARC M7 processor also features Silicon Secured Memory technology that ensures the prevention of malicious application-level attacks such as memory scraping, silent memory corruption, buffer overruns, and related attacks.

The SPARC processor enables hardware-assisted cryptographic acceleration support for over 16 industry-standard cryptographic algorithms. Together, these algorithms support most modern cryptographic needs, including public-key encryption, symmetric-key encryption, random number generation, and the calculation and verification of digital signatures and message digests. In addition, at the operating system level, cryptographic hardware acceleration is enabled by default for most core services including Secure Shell, IPSec/IKE, and encrypted ZFS data sets.

Oracle Database and Oracle Fusion Middleware automatically identify the Oracle Solaris OS and the SPARC processor used by MiniCluster. This identification enables the database and middleware to automatically use the hardware cryptographic acceleration capabilities of the platform for TLS, WS-Security, or tablespace encryption operations. The identification also allows the use the Silicon Secured Memory feature to ensure memory protection, and ensure application data integrity without the need for end-user configuration. MiniCluster supports the use of IPSec (IP Security) and IKE (Internet Key Exchange) is recommended to protect the confidentiality and integrity of VM-specific and inter-VM communications flowing over the public and private network.

On MiniCluster, ZFS data set encryption leverages a centralized Oracle Solaris PKCS#11 keystore to securely protect the wrapping keys. Using the Oracle Solaris PKCS#11 keystore automatically engages the SPARC hardware-assisted cryptographic acceleration for all encryption operations. This allows Oracle to significantly improve the performance of the encryption and decryption operations associated with encryption of ZFS data sets, Oracle Database Transparent Data Encryption (TDE), tablespace encryption, encrypted database backups (using Oracle Recovery Manager [Oracle RMAN]), encrypted database exports (using the Data Pump feature of Oracle Database), and redo logs (using Oracle Active Data Guard). Database VMs can use a shared-wallet approach by leveraging the Oracle Solaris PKCS#11 keystore or to create a directory on the ACFS share storage so that the wallet can be shared across the databases residing on VMs. Using a shared, centralized keystore at each compute node enables the system to better manage, maintain, and rotate the keys of Oracle TDE in Oracle Grid infrastructure based clustered database architectures, because the keys are synchronized across each of the nodes in the cluster. MiniCluster also features secure deletion of VMs and associated ZFS data sets by having the encryption policy and key management at that ZFS data set (file system / ZVOL) level to provide assured delete through key destruction.

Auditing and Compliance

MiniCluster relies on the use of the Oracle Solaris audit subsystem to collect, store, and process audit event information. Each VM (non-global zone) generates audit records that are stored locally to each of MiniCluster (global zone) audit store. This approach ensures that individual

VMs are not able to alter their auditing policies, configurations, or recorded data, because that responsibility belongs to the cloud service provider.

The Oracle Solaris auditing functionality monitors all administrative actions, command invocations, and even individual kernel-level system calls in the VMs. This facility is highly configurable, offering global, per-zone, and even per-user auditing policies. When configured to use VM, audit records for each VM can be stored in the global zone to protect them from tampering. The global zone also leverages the native Oracle Solaris auditing facility to record actions and events associated with virtualization events and MiniCluster administration.

MiniCluster provides tools that assess and report the compliance of the Oracle Solaris runtime environment residing in the VMs. Compliance utilities are based on the Security Content Automation Protocol (SCAP) implementation. MiniCluster supports three security compliance benchmark profiles:

- **Default Security Profile** – A CIS equivalent profile (based on the Center of Internet Security benchmark), which is more aligned with he security compliance requirements set forth by regulation, such as HIPAA, FISMA, SOX, and so on.
- **PCI-DSS Profile** – The Payment Card Industry Data Security Standard
- **DISA STIG Profile** – The Defense Information System Agency - Security Technical Implementation Guidance Standard. This profile builds on the Default Security Profile and introduces an additional 75 security controls, FIPS-140-2 cryptography, and support for setting an eeprom password.

Note - You can also change the password policy for a specific security profile. See “Change the Password Policy” on page 20.

The MiniCluster administrator can run the compliance benchmark on-demand and verify the environment for compliance and anomalies. These profiling tools map security controls to the compliance requirements mandated by the industry standards. The associated compliance reports can reduce significant auditing time and costs.

As of MiniCluster v.1.1.18, the system includes these auditing features:

- **Auditor role** – When this role is specified for an MCMU user, the user can access the auditor's review page in the MCMU BUI. The user cannot view or perform any other MiniCluster administrative tasks.
- **Auditor review page** – Is a special MCMU BUI page that only users with the auditor role can view. The page provides access to the audit pool status and provides the ability to generate audit records for all user activity on a per-zone basis. See “Generate Audit Reports” on page 49.

Understanding the Security Configuration

These topics describe the MiniCluster security controls:

Built-In Security Profiles

MiniCluster initialization is performed using the MCMU BUI or CLI. During the initialization, the MCMU requires the installer to choose one of these security profiles:

- **Default Security Profile** – Satisfies requirements comparable and equivalent to benchmarks set forth by the Center for Internet Security (CIS) and Security Technical Implementation Guidelines (STIG) assessments.
- **PCI-DSS Profile** – Complies with the Payment Card Industry Data Security Standard (PCI DSS) standard defined by the Payment Card Industry Security Standards Council.
- **DISA STIG Profile** – The Defense Information System Agency - Security Technical Implementation Guidance Standard. This profile builds on the Default Security Profile and introduces an additional 75 security controls, FIPS-140-2 cryptography, and support for setting an eeprom password.

Based on the selected policy, the MCMU configures the global zone and non-global zones with over 250 security controls.

After the initialization, as VMs are created, the MCMU requires the selection of one of the security profiles for each VM. Based on your security requirements, you can have a mix of security profiles on the VMs.

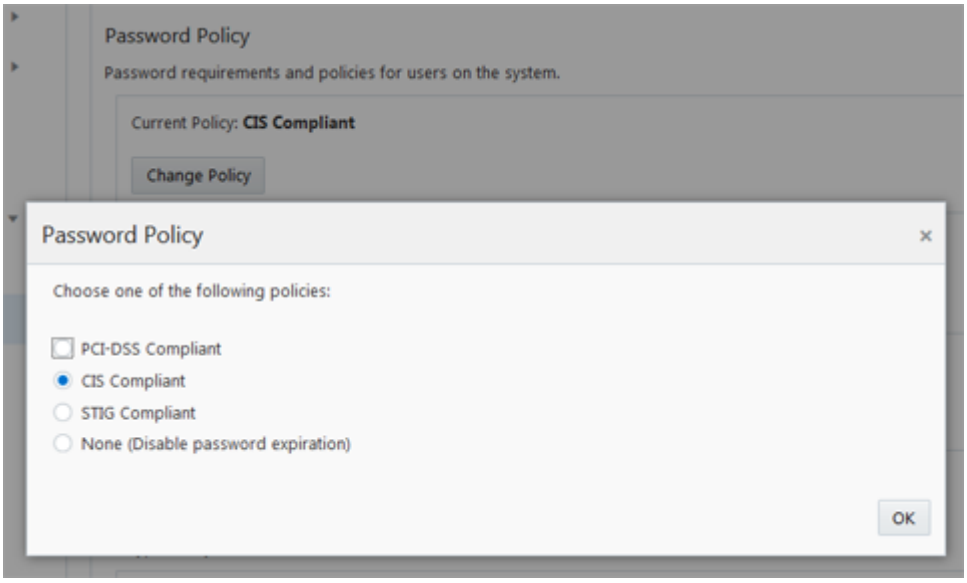
Note - After the initialization, you can also change the password policy for a specific security profile. See "Change the Password Policy" on page 20.

Change the Password Policy

When you installed the system, you specified a security profile (PCI-DSS, CIS Equivalent, DISA STIG, or None). You can use the MCMU BUI to change a user's access by choosing a different security profile, or setting it to None and changing the password policy. This feature is available only in a global zone, and is not available for VMs.

Alternatively, you can use the `mcmu security -p` command.

1. **Log in to the MCMU BUI as a primary administrator.**
   For instructions, refer to "Accessing the System" in *Oracle MiniCluster S7-2 Administration Guide*.
2. **In the navigation panel, select System Settings → Security.**
3. **In the Change Password Policy section, click Change Policy.**
   Selecting a different option makes the password adhere to that security policy.
4. **Select one of the following Password Policy options and click Confirm.**



- PCI-DSS Compliant – See "Built-In Security Profiles" on page 19.

-
- CIS Compliant – See “Built-In Security Profiles” on page 19.
- STIG Compliant – See “Built-In Security Profiles” on page 19.
- None (Disable password expiration) – If a user is locked out of an account and you need to disable or reset the password, select None. Do this only as a last resort.

  For more information on editing the `policy.conf` file, refer to “Rights Databases” in *Securing Users and Processes in Oracle Solaris 11.3*.

Note - An administrator can manually edit the policy files for these security profiles: `passwd_cis.txt`, `passwd_pci.txt`, and `passwd_stig.txt`. These files are located in the `/etc/security/` directory.

Verify the VM Security Profile (CLI)

Use this procedure to verify the security profile that is configured for the zones and VMs. To perform this procedure, you must access the system with a user account that has the `root` role.

Note - To identify the security profile assigned to the global zone, use the MCMU BUI to view System Setting → User Input Summary. The security profile is displayed at the bottom of the page.

1. **Log in to the global zone as `mcinstall`.**
   For instructions, refer to “Accessing the System” in *Oracle MiniCluster S7-2 Administration Guide*.

