v1.4 | April 2022 | TN-2133

TECH NOTE

Nutanix Pulse and Remote Diagnostics

NUTANIX
YOUR ENTERPRISE CLOUD

Copyright

Copyright 2022 Nutanix, Inc.

Nutanix, Inc.
1740 Technology Drive, Suite 150
San Jose, CA 95110

All rights reserved. This product is protected by U.S. and international copyright and intellectual property laws. Nutanix and the Nutanix logo are registered trademarks of Nutanix, Inc. in the United States and/or other jurisdictions. All other brand and product names mentioned herein are for identification purposes only and may be trademarks of their respective holders.

Contents

1. Executive Summary

Most enterprise IT solutions rely on a reactive approach to system maintenance and issue resolution. For example, when a technical issue arises, vendor support teams typically capture detailed system data from the customer and recreate the issue in a separate environment—only then can the actual debugging begin. This approach consumes unnecessary time and resources and ultimately delays resolution.

Nutanix simplifies and streamlines this process through two important support services: Nutanix Pulse and Nutanix Remote Diagnostics. When enabled, Pulse captures purpose-driven diagnostic data on a regular schedule. The Remote Diagnostics service, which is enabled by default on Pulse-enabled clusters (and which the customer can disable), is event-driven and helps to provide proactive support.

Benefits of enabling Nutanix Pulse and Remote Diagnostics include:

- Reduce resolution time by up to 40 percent.
- Personalize your Nutanix Support experience.
- Proactive issue resolution.
- Intelligent monitoring.
- Secure data transmission.

For more information, refer to the Nutanix Support Services: Pulse datasheet.

Document Version History

Version Number	Published	Notes
1.0	October 2019	Original publication.
1.1	November 2020	Refreshed content.

© 2022 Nutanix, Inc. All rights reserved

Version Number	Published	Notes
1.2	April 2021	Updated the Remote Diagnostics section.
1.3	March 2022	Updated the Nutanix Pulse section.
1.4	April 2022	Updated the Data Obfuscation section.

© 2022 Nutanix, Inc. All rights reserved

2. Nutanix Pulse

What Is Nutanix Pulse?

Nutanix Pulse is the telemetry capability built into all Nutanix clusters that sends key health metrics to the Nutanix Insights service. Nutanix can use the diagnostic system information that Pulse sends to help build better products and provide a great customer experience. At Nutanix, our vision is to enable invisible infrastructure for IT teams—Nutanix Pulse is another step in that direction.