2. **Assume the `root` role.**
   For example:

   ```
   % su root
   ```

3. **Determine the log file name for the VM.**
   In this example, there is one log file for each VM:

   ```
   # cd /var/opt/oracle.minicluster/mcmubui/MCMU/verification_logs
   # ls
   verify_appvmg1-zone-1-mc4-n1.log  verify_dbvmg1-zone-3-mc4-n1.log
   verify_appvmg1-zone-1-mc4-n2.log  verify_dbvmg1-zone-3-mc4-n2.log
   verify_dbvmg1-zone-1-mc4-n2.log   verify_dbvmg1-zone-4-mc4-n1.log
   verify_dbvmg1-zone-2-mc4-n1.log   verify_dbvmg1-zone-4-mc4-n2.log
   ```

```
verify_dbvmg1-zone-2-mc4-n2.log
```

4. **View the verification log files.**

   View the last lines of the log file. If `(PCI-DSS)` is displayed, the VM's security profile is PCI-DSS. If no profile is listed, the VM's security profile is CIS Equivalent.

   - Example of the last 22 lines of a VM with a PCI-DSS profile:

     ```
     # tail -22 verify_dbvmg1-zone-1-mc4-n2.log

     (PCI-DSS) Checking /etc/cron.d/at.allow:
     Passed/Configured

     (PCI-DSS) Checking audit configuration (user audit flags):
     Passed/Configured

     (PCI-DSS) Checking audit configuration (non-attributable audit flags):
     Passed/Configured

     (PCI-DSS) Checking audit configuration (audit_binfile plugin):
     Passed/Configured

     (PCI-DSS) Checking audit flags on root and tadmin roles:
     Passed/Configured

     Check if tenant-key exists in keystore:
     Passed/Configured

     Check if immutability is enabled:
     Failed/Not Configured
     ```

   - Example of the last 22 lines of a VM with a CIS Equivalent profile:

     ```
     # tail -22 verify_dbvmg1-zone-1-mc4-n2.log
     Checking if NDP routing daemon is disabled:
     Passed/Configured

     Checking if r-protocol services are disabled:
     Passed/Configured

     Checking if rpc/bind is enabled and configured correctly:
     Passed/Configured

     Checking if NFS v2/v3 is disabled:
     Passed/Configured
     ```

```
Checking if GDM is enabled:
Failed/Not Configured

Check if tenant-key exists in keystore:
Passed/Configured

Check if immutability is enabled:
Failed/Not Configured
```

Protecting Data

These topics describe the MiniCluster data protection technologies:

Data Protection With ZFS Data Set Encryption

In MiniCluster, data protection at rest is automatically configured using ZFS data set encryption. The encryption is configured as follows:

- All ZFS data sets are encrypted in virtual machines (VMs), including the root and swap file systems.
- All ZFS data sets re encrypted in the global zone, with the exception of the root and swap file systems.

You can verify the encryption configuration by viewing the encryption keys. See "View ZFS Data Set Encryption Keys (BUI)" on page 25.

▼ View ZFS Data Set Encryption Keys (BUI)

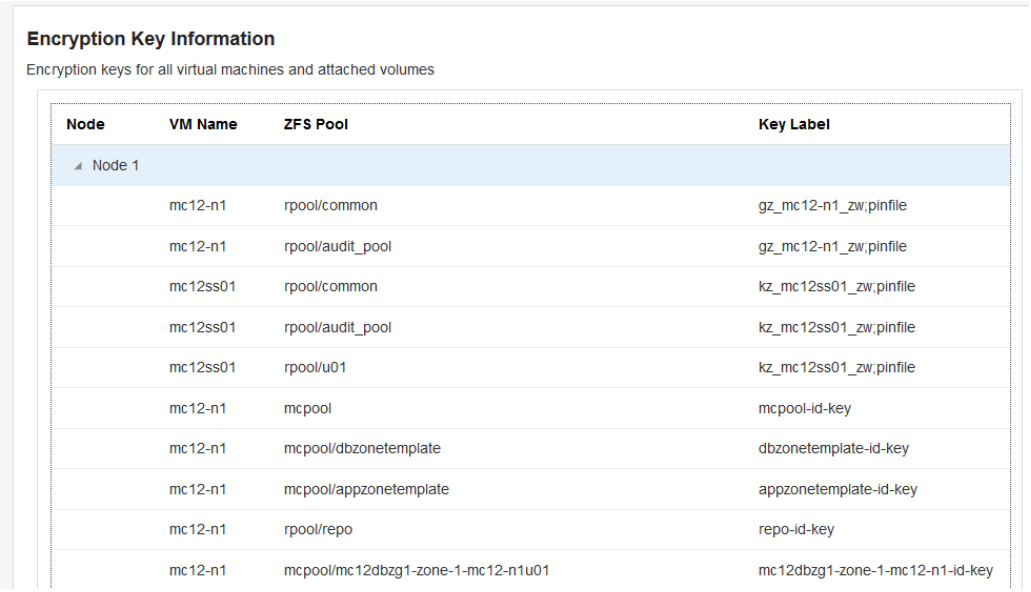
Use this procedure to view encryption key details.

1. **Access the MCMU BUI.**

For instructions, refer to "Accessing the System" in *Oracle MiniCluster S7-2 Administration Guide*.

2. **In the navigation panel, select System Settings → Security.**

   Click a node to display details.



Encryption Key Information

Encryption keys for all virtual machines and attached volumes

Node	VM Name	ZFS Pool	Key Label
Node 1			
	mc12-n1	rpool/common	gz_mc12-n1_zw;pinfile
	mc12-n1	rpool/audit_pool	gz_mc12-n1_zw;pinfile
	mc12ss01	rpool/common	kz_mc12ss01_zw;pinfile
	mc12ss01	rpool/audit_pool	kz_mc12ss01_zw;pinfile
	mc12ss01	rpool/u01	kz_mc12ss01_zw;pinfile
	mc12-n1	mcpool	mcpool-id-key
	mc12-n1	mcpool/dbzonetemplate	dbzonetemplate-id-key
	mc12-n1	mcpool/appzonetemplate	appzonetemplate-id-key
	mc12-n1	rpool/repo	repo-id-key
	mc12-n1	mcpool/mc12dbzg1-zone-1-mc12-n1u01	mc12dbzg1-zone-1-mc12-n1-id-key

▼ Back Up the Encryption Keys

Use this procedure to back up encryption keys using the MCMU BUI.

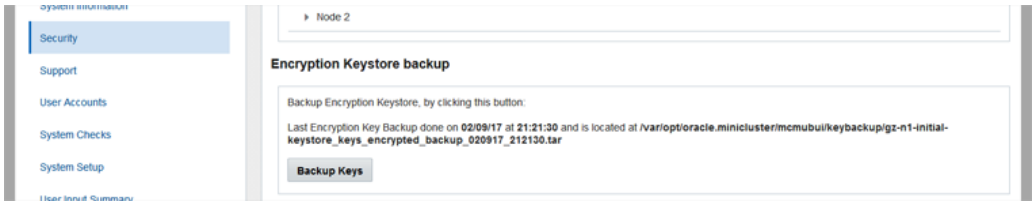
Alternatively, you can perform the same task using the CLI command: `mcmu security -b`.

1. **Access the MCMU BUI.**

   For instructions, refer to "Accessing the System" in *Oracle MiniCluster S7-2 Administration Guide*.

2. **In the navigation panel, select System Settings → Security.**

3. **In the Encryption Keystore Backup section, click Backup Keys.**



MCMU displays the path of the tar file that contains the backup.

Secure Shell Service

MiniCluster requires the use of the SSH network protocol to enable you to securely log in to MiniCluster compute nodes (global zones) and VM instances (non-global zones).

When a user logs in for the first time using SSH, the system automatically generates a new SSH key pair for the user.

▼ Change SSH Keys (BUI)

Use this procedure to change the SSH keys for a zone or VM. You must choose one of these methods:

- Insert a new key to authorize passwordless SSH – Requires you to enter the VM user name, VM machine name, and RSA public key.
- Auto generate new keys for VMs.

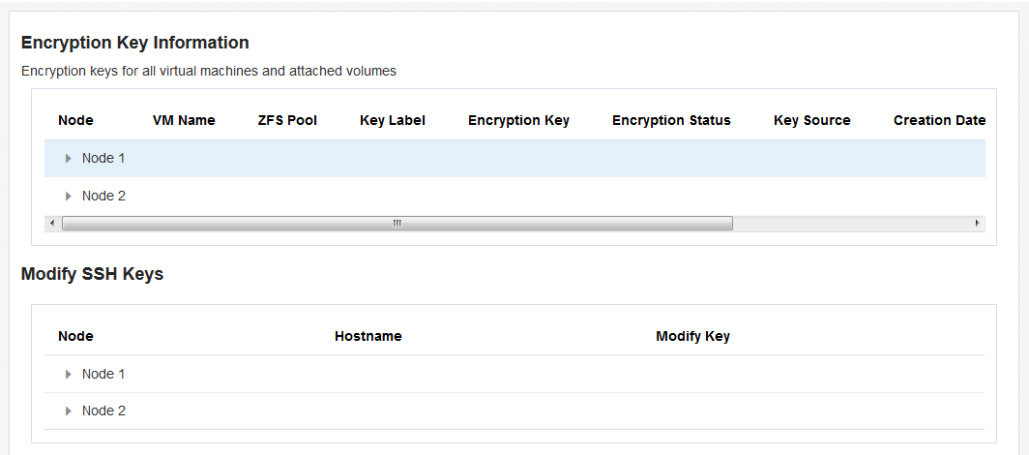
Note - To perform this procedure using the MCMU CLI, refer to "Set SSH Key Options (CLI)" in *Oracle MiniCluster S7-2 Administration Guide*.

---

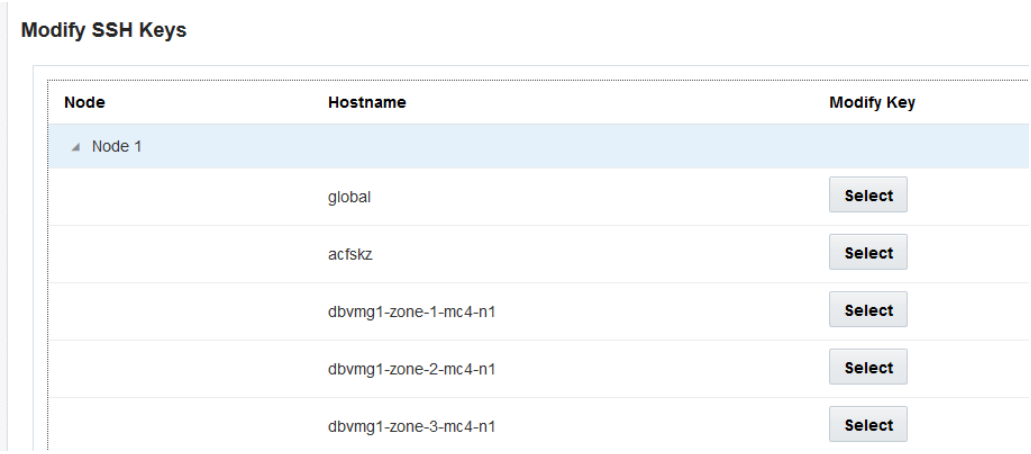
1. **Access the MCMU BUI.**

   For instructions, refer to "Accessing the System" in *Oracle MiniCluster S7-2 Administration Guide*.

2. **In the navigation panel, select System Settings → Security.**



3. **In the Modify SSH Keys panel, click a node to expand the display.**



4. **Click Select for the VM that you plan to change.**

5. **Choose one of these options.**

   - Insert New Key to Authorize Passwordless SSH

- Auto Generate New Keys for Machines

6. **Click Next.**

7. **If you selected to authorize passwordless SSH, enter this information and click Next.**

   - User name of the machine
   - Host name of the machine
   - RSA public key of the machine

8. **Click Setup SSH.**

   The change is applied.

Secure Communication With IPsec

Use IPsec (IP Security) and IKE (Internet Key Exchange) to protect the confidentiality and integrity of inter-zone IP-based communications and NFS traffic flowing over the network. IPsec is recommended because it supports network-level peer authentication, data origin authentication, data confidentiality, data integrity, and replay protection. When used on the Oracle MiniCluster platform, IPsec and IKE are able to automatically take advantage of hardware- assisted cryptographic acceleration, thereby minimizing the performance impact of using cryptography to protect sensitive information flowing over this network channel.

▼ Configure IPsec and IKE

Before you can configure IPsec, you must define the specific host names or IP addresses that are used between communicating peers.

In this procedure, the IP addresses of 10.1.1.1 and 10.1.1.2 are used to designate two Solaris non-global zones being operated by a single tenant. Communication between these two addresses will be protected using IPsec. The example is from the perspective of the non-global zone associated with IP address 10.1.1.1.

Use the following procedure to configure and use IPsec and IKE between a pair of designated (VMs) non-global zones.

1. **Define the IPsec security policy.**

Define the security policy that will be enforced between the pair of communicating zones.

In this example, all network communications between 10.1.1.1 and 10.1.1.2 will be encrypted:

```
{laddr 10.1.1.1 raddr 10.1.1.2}
ipsec{encr_algs aes encr_auth_algs sha256 sa shared}
```

2. **Store the policy in the `/etc/inet/ipsecinit.conf` file.**

3. **Verify that the IPsec policy is syntactically correct.**

   For example:

   ```
   # ipsecconf –c –f ipsecinit.conf
   ```

4. **Configure the Internet Key Exchange (IKE) service.**

   Configure the service following the host and algorithm settings in the `/etc/inet/ike/config` file.

   ```
   { label "ipsec"
   local_id_type ip
   remote_addr 10.1.1.2
   p1_xform { auth_method preshared oakley_group 5
   auth_alg sha256 encr_alg aes } }
   ```

5. **Configure the preshared key.**

   Before IPsec can be enabled, you must share key material with both peer nodes so that they can authenticate to one another.

   The Oracle Solaris IKE implementation supports a variety of key types including pre-shared keys and certificates. For simplicity, this example uses pre-shared keys that are stored in the `/etc/inet/secret/ike.preshared` file. However, organizations can use stronger forms of authentication.

   Edit the /etc/inet/secret/ike.preshared file, and enter the preshared key information. For example:

   ```
   {
   localidtype IP
   localid 10.1.1.1
   remoteid type IP
   key "This is an ASCII phrAz, use strOng p@sswords"
   }
   ```

6. **Enable IPsec and IKE services on both peers.**

   You must enable the services on both communicating peers before encrypted communication is possible.

For example:

```
# svcadm enable svc:/network/ipsec/policy:default
# svcadm enable svc:/network/ipsec/ike:default
```

Controlling Access

These topics cover the access control features available in MiniCluster:

▼ Change the Default Oracle ILOM `root` Passwords

The system ships with default passwords assigned to the Oracle ILOM root accounts on both nodes. This enables the installation process to be performed with a predictable initial access account. Immediately after installation, change the default passwords to ensure optimal security.

1. **Log into Oracle ILOM on node 1 as `root`.**

   Use the `ssh` command to connect to Oracle ILOM.

Tip - To get the host names of Oracle ILOM, log in to in the MCMU BUI as a primary administrator and use the navigation panel to select System Settings → System Information. The host names are listed under the ILOM column.

For example:

```
% ssh root@node1_ILOM_hostname_or_IPaddress
```

Type the Oracle ILOM root password: welcome1

2. **Change the Oracle ILOM `root` password.**

```
-> set /SP/users/root password
Enter new password: *********
Enter new password again: **********
```

3. **Repeat these steps to change the Oracle ILOM `root` password on node 2.**

4. **Update Oracle Engineered Systems Hardware Manager with the new passwords.**

   See "Configure the Utility's Password Policies and Passwords" in *Oracle MiniCluster S7-2 Administration Guide*.

Change the Oracle Engineered System Hardware Manager Passwords

Oracle Engineered Systems Hardware Manager is a BUI-based system-level hardware management utility intended for use by Oracle Service personnel, or under their direction. By default, utility is configured at installation.

There are two user accounts in the utility: `admin` and `service`. For security purposes, you must change the Oracle Engineered System Hardware Manager user account Passwords.

- **Change the passwords.**

  Refer to "Configure the Oracle Engineered System Hardware Manager Password" in *Oracle MiniCluster S7-2 Installation Guide*.

Configure EEPROM Passwords

Each MiniCluster node has an EEPROM, sometimes referred to as OpenBoot, which is low-level firmware that contains some configuration parameters and drivers that facilitate booting the system. By default, the EEPROM password feature is disabled.

In secure environments, use this procedure to enable the password feature and set a password. The password is automatically enabled and applied to both nodes. Once set, a password is

required to access the eeprom from OpenBoot (the ok prompt) and from the Oracle Solaris `eeprom` command.

This procedure supersedes older methods where the password is set either at the OpenBoot `ok` prompt, or in Oracle Solaris with the `eeprom` command.

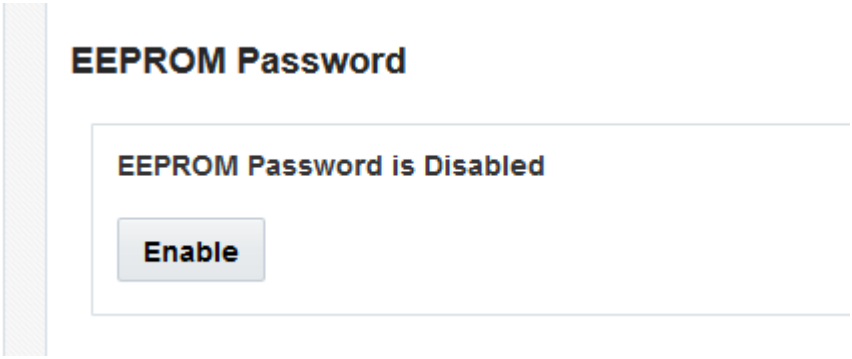
Caution - It is important to remember the password. If you forget the password, you must call support services to make your system bootable again.

This procedure describes how to set the passwords using the MCMU BUI. Alternatively, you can use the `mcmu security -e` command.

1. **Log into the MCMU as a primary admin such as `mcinstall`.**

   For instructions, refer to "Accessing the System" in *Oracle MiniCluster S7-2 Administration Guide*.

2. **In the navigation panel, select System Settings → Security.**



3. **Perform one of these actions:**

   - Enable and set the password – Click Enable, enter the password twice, and click Set Password.
   - Disable the feature – Click Disable, then Confirm.
   - Change an existing password – Change Password, enter the new password twice, and click Update.

User Provisioning

During the installation of MiniCluster, the installation process requires you to create and register the first MCMU user called `mcinstall`. The user's demographic information, including email address, and phone number are collected. The `mcinstall` user is the first primary administrator account. Upon the first `mcinstall` log in, the utility requires `mcinstall` to create a new password in accordance with Oracle Solaris password policies that are associated with the Security profile.

During the registration of the `mcinstall` user, you are required to specify a person to serve as the MCMU supervisor. The supervisor is only identified by a name and email address. The supervisor is not an MCMU user, and has no login credentials.

Both the supervisor and mcinstall users are associated with real person names and valid email addresses.

When new MCMU users are provisioned, each user account is assigned with a role of primary administrator or secondary administrator (see “Role-Based Access Control” on page 37). Before the new account is enabled, the `mcinstall` user and supervisor must both approve the new user account though a URL they receive in email (see “MCMU User Approval Process” on page 36). Upon first login, the user is forced to set a password that conforms to the MCMU password polices. See “User Authentication and Password Policies” on page 39.