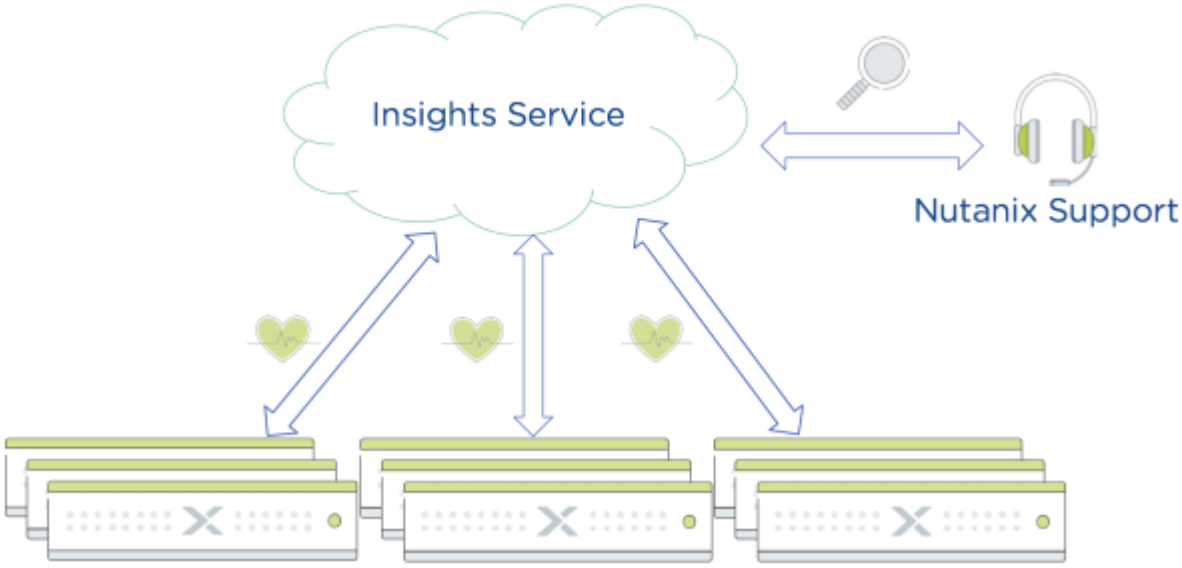

Figure 1: Pulse-Enabled Clusters Send Pulse Telemetry to Nutanix Insights

Nutanix uses this Pulse information in several important ways:

- Nutanix Support teams can use this data to deliver proactive, context-aware support for Nutanix solutions.
- IT admins can see insights and alerts from the data on the Nutanix Portal, with actionable guidance to help them address issues themselves.

© 2022 Nutanix, Inc. All rights reserved

- When a cluster encounters fatal or critical alerts, support teams can proactively create a case and kickstart the resolution process, often before IT teams have even discovered the issue.
- Nutanix can also use this information to analyze product and feature usage and effectiveness.

When Pulse is enabled, a Nutanix cluster automatically and unobtrusively collects diagnostic information. Pulse shares this system-level information to monitor the health and status of a Nutanix cluster. The shared information includes the following data points:

- System alerts.
- System tasks.
- System logs.
- System configuration.
- Performance metrics.
- Current Nutanix software version.
- Nutanix processes and Controller VM (CVM) information.
- Hypervisor details such as type and version.

All the information in the categories above is specific to Nutanix internal processes and doesn't contain information regarding customer workloads or applications.

> Note: Nutanix doesn't share any data that Pulse sends with any third parties unless permitted by your agreement with Nutanix or by the Nutanix Privacy Statement (https://www.nutanix.com/legal/privacy-statement). Certain Nutanix products require Pulse enablement for functionality and features. See the Nutanix Privacy Statement and applicable product documentation for more details.

How to Enable Pulse

We've captured the latest guidance on configuring Pulse in the Data Protection and Recovery with Prism Element guide.

© 2022 Nutanix, Inc. All rights reserved

To enable Pulse, navigate to Settings and select Pulse, either in Prism Central, if you've deployed it to manage multiple clusters, or on every Prism Element instance on the cluster.

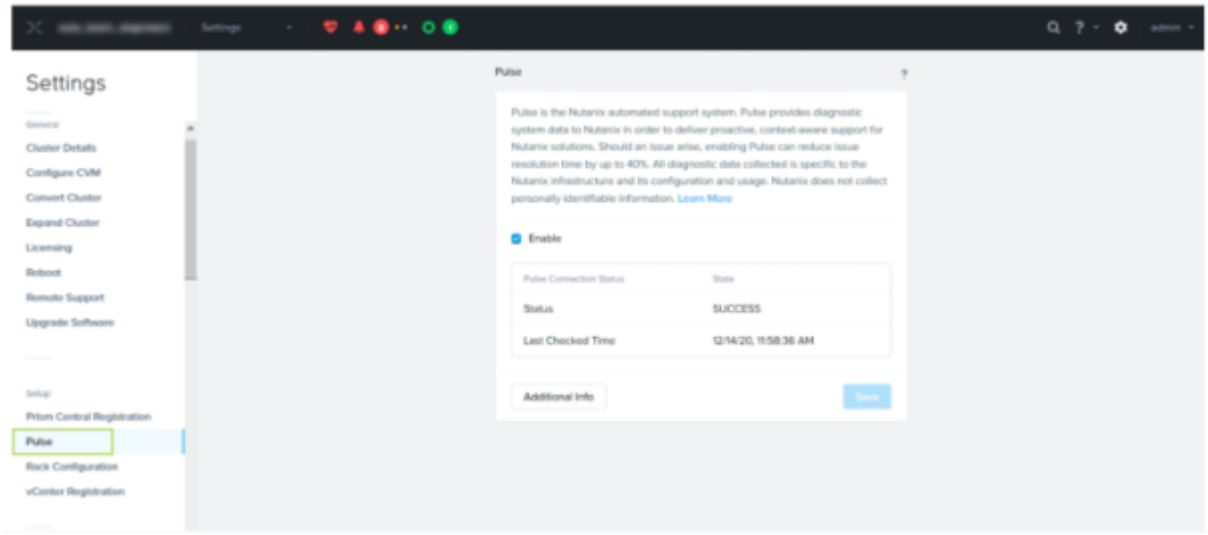

Figure 2: Select Pulse

In the dialog box that appears, select the Enable check box and click Save.