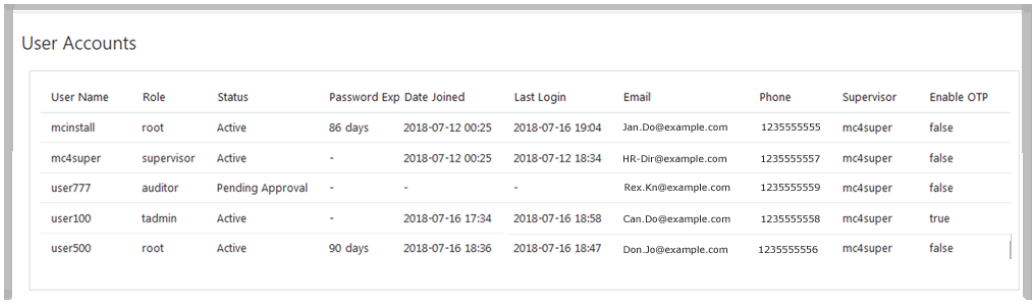
MCMU User Approval Process

All MCMU user accounts require two-person approval by the MCMU supervisor and primary admin. The process works as follows:

1. The prospective user (or an MCMU administrator on their behalf) accesses the MCMU registration page and provides these mandatory details:
   - MCMU user name
   - Email address
   - Full name
   - Phone number
   - MCMU role
2. MCMU sends the MCMU supervisor and primary administrator an email requesting approval or denial. The email includes a URL to the MCMU approval/denial feature and includes a unique key identifier.

3. When both the supervisor and primary admin approve the account, the user account is enabled, and MCMU sends the new user and email confirming the account activation. The user receives an MCMU account that can be accessed through the MCMU BUI or CLI. The user also receives an Oracle Solaris user account. If the user exists in a corporate LDAP and MiniCluster is configured with an LDAP client, the user can only use LDAP for the Oracle Solaris account.

All registered users are stored in the MCMU repository. An MCMU administrator can verify the users, including their roles and supervisor by viewing MCMU System Settings → User Accounts. For example:



Role-Based Access Control

There is no `root` user in MiniCluster. Instead, root is a role and is assigned to MCMU users that are registered as primary administrators.

When you create an MCMU user, you assign the user one of these roles:

- **Primary admin (`root` role)** – The `root` role defines the rights and privileges of primary administrators of the MiniCluster system including all its compute nodes, networks, database, and storage. Users with the `root` role can perform all installation and all critical administrative operations without any constraints. As primary administrators, they can delegate operations and approve adding and deleting users including new primary and secondary administrators. The user must login with his/her own credentials. All actions and operations carried out are logged and audited based on the user identifier, not the role identifier.
- **Secondary admin (`mcadmin` role)** – This role defines the rights and privileges of secondary administrators of the MiniCluster domains and non-global zones. By default, this role only

enables a read-only access to MCMU. All actions and operations carried out are logged and audited based on the user identifier, not the role identifier.

- **Tenant admin (`tadmin` role)** – This role defines the rights and privileges of the administrator of a MiniCluster VM. The role defines the rights and privileges of a VM administer involved with day-to-day administrative operations supporting application installations and deployment. All actions are audited based on the user identifier, not the role identifier.
- **Auditor (`auditor` role)** – Users with this role only have access to the MCMU BUI audit review page where they can view the audit pool status and generate reports for user activity. Only users with this role can access the audit review page. Auditors cannot access the MCMU (except for the audit page), nor can they log into kernel zones or VMs.

User Accounts

MiniCluster includes the user accounts listed in this table.

User	Password	Role	Description
`mcinstall`	The password is configured during the installation. It can be reset and changed through MCMU.	`root`	The installation process requires you to create `mcinstall` as the MCMU primary administrator and create a password. This account is intended to be the primary administrator for the MCMU. This user account is used for these activities: ■ Performing the system initialization at installation time by running `installmc`. ■ Administering the system, including VMs using the MCMU BUI and `mcmu` CLI. ■ To assume the `root` role (`su` to root) on application VMs and in the global zone and kernel zones for superuser privileges.
MCMU Supervisor – Account name determined at installation time	The password is configured during the installation.	root	In the MiniCluster software, the supervisor user is only intended to approve or deny MCMU users as they are created and deleted. This user receives email every time a new MCMU user is created. The new user must be approved by the supervisor and the primary admin (such as mcinstall) for the user account to be enabled.
(Optional) *Tenant Admin* – Account name determined at user registration time	Determined upon initial log in.	`tadmin`	This user can perform all post-installation activities (including using OTP to authenticate a user for a single login or session) only on VMs. This user cannot access the global zone, and cannot run the MCMU BUI or CLI. **Note -** If the user is created with the MCMU CLI, the role is identified as `tenant_admin`.
(Optional) *Secondary Admin* – Account name	Determined upon initial log in.	`mcadmin`	When an MCMU user is created and assigned as a secondary admin, and has read-only access to non-global zones.

User	Password	Role	Description
determined at user registration time			
`oracle`	Set during the DB VM group profile configuration.	`root`	This user account is used for these activities: ■ Used as the initial login account to database VMs, from which you can configure the database VMs with a database, data, and other accounts, as needed. ■ To assume the root role (`su` to root) on database VMs for superuser privileges.

When MiniCluster is accessed for the first time, you are prompted to create a new password that adheres to the password policies. See “User Authentication and Password Policies” on page 39.

All actions performed by all MCMU users are logged based on the user's identifier. For information about audit reports, see “Auditing and Compliance Reporting” on page 47.

Note - MCMU user accounts are not used for the routine use of the system, such as using the applications and databases. Those user accounts are managed through Oracle Solaris, the application, the database on the VMs, and through your site's name services.

User Authentication and Password Policies

All users provisioned in MiniCluster are assigned a role with strict password policies and password encryption that is enforced by the security profile.

The default security policy establishes these MCMU password requirements:

- Must contain a minimum of 14 characters
- Must have a minimum of one numeric character
- Must have a minimum of on uppercase alpha character
- Must differ from a previous password by at least three characters
- Must not match the previous ten passwords

All users log in to their Oracle Solaris account using the user's own password only.

Note - You can also change the password policy for a specific security profile. See “Change the Password Policy” on page 20.

▼ Verify Oracle Solaris User Roles

1. **Log into the MiniCluster global zone and assume the root role.**

   For instructions, refer to "Accessing the System" in *Oracle MiniCluster S7-2 Administration Guide*.

2. **Verify the list of roles available.**

   ```
   # logins -r
   ```

3. **Verify user role and password required for authentication.**

   ```
   # grep root /etc/user_attr
   root::::audit_flags=lo\:no;type=role;roleauth=user
   mcinstall::::auths=solaris.system.maintenance;roles=root
   ```

Firewall Protection

The firewall technology provided by MiniCluster differs based on the version of the Oracle Solaris OS that is running on MiniCluster components.

MiniCluster 1.3.0 and later

MiniCluster now uses the packet filter functionality delivered by Oracle Solaris 11.4 to enable network traffic protection. This enables MiniCluster to protect networks and virtual hosts from network-based intrusions. Packet Filtering is enabled and disabled through the use of the SMF service `svc:/network/firewall` for Global and Kernel Zones, and all VMs running Oracle Solaris 11.4.

The Firewall Manager feature is available through the MiniCluster BUI (System Settings → Firewall Manager).

MiniCluster 1.2.5.22 and earlier

MiniCluster provides network traffic protection using the Oracle Solaris 11.3 IP Filter-based firewall for virtual machines, including global, non-global, and kernel zones. The firewall allows MiniCluster to protect its networks and residing virtual hosts from network-based intrusions.

These topics describe how to configure the firewall rules:

- "Manage Firewall Rules" on page 41

- “Verify Firewall Rules” on page 41

Manage Firewall Rules

1. **Log into the MCMU as a primary administrator, such as `mcinstall`.**
   Only the primary administrator can make changes to firewall rules. For login instructions, refer to “Accessing the System” in *Oracle MiniCluster S7-2 Administration Guide*.
2. **In the navigation panel, select System Settings → Firewall Manager.**
3. **Choose the node and virtual machine host name that you want to modify.**
4. **In the Firewall Rules Editor section, edit the existing rules.**
5. **Click Apply Changes to save the firewall configuration.**
   The Solaris firewall configuration is saved for this host. Some changes take time while the correct information is gathered and displayed.

Caution - The Firewall Rules Editor does not check for proper syntax.

6. **Click Disable (or Stop) to disable the firewall services for this host.**
   The Status changes from *online* to *disabled*.
7. **Click Start to enable the firewall services for this host.**
   You must restart the firewall for the changes to take effect. The Status changes from *disabled* to *online*. You can also use the CLI to verify firewall rules. For instructions, see “Verify Firewall Rules” on page 41.

Verify Firewall Rules

1. **Log into the global zone on node 1 as `mcinstall`, and assume the `root` role.**
   For Oracle ILOM login instructions, refer to “Accessing Oracle ILOM” in *Oracle MiniCluster S7-2 Administration Guide*.

```
% ssh mcinstall@mc4-n1
```

```
Password: ***************
Last login: Tue Jun 28 10:47:38 2016 on rad/59
Oracle Corporation      SunOS 5.11      11.3    June 2016
Minicluster Setup successfully configured
Unauthorized modification of this system configuration strictly prohibited
mcinstall@mc4-n1:/var/home/mcinstall % su root
Password: ***************
#
```

2. **Check the firewall configuration.**
   Review one of the following files based on the version of the Oracle Solaris OS:
   - Oracle Solaris 11.4 – `/etc/firewall/pf.conf`
   - Oracle Solaris 11.3 – `/etc/ipf/ipf.conf`
3. **Verify that the firewall services are online.**
   Use one of the following commands based on the version of the Oracle Solaris OS:
   - Oracle Solaris 11.4 – `pfctl -sr -v`
   - Oracle Solaris 11.3 – `ipfstat -v` or `svcs | grep svc:/network/ipfilter:default`
4. **Ensure that your databases and applications are accessible without changing the firewall rules.**

Secure Deletion of VMs

Only the MCMU primary administrator can delete VMs and VM groups. When a VM component is deleted, the corresponding keys are automatically deleted, and email is sent to the primary administrator.