© 2022 Nutanix, Inc. All rights reserved

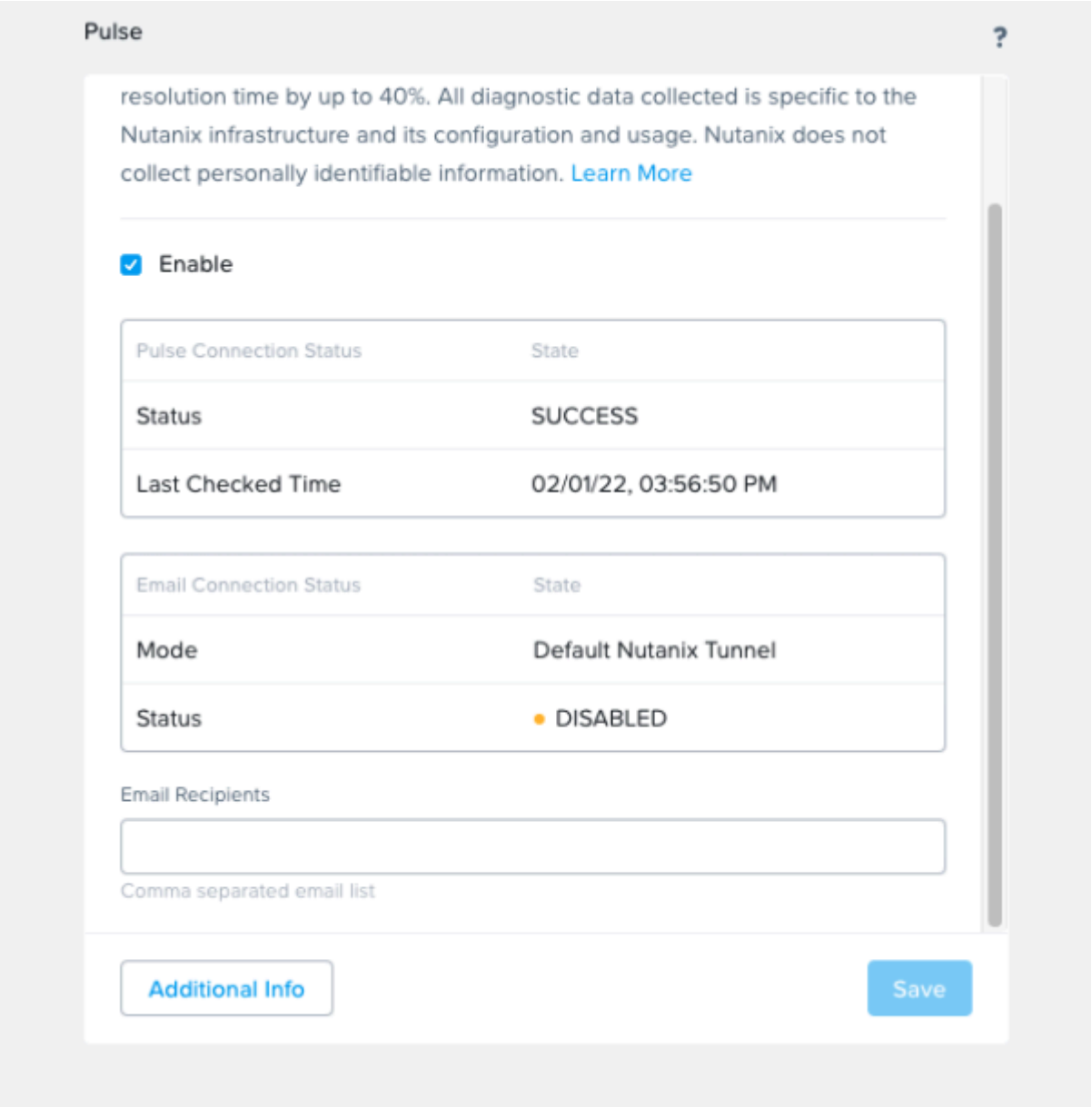

Figure 3: Pulse Dialog Box

Once you have successfully enabled Nutanix Pulse, the Pulse Connection Status box displays the connectivity status SUCCESS.

© 2022 Nutanix, Inc. All rights reserved

PULSE CONNECTION STATUS	STATE
Status	SUCCESS
Last Checked Time	09/14/18, 1:33:06 AM

Figure 4: Pulse Connection Status Box

When Pulse is enabled, all telemetry data streams to the Insights service hosted at insights.nutanix.com over port 443. Therefore, telemetry traffic must be allowed to leave the network and reach this destination.

The source of Pulse data varies depending on the deployment:

- If Prism Central is deployed, Pulse routes all info from every node in a managed cluster through this Prism Central.
- If Prism Central is not deployed, Pulse routes this info from each CVM for every node in the cluster.

The following decision tree describes the network configuration you need to enable outbound access for Pulse diagnostic data.

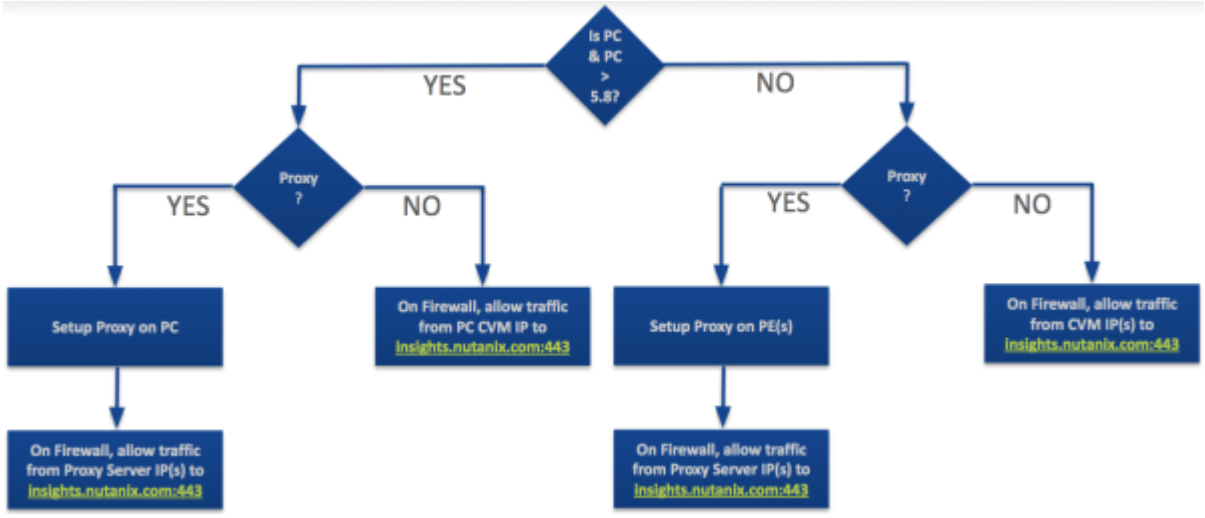

Figure 5: Network Configuration Decision Tree

© 2022 Nutanix, Inc. All rights reserved

Note: All traffic for Pulse is outbound. No inbound connection is ever initiated to the clusters. Nutanix recommends setting up Alert emails for proactive support and case creation. Follow the instructions in Configuring Alert Emails in the Prism Web Console Guide (https://portal.nutanix.com/page/documents/details?targetId=Web-Console-Guide-Prism-v5_19:wc-alert-email-enable-wc-t.html).

Software Requirements

Three key components enable Nutanix Pulse to function:

1. Nutanix Cluster Check (NCC)
   a. All diagnostic data collectors are built into NCC and are responsible for collecting and packaging the right metrics, counters, configuration details, and logs.
   b. We recommend that all Nutanix clusters always run the latest version of NCC.
   c. To enable Pulse routing through Prism Central, clusters must run NCC 3.5 or a later version.
   d. To enable Remote Diagnostics, clusters must run NCC 3.7.0.1 or a later version.
2. Prism Central
   a. Although Pulse doesn't require Prism Central to function, using Prism Central dramatically simplifies the setup and network configuration. Enabling all nodes to route Pulse data through Prism Central requires Prism Central version 5.8 or later.
3. Nutanix Insights
   a. The Insights service, operated by Nutanix, always runs the latest version and doesn't require any maintenance effort from IT teams.

What Data Does Pulse Collect?

The following categories serve as a general overview of the types of information that Pulse gathers from the clusters. Note that some of this information may be anonymized depending on your settings. This list is not

© 2022 Nutanix, Inc. All rights reserved

exhaustive; for more details about the Pulse information your clusters send to Nutanix, contact Nutanix Support.

Cluster

- Cluster name (may be anonymized)
- Uptime
- AOS version
- Cluster ID
- Block serial number
- HW model
- Cluster IOPS
- Cluster latency
- Cluster memory

Hardware

In this context, hardware can include nodes, blocks, boards, disks, BMCs, fans, DIMMs, BIOS, CPUs, NICs, storage controllers, and power supplies.

- Model number
- Serial number
- Part number
- Block number
- Node UUID
- Type
- Size
- Version
- Name (may be anonymized)

© 2022 Nutanix, Inc. All rights reserved

- Manufacturer
- Status
- Memory (size)
- Hypervisor type
- Hypervisor version
- Firmware version
- Disk type
- Disk model
- Disk capacity
- Node temperature
- Network interface model
- SATADOM firmware
- PSU status
- Node location
- IPMI version
- Fan RPM
- Component location
- DIMM bank connection
- Clock speed
- DIMM temperature
- BIOS release date
- BIOS ROM size
- CPU signature
- CPU core count

© 2022 Nutanix, Inc. All rights reserved

- CPU cores enabled
- CPU thread count
- CPU temperature
- CPU speed
- Driver version
- Power supply maximum power

Storage Pool

- Name (may be anonymized)
- Capacity (logical used capacity and total capacity)
- IOPS and latency

Container

- Container name (may be anonymized)
- Capacity (logical used and total)
- IOPS and latency
- Replication factor
- Compression ratio
- Deduplication ratio
- Inline or post-process compression
- Inline deduplication
- Post-process deduplication
- Space available
- Space used
- Erasure coding and savings

© 2022 Nutanix, Inc. All rights reserved

Controller VM (CVM)

- Details of logs, attributes, and configurations of services on each CVM
- CVM memory
- vCPU usage
- Uptime
- Network statistics
- IP addresses (may be anonymized)

VM

- Name (may be anonymized)
- VM state
- vCPU
- Memory
- Disk space available
- Disk space used
- Number of vDisks
- Name of the container that contains the VM (may be anonymized)
- VM operating system
- IOPS
- Latency
- VM protection status
- Management VM (yes or no)
- I/O pattern (read, read/write, random, sequential)
- IP address (may be anonymized)

© 2022 Nutanix, Inc. All rights reserved

Disk Status

- Performance stats
- Usage

Hypervisor

- Hypervisor software and version
- Uptime
- Installed VMs
- Memory usage
- Attached datastore

Datastore

- Usage
- Capacity
- Name

Protection Domain

- Name (may be anonymized)
- Count and names of VMs in each protection domain

Gflags

- Key and value
- State (set)
- Node ID
- Service name
- Time of modification

Feature

- Feature ID

© 2022 Nutanix, Inc. All rights reserved

- Name
- State (enabled or disabled)
- Mode

License

- License type (Starter, Ultimate, or Pro)

Alerts

- Alert ID
- Type
- Severity
- Resolution status
- Acknowledgement status
- Impact type
- Message
- Creation time
- Modification time

Tasks

- Task ID
- Operation type
- Status
- Entities
- Message
- Completion percentage
- Creation time
- Modification time

© 2022 Nutanix, Inc. All rights reserved

Logs

- Component
- Timestamp
- Source file name
- Line number
- Message

Nutanix Services

- Service-specific metrics

Data Obfuscation

Based on your Pulse settings, the following attributes and rules may be obfuscated when they are collected. The Insights platform receives this information as random strings.