To verify this feature, before you delete a VM component, log into the MCMU BUI as a primary administrator, and view the encryption keys (System Settings → Security). Delete the VM component, the view the keys again. The VM and associated key label for the deleted component is no longer displayed.

▼ Verify the Verified Boot Environment

Oracle Solaris Verified Boot is an anti-malware and integrity feature that reduces the risk of introducing malicious or accidentally modified critical boot and kernel components. This

feature checks the factory-signed cryptographic signatures of the firmware, boot system, and kernel.

By default, MiniCluster global zones are configured with Oracle Solaris Verified Boot. If you want to verify that the system is configured with verified boot, perform these steps.

1. **Log into Oracle ILOM on one of the nodes.**

   For Oracle ILOM login instructions, refer to "Accessing Oracle ILOM" in *Oracle MiniCluster S7-2 Administration Guide*.

2. **Check the verified boot configuration in Oracle ILOM.**

   Ensure that the `boot_policy` is set to `warning`.

```
-> show /HOST/verified_boot

 /HOST/verified_boot
    Targets:
        system_certs
        user_certs

    Properties:
        boot_policy = warning

    Commands:
        cd
        show
```

3. **Check the verified boot policy setting.**

   Ensure that the `module_policy` is set to `enforce`.

```
-> show /HOST/verified_boot module_policy

  /HOST/verified_boot
    Properties:
        module_policy = enforce
```

4. **Start the host console to access the global zone.**

   Log in as `mcinstall`.

```
-> start /HOST/console
Are you sure you want to start /HOST/console (y/n)? y

Serial console started.  To stop, type #.

Minicluster Setup successfully configured
mc4-n1 console login: mcinstall
```

```
Password: **************
Last login: Tue Jun 28 10:17:38 2016 on rad/47
Oracle Corporation      SunOS 5.11      11.3    June 2016
Minicluster Setup successfully configured
Unauthorized modification of this system configuration strictly prohibited
mcinstall@mc4-n1:/var/home/mcinstall %
```

5. **Check the global zone for evidence that the system booted in a verified boot configuration.**

   Check the `messages` file for the string `NOTICE: Verified boot enabled; policy=warning`.

```
mcinstall % cat /var/adm/messages | grep Verified
Jun 29 11:39:15 mc4-n1 unix: [ID 402689 kern.info] NOTICE: Verified boot enabled;
 policy=warning
```

Restrict Access to Shared Storage

MiniCluster includes a storage array with a mix of SSDs and HDDs. The HDDs can be configured to provide shared storage to the VMs.

MiniCluster includes a shared storage isolation feature – A toggle switch that facilitates isolation of shared storage applied only to global and kernel zones. This helps to isolate a security and compliance-enabled VM group environment from sharing files with the global and kernel zones. This ensures that VM groups are no longer attached to NFS mounts and that the NFS services are disabled.

For highly secure environments, do not enable shared storage for database VMs and application VMs. If shared storage is enabled, the file system must be accessible to the VMs as read-only. For instructions on how to enable or disable the shared storage, refer to the *Oracle MiniCluster S7-2 Administration Guide* available at: `http://docs.oracle.com/cd/E69469_01`.

The `/sharedstore` directory is the mount point for the shared storage:

- **Based on your security needs, configure the shared storage using these recommendations:**
  - Ensure that the shared storage is not available to database VMs and application VMs, or that it is read-only.
  - In production deployments, ensure that both kernel zones are not accessible over public networks or directly accessible to client access. All direct access and use of shared storage services from public networks or client access must be terminated. If VMs require access to the `/sharedstore` file system through NFS, ensure that they are facilitated through IPSec/IKE channels.

▼ Reverify and Update Security Controls (Sustaining Compliance)

Security controls can be changed or modified after patches and application installations, so it is important to verify and update security controls to sustain compliance policies. To assure that security controls are verified and updated to conditions before the patches and updates, this procedure describes how to use the MCMU BUI to verify and reapply security settings according to the compliance profile.

Alternatively, you can use the `mcmu security -r` command.

1. **Log in to the MCMU BUI as a primary administrator.**

   Refer to "Accessing the System" in *Oracle MiniCluster S7-2 Administration Guide* for instructions.

2. **In the navigation panel, select System Settings → Security.**

3. **In the Review Security Controls: Reverify and Update section, click Apply.**

   The current security profile is applied to the other compute node.

   Note - If an error occurs, schedule and run compliance tests and review the compliance reports to develop a mitigation plan. For DISA STIG reports, use the severity code to find the STIG recommendations for mitigation.

4. **Click Close.**

Smart Card Readers

Smart cards and smart card readers that are based on PKI credentials are supported for authentication to Application and Database VMs. MiniCluster provides two-factor authentication for SSH clients that use a smart card and smart card reader. The smart card reader is attached to one of the compute nodes. For more information, see "Smart Card Authentication" on page 15.

To learn how to access the Oracle Solaris environment in MiniCluster Application and Database VMs with a smart card and log in to the Solaris environment, refer to "Main Smart Card Configuration Tasks" in *Managing Kerberos and Other Authentication Services in Oracle Solaris 11.3*.

Auditing and Compliance Reporting

These topics describe the auditing and compliance reporting capabilities available in MiniCluster:

▼ Verify the Audit Policies

The audit policy is configured during the installation of the global zones and non-global zones upon selection of a compliance profile (Default CIS equivalent or PCI-DSS).

To verify that audit policies are enabled, perform these steps.

1. **Log into the global zone as `mcinstall`, and assume the `root` role.**

   For Oracle ILOM login instructions, refer to "Accessing Oracle ILOM" in *Oracle MiniCluster S7-2 Administration Guide*.

```
% ssh mcinstall@mc4-n1
Password: ***************
Last login: Tue Jun 28 10:47:38 2016 on rad/59
Oracle Corporation      SunOS 5.11      11.3    June 2016
Minicluster Setup successfully configured
Unauthorized modification of this system configuration strictly prohibited
mcinstall@mc4-n1:/var/home/mcinstall % su root
Password: ***************
#
```

2. **Verify that the audit service is online.**

```
# svcs | grep svc:/system/auditd
```

```
online         22:14:37 svc:/system/auditd:default
```

3. **Verify that the audit plugin is active.**

```
# auditconfig -getplugin audit_binfile
Plugin: audit_binfile (active)
        Attributes: p_age=0h;p_dir=/var/audit;p_fsize=0;p_minfree=1
```

4. **Verify the active audit policies.**

```
# auditconfig -getpolicy
configured audit policies = argv,cnt,perzone,zonename
active audit policies = argv,cnt,perzone,zonename
```

5. **Verify that all roles are captured for the `cusa` audit policy.**

```
# userattr audit_flags root
cusa:no
# userattr audit_flags mcadmin
fw,fc,fd,ps,lo,ex,ua,as,cusa:no
```

Review Audit Logs

1. **Log into the global zone as `mcinstall`, and assume the `root` role.**

   For Oracle ILOM login instructions, refer to "Accessing Oracle ILOM" in *Oracle MiniCluster S7-2 Administration Guide*.

```
% ssh mcinstall@mc4-n1
Password: ***************
Last login: Tue Jun 28 10:47:38 2016 on rad/59
Oracle Corporation      SunOS 5.11      11.3    June 2016
Minicluster Setup successfully configured
Unauthorized modification of this system configuration strictly prohibited
mcinstall@mc4-n1:/var/home/mcinstall % su root
Password: ***************
#
```

2. **Use the `auditreduce` command as shown.**

   This is syntax for viewing the audit logs:

   `auditreduce -z` *vm_name audit_file_name* `| praudit -s`

```
# cd /var/share/audit
#
```

```
# ls
20160628051437.not_terminated.mc4-n1
#
# auditreduce  -z dbvmg1-zone-1-mc4-n1 20160628051437.not_terminated.mc4-n1 | praudit -s
file,2016-06-27 22:58:53.000 -07:00,
header,127,2,AUE_zone_state,,mc4-n1.us.example.com,2016-06-27 22:58:53.354 -07:00
subject,mcinstall,root,root,root,root,26272,415120213,9462 65558 mc4-n1.us.example.com
text,boot
zone,dbvmg1-zone-1-mc4-n1
return,success,0
zone,global
header,88,2,AUE_zone_state,na,mc4-n1.us.example.com,2016-06-27 23:02:30.767 -07:00
text,reboot
zone,dbvmg1-zone-1-mc4-n1
return,success,0
zone,global
file,2016-06-27 23:02:30.000 -07:00,
```

▼ Generate Audit Reports

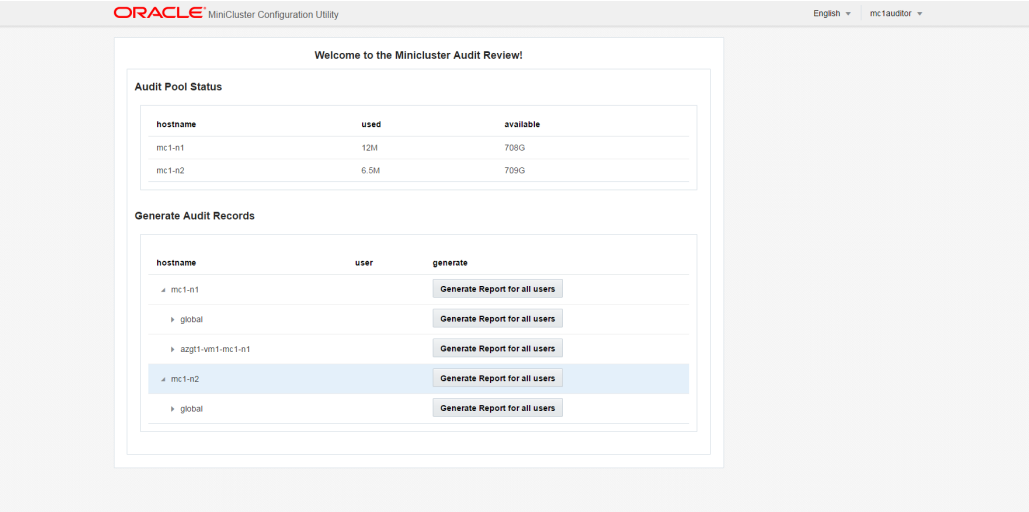
Use this procedure to generate audit reports for a node, or for individual VMs and global zones.