- cluster name
- ipv6_address
- ipv4_address
- domain
- vm_name
- container_name
- vstore_name
- remote_name
- ntp_server_list
- smtp_server
- http_proxy
- service_center

© 2022 Nutanix, Inc. All rights reserved

- directory_url
- snmp trap address
- access url
- management server name
- ipmi address
- ipmi username
- Any attribute value having regex pattern similar to IP address

What Information Does Pulse Collect and Send to Nutanix?

Network monitoring tools such as Wireshark can't analyze Pulse payloads because we encrypt all communication from clusters to the Nutanix Insights service for security reasons. For more details about the Pulse information your clusters send to Nutanix, contact Nutanix Support.

How Often Does Pulse Send Information?

Pulse sends information at different intervals, balancing bandwidth conservation, latency sensitivity, and utility. For a cluster where Pulse is enabled, the following events send a Pulse payload to the Nutanix Insights service.

- Every configuration change is streamed immediately to the Insights service.
- Select critical or fatal log messages stream immediately.
- Pulse aggregates metrics (such as resource consumption, service counters, and so on) and sends them every 15 minutes or 60 minutes, depending on the NCC version installed.
- Pulse also takes a snapshot of the current cluster configuration every 12 hours.

Note: Pulse collectors have strict resource-use limitations in place, with a clear intent to never burden CPUs, memory, or disks on the cluster.

© 2022 Nutanix, Inc. All rights reserved

3. Remote Diagnostics

What Is the Remote Diagnostics Service?

The Remote Diagnostics service enables Nutanix Support to request granular diagnostic information from Pulse-enabled clusters. While Pulse-enabled clusters stream configuration, metrics, alerts, events, and select logs back to Nutanix Insights, this data is aggregate in nature and provides representation of the cluster at a high level. This high-level cluster state is extremely useful, but there are times when Nutanix Support may require detailed information (such as specific service logs) to diagnose a specific issue. In such cases, Nutanix Support can initiate the Remote Diagnostics service.

Remote Diagnostics Workflow

When Nutanix Systems Reliability Engineers (SREs) are engaged in a Support case and assess the need to collect some diagnostic data from the relevant clusters, they go through the following workflow:

1. Notify the Cluster Admin that Nutanix needs to collect certain logs or other data from the cluster.
2. Access the Remote Diagnostics service internally operating at Nutanix, then connect to the relevant cluster.
3. On this cluster, the Nutanix SRE defines a Diagnostic Collection, which establishes:
   a. The data to collect.
   b. The specific time window for data collection.
4. The SRE then runs a diagnostic collection on the cluster and relevant diagnostic data streams to the Remote Diagnostics service, using the existing Pulse HTTPS channel. Note that this connection is not inbound; this operation uses the Pulse HTTPS channel (outbound from the cluster).

© 2022 Nutanix, Inc. All rights reserved

The Nutanix SRE now has the relevant data to proceed with case analysis and resolution.

Who Can Initiate Collection Through Remote Diagnostics?

Authenticated and authorized Nutanix employees across the Nutanix Support, Nutanix Sales Engineering, and Nutanix Customer Success organizations can use the Nutanix Remote Diagnostics service to connect to Pulse-enabled Nutanix clusters (when relevant to the case or customer) and initiate a diagnostic collection. Every use of the tool is audited, both on the Nutanix clusters and internally at the Remote Diagnostics service.

What Data Can Nutanix Collect Remotely?

Remote Diagnostics allows Nutanix Support to request a very restricted set of data for use when troubleshooting a specific issue. The service can request the following data remotely:

- Logs for Nutanix services.
- Custom gflags set for any Nutanix service.
- Activity traces for Nutanix services.
- Hypervisor logs.
- Hypervisor configuration.
- Cluster configuration.
- System statistics (for example, memory usage).
- Nutanix NCC health check reports.