1. **Log into the MCMU as a user that is assigned with the Auditor role.**

   For more information about MCMU users and roles, refer to "Managing MCMU User Accounts (BUI)" in *Oracle MiniCluster S7-2 Administration Guide*.

2. **In the navigation panel, select System Settings → Security.**

Note - Only MCMU users that are assigned the auditor role can display this page.



3. **Check the Audit Pool Status section.**

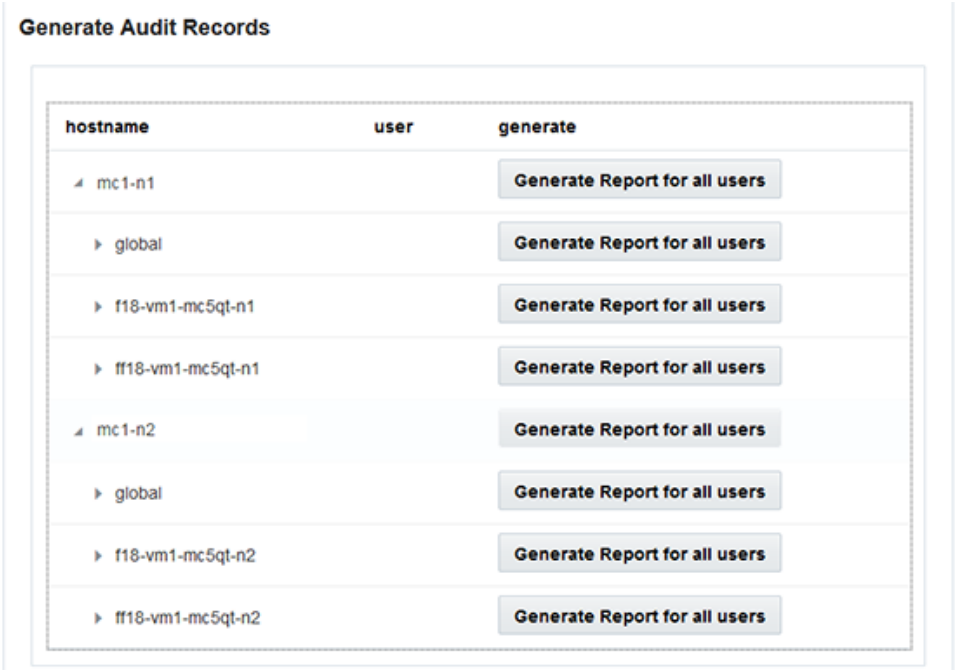
   This section lists the amount of space that is used and available for audit pools on each node.

4. **To generate a report for the entire node, click Generate Report for one of the nodes, and go to Step 6.**

   Alternatively, you can generate a report for a specific VM or zone. See Step 5.

5. **To generate a report for a specific VM or global zone, perform these steps.**

a. **Click the triangle next to a node to expand the view.**

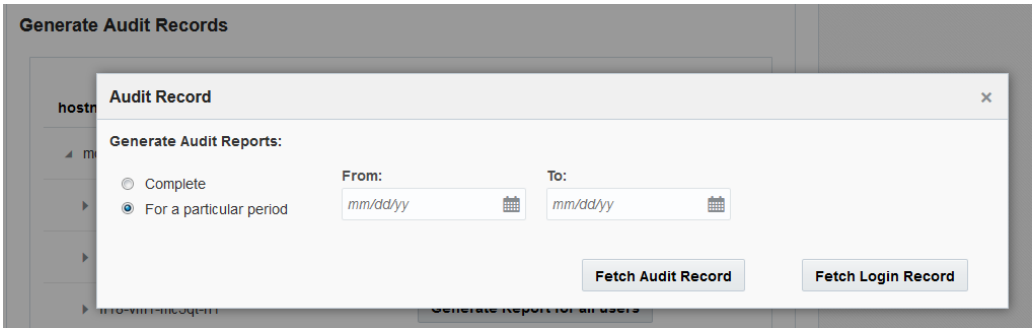


b. **For the VM or global zone, click Generate Report for all users.**

6. **In the Audit Record dialog box, select one of these options.**

   - **Complete** – Select if you want a report that includes all the audit records.

- **For a particular period** – Select if you want to specify a specific time period, then enter the from and to dates.



7. **Click one of the Fetch buttons.**

   Select one of these options:

   - **Fetch Audit Record** – Generates a complete audit record.
   - **Fetch Login Record** – Generates user activities such as logins, log outs, and user actions.

8. **Click the Click Here button and select download XML file.**

   The XML file can be imported into audit analysis applications such as Oracle Audit Vault.

9. **Click Close.**

▼ (If Required) Enable FIPS-140 Compliant Operation (Oracle ILOM)

The use of FIPS 140 validated cryptography is required for U.S. Federal Government customers.

By default, Oracle ILOM does not operate using FIPS 140 validated cryptography. However, the use of FIPS 140 validated cryptography can be enabled, if required.

Some Oracle ILOM features and capabilities are not available when configured for FIPS 140 compliant operation. A list of those features is covered in the Oracle ILOM Security Guide Firmware Releases 3.0, 3.1, and 3.2. See also “FIPS-140-2 Level 1 Compliance” on page 53.

Caution - This task requires you to reset Oracle ILOM. A reset results in the loss of all user-configured settings. For this reason, you must enable FIPS 140 compliant operation before any additional site-specific changes are made to the Oracle ILOM. For systems where site-specific configuration changes have been made, back up the Oracle ILOM configuration so that it can be restored after Oracle ILOM is reset, otherwise those configuration changes will be lost.

1. **On the management network, log into Oracle ILOM.**

2. **Determine if Oracle ILOM is configured for FIPS 140 compliant operation.**

```
-> show /SP/services/fips state status
/SP/services/fips
Properties:
state = enabled
status = enabled
```

FIPS 140 compliant mode in Oracle ILOM is represented by the `state` and `status` properties. The `state` property represents the configured mode in Oracle ILOM, and the `status` property represents the operational mode in Oracle ILOM. When the FIPS `state` property is changed, the change does not affect the operational mode FIPS `status` property until the next Oracle ILOM reboot.

3. **Enable FIPS 140 compliant operation.**

```
-> set /SP/services/fips state=enabled
```

4. **Restart the Oracle ILOM service processor.**

The Oracle ILOM SP must be restarted for this change to take effect.

```
-> reset /SP
```

FIPS-140-2 Level 1 Compliance

The cryptographic applications hosted on MiniCluster rely on the Cryptographic Framework feature of Oracle Solaris, which is validated for FIPS 140-2 Level 1 compliance. The Oracle Solaris Cryptographic Framework is the central cryptographic store for Oracle Solaris, and it provides two FIPS 140–verified modules that support the user-space and kernel-level processes. These library modules provide encryption, decryption, hashing, signature generation and verification, certificate generation and verification, and message authentication functions for applications. User-level applications that call into these modules run in FIPS 140 mode.

In addition to the Oracle Solaris Cryptographic Framework, the OpenSSL object module bundled with Oracle Solaris is validated for FIPS 140-2 Level 1 compliance, which supports the cryptography for applications based on the Secure Shell and TLS protocols. The cloud service provider can choose to enable the tenant hosts with FIPS 140–compliant modes. When running in FIPS 140–compliant modes, Oracle Solaris and OpenSSL, which are FIPS 140-2 providers, enforce the use of FIPS 140– validated cryptographic algorithms.

See also "(If Required) Enable FIPS-140 Compliant Operation (Oracle ILOM)" on page 52.

This table lists FIPS approved algorithms that are supported by Oracle Solaris on MiniCluster.

Key or CSP	Certificate Number	
	v1.0	**v1.1**
Symmetric Key		
AES: ECB, CBC, CFB-128, CCM, GMAC, GCM, and CTR modes for 128-, 192-, and 256-bit key sizes	#2311	#2574
AES: XTS mode for 256- and 512-bit key sizes	#2311	#2574
TripleDES: CBC and ECB mode for keying option 1	#1458	#1560
Asymmetric Key		
RSA PKCS#1.5 signature generation/verification: 1024-, 2048-,bit (with SHA-1, SHA-256, SHA-384, SHA-512)	#1194	#1321
ECDSA signature generation/verification: P-192, -224, -256, -384, -521; K-163, -233, -283, -409, -571; B-163, -233, -283, -409, -571	#376	#446
Secure Hashing Standard (SHS)		
SHA-1, SHA-224, SHA-256, SHA-384, SHA-512	#1425	#1596
(Keyed-) Hash-based Message Authentication		
HMAC SHA-1, HMAC SHA-224, HMAC SHA-256, HMAC SHA-384, HMAC SHA-512	#1425	#1596
Random Number Generators		
swrand FIPS 186-2 Random Number Generator	#1154	#1222
n2rng FIPS 186-2 Random Number Generator	#1152	#1226

Oracle Solaris offer two providers of cryptographic algorithms that are validated for FIPS 140-2 Level 1.

- The Cryptographic Framework feature of Oracle Solaris is the central cryptographic store on an Oracle Solaris system and provides two FIPS 140 modules. The userland module supplies cryptography for applications that run in user space and the kernel module provides cryptography for kernel-level processes. These library modules provide encryption, decryption, hashing, signature generation and verification, certificate generation and verification, and message authentication functions for applications. User- level applications that call into these modules run in FIPS 140 mode, for example, the `passwd` command and IKEv2. Kernel-level consumers, for example Kerberos and IPsec, use proprietary APIs to call into the kernel Cryptographic Framework.

- The OpenSSL object module provides cryptography for SSH and web applications. OpenSSL is the Open Source toolkit for the Secure Sockets Layer (SSL) and Transport Layer Security (TLS) protocols, and provides a cryptography library. In Oracle Solaris, SSH and the Apache Web Server are consumers of the OpenSSL FIPS 140 module. Oracle Solaris ships a FIPS 140 version of OpenSSL with Oracle Solaris 11.2 that is available to all consumers but the version shipped with Oracle Solaris 11.1 is available to Solaris SSH only. Because FIPS 140-2 provider modules are CPU intensive, they are not enabled by default. As the administrator, you are responsible for enabling the providers in FIPS 140 mode and configuring consumers.

For more information on enabling FIPS-140 providers on Oracle Solaris, refer to Using a FIPS 140-2 Enabled System in Oracle Solaris 11.3 (`http://docs.oracle.com/cd/E53394_01/html/E54966/index.html`).

Assessing Security Compliance

These topics describe the MiniCluster security benchmark feature:

Security Compliance Benchmarks

When the system is installed, a security profile (PCI-DSS, CIS Equivalent, and DISA-STIG) is selected, and the system is automatically configured to meet that security profile. To ensure that the system continues to operate in accordance with security profiles, the MCMU provides the means to run security benchmarks and access to the benchmark reports. You can administer the benchmarks using the MCMU BUI and CLI.

Running security benchmarks provides these benefits:

- Enables you to evaluate and assess the current security state of the database and application VMs.
- The security compliance tests support PCI-DSS, CIS Equivalent standards (default), and DISA-STIG based on the security level configured during the installation.

  You can also change the password policy for a specific security profile. See "Change the Password Policy" on page 20.
- The security compliance tests run automatically when the system is booted, and can be run on-demand or at scheduled intervals.
- Only available to MCMU primary admins, compliance scores and reports are easily accessed from the MCMU BUI.
- The compliance reports provide remediation recommendations.

Schedule a Security Compliance Benchmark (BUI)

Use this procedure to schedule a security benchmark using the MCMU BUI. To instead use the MCMU CLI, refer to the "Accessing the System" in *Oracle MiniCluster S7-2 Administration Guide* for instructions.

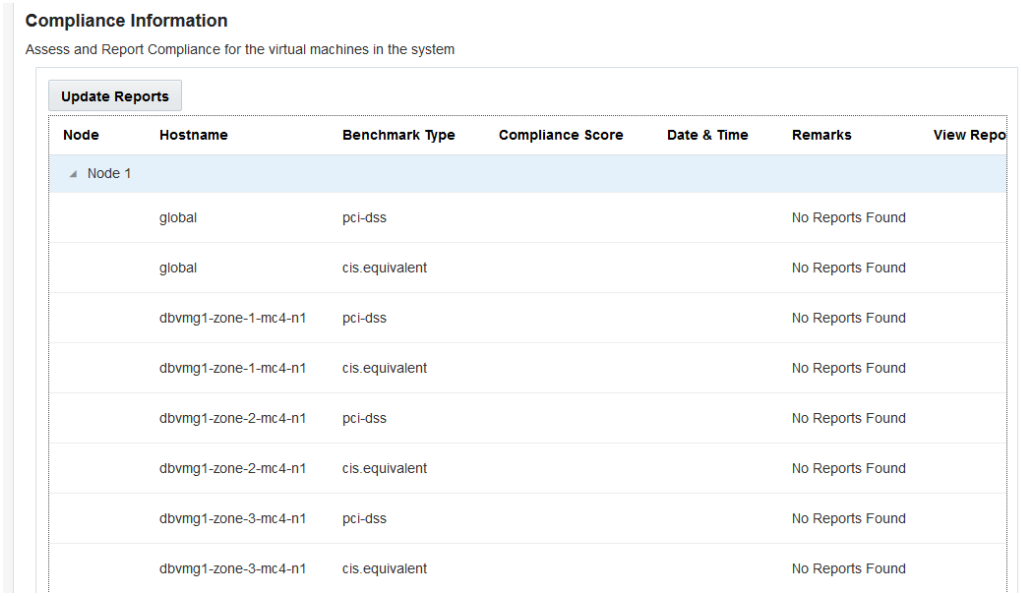
1. **Log in to the MCMU BUI as a primary administrator.**

   For instructions, refer to "Accessing the System" in *Oracle MiniCluster S7-2 Administration Guide*.

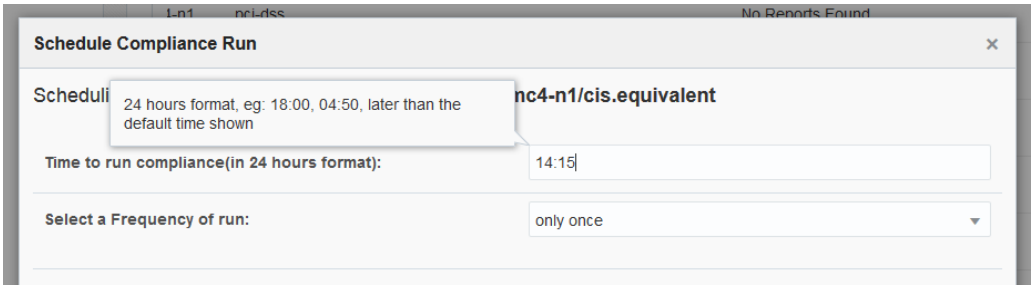
2. **In the Home page, scroll down to the Compliance Information panel.**

3. **Click on a node to expand its details.**

   Each zone and VM was configured with a security profile (either CIS equivalent or PCI-DSS). When you schedule a benchmark select a benchmark that corresponds to the component's security profile.



4. **Scroll to the right and click Schedule for one of the VMs.**



5. **Specify the time and frequency, and click Start.**

   After the security compliance test runs at the scheduled time, view the report. See "View Benchmark Reports (BUI)" on page 59.

View Benchmark Reports (BUI)

These are the acceptable compliance results:

	CIS Equivalent	PCI-DSS
Global zones	approx. 88%	approx. 88%
VMs	approx. 90%	approx. 93%

These are the known compliance test failures due to Oracle Solaris issues:

- Package integrity (core os, rad-python)
- GDM
- Routing daemon
- SSH loopback addresses – Mitigation does not fix the issue.
- Naming services not recognizing DNS.
- LDAP client.

These are the known compliance test failures due to MiniCluster customer required configuration issues:

- NFS client services – Select services need to be available.
- Setting eeprom password – Optional setting.

1. **Log in to the MCMU BUI.**

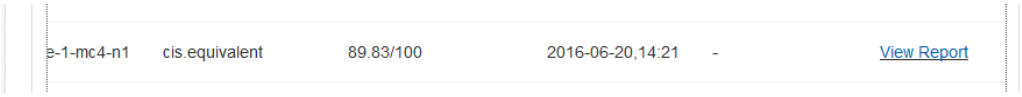
   For instructions, refer to "Accessing the System" in *Oracle MiniCluster S7-2 Administration Guide*.

2. **In the Home page, scroll down to the Compliance Information panel.**

3. **Click Update Reports.**

   The update process take a minute or so to complete.

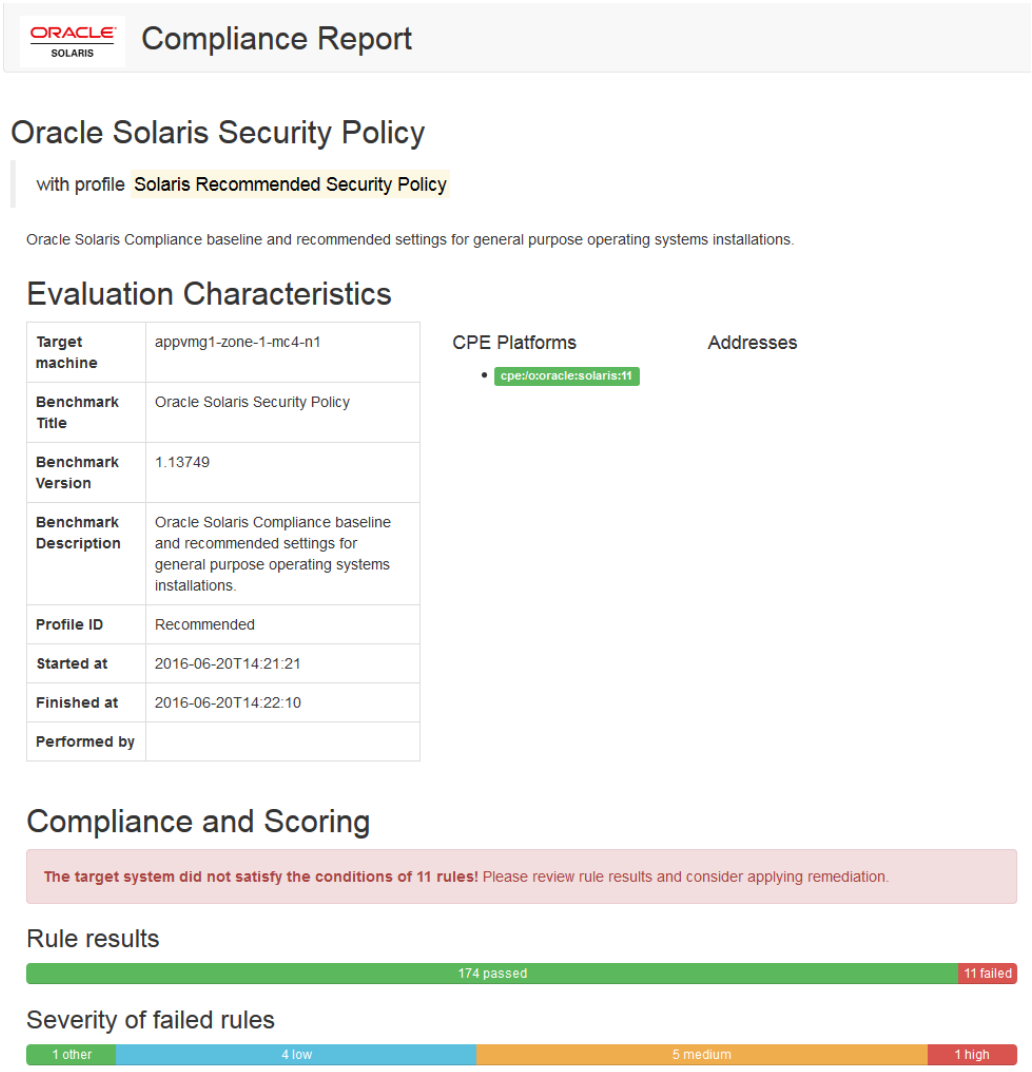
4. **Expand the node display and identify the compliance report.**



5. **Scroll to the right and click View Report.**

   The benchmark report is displayed.