Note: As Nutanix products evolve, we may add collection options. Only Nutanix Support can view uploaded log bundles.

© 2022 Nutanix, Inc. All rights reserved

How to Audit Remote Diagnostic Collections

Every time Nutanix Support uses Remote Diagnostics to trigger a diagnostic collection on the cluster, the system creates an entry in the cluster's audit trail. There are always two entries for Remote Diagnostics events:

1. Start of the diagnostic collection.
2. End of the diagnostic collection.

You can access this audit trail on the Prism Central where the cluster is registered.

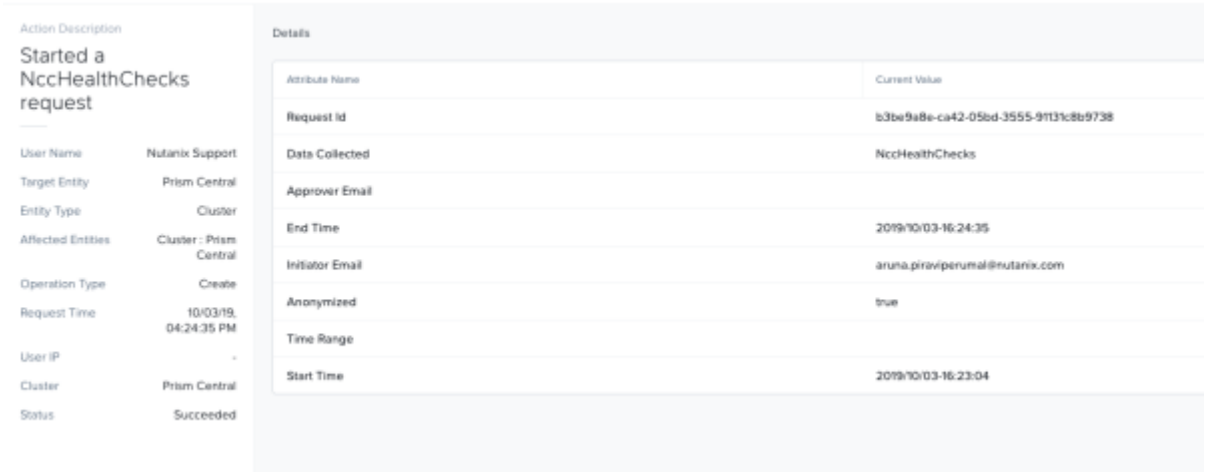

Figure 6: Sample Audit Entry Showing the Start of a Diagnostic Collection

© 2022 Nutanix, Inc. All rights reserved

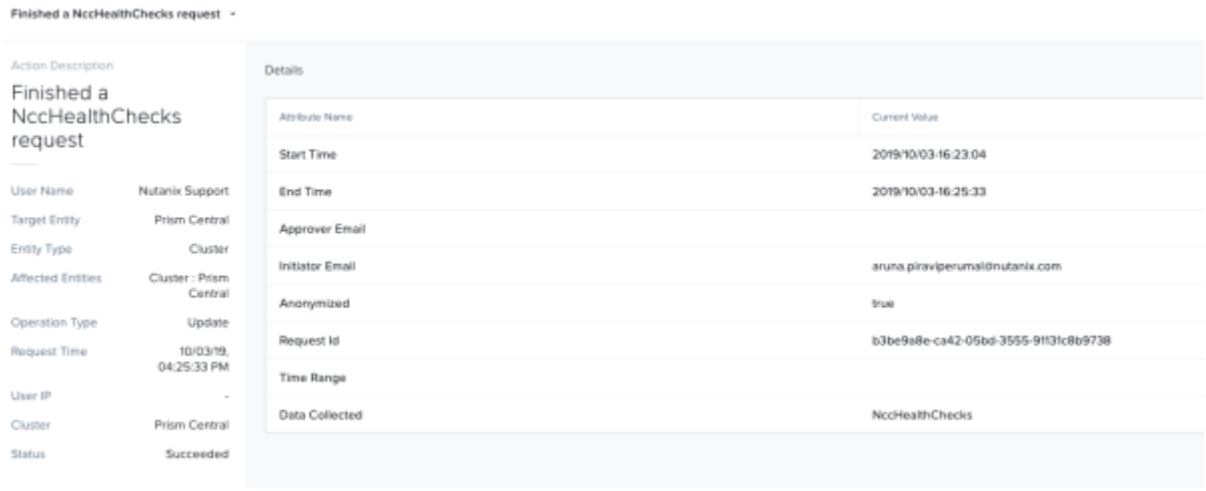

Figure 7: Sample Audit Entry Showing the End of a Diagnostic Collection

How to Enable and Disable Remote Diagnostics

We provide the latest guidance on configuring Remote Diagnostics in KB 7993.

The Remote Diagnostics service is enabled by default for every cluster where Nutanix Pulse is enabled.

If for some reason a customer isn't comfortable allowing Nutanix Support to initiate collections, you can disable Remote Diagnostics without disabling Pulse. With this configuration, Nutanix Support can still provide seamless proactive support based on Nutanix Pulse.

Enable Remote Diagnostics on the Cluster

To enable Remote Diagnostics, use SSH to connect to any CVM on the cluster and enter the following command.

```
nutanix@CVM$ /home/nutanix/ncc/bin/nusights/set_remote_diagnostics_status --
enable=true --reason=<text>
```

The optional parameter --reason is a text entry that allows you to capture your rationale for enabling Remote Diagnostics.

Disable Remote Diagnostics on the Cluster

To disable Remote Diagnostics, use SSH to connect to any CVM on the cluster and enter the following command.

© 2022 Nutanix, Inc. All rights reserved

```
nutanix@CVM$ /home/nutanix/ncc/bin/nusights/set_remote_diagnostics_status --
enable=false --reason=<text>
```

Check Remote Diagnostics Status on the Cluster

To check the status of Remote Diagnostics, use SSH to connect to any CVM on the cluster and enter the following command.

```
nutanix@CVM$ zkcat /appliance/logical/nusights/collectors/kCommand/
override_config
```

Required Software

To support the Remote Diagnostics capability, you must have NCC version 3.7.0.1 or later on Pulse-enabled clusters. Nutanix recommends that you always run the latest NCC version available.

Remote Diagnostics: Secure by Design

Security is a prime consideration at Nutanix and central to the design of the Remote Diagnostics service. To better understand how this functionality is secure by design, let's look at the internal communication mechanism that allows Remote Diagnostics to work.

- While Remote Diagnostics allows Nutanix Support to remotely initiate a diagnostic collection on a cluster, this connection is never inbound to a cluster (which requires opening firewall holes in the customer's network). To ensure a better security posture, all communication from a cluster is outbound.
  - Pulse collectors on the cluster poll the Remote Diagnostics service every 2 minutes to check for a diagnostic collection request initiated by Nutanix Support. When a collection request is pending, the cluster's poll action picks up the relevant request payload.

© 2022 Nutanix, Inc. All rights reserved

- The outbound poll request and all subsequent traffic travels over HTTPS (port 443) via TLS 1.2.
  - The HTTPS request uses certificate authentication to validate that Pulse has established communication with the Nutanix Remote Diagnostics service.
  - The TLS 1.2 protocol uses public key cryptography and server authentication to provide confidentiality, message integrity, and authentication for traffic passed over the Internet.
- Pulse collectors on the cluster interpret the curated set of commands in the request payload that the cluster's poll action picked up. To protect this payload from malicious commands, Pulse collectors can only process a tightly limited set of commands, ignoring everything else. The collector currently understands the following command requests:
  - Log bundle
  - Log summary
  - NCC health check

© 2022 Nutanix, Inc. All rights reserved

About Nutanix

Nutanix is a global leader in cloud software and a pioneer in hyperconverged infrastructure solutions, making clouds invisible and freeing customers to focus on their business outcomes. Organizations around the world use Nutanix software to leverage a single platform to manage any app at any location for their hybrid multicloud environments. Learn more at www.nutanix.com or follow us on Twitter @nutanix.

© 2022 Nutanix, Inc. All rights reserved

List of Figures