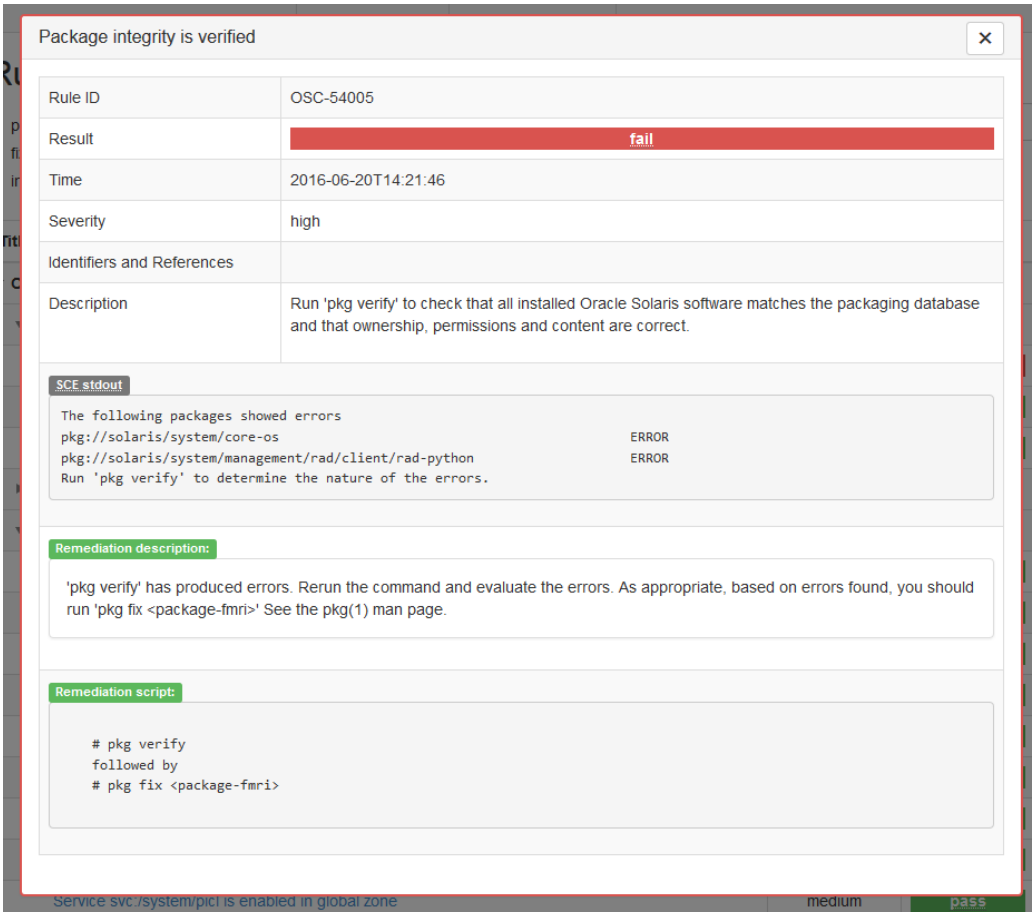
Under Rule Overview, you can select which types of test to display based on their results. You can also specify a search string in the search field.



6. **Use the report to verify the security controls, compliance scores, anomalies, and remediation procedures.**

7. **Select a test to get details and recommended remediation information.**

Note - You can display all the details of all tests by clicking Show all Result Details at the bottom of the report.



Understanding SPARC S7-2 Server Security Controls

These topics describe security controls for the hardware and the OpenBoot environment.

Understanding Hardware Security

Physical isolation and access control are the foundation on which you should build the security architecture. Ensuring that the physical server is installed in a secure environment protects it against unauthorized access. Likewise, recording all serial numbers helps to prevent theft, resale, or supply chain risk (for example, the injection of counterfeit or compromised components into your organization's supply chain).

These sections provide general hardware security guidelines for MiniCluster:

Access Restrictions

- Install servers and related equipment in a locked, restricted-access room.
- If equipment is installed in a rack with a locking door, always lock the rack door until you have to service the components within the rack. Locking the doors also restricts access to hot-plug or hot-swap devices.
- Store spare field-replaceable units (FRUs) or customer-replaceable units (CRUs) in a locked cabinet. Restrict access to the locked cabinet to authorized personnel.

- Periodically, verify the status and integrity of the locks on the rack and the spares cabinet to guard against, or detect, tampering or doors being accidentally left unlocked.
- Store cabinet keys in a secure location with limited access.
- Restrict access to USB consoles. Devices such as system controllers, power distribution units (PDUs), and network switches can have USB connections. Physical access is a more secure method of accessing a component since it is not susceptible to network-based attacks.
- Connect the console to an external KVM to enable remote console access. KVM devices often support two-factor authentication, centralized access control, and auditing. For more information about the security guidelines and best practices for KVM, refer to the documentation that came with the KVM device.

Serial Numbers

- Keep a record of the serial numbers of all your hardware.
- Security-mark all significant items of computer hardware, such as replacement parts. Use special ultraviolet pens or embossed labels.
- Keep hardware activation keys and licenses in a secure location that is easily accessible to the system manager in system emergencies. The printed documents might be your only proof of ownership.

Wireless radio frequency identification (RFID) readers can further simplify asset tracking. An Oracle technical paper, *How to Track Your Oracle Sun System Assets by Using RFID*, is available at `http://www.oracle.com/technetwork/articles/systems-hardware-architecture/o11-001-rfid-oracle-214567.pdf`.

Hard Drives

Hard drives are often used to store sensitive information. To protect this information from unauthorized disclosure, sanitize hard drives prior to reusing, decommissioning, or disposing of them.

- Use disk-wiping tools such as the Oracle Solaris `format` (1M) command to completely erase all data from the disk drive.
- Organizations should refer to their data protection policies to determine the most appropriate method to sanitize hard drives.
- If required, take advantage of Oracle's Customer Data and Device Retention Service at `http://www.oracle.com/us/support/library/data-retention-ds-405152.pdf`.

Restricting Access to OpenBoot

These topics describe how to restrict access at the OpenBoot prompt.

For instructions on how to configure a password for OpenBoot, see “Configure EEPROM Passwords” on page 34.

For information about setting OpenBoot security variables, refer to the OpenBoot documentation at:

`http://www.oracle.com/goto/openboot/docs`

▼ Get to the OpenBoot Prompt

This procedure describes how to get to the OpenBoot prompt on the MiniCluster compute nodes to configure the security controls.

You must shutdown the system to reach the OpenBoot prompt. Follow appropriate procedures for shutting down the VMs cleanly, as described in “Shut Down, Reset, or Power Cycle the System” in *Oracle MiniCluster S7-2 Administration Guide*.

1. **Log into Oracle ILOM on a node and issue this command.**

```
-> set /HOST/bootmode script=”setenv auto-boot? false
-> start /HOST/console
```

Log in to the host console as the `mcinstall` user and `su` to `root`.

2. **After all the VMs are shutdown, as the root role, halt the global zone.**

```
# init 0
.
.
.
{0} ok
```

Check for Failed Log-Ins

1. **Determine if someone has attempted and failed to access the OpenBoot environment by using the `security-#badlogins` parameter, as in the following example.**

   ```
   {0} ok printenv security-#badlogins
   ```

   If this command returns any value greater than Ø, a failed attempt to access the OpenBoot environment was recorded.

2. **Reset the parameter by typing this command.**

   ```
   {0} ok setenv security-#badlogins 0
   ```

Provide a Power-On Banner

Although it is not a direct preventative or detective control, a banner can be used for these reasons:

- Convey ownership.
- Warn users of the acceptable use of the server.
- Indicate that access or modifications to OpenBoot parameters is restricted to authorized personnel.

- **Use the following commands to enable a custom warning message.**

  ```
  {0} ok setenv oem-banner banner-message
  {0} ok setenv oem-banner? true
  ```

  The banner message can be up to 68 characters. All printable characters are accepted.

Glossary

C

compute node Short name for the SPARC server, a major component of MiniCluster.

G

GbE Gigabit Ethernet.

H

HMAC Hashed Message Authentication Code. An algorithm used to generate one-time passwords.

I

ILOM See Oracle ILOM.

IPMP IP network multipathing.

O

Oracle ILOM Oracle Integrated Lights Out Manager. Software on the SP that enables you to manage a server independently from the operating system.

Oracle Solaris SMF Oracle Solaris Service Management Facility. Ensures that essential system and application services run continuously even in the event of hardware or software failures.

OTP A One-time Password. A MiniCluster administrator in the tenant admin role can enable two-factor authentication for a specific user.

S

SPARC server A major component of SuperCluster that provides the main compute resources. Referred to in this documentation as compute node.

T

transparent data encryption Transparent Data Encryption. Used to protect data at rest, encrypting databases on the hard drive and consequently on backup media.

two-factor authentication Strong authentication that is enforced with OTP.

Z

ZFS A file system with added volume management capabilities. ZFS is the default file system in Oracle Solaris 11.

Index

T

U

V

Z